

Research Article

Survey on Reversible Watermarking Techniques of Echocardiography

Rabiya Ghafoor,¹ Danish Saleem,¹ Sajjad Shaukat Jamal ,² M. Ishtiaq ,¹ Sadaf Ejaz,¹ Arif Jamal Malik,¹ and M. Fahad Khan¹

¹Department of Software Engineering, Foundation University Islamabad, Islamabad 46000, Pakistan

²Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia

Correspondence should be addressed to M. Ishtiaq; imishtiaq@gmail.com

Received 3 September 2020; Revised 6 November 2020; Accepted 30 December 2020; Published 26 March 2021

Academic Editor: Emanuele Maiorana

Copyright © 2021 Rabiya Ghafoor et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In critical domains such as medical and military, reversible watermarking (RW) has been used. In the medical domain, different modalities are used to store patient information. The current study focuses on the application of RW in echocardiography data. Mostly, RW is applied to protect patient data without affecting the quality of the decoded image. The RW methods are benchmarked as per imperceptibility, robustness, and payload. The survey presents a comparison of state-of-the-art RW techniques. The imperceptibility and payload are balanced through a tradeoff. It has been observed in the literature that most of the RW methods lack robustness, and very small-scale robustness has been achieved in this domain of watermarking. Different types of RW, i.e., fragile, semifragile, and robust methods, are being compared and reviewed. Mostly, fragile methods are developed on the error-expansion techniques built on histogram shifting-based approach. In this study, several RW methods are compared and the results are presented.

1. Introduction

Medical imaging (such as echocardiography and ultrasonography) holds vital details about the patient. Echocardiography with its different flavors is eminent for rendering information regarding the size and shape of the heart, identification of cardiological risks, pumping capacity, and location and severity of tissue damage [1–3]. The information comprised by these modalities is outstandingly critical that makes it very challenging for video processing and image processing. It ultimately results in a strong urge for lossless and robust data hiding for such data processing [4, 5].

Continuous advancements in technology have done a marvelous job transforming every facet of human life, and the quest for further improvement and technological advancement is perpetual. Computer technology, with all its power, has shrunk into palms with the advent of smartphones and other handheld devices. This has completely

revolutionized the communication and data processing domains with an ever-increasing data transfer volume. In the information technology jargon, this transfer could be broken into Store, Retrieve, and Transmit.

One of the biggest beneficiaries of this transformation is the medical domain which has benefited tremendously over the years with the innovations in information technology. Health information technology (HIT) has gained popularity, and many health institutes are exploiting information technology for storing patient's information. This electronic medical record (EMR) holds complete information about a patient's current and past ailments, laboratory test data, medical imaging results, diagnosis, and drug information, etc. All these data can be transformed into a single database that can be stored, accessed, and transmitted to other medical institutions as per requirement. This encourages a paperless environment and enables different stakeholders to access complete information about the patient with a single mouse click.

This digitization of medical records potentially poses a threat to the data integrity from both intentional or unintentional changes and misuse which has increased the tendency of attacks on digital data [6]. Manipulation, unauthorized access, deletion, and distribution of medical data are increasing [7, 8]. Patient data theft crimes are on the rise, and this can have a severely adverse effect on the efficacy of telemedicine and E-health applications [9, 10].

Although techniques like DICOM (Digital Imaging and Communications in Medicine) mitigate many of these risks that arise during transmission of digitized medical data, the overhead of extra information makes it a lesser candidate if the same is to be transmitted over public networks or low bandwidth connections [10].

All the data protection techniques such as cryptography, steganography, and watermarking, etc., have their own advantages, but for authentication of medical data [11], watermarking has been the most popular and robust technique adopted [12]. A digital identification mark or message is embedded into the cover medium, i.e., the digital medical data like images, videos, text, etc. This not only secures the data authenticity but also nullifies any ownership disputes [8, 12, 13]. When used in conjunction with cryptographic techniques, digital watermarking provides a highly resolute solution against data tampering [10]. Another perk is that it is a well-established research area and the application spans over various prominent areas such as broadcast monitoring. Therefore, a lot of research onus has been towards the medical image and video watermarking to secure the communication of highly confidential patient data. Modern data hiding techniques and their application classification are shown in Figure 1. A general framework of the digital watermarking technique for medical images is presented in Figures 2(a) and 2(b). The data embedding process requires a cover image, digital watermark, and a non-compulsory secure key. The output of this embedding function will be a watermarked image that can be transmitted or stored as per requirement. When the watermark is extracted, the encoding process is generally performed in a reverse order to extract the embedded data. These data are subsequently used to authenticate the original content and for tamper detection [15, 16].

An efficient watermarking system must ensure certain attributes that are pivotal in ensuring data security. These parameters or attributes are generally conflicting and require a certain degree of compromise made between them by the watermarking algorithm [9]. The four major characteristics are capacity, security, perceptibility, and robustness. In this paper, we aim to review reversible data hiding techniques which are being utilized for hiding information in echocardiography (ultrasound) for the security of healthcare systems.

2. Literature Review

In 2019, Kaw et al. [17] submitted an RDH scheme using optimal pixel repetition for securely hiding information. It results in a histogram invariant stego image. High robustness is achieved from statistical attacks due to

histogram invariance. PSNR acquired after experiments is 42 dB for 1.25 bpp payload by applying the scheme for X-ray.

In 2018, Geetha and Geetha [18] proposed a scheme for hiding data utilizing expansion on prediction error on image points obtained by integer-integer wavelet transform (I-IWT). Subbands are used in this technique for employing I-IWT, and embedding of secret bits is done on subbands. 52.6 PSNR is obtained for 75285 bpp payload for an X-ray image.

In 2020, spatial domain-based method was proposed by Dutta et al. [19] for watermarking. By exploiting spatial redundancy of vastly correlated pixels, this technique achieved robustness and visual quality. Accurate reversibility is demonstrated even in error-prone transmission channels. Parah et al. [20] purposed a reversible and high capacity system that utilized the pixel repetition technique. The proposed system has the capability of detecting tampering by using Block Checksum Embedding. Experiments were carried out on CT scans and witnessed an average of 46 dB PSNR as an output for a 1,96,608-bit payload.

Bhardwaj and Aggarwal [21] proposed an encrypted RDH algorithm based on hierarchical absolute moment block truncation coding. Hierarchical AMBTC is used to obtain a table having a high mean, low mean table, and bitmap sequence table. Encryption is done at a first place through a homomorphic-based cryptosystem, and then, every grey pixel having a high mean table is utilized for data embedding. In addition to that, each pixel having tables with low mean and bitmap sequence (except zero (0) value) is utilized in the embedding process without any underflow or overflow issue. Investigational outcomes showed that the proposed method was performed possessing a peak embedding rate of 1.80 bits per pixel and 49.89 dB PSNR value. Geetha and Geetha presented the RDH technique with high embedding capacity without degrading the quality of the cover image [22].

Interpolated points of the cover image are predicted by employing the Rhombus Mean Interpolation technique. For the discovery of tampering and authenticity of the content, the patient's data as secret information along with checksum for the nonoverlapping of 2×2 pixel block are inserted. The results for the CT scan depicted that 42.398 dB PSNR achieved 1.5 bpp payload.

In 2014, Acharjee et al. [4] proffered the technique of watermarking for echocardiograph video. After computing the motion vector of two adjacent frames, the image is watermarked. Results showed SSIM between the original and restored frames (2–6) was between 0.9902 and 0.9943 whereas PSNR of the original and recovered frames for the same number of frames was between 163.95 dB and 165.23 dB.

Dey et al. proposed a DWT-DCT-SVD-based technique for watermarking intravascular ultrasound video [23]. Watermark embedding is achieved by splitting IVUS video into frames and with the employment of discrete wavelet transformation (DWT) along with discrete cosine transformation (DCT) followed by singular value decomposition

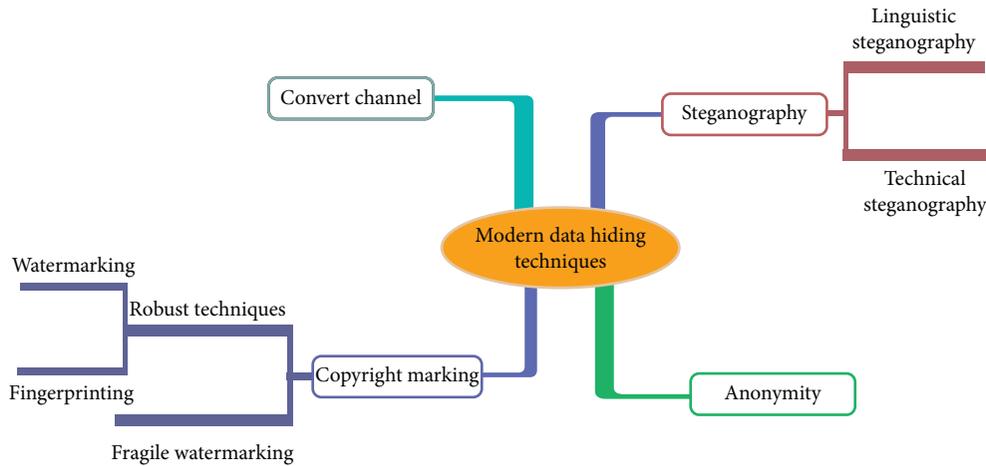


FIGURE 1: Classification of modern data hiding techniques [14].

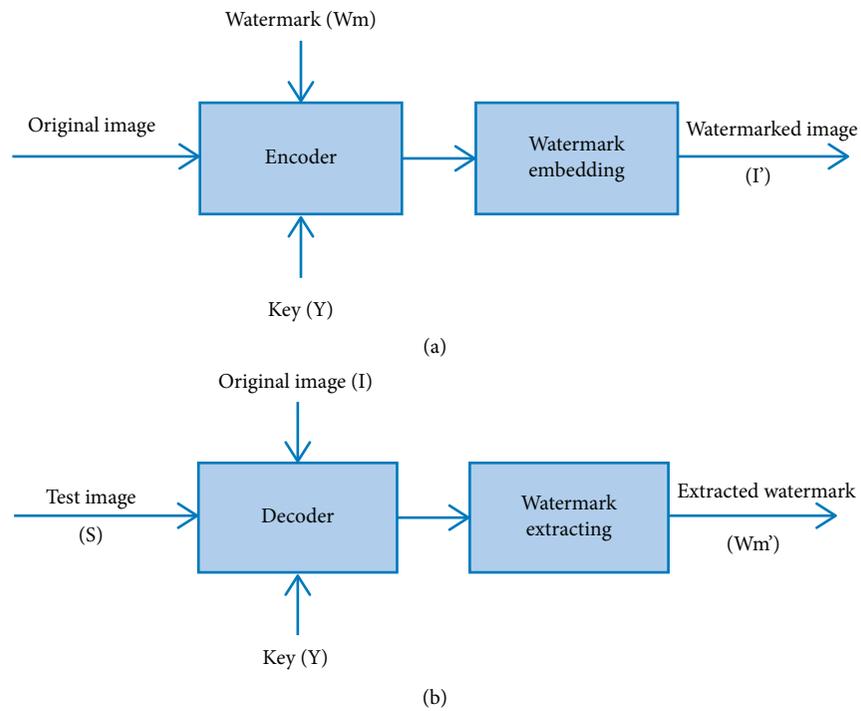


FIGURE 2: Watermarking. (a) Embedding and (b) extraction process [15].

