Advancements in Reversible Data Hiding Techniques and Its Applications in Healthcare Sector

Buggaveeti Padmaja, Maharana Suraj, and V. M. Manikandan

Abstract Among all the approaches, Digital watermarking is the most widely implemented approach for copyright protection and authentication of data. In this technique, a unique piece of information is known as a watermark. Then the watermark gets into an image, later, to achieve its objective the watermark will be extracted. For the transmission of medical images, digital watermarking schemes are mostly used to ensure that the image has not gone through any unauthorized or illegal modifications during the transmission. Since conventional watermarking schemes alter the pixels in the original image, it is not suited for watermarking medical images. In medical images, permanent modifications may adversely affect the diagnosis process at the receiver side, caused by watermarking, especially when we are using some computer-aided diagnosis tools. This motivated computer scientists to work on reversible watermarking schemes. The reversible watermarking technology makes it possible to recover the required medical image from the watermarked image, while extracting the hidden watermark. So, the reversible watermarking technique does not affect the diagnosis in any way since the recovered image will be equivalent to the original image. This recovered image will be used by the user. The use of reversible watermarking techniques to send patient reports along with medical images is also explored, with the patient reports being embedded in the medical picture itself rather than the watermark. These techniques are commonly known as reversible data hiding techniques. This book chapter gives a brief overview of reversible data hiding techniques, reversible watermarking methods, and the major applications in medical image transmissions. In addition, the chapter addresses contemporary reversible data hiding and reversible watermarking algorithms intended specifically for medical picture transmission. The

B. Padmaja · M. Suraj · V. M. Manikandan (✉)
Department of Computer Science and Engineering, SRM University-AP, Amaravati, Andhra Pradesh, India
e-mail: manikandan.v@srmap.edu.in

B. Padmaja
e-mail: padmaja_buggaveeti@srmap.edu.in

M. Suraj
e-mail: maharana_suraj@srmap.edu.in

H. K. Thakkar et al. (eds.), *Predictive Data Security using AI*, Studies in Computational Intelligence 1065, https://doi.org/10.1007/978-981-19-6290-5_8

chapter also discusses some of the obstacles that must be overcome when developing a reversible watermarking system for healthcare applications.

Keywords Data security · Medical image security · Data hiding · Watermarking · Reversible watermarking · Clinical data transmission · Health care

1 Introduction

Information security is one of the emerging domains in the communication system. It is a set of techniques and methodologies which are designed to ensure the security of electronic, confidential, and private data. It prevents breaches of data. It helps the healthcare industry to keep health records safe from unauthorized use. In the healthcare industry, data is confidential and sensitive as it carries medical information and drug-related data. Nowadays, those data are stored in electronic form. Information security approaches can be applied to this information to ensure its integrity, facilitating secure connection among healthcare providers, and improvising safety of medication, reporting, and tracking. The benefits of health information technology include improved access to and compliance with guidelines, as well as improved healthcare quality [1].

Between 2009 and 2020, around 3,709 data of health care reported breach of 400 or more records. Theft, loss, exposure, or unauthorized disclosures of 268,190,493 hospital records resulted because of those breaches. In the year 2020, on average 1.75 breaches took place per day. One cannot risk losing the clinical data of a patient in the process of transferring it from one source to another. It may cause major issues like loss of that information and can lead to inaccurate treatment and many such losses.

For healthcare organizations, one of the most useful data protection methods is encryption. Encrypting the data in transit and at rest, by healthcare authorities and businessmen, makes it impossible for attackers to decode the patient's information even if they manage to gain access to any sensitive data. Data hiding is an important method of ensuring secure communication. It is a technique where the sender embeds private information in a medium like an image, video, watermark, etc. When the data hiding techniques are applied to medical information, we must ensure that there is no loss of data when the receiver extracts it. One cannot risk losing the clinical data of a patient in the process of transferring it from one source to another. It may cause major issues like loss of that information and can lead to inaccurate treatment and many such losses. To avoid these, reversible data hiding (RDH) techniques come into play [2–6]. This process of securely sending data to the receiver from the sender with zero loss of information and distortion in the image is called RDH. These techniques came into existence in the year 2002.

Digital watermarking is a method where confidential information is embedded into an image [7]. A watermark is a logo, text, or pattern that is almost transparent in an image. Digital watermarking schemes are used in many applications like copyright

protection, fingerprinting and digital signatures, data authentication, protection, etc. The objective of this process is to save the integrity of information. Medical data of a patient needs to be taken care of when it is transferred between two sources. Watermarking is one of those methods which ensures the security of data. So, this method is also used in the transfer of clinical data.

There are two things to be considered when the digital watermarking technique is applied:

- There should be no loss of information.
- Original image must be restored perfectly without any distortion in pixels.

The process of perfectly restoring the real image after extraction of the watermark information is said to be reversible digital watermarking. When the technique is applied to medical information, the user must ensure that it is reversible.

In the further sections of the chapter, we will discuss various methods for secure data transmission, data hiding schemes in detail, the eversible data hiding approaches, reversible watermarking, some related work, and the challenges in this area.

