Journal of Medical Imaging

MedicalImaging.SPIEDigitalLibrary.org

Watermarking of ultrasound medical images in teleradiology using compressed watermark

Gran Badshah
Siau-Chuin Liew
Jasni Mohamad Zain
Mushtaq Ali

Watermarking of ultrasound medical images in teleradiology using compressed watermark

Gran Badshah,* Siau-Chuin Liew, Jasni Mohamad Zain, and Mushtaq Ali

Universiti Malaysia Pahang, Faculty of Computer System and Software Engineering, Gambang 26300, Kuantan Pahang, Malaysia

Abstract. The open accessibility of Internet-based medical images in teleradiology face security threats due to the nonsecured communication media. This paper discusses the spatial domain watermarking of ultrasound medical images for content authentication, tamper detection, and lossless recovery. For this purpose, the image is divided into two main parts, the region of interest (ROI) and region of noninterest (RONI). The defined ROI and its hash value are combined as watermark, lossless compressed, and embedded into the RONI part of images at pixel's least significant bits (LSBs). The watermark lossless compression and embedding at pixel's LSBs preserve image diagnostic and perceptual qualities. Different lossless compression techniques including Lempel-Ziv-Welch (LZW) were tested for watermark compression. The performances of these techniques were compared based on more bit reduction and compression ratio. LZW was found better than others and used in tamper detection and recovery watermarking of medical images (TDARWMI) scheme development to be used for ROI authentication, tamper detection, localization, and lossless recovery. TDARWMI performance was compared and found to be better than other watermarking schemes. © 2015 Society of Photo-Optical Instrumentation Engineers (SPIE) [DOI: 10.1117/1.JMI.3.1.017001]

Keywords: ultrasound image; Lempel-Ziv-Welch compression; region of interest; region of noninterest; tamper detection and recovery watermarking of medical images watermarking scheme.

Paper 15179R received Sep. 6, 2015; accepted for publication Dec. 8, 2015; published online Jan. 25, 2016.

1 Introduction

The invention and development of digital imaging technology has made possible to transform real-world images to computer understandable formats called digital images. Easy communication, meaningful manipulation, and making the desired number of copies of a digital image similar to the original one are the well-known advantages of digital imaging technology.¹ Digital imaging technology has been used in every field of life, such as in defense, education, business, engineering, air space, and medical for effective results. The current healthcare industry is dependent on digital medical imaging. Different imaging modalities, such as x-ray, computed tomography, nuclear medicine, positron emission tomography, magnetic resonance imaging, ultrasound (US), etc., have been used for medical imaging.² Teleradiology is a medical image processing utility to share medical images remotely to get better diagnostic results and analysis. Internet-based medical image communication has proved its best services in distributed healthcare system but is still facing security threats. Distributed healthcare literature reports a number of security techniques, including digital watermarking, to overcome the threats associated with communicating medical images. Digital watermarks may be a secret code, picture, symbol, an image, or a part of image used to prove ownership, unique identification, authentication, and recovery of a tampered digital image to its original version.³ The hiding of watermark into an image is known as digital image watermarking. Digital image watermarking should be done in such a way as to keep the image perceptual and diagnostic qualities unchanged, and watermark should not be removed or disturbed

due to the image processing operations such as filtering, compression, rotation, etc.⁴ A watermark insertion, detection, and extraction should be carried out in a proper way. The detection and extraction is called blind process if it does not need the presence of original image, and nonblind if it needs the existence of original image. Generally, a watermark insertion into an image can be shown mathematically as in Eq. (1).

$$I_w = F(I_o, W), \quad (1)$$

where I_o is the original image to be watermarked, F is the watermarking function, W is the watermark, and I_w is the watermarked image. Similarly, watermark detection and extraction can be represented mathematically as in Eq. (2).

$$W_{ex} = D(I_w, [I_o]), \quad (2)$$

where W_{ex} is the extracted watermark, D is the detection and extraction function, and I_o is the original image whose presence is optional. A particular two-dimensional medical image I , represented as a two-dimensional array of size $(m \times n) * kb$, is consisting of a number of positive integers $I(x, y)$, called pixel or picture element, where n, m are the number of columns and rows, respectively, such that $n \geq y \geq 1$ while $m \geq x \geq 1$ and kb is the gray-level range. $I(x, y)$ is a particular pixel, while $f(x, y)$ is its gray level, also known as functional value. Every pixel is represented by the combination of bits. A bit is a smallest unit of digital memory where only a binary value, 0 or 1, can be stored at a time. Changing a bit value causes a change in the pixel value. There are different gray-level imaging systems with their specific range of pixels, such as

*Address all correspondence to: Gran Badshah, E-mail: gran16178@gmail.com

Fig. 1 Eight-bit memory system.