(SVD). The extraction process involved the application of inverse of both DWT and DCT along with SVD. The assessment of the proffered technique is done through PSNR along with the correlation coefficient. 50.8122 PSNR achieved between the original IVUS video and watermarked video, and the correlation coefficient was 0.9990 between the original and watermarked video. The reversible watermarking technique was presented by Fadoua and Hamid [24] for the security of medical video. Patient identity is embedded into the host video, for that matter polynomial transform methods were utilized for the identification of optimal frames in each video shot. After experimentation average, PSNR and NC obtained are 61.4394 and 1.0000, respectively, for the frame size 120×120 .

3. Methodologies

In this section, three types of watermarking techniques are discussed, i.e., spatial domain, frequency domain, and hybrid domain methods. These methods are mostly classified into fragile, semifragile, and robust techniques. In Table 1, the methods are being summarized.

3.1. Spatial Domain

3.1.1. Watermarking with Tamper Detection and Retrieval Using Lossless Watermarking with LSB Modification. In 2012, Agung et al. proposed a reversible technique based on

TABLE 1: Different types of watermarking.

Watermarking type	Characteristics
Fragile	The fragile methods are mostly used in application where content authentication is desired. Detection of forgeries/temper, unauthorized processing, and transmission is carried out using fragile methods of watermarking.
Semifragile	Application which has privacy constraints along with content authentication uses semifragile methods.
Robust	The method of watermarking is used in situation where protection of copyright and digital rights management is desired. These kinds of watermarks survive malicious/nonmalicious attacks on the marked media.

LSB modification for watermarking the medical images [25]. Liew's design-based technique [26] used in this paper in terms of original LSBs is embedded in the region of interest by utilizing run-length encoding. Jasni's scheme [27] for temper detection and watermark recovery is also the base of this technique. Synopsis of the technique is presented as follows.

(a) Image preparation: for experimentation, images of ultrasound (8 bit) with a resolution of 640×480 pixels are used. The image is segregated into RONI and ROI. For temper detection and recovery, ROI is utilized for watermarking. RONI is utilized for embedding the original LSBs for the reversibility of the watermark. For generalizing, the static sizes of samples of ROI along with RONI are used as demonstrated.

The red rectangular region depicts the ROI in Figure 3. For achieving the best precision of temper localization and better quality of the recovered image, smaller block size of 6×6 is used instead of 8×8 . A mapping ($A \rightarrow B \rightarrow C \rightarrow D \rightarrow \dots \rightarrow A$) sequence prepared for subjecting ROI to embed watermark is one to one block mapping, and a specific block is denoted by each symbol. Information for the reconstruction of every previous block is injected in the adjacent next block [27].

$$\vec{B} = [(k \times B) \bmod N_b] + 1, \quad (1)$$

where k denotes the prime number and N_b is the representation of total blocks that exist in ROI. A distinct integer $\{1, 2, 3, \dots, N_b\}$ as B is allocated to each ROI block. Raster scan {left-right top-bottom} is utilized for the allocation of a number to every block. After that, RONI is split into 6×1 pixel blocks. The compression of actual LSBs is done by applying RLE, and a block in the region RONI is then utilized for embedding the resultant package of RLE.

(b) Watermarking procedure in ROI: the watermarking technique is based on Jasni's scheme [27] with a block size of 6×6 pixels in ROI. Ahead of inserting the watermark, the native LSBs are removed and each one is set to zero. Each 6×6 block is segregated further into 3×3 pixel subblock. For every single subblock, a watermark of 3×3 bits consists of an authentication watermark of a 2-bit and recovery watermark having 7 bits (r).

Create a watermark v for every single subblock after calculating the average intensity of block (Avg_B) and its subblock (Avg_{Bs}) as

$$v = \begin{cases} 0, & \text{if } \text{Avg}_{Bs} > \text{Avg}_B, \\ 1, & \text{otherwise.} \end{cases} \quad (2)$$

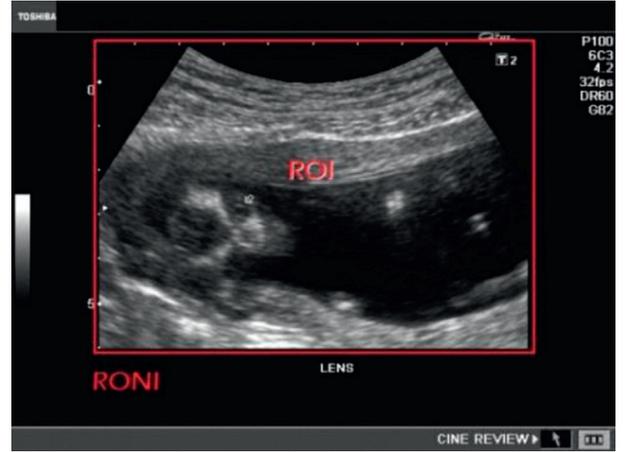


FIGURE 3: Locations of ROI and RONI [26].

The watermark p is generated as

$$v = \begin{cases} 1, & \text{if } \text{Avg}_{Bs} \text{ is odd,} \\ 0, & \text{otherwise.} \end{cases} \quad (3)$$

The watermark (v, p, r) is then embedded for every single subblock in its LSBs as illustrated in Figure 4.

(c) Embedding in the RONI: the actual LSBs are stored in RONI after compression. These stored values are then used for the image restoring process. Removed LSBs are depicted as a $640 \times 480 \times 1$ -bit binary LSB matrix. For achieving higher embedding capacity, an RLE-based compression is used. A matrix having LSBs is split into 3×3 bit LSB blocks first, and then, all the bits of the block are converted into decimal according to the demonstration mentioned in Figure 5.

The decimal value range is 0–511 (9 bits). An acquired collection of converted values of every single LSB block is then subjected to a raster scan, and obtained data run is then utilized as an input of RLE. The result of the RLE process will be a package containing the run value (RV) and run count (RC).

Each 12-bit RLE package of injected into 6×1 pixel block in the RONI. RV range is 511, so 9-bit storage is required whereas RC is limited to 7, for that matter only 3 bits are required. A complete scheme for the RLE package having 12 bits in RONI is depicted in Figure 6.

Established from the experiments, second LSB (LSB 2) needs to be used to avoid storage issues and embedding all the RLE packages in RONI.

(d) Identification of tamper and recovery: the presumed image is decomposed into RONI and ROI and ROI is split into 6×6 pixel block. Each block of ROI is then further

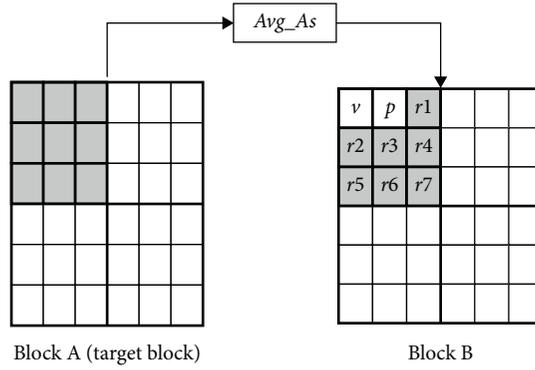


FIGURE 4: Watermarking in ROI [25].

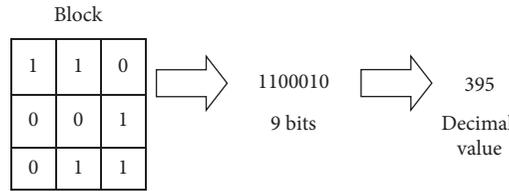


FIGURE 5: Decimal conversion of 9-bit LSB block [25].

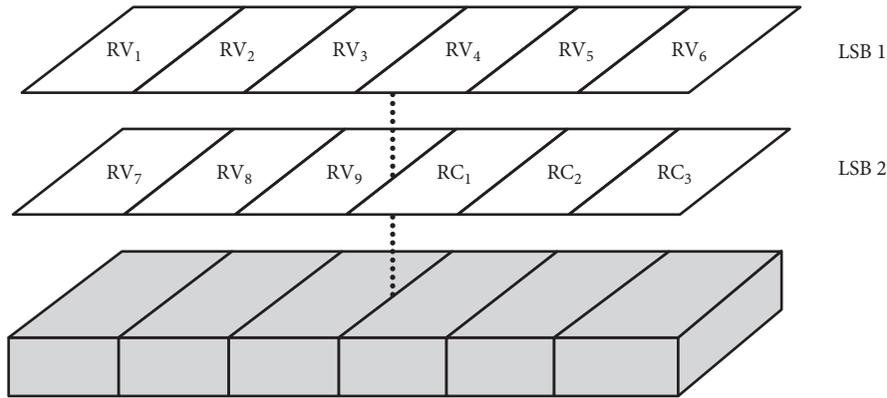


FIGURE 6: Embedding of an RLE package into a RONI block [25].

divided into subblock of 3×3 pixels. As proposed in [27], for every subblock, parity bit p and authentication bit v will be extracted. After adjusting the block's LSBs to zero, calculate the average intensity of block (Avg_B) and its subblock (Avg_Bs). Populate the parity bit p' and authentication bit as v' and compare these bits with the extracted bits p and v for the authentication of the block whether it is tempered or not. Tempered blocks will be revived by spotting recovery blocks utilizing the continuous pattern of the mapping which is utilized in the preparation of the image. As illustrated in Figure 7, let A be a block that is tempered. For the recovery of the block, information embedded in the block B will be used. For every single subblock in A block, substitute 7-bit MSB containing recovery data acquired from its corresponding subblock in the block B .

(e) Restoring the actual LSBs: after splitting RONI into 6×1 pixel block, the block of RONI which is utilized for injecting each RLE package will be extracted and decoded as

shown in Figure 6. A collection of decimal values in the range of 0–511 will be obtained after decoding RLE. Each decimal value will be transformed into a binary number of $3 \times 3 \times 1$ bits. This whole procedure is opposite to the one illustrated in Figure 6. A matrix containing $3 \times 3 \times 1$ bits will be the 3×3 pixel block's LSBs. After dividing the image into 3×3 pixels block by using a raster scan, each $3 \times 3 \times 1$ bit LSB is then restored to each block of the image.

The second LSB used to embed RLE packages cannot be restored because that was not stored. Due to one of the qualities of ultrasound that nearly every pixel value of RONI is depicting black having value zero, the second LSB is set to zero for every pixel with a value less than 3 to boosting the PSNR of the recovered image. For the case of ROI, it can be claimed that every pixel is reversible. MATLAB is used for the implementation purpose to evaluate the watermark reversibility as well as to spot the tamper and repossession of the image.