2 Methods of Secure Communication

One of the two important strategies for secure communication is cryptography. Cryptography's purpose is to render data unreadable to a third party. Network security protocols are separated into symmetric (secret-key) and asymmetric (public-key) cryptography techniques. By employing the same key, symmetric algorithms are utilized to cipher and decrypt original messages. Asymmetric algorithms, on the other hand, use a public-key cryptosystem to exchange keys and then apply quicker secret key algorithms to assure stream data secrecy. A pair of keys is used in public-key encryption techniques, one of which is known to the public and is used to encrypt data to be transferred to a receiver who has the corresponding private key. Both private and public keys are distinct and require a key exchange. Encryption is one of the efficient ways to provide confidentiality to the content by changing them into an unreadable form. Encryption of medical images and healthcare data before transmission is very common in the healthcare industry which will help secure the data from unauthorized access (Fig. 1).

The data is disguised in a cover file and transferred across the network which is known as Data Hiding. The fundamental benefit of data concealing techniques over encryption is that they can hide the existence of secret information. On the other hand, one can easily recognize an encrypted data file by seeing the content even though they cannot infer anything from that. Data hiding is a useful approach to safeguard data since it allows you to conceal data in a host (cover) without losing its value. Data hiding methods may be used to hide secret messages in photographs in an undetectable fashion, such that the original image and the image with embedded data appear to be the same. Every difference between the tagged and original image is considered noise, making it harder for a third party to decode the encoded data.

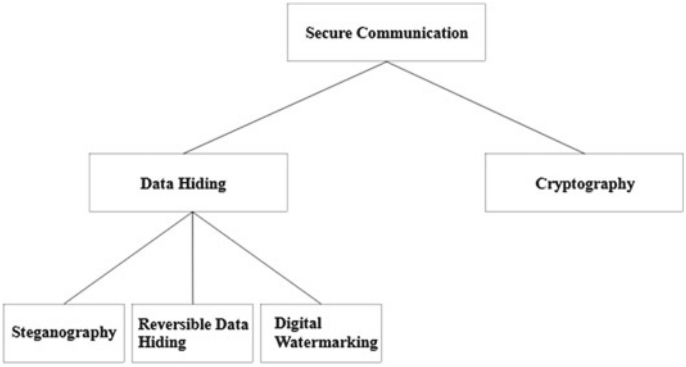

Fig. 1 Classification of secure communication techniques

Existing data concealing methods, on the other hand, have a relatively limited embedding capacity (the number of bits that can hide in an image). As a consequence, the embedded message is relatively brief (very). To increase picture embedding capacity while keeping the peak signal-to-noise ratio (PSNR) below allowable levels, several data concealment strategies have been applied. To assess the image's visual quality, PSNR is used. There are 2 types of data hiding methods: RDH and non-RDH. In RDH approaches, the actual cover medium can be restored while extracting the hidden details. In non-RDH methods, the original cover medium is irrevocably corrupted and cannot be recovered later. Military and intelligence communication, private communication, and protecting civilian speeches from attackers all use RDH algorithms. The RDH schemes are very popular in medical image transmission to hide patient reports in the medical image. This provides a way to transmit the medical image text files as a single entity instead of sending them as two different entities.

Data hiding techniques include steganography, digital watermarking, and reversible data hiding (RDH). These topics are detailed in subsequent subsections.

2.1 Steganography

Steganography is a secret communication technique [8, 9]. The technique of concealing information is referred to as steganography. Any type of digital file, particularly image files, is most commonly used to conceal data. The host files (which contain hidden information) can then be transferred via an unsecured channel without anyone knowing what's inside. The existence of the message is known in steganography but in cryptography the meaning is unknown. Information is hidden using steganography software. The overview of an image steganography scheme is shown in Fig. 2.

By considering the nature of the cover item, steganography is divided into five types: audio steganography, image steganography, network steganography, text

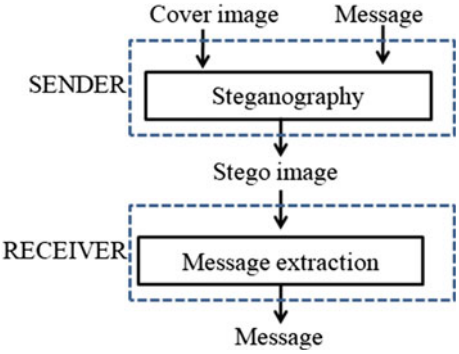

Fig. 2 Overview of image steganography scheme

steganography, and video steganography. We will go through the various forms of steganography briefly. The practice of concealing information inside text files is called text steganography. Image steganography is the process of concealing information by using an image as the cover object. In audio steganography, the confidential information is encrypted in an audio signal that alters the binary sequence of the corresponding audio file. When compared to other methods, hiding hidden messages in digital sound is far more challenging. You may use Video Steganography to hide any sort of data in a digital video. This kind has the benefit of being able to store a vast quantity of data and being a moving stream of pictures and sounds. The process of embedding information in data transmission network control protocols, such as Internet control message protocol (ICMP), transmission control protocol (TCP), and user datagram protocol (UDP), is known as network steganography. In several covert channels included in the open systems interconnection (OSI) model, steganography can be used. All of these technologies appear to be of tremendous assistance, but criminals and terrorist organizations are taking advantage of them. Understanding how to utilize steganography to obscure data and prevent it from being abused may be incredibly beneficial in both attack and defensive scenarios.