8 bits (0 to 255), 9 bits (0 to 511), 10 bits (0 to 1023), 11 bits (0 to 2047), 12 bits (0 to 4095). If we consider an 8-bit system, then the pixel values range from 0 to 255, represented by different combinations of 0's and 1's. If all the pixels of an image have 255 (11111111) values, then the whole image will be looking white. If all the pixel values are replaced by 0's (00000000), then the image will be looking totally dark. These values can be changed by changing the bit values. This change has different effects depending on the bit positions. If we start reading a pixel bit from left to right, then we are starting from the most significant bit (MSB) and at last we reach the least significant bit (LSB) as shown in Fig. 1, for a pixel of value 21. In Figs. 2–4, (a) the Lena image is watermarked using (b) the Baboon image as watermark to get (c) the watermarked image. In Fig. 2, the image is watermarked at LSBs, while in Figs. 3 and 4, the image degradation is clear as they are watermarked at seventh and eighth MSBs. MSBs are rich of information; if we change their values, then the image is degraded, and this degradation can be felt visually as shown in Figs. 3 and 4. If we restrict this change to the LSBs, then usually up to two or three bits, the image was not degraded and looked like the original one as shown in Fig. 2. So, here in this work, we have focused on the watermark embedding into two LSBs for US medical images to keep the image degradation under control.

In this paper, our purpose is to develop a spatial domain LSB based tamper detection and recovery watermarking of medical images (TDARWMI) scheme for US medical images, which could ensure minimum or negligible degradation of watermarked image to preserve its diagnostic and perceptual qualities.

2 Materials and Methods

The study of medical image watermarking reports a number of techniques used for image watermarking. Broadly, these techniques can be divided into two major groups, transform and spatial domains watermarking.⁵ In frequency domain watermarking, the watermark is embedded into the image after its transformation to one of the specific format, discrete Fourier transform, discrete cosine transform, or discrete wavelet transform. This indirect embedding is complex in terms of image conversion process but more robust to watermark attacks. Frequency domain watermarking is invisible and classified into robust and fragile types.¹ Robust watermarking aims to defend the watermark against malicious attacks, such as image lossy compression, cropping, scaling, and so on.⁶ Robust watermarking has been used mostly for copyright protection and ownership verification.⁷ An attack tries to remove or alter watermark for illegal uses, violating patient privacy rules.⁸ On the other hand, fragile watermarking techniques have been used for integrity and contents authentication of digital images.^{9–11}

In spatial domain watermarking, the watermark is directly embedded into image pixels in a simple way without any transformation.¹² The main disadvantage of this method is the weak robustness of watermark to external attacks.¹³ The watermarking process may be blind or nonblind.¹⁴ The nonblind process creates a burden on computer memory to keep all the original

Fig. 2 (a) Lena image watermarking using (b) Baboon image as watermark at first LSB.

Fig. 3 (a) Lena image watermarking using (b) Baboon image as watermark at seventh MSB.

Fig. 4 (a) Lena image watermarking using (b) Baboon image as watermark at eighth MSB.

images for thousands of watermarked images. On the other hand, in the blind watermarking, also known as oblivious watermarking, there is no need for the original image to detect or extract watermark from the watermarked image, resulting in processing time reduction as well as control of excessive storage requirements.¹⁵ However, the nonblind process makes sure the exact recovery of tampered image because of the replacement of tampered portions by the original one obtained from the available original image.

Different methodologies have been used for spatial domain watermarking of medical images. One such method works on the basis of computation of average intensity of tampered block pixels and is used to replace the tampered pixel values.¹⁶ The main disadvantage of this method is the replacement of tampered values by approximated values without the calculation of exact values. This scheme has been modified by Zain and Fauzi using the evaluation of medical image watermarking for authentication with tamper detection and recovery scheme with better capabilities of recovery closer to the original one.¹⁷ Later on, Al-Qershi and Khoo have improved the recovery scheme by using reversible region of interest (ROI)-based digital watermarking scheme.¹⁸ In reversible tamper localization and recovery technique, the watermark is extracted and used for its restoration to original version without ignoring any important information.¹⁹ Liew and Zain have proposed another reversible tamper localization and recovery scheme for US medical images based on the fact that most of the LSBs in region of noninterest (RONI) pixels have zero values, so the default values are reversed after tamper detection.²⁰ This technique divides the