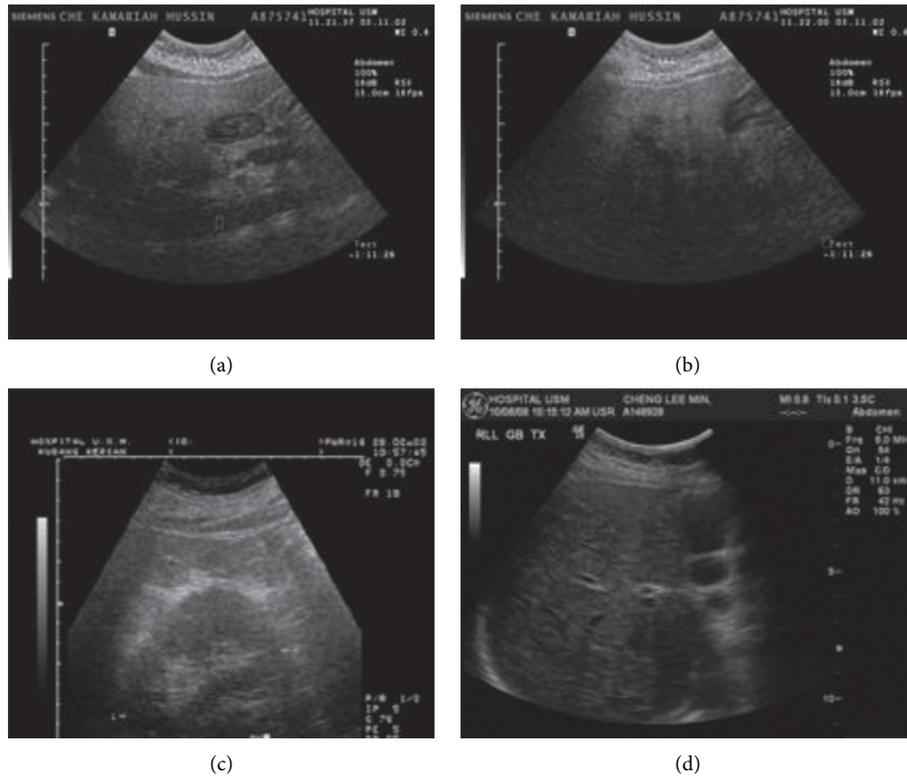


FIGURE 7: Images utilized for the experiment [28]. (a) Ultrasound 1 (888×666 pixels), (b) ultrasound 2 (888×666 pixels), (c) ultrasound 3 (704×576 pixels), and (d) ultrasound 4 (640×480 pixels).

Results illustrated the PSNR of the watermarked image is above 46 dB which means that the technique can originate watermarked images with lower deterioration and identical to the actual.

From the reversibility point of view, the results depicted in Figure 8 show that the technique is reversible for that region which comprises the ROI, but the RONI-acquired image is close to the original due to the inclusion of the second LSB. Temper detection results showed that the scheme performed 100% for temper localization whereas for sharpening attack it performed 99%, and for brightness and contrast adjustment attacks, the performance was between 60% and 98%. Recovery performance was 100% in terms of recovery and PSNR for the area $<20\%$. For the manipulations containing sharpening adjustments, brightness adjustments, and contrast adjustments, the recovery rate was low (6%–48%). Further improvements are desired to make this scheme completely lossless for a wider range of attacks.

3.1.2. ROI-Based Tamper Detection and Recovery for Medical Images Using Reversible Watermarking Technique. Al-Qershi and Khoo [28] coined a technique comprised of difference expansion for reversibly embedding watermark in ultrasound images. Embedding is done into changeable and expandable groups, and difference groups are distinguished by the location map. This technique can be utilized for hiding information related to the patient, authentication of

ROI, locating the area tempered inside the ROI, and recovery of the tempered regions. After splitting the original image into ROI, RONI, and border regions, RONI is used for embedding payload through 2D-DE. The location map is generated which is then used at the extraction phase. The payload is the combination of the following:

- (a) Patient's information
- (b) ROI's hash message for authentication
- (c) ROI pixels for locating tempering
- (d) Recovery along with the LSBs of pixels located border of the image
- (a) Embedding phase:
 - (i) After decomposition of the image into ROI, RONI, and border
 - (ii) By utilizing the MD5 algorithm a hash message "H" is computed for ROI after dividing it into 16×16 pixels
 - (iii) Bits of ROI pixels "P" and LSBs of border pixels "L" are collected
 - (iv) The patient's information "D" is appended in these collected bits "P" and "H" along with the hash message "H"
 - (v) After the concatenation of bits in the previous step, the payload is formed by compressing string through Huffman coding
 - (vi) RONI is utilized to embed payload in it using 2D-DE [29]

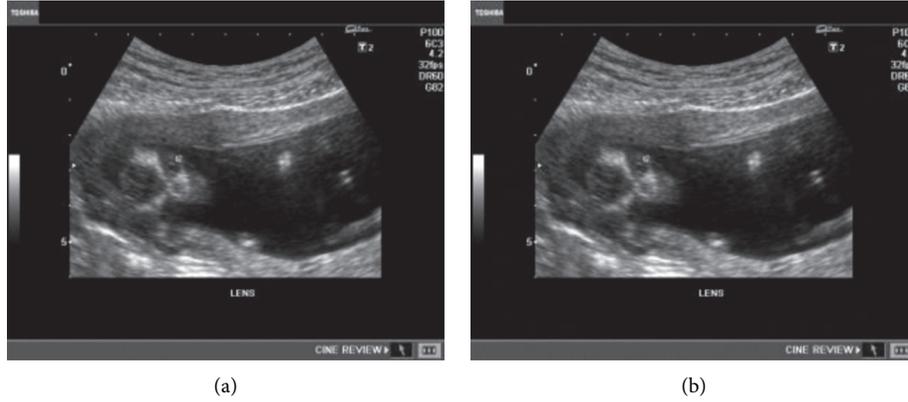


FIGURE 8: (a) Actual image and (b) watermarked image [27].

- (vii) The location map generated is then appended with the coordinates of ROI and after compression embedded in border pixels LSBs
- (b) Extraction phase
 - (i) For extraction, the location map is populated along with the extraction of ROI coordinates by decompressing the bitstream collected from border pixels.
 - (ii) RONI is identified by utilizing ROI coordinates.
 - (iii) Extraction of the payload is done from RONI which is disintegrated into H , P , L , and D parts after decompressing.
 - (iv) For the authenticity of the image, the hash is calculated for the ROI and matched with the extracted one. If values are different, that shows tempering.
 - (v) The tempered part is recovered by dividing the ROI into 16×16 pixel block, computing the average of each block, and replacing with the average value of corresponding pixels of extracted ROI " P ". Bits of L are utilized to recover LSBs of border pixels.

The proposed technique is experimented using four DICOM images shown in Figure 7 having different sizes of the ROI and distinct data sizes of patients.

Reversibility can be assessed with the help of pixel-by-pixel comparison of the original and recovered image whereas tempering can be located by the comparison of hash values collected at the embedding phase and extraction phase.

Temper detection and recovery were demonstrated by replacing some pixels from RONI with pixels in ROI. During extraction, the scheme successfully located the tempered region and recovered area which is shown in Figure 9.

The embedding results with variant sizes of ROI and patient's data sizes are illustrated in Table 2.

Results illustrated that technique performed well with regard to PSNR, increased capacity of embedding, and reversibility in case of no major tempering. The abovementioned

technique performed very well in terms of higher hiding capacity as well as visual quality by utilizing hiding techniques that provide higher embedding room to compensate for the issues of ROI size and image size. Further improvements in terms of multiple-ROI concept can also be incorporated for facilitating medical informatics.

3.1.3. Harris Corner Detection and Fuzzy C-Means. In 2013, Debalina Biswas proposed a method that uses a clustering method for the recognition of the pattern known as fuzzy c-means (FCM) [30]. In this technique of clustering, one set of data can belong to two or even more than two clusters. It also permits the data when they belong to more than one class; then, its membership function degree will vary between 0 and 1.

There is a rare advantage of the FCM that linguistic variables can be grading based on pro-rata data and after the accurate analysis fit easily in the domain of the discrete. FCM uses an iterative approach to reduce the function of the dissimilar and computes the centers of the cluster. After updating, the centroid within the pixels set will be shifted to the right location.

The membership matrix, u_{ij} is used for the membership degree for the points of data of x_i cluster which starts from

$$\sum_{i=1}^c u_{ij} = 1, \quad \forall j = 1, \dots, n, \quad (4)$$

performance index (PI) which is used for the center of cluster and matrix of membership is provided as given below:

$$\begin{aligned} J(U, c_1, c_2, \dots, c_c) &= \sum_{i=1}^c (i = 1, \dots, c) J_i \\ &= \sum_{i=1}^c (i = 1, \dots, c) \sum_{j=1}^n u_{ij} j^m d_{ij}^2. \end{aligned} \quad (5)$$

Euclidian distance (d_{ij}) is between the data point and the center of the cluster. The weighting exponent is m which belongs to $[1, \text{infinity}]$. There are two conditions which can be used to reduce the function of dissimilarity given below:

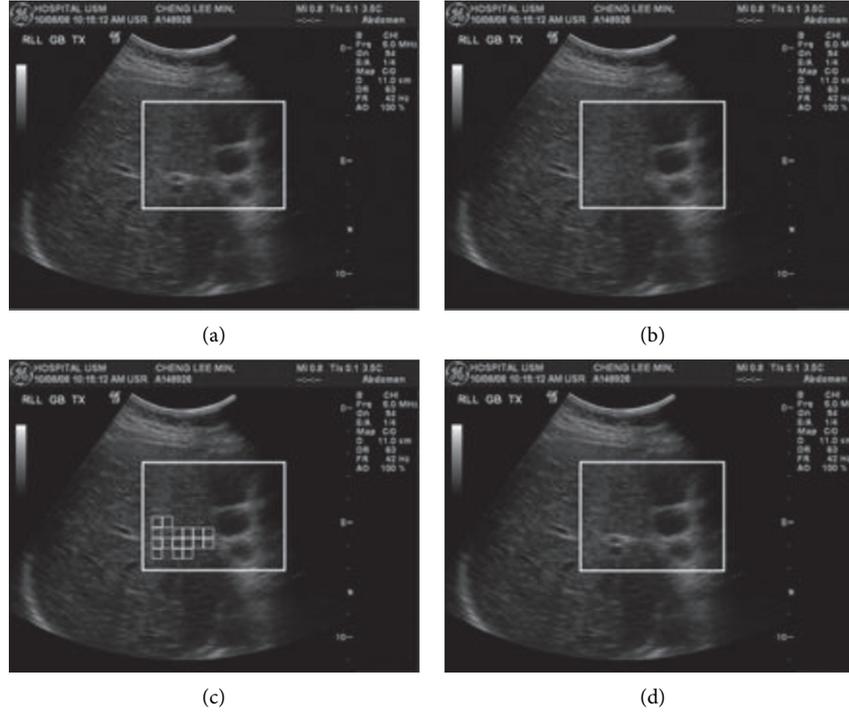


FIGURE 9: Temper detection and recovery [28]. (a) Watermarked image, (b) image after tempering, (c) temper detection, and (d) recovered image.