2.2 Reversible Data Hiding (RDH)

The RDH enables you to embed a huge quantity of data inside an image, allowing you to extract the hidden data while recovering the original image [2–6]. This makes it a good choice for instances where metadata has to be preserved in the cover signal, but the original signal needs to be retrieved without a loss following data extraction. These schemes are used for many applications. Some of the important applications are

- For authentication purposes, include authentication data in medical photographs or other very sensitive images.

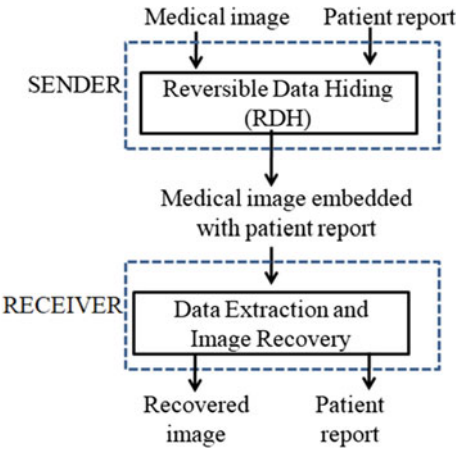

Fig. 3 Overview of RDH scheme in medical image transmission

- Before digital material can be uploaded to a cloud service provider, metadata must be incorporated into it.
- For the purpose of concealing some inquiry details in forensic pictures.
- Embedding and transferring clinical data into a medical image.

The overview of an RDH scheme for patient transmission along with the medical image is illustrated in Fig. 3.

2.3 Digital Watermarking

The copyright of digital files can be protected via digital watermarking techniques. To protect digital assets such as music, photos, and formal documents, a number of watermarking systems have been proposed. Digital watermarks can be visible, and they might be in the shape of logos or pictures in the corner of the digital content [7]. A number of invisible watermarking schemes are also there. Digital watermarking is frequently used in E-commerce to provide conditioned and consumer access to specified resources. As a result, digital watermarking allows artists to use the Internet to reach a larger audience for their work. Over the past few years, there have been many watermarking techniques that were introduced. The classification is shown in Fig. 4.

Techniques for watermarking may be classified into two groups: human perception-based and domain-based. The watermark information in digital watermarking might be fragile, semi-fragile, robust, or hybrid. Watermarks that are fragile are used to detect tampering, whereas robust watermarks are used to withstand standard image processing procedures. Semi-fragile watermarks are strong against friendly attacks but fragile against malicious attacks, while hybrid watermarks have mixed features.

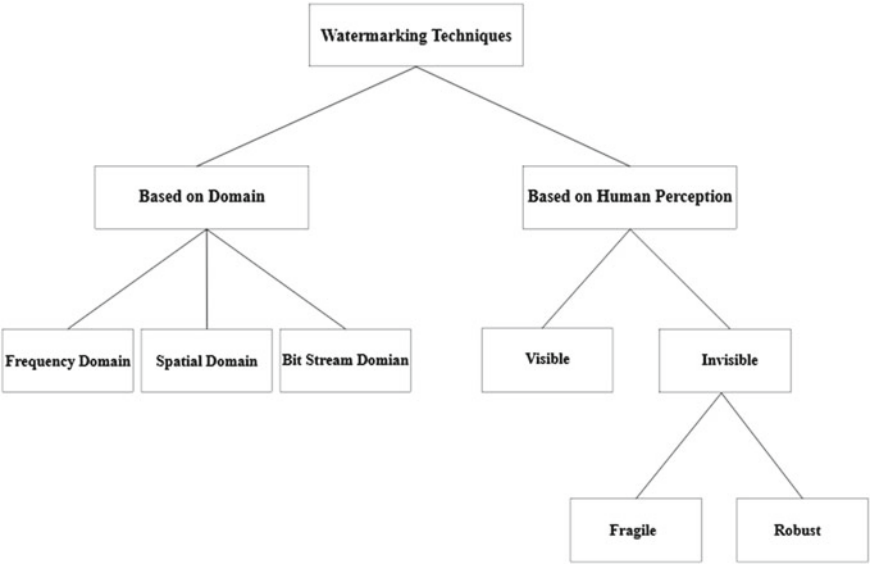

Fig. 4 Classification of watermarking Techniques

Fragile watermarking schemes are widely used for data authentication during medical image transmission. The sender and receiver will agree with a watermark at the beginning itself. When the sender wants to send some medical images from one place to another, the watermark will be embedded in the medical image. At the receiver side, the receiver will attempt to extract the embedded watermark using the watermark extraction procedure. Further, the extracted watermark will be compared with the original watermark. If these two are highly correlated then it indicates less alterations in the content during transmission. The changes in the content may be due to loss of information during transmission or due to an attack by an unauthorized person.

The conventional digital watermarking methods modify the original content permanently while embedding the watermark. This is a major concern when using digital watermarking techniques in medical image transmission since the changes in the medical images during watermarking may lead to a wrong diagnosis on the receiver side. This motivated the researchers to work on an area called reversible watermarking in which the receiver can extract the watermark and also the recovery of the original image is possible at the receiver side.