image into blocks based ROI, RONI to make the detection and recovery task more secured and efficient. Liew et al. have proposed another scheme, tamper localization and lossless recovery with ROI segmentation and multilevel authentication (TALLOR-RSMA), for tamper localization and lossless recovery, for reducing time in accessing the tampered segments and recovery.²¹ TALLOR-RSMA scheme uses image block watermarks using JPEG compression with reduction of block size but does not reduce the number of bits. The blocks embedding as watermarks cause image degradation and also problem in image lossless recovery. In TALLOR-RSMA scheme, the ROI division into segments makes the watermarking process of many parts of a single image at a time. This is a time-consuming process to authenticate an image at multiple levels. In medical image watermarking, the watermark must be clearly and losslessly compressed. For medical image compression, only lossless schemes are applicable because this is very sensitive data and any data loss is not affordable, as it can lead to wrong medical decision making.^{22,23}

We have developed TDARWMI, tamper detection, localization, and recovery of medical image watermarking scheme with watermark lossless compression using LZW technique^{24,25} to overcome the drawbacks of TALLOR-RSMA scheme. For this purpose, image ROI is defined, and its SHA-256 hash value is calculated. ROI and its hash are combined to get a single watermark. The watermark is compressed using different lossless compression techniques and LZW is found to be better than all others as shown in Table 1. LZW is chosen as the best one due to its good compression ratio and more bits reduction.

Table 1 Watermark compression ratio calculation using different compression techniques.

Lossless compression technique	Ultrasound image size	ROI size	Watermark bytes before compression	Watermark bytes after compression	Compression ratio
LZW	480 × 640	70 × 115	8050	103	0.001
GIF	480 × 640	70 × 115	8050	1338	0.166
PBM	480 × 640	70 × 115	8050	1060	0.132
JPG	480 × 640	70 × 115	8050	1385	0.170
JPEG2000-j2c	480 × 640	70 × 115	8050	636	0.079
JPEG2000-jp2	480 × 640	70 × 115	8050	721	0.089
JPEG2000-j2k	480 × 640	70 × 115	8050	636	0.079
PNG	480 × 640	70 × 115	8050	488	0.060

Compressed watermark was embedded into the image at first and second LSBs of RONI part. On the receiver end, watermark is extracted and successfully used for ROI authentication, tamper detection, localization, and lossless recovery.

2.1 Watermark Lossless Compression Using Lempel-Ziv-Welch Technique

LZW has been used to eliminate the repeating sequences of image pixel and text characters.^{26,27} Here we use LZW for binary watermark bits repeated sequences elimination to reduce watermark payload. In this paper, ROIs of different sizes of three different US medical image samples are selected to get watermark. The watermark is converted to binary and stored in an array forming a stream of binaries. Another array initialized with two strings 0, 1 is defined to store the binary watermark repeating sequences during compression. The dictionary is initialized only to two strings because the whole binary stream is consisting of only two distinct values of 0's and 1's. These strings are allotted codes 1 and 2, respectively, as translating codes, stored in the defined code table. The watermark stream is accessed in a way that every member of the stream is accessed, forming unique strings and decimal codes are allotted, the strings and decimal codes are inserted into dictionary and code table respectively. This process continues until the whole watermark is compressed. Every time the new string is checked in the dictionary; if it does not exist, then it is inserted, otherwise discarded. In such a way, dictionary grows up and the translated codes are stored in codes table. At completion, the codes table values collectively form the compressed watermark. The compressed watermark is converted to binary and inserted into image in RONI pixels at LSBs. At destination, watermark is extracted and separated to ROI hash, ROI parts. ROI hash is used for ROI authentication and the recovered ROI is used for image tamper detection, localization, and lossless recovery.²⁸ Figure 5 shows the LZW compression process applied to a string of 25 characters, rrrggrrggbbbbbbbbbbbbbb, which is helpful to understand the binary watermark compression using LZW compression. The process shows if a character is repeated and makes a longer sequence, then it directly affects the compression performance to give a good compression ratio. We see from Fig. 5 the repetition of characters g and b, which indicates that more characters are coded in less number of decimal codes. It means that a binary sequence has large number of 0's and 1's