TABLE 2: Embedding results with variant sizes of ROI.

ROI size	2K			6K			10K		
	Payload (bits)	Capacity of hiding (bpp)	PSNR	Payload (bits)	Capacity of hiding (bpp)	PSNR	Payload (bits)	Capacity of hiding (bpp)	PSNR
<i>Ultrasound 1</i>									
4%	169,424	0.287	37.01	209,520	0.354	36.42	246,768	0.417	36.07
8%	260,704	0.441	35.99	299,760	0.507	35.54	335,312	0.567	35.28
12%	395,680	0.669	35.63	436,528	0.738	35.60	n/a	n/a	n/a
<i>Ultrasound 2</i>									
4%	155,808	0.264	37.46	194,816	0.329	36.81	230,112	0.389	36.46
8%	245,376	0.415	36.45	283,872	0.480	36.09	319,024	0.539	35.86
12%	376,368	0.636	36.13	417,056	0.705	36.09	n/a	n/a	n/a
<i>Ultrasound 3</i>									
4%	122,848	0.303	41.88	163,136	0.402	40.13	200,176	0.494	39.15
8%	207,776	0.512	39.36	245,824	0.606	38.34	281,200	0.694	37.75
12%	263,984	0.651	38.24	n/a	n/a	n/a	n/a	n/a	n/a
<i>Ultrasound 4</i>									
4%	82,832	0.270	41.25	119,088	0.388	39.81	153,968	0.501	38.57
8%	151,552	0.493	38.84	191,024	0.622	37.94	n/a	n/a	n/a
12%	190,912	0.622	38.10	n/a	n/a	n/a	n/a	n/a	n/a

$$c_i = \sum_{j=1, \dots, n} \frac{u_i j^m x_j}{u_i j^m} \quad (6)$$

(a) FCM algorithm: following are the steps:

- (i) The matrix which is used for the membership is initialized randomly.
- (ii) Using equation (3), centers of clusters are calculated.

(iii) Using equation (2), dissimilarity function is computed. Halt if the perfections in the results are below the taught pixel of the line of the threshold.

(iv) Using equation (4), a new matrix of membership is calculated and then the steps are repeated.

(b) Alpha blending: this blending technique is used to blend the first image source with the pixel equivalent in the

second image source. Following is the execution of the alpha blending:

$$\begin{aligned} \text{pixel} &= \text{alpha} * (\text{source pixel of first image}) + (1 - \text{alpha}) \\ &* (\text{source pixel of the second image}). \end{aligned} \quad (7)$$

For the blending of the images, the blending factor is taken from the first image that is why it is known as alpha blending [31, 32]. The range which is used for the alpha in the algebraic is between 0.0 and 1.0. Using this technique, watermark is generated which is given as follows:

$$(\text{WII}) = \text{alpha} * (\text{CI}) + (1.0 - \text{alpha}) * (\text{WI}), \quad (8)$$

where WII is the watermarked image, CI is the selected image, and WI is the selected equivalent image. The output of the process is shown in Figure 10.

(c) Embedding process of watermarking: in the embedding process of watermarking, the grey medical image segmentation is applied using fuzzy *c*-means. Then, the binarization is employed on the image. From the image, which is binarized, an open binary area is used to clean the smaller objects. For the detection, Sobel edge is employed. Then, the algorithm of Harris corner detection [33, 34] is practical. The maximum diameter is taken, and based on the points of Harris, the center is calculated. The boundary is marked between the region of the noninterest (RONI) and region of interest (ROI) based on the circle which is drawn on the diameter and the center point. Watermarked image size is used to select an area from the RONI. The alpha blending technique is used to embed the watermarking on the area which is selected.

(d) Discussion and results: for the study of the effect of watermark embedding on the medical images, results were compiled and shown in Figure 11.

Section of RONI is exploited for the insertion of the watermark using the alpha blending technique shown here.

(e) PSNR applied on the signal of watermark: PSNR between the watermarked MRI image and the original image is 28.8255, and PSNR between the watermarked IVUS image and the original image is 23.504.

3.1.4. Protection of Ultrasound Image Sequence: Employing Motion Vector Reversible Watermarking. With the induction of new techniques for medical imaging, the diversity of imaging modalities has increased twofold. Every modality has its own requirements for a reversible watermarking strategy to be employed for data safety for HIS. In 2019, Habib and Al-Fayez [36] presented an approach for digital security of ultrasound imaging videos or image sequences using motion vectors. Motion vector prediction is a popular technique in video compression and utilizes a comparison between two images or frames for providing data compression at the encoder side. This is a very promising and computationally inexpensive (when large blocks are used) method for videos and image sequences that have a low relative motion rate between frames such as ultrasound imaging.

The proposed methodology, after a histogram pre-processing stage (to minimize overflow/underflow), subjected the image sequence to a full search block-matching algorithm (BMA) with a 16×16 block size. The magnitude of the calculated motion vector designated as $MV_{i,j}$, where I is the i^{th} frame and j is the j^{th} motion vector of the frame, is used to define an embedding threshold value. These horizontal and vertical magnitude values MV_H and MV_V of the motion vectors, selected on the basis of the threshold value, are used to calculate the phase angle using $\theta = \tan^{-1}(MV_V/MV_H)$ which is subsequently used for data embedding. The side information about the frames that were calculated during histogram modification and motion estimation is also embedded alongside the watermark. This ensures accurate data extraction at the decoder/extraction side and increases the robustness.

The authors have been able to achieve infinite PSNR between the sending and receiving side images, meaning both were identical after data extraction. PSNR value of the original versus the watermarked image was around 41 dB with an SSIM of about 0.92. The maximum embedding capacity achieved was 0.29 bits per block, and the ratio of side information to the watermark data was about 1.65% which is highly promising. The downside, as mentioned by the authors, is the applicability of the algorithm being limited to large block sizes only as reducing the block size not only increased the computational overhead but also involved adding large amounts of side information data mandatory accurate retrieval.

3.2. Frequency Domain

3.2.1. A New Approach to Fully Reversible Watermarking in Medical Imaging with Breakthrough Visibility Parameters. Alěsat et al. formulated a reversible scheme for watermarking of medical images based on the alloying advantages of different three conventional approaches—zero, reversible, and RONI watermarking [37]. The basic purpose of combining different approaches is to eradicate the disadvantages and exploit the strengths of the approaches. The input media is split into different two categories RONI and ROI; RONI is the zone of the image where minute variations do not affect the medical information as a whole. Area, other than RONI, falls under the umbrella of ROI.

The identification of RONI is based on the pair's comparison of neighbor vectors where vectors consist of the pixel's values of rows along with columns. A comparison between neighbor vectors is made in each direction. A threshold is used to differentiate between the boundary of ROI and RONI. For experimentation for this technique, the defined threshold has 10% similarity based on the different tests [38]. The sample utilized for experimentation purposes in this study contained RONI of size 11%.

(a) Watermark concealment.

- (i) After the detection of ROI, it is subjected to the DT-CWT transform.
- (ii) Select DT-CWT numbers LL.

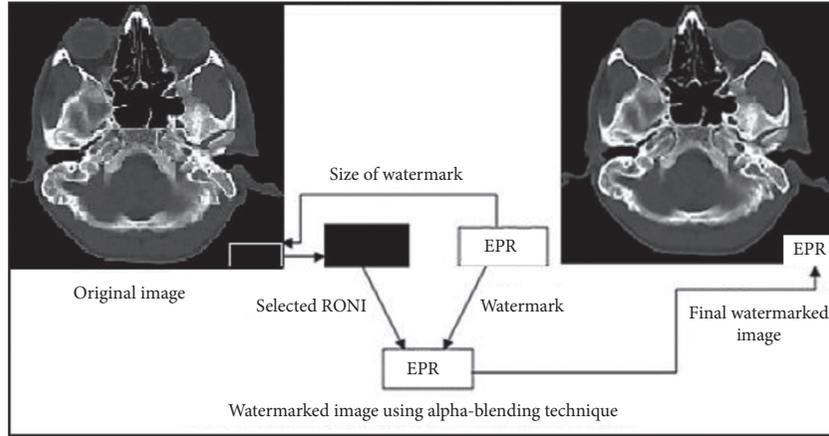


FIGURE 10: Alpha blending technique [30].

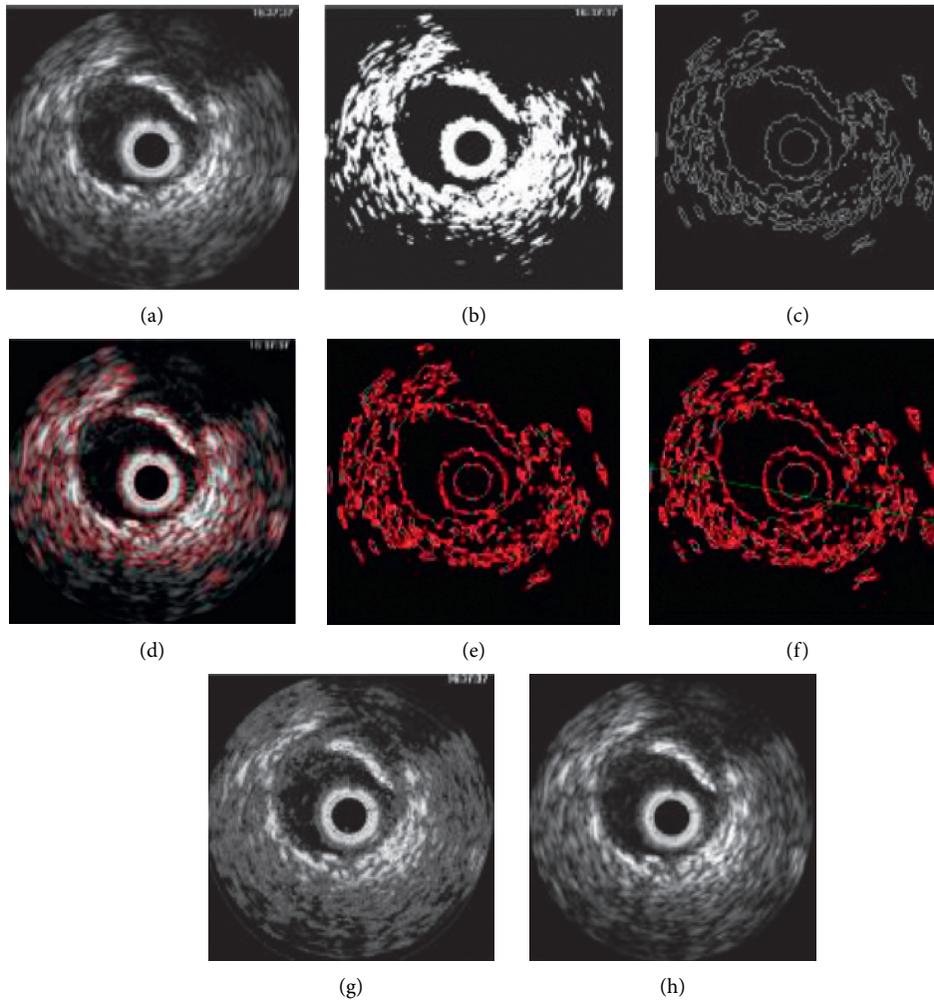


FIGURE 11: Watermarking embedding process in IVUS [35].