Because of its increasing applications in many different fields, in recent years, reversible watermarking has received a lot of interest. Reversible watermarking techniques were developed to be used primarily in situations where the validity of a digital image must be guaranteed, and the original content must be decoded. Patients' privacy must be secured due to the ever-increasing volume of medical digital photos and the necessity to send them between experts and hospitals for more accurate and better treatment. On the concept of ensuring the visual quality of the image, this method

embeds the information into a carrier image. The goal is to recreate the host image without loss after the watermark has been extracted. As a result, the amount of embedding information is more demanding than typical watermarking methods. Hence, it has more broad study and application value in the sectors of legal, military, medical, and other fields that demand high-image authenticity and integrity. The research on reversible image watermarking techniques aims to produce the highest embedding capacity of effective information with the least amount of distortion.

The next section of the book chapter introduces you to the efforts and research that researchers have done in recent years in the area of reversible watermarking.

3 Related Work

This section provides an overview of recent related research on reversible watermarking and reversible data hiding in medical image transmission, both of which have received widespread recognition in the scientific world. Before discussing the related works, the efficiency parameters used to analyze reversible data hiding schemes or reversible watermarking schemes are listed below. This discussion will help the readers to understand the further discussions in a better way.

3.1 Efficiency Parameters

In the process of analyzing different works, we will come through the following efficiency parameters:

- **Bit Error Rate**: The quality of data extraction is checked using this efficiency measure. In general, if the bit error rate is 0, it signifies that the data encoded in the image has been correctly retrieved, meaning that no data bits have raised an error.
- **Embedding Rate**: The ratio between the greatest number of bits that can be contained in a picture and the complete number of bits in the image is used to compute it. Schemes having a high embedding rate are frequently used in order to embed the greatest number of bits.
- **Peak Signal-to-Noise Ratio (PSNR)**: This parameter determines the visual quality of a picture. A high PSNR number indicates that the picture quality is rather excellent and that the mistake or corrupting noise that affects the image's visual quality is minimal. The PSNR of infinity indicates that the original and restored images are identical.
- **Structural Similarity Index (SSIM)**: The SSIM values vary from 0 to 1, with 0 being the lowest and 1 being the highest. When the SSIM value is 1, the recovered image is a perfect match to the original. For any RDH scheme, it is suggested to make sure that the SSIM is 1.

- **Natural Image Quality Evaluator (NIQE)**: It determines the image quality without a reference and compares the restored image to the original. The lesser the NIQE value, the better the perceptual quality.
- **Blind/Referenceless Image Spatial Quality Evaluator (BRISQUE)**: BRISQUE calculates the image quality without a reference and compares it to the original image, just like the NIQE parameter. Its value ranges from 0 to 100 in most cases. The lower the score, the better the image quality.

3.2 Related Works on Reversible Data Hiding

Reversible Data Hiding methods have been used on both natural and encrypted images. We will look at some of the more extensive efforts that have been done on natural images. As we've seen, it's critical to ensure that, regardless of the algorithm used, the original image is restored following data extraction.

A RDH scheme based on a prediction error histogram is discussed in [2]. The method worked by shifting pixels into black and white groups depending on prediction error histogram shifting. The pixels were classified using a checkerboard pattern. A black pixel will have four 4-neighbor pixels, as shown in the checkerboard pattern (top, right, bottom, and left). An average of three pixels from a four-neighborhood region that is extremely close to the center pixel value is used to estimate the value of the black pixel in the middle. The prediction error is then computed by comparing the value of the predicted pixel to the value of the actual pixel. The prediction error that correlates to all of the black pixels in the image is shown by the histogram of the prediction error. The histogram of prediction error is investigated for additional data concealment using the histogram shifting technique. Overflow and underflow, on the other hand, constitute a major issue in the RDH process. The results, on the other hand, show that image retrieval was successful and that image quality was improved. The embedding rate is high according to the approach, implying that the number of bits that may be embedded is similarly considerable. The BER is also included, resulting in a zero error rate. The images used in the approach were taken from the USC-SIPI image collection. The theoretical temporal complexity of the preceding approach was O(N), which may be decreased for better results.

A RDH strategy on the basis of a histogram of the blocks of the host image is discussed in [10]. To ensure the accurate recovery of the original picture, each block's maximum intensity value is utilized for data hiding, and the grayscale value is used for data concealment by altering the least significant bits of eight selected pixels; each block is embedded in the same block. To hide the secret data in a cover image I, according to this approach, the I should be divided into sections. Every piece will be BxB pixels in size. Only if the peak intensity value's height is greater than (F + 8), in which F is the number of 254 s and 255 s in that block, and one block will be used for data concealing. Whether a given block is suitable for data concealing or not is determined in the first phase, and a status sequence for embedding, M, is generated. If Mi is 0, it means that the I-th block is not utilized for data concealing,

and if Mi is 1, it means that the I-th block is. It's worth noting that the blocks are accessed and/or numbered in row-by-row linear order, ignoring the initial block. By altering the LSBs of the initial (N_B-1) pixels, the details about the embedding status will be buried in the first block of the picture, where N_B is the total number of blocks in the image. Because the original picture must be retrieved before the LSBs may be changed, the LSBs are encoded in the image itself, together with a coded message. Overflow pixels (initial pixels with pixel value 255) and pixels taken 255 after histogram shifting are differentiated with help of marker bits. The pixel with marker information 0 was originally 254, whereas the pixel with marker information 1 was originally 255. All of these details will be presented in a single image block. At the receiver's end, the overhead information may be retrieved, and this data will allow the recipient to recover the actual image to its original state. The visual quality of the recovered image was assessed using the SSIM and PSNR efficiency criteria. The PSNR is high, and the SSIM is near to but not quite one. This may be improved so that the system can be utilized in everyday situations.