To compress string = rrrggrrggbbbbbbbbbbbbbb		
Length (string) = 25 characters (25x8=200 bits) in 8-bits system.		
String codes	String	Compression result
0	r	empty
1	g	empty
2	b	empty
3	rr	0
4	rrg	0 3
5	gg	0 3 1
6	ggr	0 3 1 5
7	rrgg	0 3 1 5 4
8	gb	0 3 1 5 4 1
9	bb	0 3 1 5 4 1 2
10	bbb	0 3 1 5 4 1 2 9
11	bbbb	0 3 1 5 4 1 2 9 10
12	bbbbb	0 3 1 5 4 1 2 9 10 11
Compression result:		0, 3, 1, 5, 4, 1, 2, 9, 10, 11, 12
Length (compressed string) =		11 characters (11x8=88 bits)

Fig. 5 A string compression example using LZW lossless compression technique.

repetition, which will give good compression ratio for a binary watermark compression using LZW technique.

The compression results in the code table values 0, 3, 1, 5, 4, 1, 2, 9, 10, 11, 12, and this is the final compressed watermark. In this example, LZW compresses 25 characters ($25 \times 8 = 200$ bits) string to 11 characters ($11 \times 8 = 88$ bits). This reduction will be higher for a binary stream having thousands of binary bits, 0's, and 1's because there will be longer sequence of binary repeating sequences and the compression ratio will be definitely high. As watermark is represented in a binary stream and consists of longer sequences of 0's (00000 ...) and 1's (11111 ...), LZW gets good compression ratio, as shown in Table 1. If Bc is the number of bytes before compression and Ac is the number of bytes after compression, then Eq. (3) gives the compression ratio.

$$\text{Compression ratio} = \text{Ac/Bc.} \quad (3)$$

Table 1 summarizes a fixed size ROI lossless compression of image sample 1 shown in Fig. 6 using different compression techniques, showing that the LZW technique performs better than the others.

Analyzing Table 1 data, each row gives the required information in detail of each compression technique including LZW. The better compression ratio and more bytes reduction of watermark payload make clear the selection of LZW as the best among the mentioned compression techniques to be used in image watermarking of TDARWMI scheme.

At the receiver end, watermark is retrieved and decompressed using the LZW technique as shown in Fig. 7 for a compressed string decompression. The compressed string decompression is carried out from the codes 0, 3, 1, 5, 4, 1, 2, 9, 10, 11, and 12, which are already available in the code table. The code values are used to access the equaling strings already stored in the dictionary. The accessed strings are concatenated and finally the decompressed string is obtained in original. Figure 7 shows the decompressed string, which is similar to the original one, meaning LZW is a lossless compression technique and can be used for medical image watermarking.

Figures 5 and 7 give an example string compression and decompression process in detail to show how LZW will work for a binary watermark compression and decompression losslessly. The main purpose of the string example is to provide the detail process for characters more than two binaries in a binary watermark. It shows that if a character is repeated in a

Fig. 6 Original US image sample 1.

Final output	0 3 1 5 4 1 2 9 10 11 12											
Code	String	Output										
0	r	r										
3	rr	rrr										
1	g	rrrg										
5	gg	rrrggg										
4	rrg	rrrggrrg										
1	g	rrrggrrgg										
2	b	rrrggrrggb										
9	bbb	rrrggrrggbbb										
10	bbb	rrrggrrggbbbbbb										
11	bbbb	rrrggrrggbbbbbbbbb										
12	bbbb	rrrggrrggbbbbbbbbb (lossless decompressed string)										

Fig. 7 The compressed string decompression using LZW technique.

string, which is very true for binary watermark to build longer sequences, then the compression will be high. For medical image watermarking, we need a high compression value to preserve the original image qualities.