- (iii) Determine the arithmetic average of coefficients (\varnothing_{LL}).
- (iv) The random location of pixels comprising the same number of pixels as a watermark is identified in the LL coefficient region. Locations must not be too close to the edge of the image.
- (v) Let $R_i(x, y)$ be the i^{th} random location, then neighboring region comprising 7×7 pixels is elected by placing $R_i(x, y)$ at the center.
- (vi) A feature image F equivalent to watermark size. The average of neighboring 7×7 block selected for the i^{th} random location must be equal to the individual averages of feature image F . The following formula is utilized to create matrix B from feature image F :

$$B(x, y) = \begin{cases} 1, & \text{if } F(x, y) \geq \varnothing_{LL}, \\ 0, & \text{if } F(x, y) < \varnothing_{LL}, \end{cases} \quad (9)$$

where \varnothing_{LL} is the arithmetic average of LL band coefficients.

- (vii) A secret share is generated which is used as a watermark to RONI by combining matrix B and a watermark as shown in Figure 12.
- (b) Watermark extraction.
 - (i) Region of noninterest and region of interest of the image which is watermarked are isolated.
 - (ii) LL subband of coefficients is selected after the DT-CWT transformation with RONI.
 - (iii) The same seeding process would be repeated with the help of secret key S for the generation of the same random pixels within the LL region as in the embedding process.
 - (iv) For each $R_i(x, y)$ location, by keeping $R_i(x, y)$ at the center and selecting the neighbor 7×7 pixels, the average is obtained.
 - (v) This value is utilized at the time of feature image which must be of the size of the inserted watermark.
 - (vi) The feature image is then used to create binary matrix B from the same formula used in the concealment process. The public share will be generated by the combination of the binary matrix B and Figure 13.
 - (vii) For the extraction of watermark, logical OR operation is performed created in the present process with the undisclosed share and free share.
 - (viii) The utilization of the process depicted in Figure 12. Reduction of watermark than its actual size.

Reversible contrast mapping is utilized for the reversible watermarking. RCM utilization required segmentation of the image into a group of two pixels called pairs. For the transformation, pairs are utilized:

$$\begin{aligned} x' &= 2x - y, \\ y' &= 2y - x. \end{aligned} \quad (10)$$

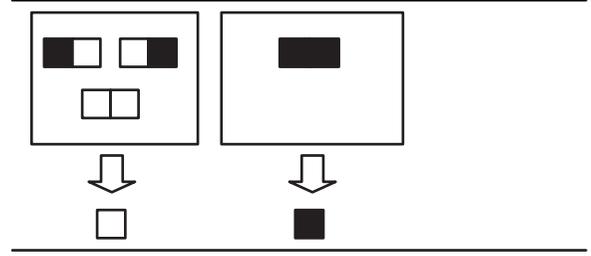


FIGURE 12: Reduction process [38].

Pixel				
matrix B	0	1	0	1
Public share				
Secret share				
Public share \oplus secret share				

FIGURE 13: Cookbook for public share and secret share [37].

However, (x, y) are the original and (x', y') are the values that are transformed. To avoid the underflow overflow, put a limit on the transformation subdomain.

(c) Watermark embedding.

- (i) Pixels (x', y') are isolated in the region of noninterest.
- (ii) For every value of (x, y) if the values of the x and y belong to the domain and if its conformation is based on the odd value of pixels, then the pair is exposed to transformation. The new value of x LSB is set as "1" and LSB of the new value of y is possibly utilized for data insertion.
- (iii) If the values of x and y belong to the domain and if its conformation is not based on the odd value of pixel, then the new value of x LSB is set as "0" and LSB of the new value of y is possibly utilized for insertion of data.
- (iv) If the values of x and y do not belong to the domain, zero is assigned for LSB and the actual value is persisted. The locations identified for bits above are utilized to embed a watermark in RONI.

(d) Watermark extraction.

- (i) To the new values of x and y , the region of non-interest is isolated.
- (ii) For every new value of x and y , apply steps (iii)–(v):
- (iii) If the new value of x has LSB of 1, then LSB of y' is appended after retrieval in the watermark sequence. LSBs of both transformed pixels are set to zero, and the original values are filled by taking the inverse form of transform.
- (iv) If the LSB of the new value of x is zero and the pairs have their LSBs set to one and are in the domain, then the LSB of the new value of y is appended to the

sequence of watermark and the original pair is returned by fixing the LSB of new pair to one.

- (v) If the new value of x has its LSB zero and the new pair having LSB one is not in the domain, original values are filled by replacing the LSB of the new value of x with the concerned value from the already having sequence of the watermark.

For examination purposes, experiments are performed using 6000 selected medical images from the database which contains 60,000 medical images [38]. Test images consist of 9 different modalities including ultrasound. The average PSNR obtained is 81 when the RONI size was 10% of the original image. The average SSIM obtained is 0.999974. For extensively testing the proposed technique, it can be tested on a larger medical database.

3.2.2. Detection of Accurate Tamper in Region of Interest. In 2014, Eswaraiyah proposed a watermarking technique for medical images [5, 39, 40]. In the medical images in the form of different shapes, there is an area of the region that is of no interest to the physician. In this work, those medical images are considered which contain a single ROI. The border of the image is the pixels outermost three lines. Pixels are divided into three respective sets: pixels of ROI, pixels of border, and pixels of RONI. For authentication purposes, SHA-1 technique is used to calculate the ROI hash code. Any kind of change in the code of hash will be quickly identified. Areas of medical images ROI are divided into 4×4 blocks and those of RONI are divided into 8×8 blocks, so they do not overlap. Now the ROI blocks are plotted to the RONI blocks. This is done to embed the information to be recovered. The following equation is used:

$$B_{\text{RONI}} = [(k \times B_{\text{ROI}}) \bmod N_b] + 1. \quad (11)$$

Lastly, the ROI information and value of hash are implanted into the pixels of border LSBs.

(a) Algorithm for the embedding: medical images are divided into sections of 3 which contain pixels of region of interest, pixels of border, and pixels of region of noninterest. SHA-1 technique is used to calculate the ROI hash value. ROI area is divided into the blocks of 4×4 . RONI is divided into the blocks of 8×8 . Map each individual block of ROI on the area of RONI. In this way, the data to be recovered are embedded. Secret key ROI information and the value of the hash are used for encrypted. Pixels of the border are used for the bits of encryption to be embedded. Now the medical image can be sent to remote locations.

(b) Algorithm for the extraction: pixels of the border are used for the encryption bit extraction. Decryption is applied to get the ROI information and value of the hash. SHA-1 technique is used to calculate the value of the hash of ROI. Both values of the hash will be compared, and if the values get equaled, the process of extraction will be stopped. ROI is divided into the blocks of 4×4 and RONI into the blocks of 8×8 . For each block of ROI, steps are repeated so that the block of ROI which is tampered will be identified. The value of variance and average for each block will be calculated. If both variance and the average value of the blocks are not equaled, it means it is tampered and replaced with the pixel bits.

3.2.3. A Novel Texture Quantization-Based Reversible Watermarking Scheme for Information Health Systems. In 2017, Turuk and Dhande [41] presented a novel approach for making transactions of information via health information systems (HIS) more secure. An argument in the favor of digital watermarking is a promising solution aptly suited for securing HIS data from sniffing and snooping by unauthorized users. The proposed novel approach used a hybrid method that utilized a combination of image quantization and its texture treated as a feature to hide patient data segmented into multiple watermarks. The preliminary feature extraction was done using a discrete wavelet transform (DWT) with a ‘‘HAAR’’ mother wavelet, and further quantization approach for transform coefficients was presented by the authors which were the most noteworthy contribution.

The proposed method first used a level 2 DWT to find the downsampled coefficients from the cover image, as depicted in Figure 14. As DWT is very effective in segregating the textured areas and edges, it provides a good basis for improving the imperceptibility of the watermark addition. Figure 15(a) shows an example of the level 2 DWT being applied to a CT modality image. To increase the robustness, the energy of each decomposed subband was calculated using the following equation:

$$e_k = \frac{1}{N_k M_k} \sum_i \sum_j |J_k(i, j)|, \quad (12)$$

where k points to the approximation and subbands at a certain decomposition level while J_k is the subband coefficient of dimension $N_k M_k$. A texture map was generated by obtaining a relationship between the spatial change and the energy variance by combining coefficients of the lowest matrix of the subband (LL) with the energy as given below:

$$\text{txtFeatures}_r(i, j) = [W_r(i, j)]^2 + \text{var} \left[\text{LL}_d \left(\left[\frac{i}{2} \right] + 1, \left[\frac{j}{2} \right] + 1 \right), \text{LL}_d \left(\left[\frac{i}{2} \right] + 2, \left[\frac{j}{2} \right] + 2 \right) \right]. \quad (13)$$

This texture map is used to calculate the threshold value to preserve the most prominent edge features and texture details. Based on this threshold value, all

subbands apart from LL are used to embed the watermark data. As wavelet coefficients obtained are real numbers, their mapping to binary watermark data involved a

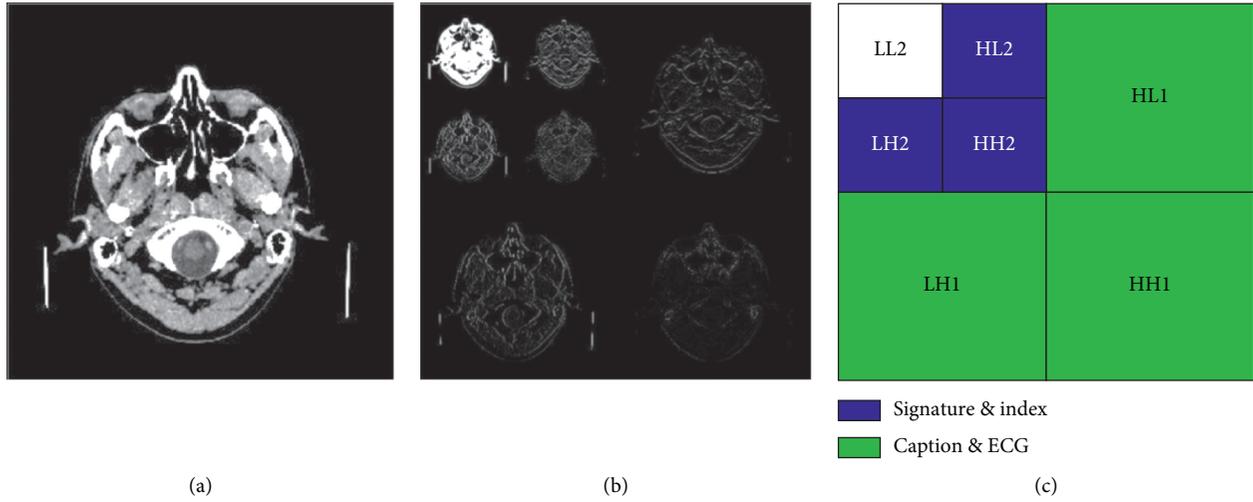


FIGURE 14: DWT of CT modality image and texture areas and texture map of the subbands [41].