The introduction of an effective overflow handling solution based on histogram shifting is discussed in [4]. Images from the USI-SIPI dataset were used to test the approach. Pixel values in a grayscale picture generally range from 0 to 255. As a result, histogram shifting converts a pixel value of 255 to 256, which is theoretically impossible. The term "overflow" is used to characterize this condition. To deal with the overflow, this technique was implemented. In this procedure, the histogram of the original picture I is displayed first. The peak of the histogram is located, and P_k is assigned to it. Pixel values greater than the histogram's peak are displaced, resulting in a gap in the histogram immediately following the peak. For the data hiding approach, all of the pixels are available in a predetermined sequence. If the pixel value is P_k, the data embedding method is performed on that pixel. To embed a message in a pixel, bit b, with P_k intensity value, b adds P_k. As a result, the altered image seems to be similar to the original. This picture contains fragments of a hidden message. The name of this image is Stego Image. Each pixel is examined after the data concealing method, and if its value exceeds the histogram's peak by b, those pixels are decremented by b, and message bit b is extracted. If the value of the pixel is the same as the actual value, the value is set to 0 and the pixel remains unchanged. As a consequence, the original pixel values have been restored, and the Stego image's message has been retrieved. Although two images produced a high embedding rate, which is laudable, this method asserts that the embedding rate is only determined by the histogram's peak. This approach may fail if the peak value is 255 since we can't increase it by one, resulting in a pixel value of 256.

In [6], a separable reversible data hiding mechanism is found. The suggested method is divided into three phases: data embedding, picture encryption, and data extraction/image recovery. To create an encrypted image, the content owner encodes the original uncompressed image with an encryption key. The data-hider then uses a data hiding key to compress the encrypted image's least important bits, resulting in a thin region that may take the extra data. The data encoded in the generated space may be simply retrieved at the receiver's end using the data hiding key from the

encrypted picture containing extra data. As the data embedding modifies only the LSB, the decryption with the help of the encryption key might result in a picture that appears exactly like the original. When both the data hiding keys and encryption are employed, the additional embedded data can be effectively recovered, and the actual picture then can be flawlessly reproduced by making use of the spatial correlation found in natural images.

As a result of the foregoing approach, the PSNR of a natively decrypted picture has been observed to be high but not infinite. The recovered picture has a PSNR of infinity, suggesting that it has been fully restored. However, the embedding rate for this technology may have been higher in order for it to be more useful in a wider range of applications.

Following a review of important publications on RDH, we may conclude that a few considerations must be made:

- To guarantee that the maximum amount of message bits may be embedded, the embedding rate must be as high as feasible.
- The image's visual quality must be excellent, which implies the PSNR and SSIM must be acceptable at the end.
- The bit error rate should be 0 at all times. Because the data is precisely extracted, the algorithm becomes more efficient.

3.3 Related Works on Reversible Watermarking

Before looking at the related works, let us understand the basic and important terms that we will come across in the watermarking techniques for a better understanding.

In general, the regions in medical images are divided into two sections: ROI and RONI. ROI stands for the region of interest and RONI started the region of non-interest. The ROI area is a diagnostically important part of the image that must be kept as much as feasible. The non-critical component of the picture is included in RONI like the background. When the ROI component is used to hide the watermark, the pixel intensities in this region may be deformed, resulting in misperceptions and, as a result, misdiagnosis. Watermarking techniques developed by RONI incorporate data in areas that are deemed insignificant in medical examinations. However, this can only be done if RONI is installed. The quantity of data that can be implanted is greatly dependent on the RONI size. The algorithm used by the researcher determines if the picture should be divided into ROI and RONI. Only a few methods don't need picture segmentation, and only a few do.

A novel robust reversible watermarking scheme for protecting medical image authenticity and integrity is presented in [11]. Robustness refers to a watermarking algorithm's capacity to survive operations like compression, filtering, and geometric assaults like rotation, scaling, and translation. A verification method for medical photos was included in this technique. It is broken down into four stages, as follows:

- Watermark Generation Phase: Watermarks, as well as integrated and authenticity data, are created during this phase.
- Phase of embedding watermark: Embedding of a watermark is done with the help of SLT at this phase (slantlet transform). The usage of single value decomposition (SVD) improves the watermarking robustness by making the value invariant to diverse attacks.
- Watermark extraction phase: At this phase, the watermark is removed, which is the opposite of the embedding process.
- Security verification phase: Integrity of the information and the ability to recover from tampering are checked in this phase.

The approach makes use of the SLT-SVD hybrid transform. In this design, the ROI and RONI are simply employed to create the watermark. The previous method reconstructs ROI and RONI pictures without loss using an RDM-based reversible function. By integrating the watermark into the full medical image by not separating ROI and RONI, the suggested watermarking technique solves the privacy issues associated with geographically partitioned picture partitioning, exceeding conventional ROI-lossless watermarking. The PSNR values of the recommended design are higher than those of the other schemes, and the SSIM was nearly one. However, because it is being used for medicinal purposes, the outcomes may be more favorable. The Bit Error Rate (BER), which is not zero, is accustomed to determining robustness.

A technique that uses the Integer Discrete Cosine Transform (InDICT) and Difference Expansion for reversible watermarking (DE) [12]. Frequency domain watermarking includes this notion. Using this method, the image is divided into non-overlapping chunks. The difference in expansion inserting and extraction process is applied to the separated blocks. In the transform processing stage, the integer-based DCT transform is applied to increase correctness and computation performance. For each block, the technique starts with an 8×8 image that is subjected to 2D-DCT. A zigzag scan is used to convert the watermark image into a 1D vector, which may also be done after the watermark image has been encrypted. The zigzag scan is used because it spreads out the neighboring pixels and strengthens the picture. To evaluate whether there is any overflow or underflow, a reconstructive stimulation method is performed on each block. According to the experimental results, PSNR is high and provides reversibility, which is vital for medical applications. The algorithm's embedding capacity is represented by the number of blocks with the proper energy. The amount of blocks varies depending on the images. It's possible that the rate of embedding was higher.

Another reversible watermarking scheme is discussed in [13]; it's been disclosed that there's a reversible invisible digital watermarking method for medical image ownership security and content authentication. This solution is designed in the geographical domain using meaningful data from patients as ownership data and a SHA256 hash function built using an adaptive prediction algorithm and additive predictor error technique. Hash functions are used for mapping. The hash function H for a hash value h getting a variable-sized input x can be written as $H = h(x)$. Hash functions are called collision-free when no messages x and y have the same

H(y) = H(x). SHA256 is one of the widely adopted collision-free hash functions. It has also been adopted by NSIT. In the proposed RDH algorithm, the idea is to create 64 hexadecimal-size authentic watermark information for healthcare pictures, by using SHA 256 hash function. In this work, there has been a discussion about both, the extraction of watermark and medical images. In the receiver end, at the decoder, watermark from the clinical image and the watermark of ownership, both can be extracted. The use of the additive prediction error technique is done to extract both watermarks.

This algorithm has been implemented on MRI and X-ray images. Anything unique to the patient, such as a mobile number or an Aadhar number, might be used as ownership information. The ownership information is then incorporated 10 times in the image as a watermark. The content authentication watermark is created using the hash algorithm. The study goes into great detail on how PSNR varies when watermark hiding parameters vary.

A scheme for medical image watermarking with tamper detection and recovery using reversible watermarking with LSB Modification and run length encoding (RLE) compression is explored in [5]. This method uses the LSB modification to detect and recover tampering in the ROI. The ROI and RONI of a photograph are first separated. To detect and recover tampering, watermarking would be completed in ROI. RONI will be put to use to integrate the image's actual LSBs, making the watermark reversible. Only the LSBs from the ROI are used, rather than all of the LSBs in the image. Before adding the watermark, the picture's original LSBs are eliminated, and the LSB of each pixel is set to zero. After that, the LSBs that were removed will be compressed and placed into the RONI. The original LSBs of the image will be compacted and saved in the RONI. The LSB is saved and can later be used to restore the image's pixel values to their original state. A watermarked image's PSNR is around 46 dB, implying that the watermarking method may create a watermarked image with the least amount of deterioration and that appears extremely same as the initial one. During the trial of watermark reversibility, the actual LSBs of the watermarked picture are restored with no modification. The compacted LSBs from the RONI would be retrieved, decrypted, and recovered to every pixel. This procedure's outcome, the recovered picture, is then compared to the original image. While the recovered image is nearly similar to the initial one, the PSNR is in the range of 56 and 61 dB, showing that there is still a minor difference. The PSNR might be upgraded to make it more useful in medicine.

In [14], in CT SCAN images, a method for reversible watermarking was discovered. This process employs the ROI and RONI watermarking techniques. With the help of a segmentation algorithm, the procedure segments the actual image into ROI and RONI. It embeds a fragile watermark in the ROI to maintain the fairness of the captured image, while a compound robust watermark is implanted in the RONI to safeguard client data and copyright of medical pictures. The method uses prediction-based reversible watermarking to integrate ROI repair data into RONI. Following the embedding step's segmentation of ROI and RONI, the LSBs of ROI are segregated and preserved in an isolated storage. Watermarks are made that are both delicate and durable. The LSBs of ROI are replaced with delicate watermarks to

create watermarked ROI. This process is repeated for each RONI pixel until all of the watermark data is implanted. The watermarked picture is now segmented into ROI and RONI with the help of the segmentation procedure. Watermarked ROI's LSBs are extracted. The approach determines that the restored picture has not been altered in any manner. The PSNR values were good, and the technology permits CT scan images to be transferred from one source to another without fear of losing medical information.

A few works and its characteristics are summarized in Table 1.