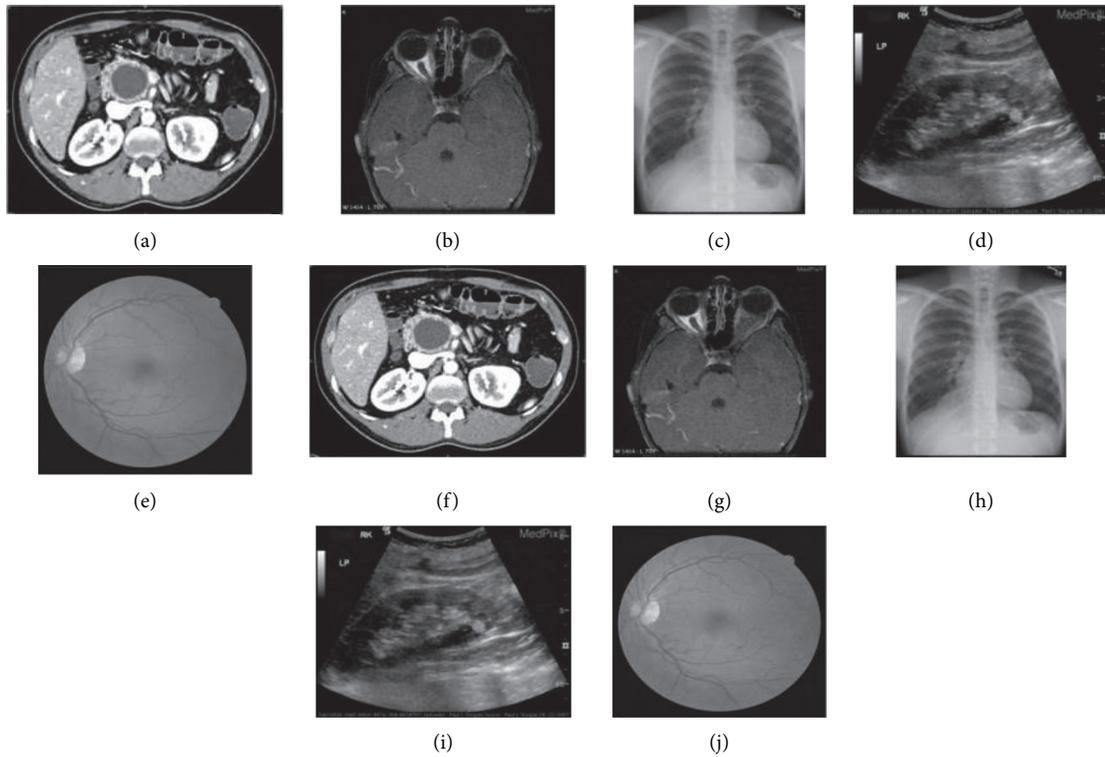


FIGURE 15: Evaluating the watermarking imperceptibility. (a-e) Original images. (f-j) Watermarked images [42].

quantization function $Q(f)$ and its variation was defined as follows:

$$Q(f) = \begin{cases} 0, & \text{if } \text{floor}\left(\frac{f}{\Delta}\right) \text{ is even,} \\ 1, & \text{if } \text{floor}\left(\frac{f}{\Delta}\right) \text{ is odd,} \end{cases} \quad (14)$$

where $\Delta = 2L$ in which L is the decomposition level. As the same constant value is being added and subtracted, to ensure data integrity, a tracking key was used to signify the coefficient sign change and duplicate coefficients. Watermark data were created using the BCH error-correcting code which ensures data integrity. In the experiment, the watermarked data were performed which comprised of a caption, an ECG signal, the physician's electronic signature, and ICD-10 diagnostic data. The researchers were able to embed a maximum of 22,600 bits

with a PSNR of 53.60 along with encouraging numbers for both MSSIM and UIQI. This was a major improvement considering the contemporary methods and made this research a major contribution to reversible medical image watermarking.

3.2.4. A Hybrid Cryptography-Based Watermarking Technique for the Secure Transmission of Medical Data for Telehealth Applications. Thakur et al. [43] presented an approach employing a hybrid cryptographic-watermarking methodology for the applications of telehealth. Logistic maps, which were initially employed for modeling animal populations, have been extensively studied as an effective cryptographic tool as they provide pseudorandomness and chaotic behavior. The researchers used two-dimensional logistic maps to encrypt the watermarked host image enabling secure transmission/communication.

In a bid to improve imperceptibility, the authors used a combination of three transform domain techniques, i.e., DCT, DWT, and SVD, on the host image. The watermark image was subjected to DCT and SVD only to get a singular matrix S_1 . In the first step, a 2nd level “Haar” DWT is performed on the host image resulting in the approximate image (cA_1) and the coefficient matrices. cA_1 is further transformed using DCT and the resulting matrix is singularized using SVD (matrix S). SVD matrices are used for watermark embedding (based on gain factor α), and inverse DCT and DWT are performed to get the final watermarked image. The inverse resultant matrix of DCT was then obtained.

- (a) The host image which is of size 512×512 read as $C_{W_{image}}$ and the image which is watermarked of size (256×256) read as WM_{image}
- (b) Utilize the second level of DWT on the DWT cover
- (c) Utilize DCT which will provide B
- (d) Utilize the SVD on B which provides S
- (e) For the image of watermark, utilize DCT on WM_{image} to provide D
- (f) Utilize SVD on the D which will provide S_1
- (g) Using the gain factor, embed the watermark image in the cover; now utilize the inverse of DWT, the inverse of DCT, and the inverse of SVD to get watermark with the cover image
- (h) Using private key, encryption is applied to the Wd_{image}

The time of encryption and decryption of the proposed method and survival against different attacks were tested in the experiments, and all parameters and the results were highly promising for the proposed method. NC, SSIM, and PSNR were greater than 74.61, 0.998, and 0.900 dB, respectively, which proved that the proposed method is a highly secure and robust methodology for telemedicine applications. In the start, the MRI image of the brain having size 512×512 and the size of the part of the body between the neck and abdomen 256×256 is taken as cover and watermark image, respectively.

The proposed algorithm is implemented using MATLAB R2013a on a 64-bit machine having a Core-i5 processor and 4 GB RAM.

3.2.5. A Novel Robust Reversible Watermarking Scheme for Protecting Authenticity and Integrity of Medical Images.

In 2019, Liu et al. [42] presented a technique for protecting medical imaging content from tampering. The methodology was based on an improved ROI- and RONI-based reversible watermarking technique that ensured the integrity of both regions and avoided the spatial segmentation of the image. The watermarking scheme consisted of four major proposals for improvement. The first was slantlet wavelet transform- (SWT-) and singular value decomposition- (SVD-) based reversible watermarking method which provided watermark robustness which ensured the lossless recovery of both ROI and RONI. The second generation of the watermark is based on a combination of integrity and authenticity data for increased image security.

This included the hash value of the hospital logo as the validity of data and the information of tamper detection for both the image and the ROI. Thirdly, a grouping of integer wavelet transform (IWT) and block truncation coding (BTC) was used for encoding tamper recovery data of ROI which offered a great compromise between the recovered visual quality and embedding capacity. Finally, there was no image segmentation in the domain of spatial and watermarks embedded in the whole image which mitigated any additional security risks.

Watermark generation consisted of a generation of authenticity data (SHA-1 hash of hospital logo), tamper detection (SHA-1 hash of image), tamper localization (CRC-16 based error-checking of ROI), and tamper recovery information. The watermark was embedded using SWT which offers better spatial and frequency localization as compared to DWT and hence better imperceptibility versus robustness results. An added layer of SVD, which was utilized for selecting the significant (from the generated singular matrix) values for watermarking, reinforced the watermark robustness.

The authors performed experiments on various image modalities that included 200 medical images and 40 each of X-ray, CT, ultrasound, and fundus images. All the experiments demonstrated high levels of imperceptibility with an average PSNR of 41.2995 and SSIM of 0.9607. The robustness of the scheme was also commendable as the average of the mean BERs of all experiments was 0.0476, and NCCs were 0.9624. The scheme also performed better than the spatial-domain methodologies when subjected to various attacks.

3.2.6. Spiral Order Technique Reversible Watermarking.

In 2018, S. Lakshmi and Ayyappan [44] proposed a method of data hiding which is reversible in nature in the medical images using spiral order. The order of traversal is depicted in Figure 16. It is suitable to use for images that are confidential in nature as the patient data are very important to hide the data in the medical images using this technique. In the grayscale image, there are no data present in the region of

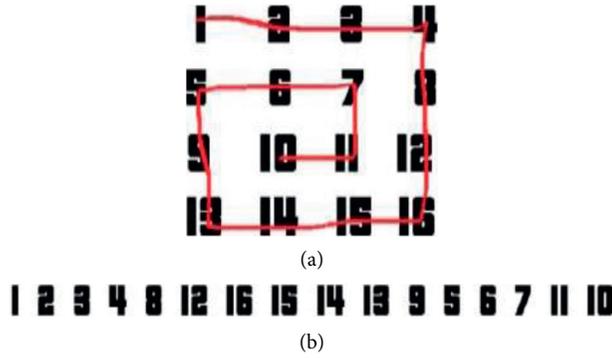


FIGURE 16: Spiral order technique [8].

the background, and to hide the data, this region can be utilized. For the embedding of data modification, a histogram is utilized, and to hide the data, spiral order is applied.

(a) Using spiral order to hide data: the cover image is read first for the hiding of data and then spiral order is used to convert it into the form of a vector. To hide the information, positions are identified first. There are four stages involved: take the first row from the rest of the rows, the last column from the rest of the column, the last row from the rest of the rows, and the first column from the rest of the columns. The results of the technique are presented in Figure 17.