Following the analysis of various situations, it can be stated that the majority of works were primarily focused on the following:

Table 1 A few schemes for reversible data hiding/reversible watermarking

Reference No.	Secure communication technique	Algorithm used	Quality measures
[2]	Reversible Data Hiding	Prediction error-based histogram shifting	0.0948bpp PSNR—Infinity SSIM—1
[6]	Reversible Data Hiding	Separable Reversible Data Hiding in Encrypted Image	ER—0.017 bpp PSNR—Infinity SSIM—1
[15]	Reversible Data Hiding	High capacity using histogram shifting of each image between minimum and maximum frequency	0.045–0.14 bpp PSNR—49–53 dB
[10]	Reversible Data Hiding	Block-wise histogram shifting	ER-0.058–0.11bpp PSNR—50–52 dB SSIM—0.99
[16]	Reversible Watermarking	Difference Expansion Method	BER—0.39–0.49 PSNR—Infinity RMSE—0
[17]	Reversible Data Hiding	Interpolation-based Reversible Data Hiding (IRDH)	PSNR—39–47 dB SSIM—0.85–0.92
[5]	Reversible Watermarking	LSB modification and Run Length Coding Compression	PSNR of watermarked image—46 dB PSNR of extracted image—56–61 dB
[18]	Reversible Watermarking	Modulation mode of Discrete Cosine Transform coefficients	PSNR—70 dB SSIM—1
[19]	Reversible Watermarking	Difference expansion technique	PSNR—Infinity SSIM—1 RMSE—0
[3]	Reversible Watermarking	Recursive Dither Modulation (RDM) technique	PSNR—45–66 dB SSIM—0.97–0.99

- Reversible data hiding schemes are more popular for clinical data transmission along with medical images.
- Reversible watermarking is an extension of reversible data hiding scheme in which a watermark will be embedded in the image using a reversible data hiding technique. The watermark can be extracted at the receiver side for ensuring data authenticity.
- The quality of the watermarked image and embedding rate is a major concern
- The image recovery process is expected to be lossless at the receiver side.
- Robust reversible data hiding schemes are the recent advancements in this domain in which the image can be recovered at the receiver side even though some distortions happened in the image during transmission.

4 Medical Image Datasets for the Research Work

In this part, we'll go through the key datasets that were considered for various methodologies.

- Natural photos were acquired from a dataset named USC-SIPI, which is supervised by the University of Southern California [20]. It's a collection of photographs that are mostly kept for the purposes of image processing, image analysis, and machine learning. There are four volumes in this database, namely
  - Textures
  - Aerials
  - Miscellaneous
  - Sequences.
- Several strategies were also carried out using DICOM image collections. These datasets are only available for use in research and education. Digital Imaging and Communications in Medicine (DICOM) is a standard for the sharing and administration of medical imaging data and related information. DICOM files can be shared between two organizations that can receive DICOM-formatted pictures and patient data. A set of DICOM images are available in OsriX DICOM image set [21].
- Open Access Series of Imaging Studies (OASIS) is an initiative whose goal is to make neuroimaging datasets publicly available for medical study. The most recent release is OASIS-3, which is a longitudinal neuroimaging, clinical, cognitive, and biomarker dataset for normal aging and Alzheimer's disease [22].
- National Biomedical Imaging Archive (NBIA) is a repository that provides access to imaging resources that will increase the use of imaging in biomedical research and practice today by improving the efficiency and repeatability of cancer detection and diagnosis using imaging. Imaging can be used to offer an objective assessment of a patient's reaction to treatment. Ultimately, this will enable the development of imaging resources that will improve clinical decision support [23].

5 Research Challenges

In this part, we'll look at some of the research problems that came up throughout the implementation phase. Every algorithm or scheme, when it is being implemented for practical applications, must make sure that the following points are considered:

- When the technique is used for medical purposes, one must ensure that the medical image is perfectly restored on the receiver side. This can be verified using a parameter PSNR. Peak Signal-to-Noise Ratio is shortly called PSNR.

  The formula of PSNR is 10 log 10 ((P EAK) ^{2}/MSE) dB.

  PEAK denotes the image's highest pixel intensity, while MSE denotes the noise-measuring metric known as mean square error. When the mean square error is 0, it means that the image is perfectly restored without any distortion and thus PSNR results to be infinity.

- Similar to the PSNR, Structural Similarity Index (SSIM) is also considered to verify the image reversibility. To understand that image retrieval is perfect, SSIM should be 1. It generally ranges from 0 to 1.
- The data that is embedded in the images are confidential. So, the factor Bit Error Rate is taken into account to check the accuracy of the message retrieved from the picture at the receiver end. When the Bit Error rate is 0, it suggests that there is no message bit that has raised an error during the extraction process.
- Embedding rate should be higher, which means that the amount of data users can embed should be high for better usage. It is computed in Bits per Pixel (bpp).

Along with reversible data hiding, reversible watermarking techniques are also commonly utilized. There are a few obstacles to overcome throughout the implementation of this process:

- It's critical to have a strong embedding capability that can allow embedding the necessary legitimate data.
- Even after inserting the watermark or information, the quality of the tagged photos must be maintained. The imperceptibility factor is reflected in the quantity of invisibility of the watermark.
- The picture's durability should be considered. Misdiagnosis might occur if the picture is altered during transmission.
- The receiver must have the flexibility to restore the original image without distortion after removing the encoded watermark.

The elements listed above are frequent research problems that every researcher encounters throughout implementation. Only if the aforesaid variables are taken into account will a scheme be entirely acceptable for all purposes.