(b) Modification through histogram: the difference between the adjacent pixels is calculated. It will be close to zero as these are closely packed. The high point will be the most occurred value of difference. In three ways, pixels are altered depending on the difference value how much it is above or below the high point.

(c) Recover the information: the bit of text can be extracted using the following equation:

$$B = \begin{cases} 0, & \text{if } |Y_i - A_i - 1| = PP, \\ 1, & \text{if } |Y_i - A_i - 1| = PP + 1. \end{cases} \quad (15)$$

The values of the pixels of the image were originally reconstructed using the following equation:

$$A_i = \begin{cases} Y_i + 1, & \text{if } |Y_i - A_i - 1| > PP \text{ and } Y_i < A_i - 1, \\ Y_i - 1, & \text{if } |Y_i - A_i - 1| > PP \text{ and } Y_i > A_i - 1, \\ Y_i, & \text{otherwise.} \end{cases} \quad (16)$$

(d) Experiments and results: PSNR and MSE are the performance metrics to be applied to the medical images. To check the similarity among the images, SSIM is used. Improvement in the results with the proposed method is shown as follows.

3.2.7. *Hybrid Estimate Reversible Watermarking*. In 2018, Fatima proposed estimate-based hybrid reversible watermarking [44] in the domain of medical images. It is a four-stage process that contains cover image, processing of the

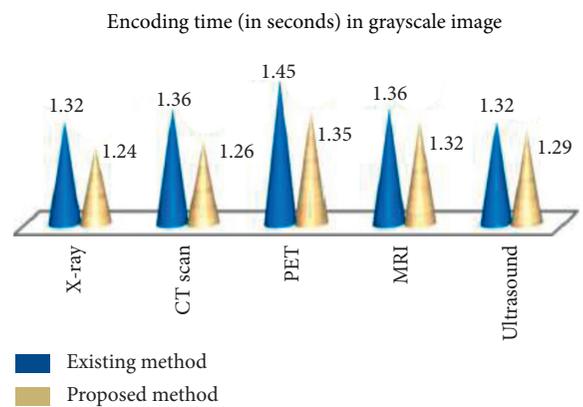


FIGURE 17: Comparison of embedding time [8].

images, encoding using watermarking, and lastly decoding using watermarking.

(a) Encoding using watermarking: break the original image which consists of four phases in encoding through watermarking. The image is taken as input and then it is further divided into subblocks of 8×8 , and for each individual block, representation of four phases is used. A predictor of three different types is utilized for the expected value of the pixel. A window of 3×3 is used in both perpendicular and parallel directions so that the initial position of the pixel varies. Pixels in the neighboring are used for the variance calculation, and as a result, predicted values are found out. To improve the quality of the results, projected error is also calculated.

(b) Utilizing sliding window four-stage representation: taking two as the size of the step, the window glides through the image cover. The center value of the pixel is to be projected. The context of projection will include eight values of adjacent pixels. The projection will be accomplished by using eight values of adjacent pixels to calculate the variance. Projection values in the range are found out and replaced with the value of a pixel in the center.

(c) Division of the image using four stages: blocks are divided into 8×8 of the image which is taken as input, and on each individual phase, hybrid prediction is applied to find out the pixel projection value. 8 adjacent values of pixels are used to compute the variance which is used to find out the

value of projection. The procedure is repeated for the rest of the blocks. Encoding and decoding are done on the phases.

(d) Hybrid projection: the reason to use hybrid projection is to lessen the distortion in the image which occurs owing to reversible watermarking. Here, the position is found out to embed the watermark. According to the different adjacent ranges of the variance, three types of projection are used. The projection comes in the range of 0–10 considered as low range of variance, 10–40 as a medium range of variance, and greater than 40 as a high range of variance. Mean projection is utilized for a low range of variance, the trimmed mean projection is utilized for a medium range of variance, and MED projection is utilized for a high range of variance. For the computation of the variance, mean projection is used. For the calculation of the variance, trimmed mean projection uses the 8 adjacent pixel values. For finding the projection value, the mean of the values sorted is utilized. The window is slid over the image to calculate the variance. Change in the context of the projection means the order of sorting is changed in the encoding and decoding. Variance is computed using the following equation:

$$\sigma_x = \frac{1}{8} \sum_{i=1}^8 (xi - \mu), \quad (17)$$

where xi represent the adjacent pixel values and μ represents the mean. To define the projection pixel value of the center, the following equation is utilized:

$$C' = \begin{cases} \sum_{i=1}^8 \frac{X_i}{8}, & \text{if } \sigma_x \geq 0 \text{ and } \sigma_x < 10, \\ \sum_{i=3}^6 \frac{K_i}{4}, & \text{if } \sigma_x \geq 10 \text{ and } \sigma_x < 40, \\ \sum_{i=2}^3 \frac{KM_i}{2}, & \text{if } \sigma_x > 40. \end{cases} \quad (18)$$

All four corners of the window are utilized for the MED projection. KM is the total count of the values when arranged in order of increasing.

(e) Error of prediction: the input image is used for finding the projection value of the image. Projection error is computed between the image original version and the projection image, and when the error is expanding, data will be embedded into the image. The value of the edge is set over the error of prediction and depends on how the edge of encoding and decoding is done.

(f) Process of embedding: edge values lie in the range of the error of prediction. If the text fits within the range, then the edge values are utilized; otherwise, the values of error projection will be moved left.

(g) Message digest 5 algorithm: for the secure transfer of the data, MD5 has been used which generates a 128-bit value of hash. This value of the hash is represented in the hexadecimal number. Further, this value will be converted into the binary form using LSB embedding. For the secure data transmission, both hash values should be matched the one which is extracted and text bit.

(h) Extraction: a decoder is used to recover the original image and data which were embedded. For the full retrieval of the data, it is important to match the hash values of the extracted data and text bit. The original image is recovered by adding the error of the original projection and the value of projection.

(i) Experimental results: PSNR and the capacity of embedding performance metrics are used for reversible watermarking. Both are inversely proportional to each other. A higher value of PSNR means the quality of the image is good. A medical image of size 256×256 is used. Testing is important for the complete recovery of the image. The results are shown in Table 3.

3.2.8. *Reversible Watermarking for Medical Video.* Fadua and Hamid proposed the reversible watermarking technique for medical videos by exploiting the polynomial transformation methods [24]. Polynomial transformation methods are used for the identification of suitable watermark regions. The cover video is initially fragmented into keyframes, and subsequently, these frames are shattered into substantial components for opting suitable regions for watermarking.

After selecting the keyframes of individual video shots, their location is persisted in key information K .

Polynomial transform is applied to the selected keyframes to obtain a textured region. After dividing the texture component into 8×8 blocks, the watermark w_i bit is inserted in k blocks $FB_i (FB_1, \dots, FB_k)$.

Watermark insertion is done by the following equation:

$$FB_i^* = FB_i (1 + w_i * S), \quad (19)$$

where S is the strength of watermarking. Watermark blocks are used to construct the watermarked texture. Original structure parts and watermarked texture are combined to obtain a watermarked image I_w .

Similar action with inverse logic is applied for the extraction of the watermark. The watermarked video is divided into shots. Key information K (as provided before) is utilized to determine the keyframe from the individual shot with its location. Polynomial transform was applied to disintegrate the watermarked frame F_w into the best regions: watermarked texture. The watermarked texture component is segmented into 8×8 blocks to get the altered frame's blocks $FB^* (FB_1^*, FB_k^*)$.

$w_i^* = FB_i^* / FB_i$ is utilized to compute the new coefficients (w_{11}^*, w_{88}^*). If $w_i^* < 0$, then watermark $_i = 0$ bit; else, watermark $_i = 1$ bit, and this way, watermark is constructed.

Two optimized frames as keyframes from individual video shots of echocardiography are used. 512×512 is frame size medical video whereas the watermark size is 120×120 . The vital ingredient for these tests is opted experimentally and fastened on $S=0.1$ for this particular technique. Figure 18 demonstrates the sample frame of the original medical video and two watermarks, which are utilized for visual illustration.

PSNR and NC are used for performance assessment of the abovementioned scheme. For shot 1 and shot 2 obtained, PSNR results are 60.1278 dB and 60.4540 dB, respectively,

TABLE 3: Medical image capacity and PSNR.

Positive threshold	Heart	Brain	Kidney	Liver	Ultrasound
<i>Embedding capacity</i>					
2	0.0007	0.0058	0.0048	0.0050	0.0010
5	0.0047	0.0065	0.0079	0.0060	0.0014
7	0.0048	0.0070	0.0230	0.0068	0.0015
10	0.0052	0.0074	0.0250	0.0076	0.0120
15	0.0396	0.0098	0.0312	0.0085	0.0170
<i>PSNR</i>					
2	74.31	73.67	75.25	72.88	63.13
5	64.51	72.17	68.07	63.21	60.66
7	63.94	66.18	64.80	59.11	55.40
10	61.95	58.41	59.43	54.35	55.35
15	53.86	50.21	52.45	48.75	43.89

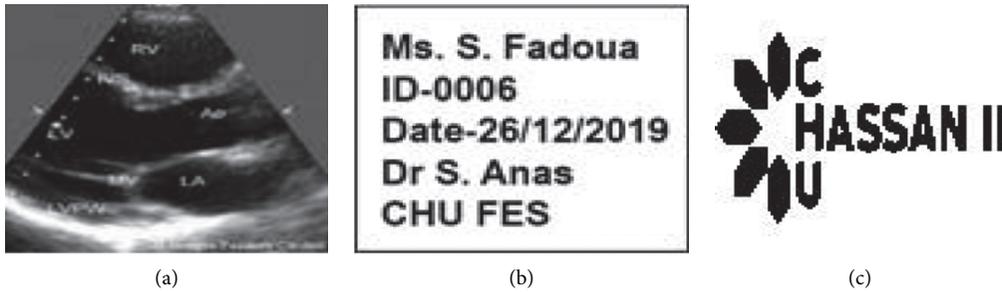


FIGURE 18: (a) Ultrasound, (b) watermark 1, and (c) watermark 2 [24].

TABLE 4: Comparison of reviewed watermarking techniques.

Articles	Parameters							
	Reversible	Robust	PSNR (dB)	NC	SSIM	Temper detection	Recovery	Media type
Turuk and Dhande [41]	✓	✗	53.64	✗	~1	✗	✗	Images
Thakur et al. [43]	✓	✓	74.60	0.910	0.999	✗	✗	Images
Habib and Al-Fayez [36]	✓	Semifragile	Inf	✗	≈0.92	✗	✗	Video
Faduo and Hamid [24]	✓	✓	60.2909	1.0000	✗	✗	✗	Video
Agung et al. [25]	✓	✗	58.5	✗	✗	✓	✓	Images
Al-Qershi and Khoo [28]	✓	✗	37	✗	✗	✓	✓	Images
Roček et al. [37]	✓	✗	81	✗	0.999974	✗	✗	Images
Liew and Zain [26]	✓	✓	23.5042	✗	✗	✗	✓	Images

whereas for NC result obtained for the same both shots are 1.0. Hence, the performance of this technique was without exhibiting any apparent variance between actual and watermarked videos. Besides, it addressed the watermark capacity problem as well.

For the evaluation of the robustness of the technique, watermarked frames were subjected to 3 different attacks: JPEG compression, median filtering, and histogram equalization. The techniques illustrated above are compared in Table 4.

4. Conclusion

In today's era, the protection of the data is crucial to overcome the problems of tempering, integrity, and authentication of data and the rights of ownership. A

comprehensive survey of reversible watermarking techniques of echocardiography was presented. The increasing spectrum of a threat to digital security demands consistent efforts for safeguarding data integrity. The intricacy of conflicting performance parameters in data hiding and reversible watermarking makes it difficult to put forth a comprehensive technique. This provides heaps of room for improvements in this field in the near and far future.

Data Availability

The detailed results which cannot be included in this article due to the length of the article will be available on the authors' website after the acceptance/publication of the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The author Dr. Sajjad Shaukat Jamal extends his gratitude to the Deanship of Scientific Research at King Khalid University for funding this work through research groups program under Grant number R.G.P. 1/234/41.

References

- [1] J. A. Panza, "Real-time three-dimensional echocardiography: an overview," *The International Journal of Cardiac Imaging*, vol. 17, no. 3, pp. 227–235, 2001.
- [2] J. S. Gottdiener, "Overview of stress echocardiography: uses, advantages, and limitations," *Current Problems in Cardiology*, vol. 28, no. 8, pp. 485–516, 2003.
- [3] T. Araki, N. Ikeda, F. Molinari et al., "Effect of geometric-based coronary calcium volume as a feature along with its shape-based attributes for cardiological risk prediction from low contrast intravascular ultrasound," *Journal of Medical Imaging and Health Informatics*, vol. 4, no. 2, pp. 255–261, 2014.
- [4] S. Acharjee, R. Ray, S. Chakraborty, S. Nath, and N. Dey, "Watermarking in motion vector for security enhancement of medical videos," in *Proceedings of the 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, Kanyakumari, India, July 2014.
- [5] B. Lei, E. L. Tan, S. Chen, D. Ni, T. Wang, and H. Lei, "Reversible watermarking scheme for medical image based on differential evolution," *Expert Systems with Applications*, vol. 41, 2014.
- [6] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, "Watermarking techniques used in medical images: a survey," *Journal of Digital Imaging*, vol. 27, no. 6, pp. 714–729, 2014.
- [7] W. Mazurczyk and S. Wendzel, "Information hiding: Challenges for forensic experts," *Communications of the ACM*, vol. 61, pp. 86–94, 2018.
- [8] M. T. Ahvanooy, Q. Li, H. J. Shim, and Y. Huang, "A comparative analysis of information hiding techniques for copyright protection of text documents," *Security and Communication Networks*, vol. 2018, Article ID 5325040, 22 pages, 2018.
- [9] A. Singh, B. Kumar, G. Singh, and A. Mohan, *Medical Image Watermarking: Techniques and Applications*, Springer, Berlin, Germany, 2017.
- [10] C. K. Tan, J. C. Ng, X. Xu, C. L. Poh, Y. L. Guan, and K. Sheah, "Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability," *Journal of Digital Imaging*, vol. 24, no. 3, pp. 528–540, 2011.
- [11] L. Chia-Pin, J. Honye, C.-J. Chang, and C.-T. Kuo, "Clinical application of intravascular ultrasound in coronary artery disease: an update," *Acta Cardiologica Sinica*, vol. 27, 2011.
- [12] L. Singh, A. K. Singh, and P. K. Singh, "Secure data hiding techniques: a survey," *Multimedia Tools and Applications*, vol. 79, no. 23–24, pp. 15901–15921, 2020.
- [13] A. Umamageswari, M. Ferni Ukrit, and G. R. Suresh, "A survey on security in medical image communication," *International Journal of Computer Applications*, vol. 30, no. 3, pp. 41–45, 2011.
- [14] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.
- [15] D. D. Brabin and J. J. Tamilselvi, "Reversible data hiding: a survey," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 1, no. 3, 2013.
- [16] A. Sonal and C. Lakshmi, "A review on reversible data hiding techniques," *International Journal of Applied Engineering Research*, vol. 13, no. 5, pp. 2857–2864, 2018.
- [17] J. A. Kaw, N. A. Loan, S. A. Parah, K. Muhammad, J. A. Sheikh, and G. Bhat, "A reversible and secure patient information hiding system for IoT driven ehealth," *International Journal of Information Management*, vol. 45, 2019.
- [18] R. Geetha and S. Geetha, "Improved reversible data embedding," in *Proceedings of the International Conference on Next Generation Computing Technologies*, Dehradun, India, November 2018.
- [19] T. Dutta, R. Bagi, and H. Gupta, "Robust reversible watermarking for grayscale medical images," in *Advances in Data and Information Sciences*, Springer, Berlin, Germany, 2020.
- [20] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, "Pixel repetition technique: a high capacity and reversible data hiding method for E-healthcare applications," in *Intelligent Techniques in Signal Processing for Multimedia Security*, Springer, Berlin, Germany, 2017.
- [21] R. Bhardwaj and A. Aggarwal, "Hiding clinical information in medical images: an enhanced encrypted reversible data hiding algorithm grounded on hierarchical absolute moment block truncation coding," *Multidimensional Systems and Signal Processing*, vol. 31, no. 20, pp. 1051–1074, 2020.
- [22] R. Geetha and S. Geetha, "Embedding electronic patient information in clinical images: an improved and efficient reversible data hiding technique," *Multimedia Tools and Applications*, vol. 79, no. 20, pp. 12869–12890, 2020.
- [23] N. Dey, P. Das, A. B. Roy, A. Das, and S. S. Chaudhuri, "DWT-DCT-SVD based intravascular ultrasound video watermarking," in *Proceedings of the 2012 World Congress on Information and Communication Technologies*, Trivandrum, India, November 2012.
- [24] S. Fadoua and T. Hamid, "Medical video watermarking scheme for telemedicine applications," in *Proceedings of the 2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, Meknes, Morocco, March 2020.
- [25] T. Agung, B. W. Adiwijaya, and F. P. Perman, "Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression," in *Proceedings of the 2012 IEEE International Conference on Communication, Networks and Satellite (ComNetSat)*, vol. 3, Bali, Indonesia, July 2012.
- [26] S.-C. Liew and J. M. Zain, "Reversible medical image watermarking for tamper detection and recovery with run length encoding compression," *World Academy of Science, Engineering and Technology*, pp. 674–678, 2010.
- [27] J. Zain and A. Fauzi, "Medical image watermarking with tamper detection and recovery," in *Proceedings of the 2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, New York, NY, USA, September 2006.
- [28] O. M. Al-Qershi and B. E. Khoo, "ROI-based tamper detection and recovery for medical images using reversible watermarking technique," in *Proceedings of the 2010 IEEE*

- International Conference on Information Theory and Information Security*, Beijing, China, December 2010.
- [29] Khoo and O. M. Al-Qershi, "Reversible watermarking scheme based on two-dimensional difference expansion (2D-DE)," in *Proceedings of the The 2010 International Conference on Computer Research and Development*, Kuala Lumpur, Malaysia, May 2010.
- [30] M. G. Jessica Fridrich, "Invertible authentication," in *Proceedings International Conference on Information Technology: Coding and Computing*, Las Vegas, NV, USA, April 2001.
- [31] N. Dey, P. Das, A. Das, and S. S. Chaudhuri, "Feature analysis for the blind-watermarked electroencephalogram signal in wireless telemonitoring using alattar's method," in *Proceedings of the Fifth International Conference on Security of Information and Networks-SIN'12*, New York, NY, USA, October 2012.
- [32] N. Dey, S. Mukhopadhyay, A. Das, and S. S. Chaudhuri, "Analysis of P-QRS-T components modified by blind watermarking technique within the electrocardiogram signal for authentication in wireless telecardiology using DWT," *International Journal of Image, Graphics and Signal Processing*, vol. 4, 2012.
- [33] N. Dey, A. B. Roy, A. Das, and S. S. Chaudhuri, "Stationary wavelet transformation based self-recovery of blind-watermark from electrocardiogram signal in the wireless telecardiology," *Communications in Computer and Information Science, Recent Trends in Computer Networks and Distributed Systems Security*, Springer, Berlin, Germany, 2012.
- [34] N. Dey, P. Maji, P. Das, A. Das, and S. S. Chaudhuri, "An edge based watermarking technique of medical images without devalorizing diagnostic parameters," in *Proceedings of the International Conference on Advances in Technology and Engineering (ICATE)*, Mumbai, India, January 2013.
- [35] G. Coatrieux, H. Sankur, and B. Rolland, "Relevance of watermarking in medical imaging," in *Proceedings 2000 IEEE EMBS International Conference on Information Technology Applications in Biomedicine*, Arlington, VA, USA, November 2000.
- [36] R. Habib and F. Al-Fayez, "Protection of ultrasound image sequence: employing motion vector reversible watermarking," *International Journal of Advanced Computer Science and Applications*, vol. 10, 2019.
- [37] A. Rócek, K. Slavíček, O. Dostál, and M. Javorník, "A new approach to fully-reversible watermarking in medical imaging with breakthrough visibility parameters," *Biomedical Signal Processing and Control*, vol. 29, pp. 44–52, 2016.
- [38] A. Rócek, K. Slavíček, and M. Javorník, "RONI size and another attributes of representative sample of medical images in common hospital operation, related to securing by watermarking methods," in *Proceedings of the International Conference on Image Processing, Production and Computer Science*, London, UK, October 2016.
- [39] J. J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar costa scheme for information embedding," *IEEE Transactions on Signal Processing*, vol. 51, 2003.
- [40] S. Rani and R. Euphrasia, "Dynamic hiding of message in rgb domain based on random channel indicator," *International Journal of Applied Engineering Research*, vol. 10, 2015.
- [41] M. Turuk and A. Dhande, "A novel texture-quantization-based reversible multiple watermarking scheme Applied to health information system," *Journal of Digital Imaging*, vol. 31, no. 2, pp. 167–177, 2018.
- [42] X. Liu, J. Lou, H. Fang et al., "A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images," *IEEE Access*, vol. 7, pp. 76580–76598, 2019.
- [43] S. Thakur, A. K. Singh, S. P. Ghrera, and M. Elhoseny, "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3457–3470, 2019.
- [44] F. A. Memon and N. Ahmed, "Reversible watermarking for the security of medical image databases," in *Proceedings of the 2018 21st Saudi Computer Society National Computer Conference (NCC)*, Riyadh, Saudi Arabia, April 2018.
- [45] Lakshmi and S. Ayyappan, "A review on reversible data hiding techniques," *International Journal of Applied Engineering Research*, vol. 48, pp. 2857–2864, 2018.