6 Conclusion

In this book chapter, we have discussed the importance of secure communication, especially during medical image transmission. A detailed discussion is done on various ways to transmit data securely through an unsecured channel. This chapter also discussed the motivation to work in the domain of reversible data hiding. The extension of reversible data hiding called reversible watermarking schemes is also discussed in detail in this chapter. Various well-known reversible data hiding schemes are briefed along with their merits and demerits. The well-known datasets available for the study are also summarized in the chapter. The researchers working in this domain can use those datasets for the experimental study. A number of research challenges are also discussed in this chapter so that the researchers can focus on these areas to design and implement new reversible data hiding schemes suited for the healthcare sector.

References

1. Box, D., Pottas, D.: Improving information security behaviour in the healthcare context. Procedia Technol. **9**, 1093–1103 (2013)
2. Padmaja, B., Manikandan, V.M.: A novel prediction error histogram shifting-based reversible data hiding scheme for medical image transmission. 2021 4th International Conference on Security and Privacy (ISEA-ISAP), pp. 1–6 (2021). https://doi.org/10.1109/ISEA-ISAP54304.2021.9688572
3. Ribina, B., Jeena, R.S.: Recursive dither modulation based reversible watermarking scheme for medical images. 2015 International Conference on Control Communication & Computing India (ICCC), pp. 375–379 (2015). https://doi.org/10.1109/ICCC.2015.7432924
4. Manikandan, V.M., Renjith, P.: An efficient overflow handling technique for histogram shifting based reversible data hiding. 2020 International Conference on Innovative Trends in Information Technology (ICITIIT), pp. 1–6 (2020). https://doi.org/10.1109/ICITIIT49094.2020.9071553
5. Tjokorda Agung, B.W., Adiwijaya, Permana, F.P.: Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression. 2012 IEEE International Conference on Communication, Networks and Satellite (ComNetSat), pp. 167–171 (2012). https://doi.org/10.1109/ComNetSat.2012.6380799
6. Zhang, X.: Separable reversible data hiding in encrypted image. IEEE Trans. Inf. Forensics Secur. **7**(2), 826–832 (2012). https://doi.org/10.1109/TIFS.2011.2176120
7. Katzenbeisser, S., Petitcolas, F.A.P.: Digital watermarking. Artech House, London 2 (2000)
8. Kahn, D.: The history of steganography. International Workshop on Information Hiding. Springer, Berlin, Heidelberg (1996)
9. Cheddad, A. et al.: Digital image steganography: Survey and analysis of current methods. Signal Proc. **90**(3), 727–752 (2010)
10. Murthy, K.S.R., Manikandan, V.M.: A block-wise histogram shifting based reversible data hiding scheme with overflow handling. 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1–6 (2020). https://doi.org/10.1109/ICCCNT49239.2020.9225552

11. Liu, X. et al.: A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images. IEEE Access **7**, 76580–76598 (2019). https://doi.org/10.1109/ACCESS.2019.2921894
12. Gao, L., Gao, T., Sheng, G., Cao, Y., Fan, L.: A new reversible watermarking scheme based on Integer DCT for medical images. 2012 International Conference on Wavelet Analysis and Pattern Recognition, pp. 33–37 (2012). https://doi.org/10.1109/ICWAPR.2012.6294751
13. Kunhu, A., Al-Ahmad, H., Mansoori, S.A.: A reversible watermarking scheme for ownership protection and authentication of medical Images. 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), pp. 1–4 (2017). https://doi.org/10.1109/ICECTA.2017.8251971
14. Memon, N.A., Alzahrani, A.: Prediction-based reversible watermarking of CT scan images for content authentication and copyright protection. IEEE Access **8**, 75448–75462 (2020). https://doi.org/10.1109/ACCESS.2020.2989175
15. Fallahpour, M., Megias, D., Ghanbari, M.: High capacity, reversible data hiding in medical images. 2009 16th IEEE International Conference on Image Processing (ICIP), pp. 4241–4244 (2009). https://doi.org/10.1109/ICIP.2009.5413711
16. Qasim, A.F., Meziane, F., Aspin, R.: A reversible and imperceptible watermarking scheme for MR images authentication. 2018 24th International Conference on Automation and Computing (ICAC), pp. 1–6 (2018). https://doi.org/10.23919/IConAC.2018.8749000
17. Wahed, M.A., Nyeem, H., Elahi, M.F.: An improved interpolation based reversible data hiding for medical images. 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), pp. 1–6 (2019). https://doi.org/10.1109/ECACE.2019.8679278
18. Bahrushin, A.P., et al.: J. Phys. Conf. Ser. **1399**, 033025 (2019)
19. Qasim, A.F., Aspin, R., Meziane, F., et al.: ROI-based reversible watermarking scheme for ensuring the integrity and authenticity of DICOM MR images. Multimed Tools Appl **78**, 16433–16463 (2019)
20. USC-SIPI by University of Southern California. https://sipi.usc.edu/database/database.php?volume=rotate
21. DICOM Image Library. https://www.osirix-viewer.com/resources/dicom-image-library/
22. OASIS Brains—Open Access Series of Imaging Studies. https://www.oasis-brains.org/
23. National Biomedical Imaging Archive—NBIA. https://www.re3data.org/repository/r3d100012650