2.2 Tamper Detection and Recovery Watermarking of Medical Image Watermarking Scheme

TDARWMI is a newly developed watermarking scheme, capable of tamper detection, localization, and lossless recovery of US medical images. This scheme fulfills the rule that the medical images should not be degraded to be used for diagnostic purpose.²⁹ If the watermark is not compressed, then the image will have to be watermarked with heavy payload, which will definitely degrade its perceptual and diagnostic qualities. Another need for watermark compression is to make available sufficient LSBs in RONI pixels for watermark encapsulation.³⁰ If the number of watermark bits becomes more than the available LSBs, then the whole watermark insertion may be possible. The reduced number of bits as watermark were embedded into the first and second LSBs of RONI using MATLAB[®] as the implementation tool. For compressed watermark insertion, the RONI pixels are visited from the start and every accessed pixel's first and second LSB values are replaced by the watermark one. To avoid actual information from distortion, the watermark bits are not encapsulated in the ROI part. There are two possible ways to divide the image into ROI and RONI parts, the automatic and semiautomatic. In the semiautomatic method, the ROI coordinates are provided as input during the runtime of TDARWMI. In the automatic method, the ROI coordinates are specified and assigned before the scheme runtime. In this paper, we use fixed size ROI to compare our scheme results with TALLOR-RSMA²¹ while processing the same images as the comparison results shown in Tables 2 and 4. The watermarked image is perceptually similar to the original one as shown in Figs. 6 and 8 for image sample 1. TDARWMI was used successfully for watermark extraction, ROI authentication, tamper detection, localization, and lossless recovery. Figures 6 and 8–10 show the original, watermarked, tampered, and recovered versions of image sample 1, respectively. The original, watermarked, and recovered images are identical perceptually, which shows the effectiveness of the scheme. Figure 9 shows the tampered version of the original image, tampered by adding salt and pepper noise through the application of imageJ software. To summarize the experiment results, algorithm runtime combined figure is also shown in Fig. 11 for sample 1. ROI is the major part of watermark, so we add noises only to ROI to test the TDARWMI scheme performance.

Fig. 8 Watermarked US image sample 1.

2.3 Image Tamper Detection, Localization, and Lossless Recovery

Tamper detection is a process used to point out the altered portion of the image. In this work, tamper detection and localization is limited to ROI because this is the defined important portion of

Fig. 9 Tampered US image sample 1, adding salt and pepper noises.

Fig. 10 Recovered US image sample 1

Fig. 11 TDARWMI run time output for image sample 1.

the image. If the recovery of a tampered portion is totally without loss, then it is called lossless recovery. There are many ways to alter the image; some of them are intentional while others are accidental. Different types of noises, such as salt and pepper, cropping, adding normal noises in percentage, were added to the image through imageJ software to get the intentionally tampered versions of the image for testing purpose. TDARWMI scheme uses pixels for one-to-one comparison of suspicious image ROI to the same size ROI of the recovered watermark part. During comparison, the nonmatching pixels are marked as tampered and replaced by the watermarked one. If the values exactly match, then it means the pixel is original and no need for replacement. This process continues till the complete scanning of the communicated image ROI. Our watermarking scheme was tested and was found to be more accurate than TALLOR-RSMA scheme.²¹ The comparison was made on the basis of compression ratio and peak signal-to-noise ratio (PSNR). Table 1 and Fig. 11 summarize the results obtained for the same size ROI processing of image sample 1, which

Table 2 Calculation of watermark (including 70×115 size ROI) compression ratio and PSNR of watermarked images.

Sample number	Compression ratio	Noise type	Watermarked image PSNR (dB)
1	0.0898	Salt and pepper	53.661
2	0.0918	Crop	54.888
3	0.0478	50% added noise	56.040

show that our scheme is better. The recovered images of samples 1, 2, and 3 perceptually looked like the original, but for non-perceptual accuracy measurement, the calculated PSNR values are tabulated in Tables 2–4 to compare the schemes. For all of the three US image samples 1, 2, and 3 shown in Figs. 6, 12, and 13, results are tabulated in Tables 2–4 for better understanding.

2.4 Region of Interest Authentication

Before starting tamper detection and recovery process at destination, first the authentication process is performed. The extracted watermark is separated to ROI and ROI hash code. SHA-256 function is applied to hash the same ROI of the communicated image to get the new hash value. The extracted and newly computed hash values are compared. If the values are same, then there is no need of performing tamper detection

Table 3 Calculation of watermark (including 160×240 size ROI) compression ratio, elements reduction and PSNR of watermarked images.

Sample number	Number of elements of compressed watermark	Compression ratio	Noise type	Watermarked image PSNR (dB)
1	24,938	0.0714	Salt and pepper	48.50
2	22,076	0.0718	Cropping	49.61
3	69,300	0.0225	50% added noise	52.970
Average	38,772	0.2706	—	50.282

Table 4 Comparison of TDARWMI and TALLOR-RSMA schemes for watermark (including 160×240 size ROI).

Sample number	Number of elements of compressed watermark		Compression ratio		Noise type	Watermarked image PSNR (dB)	
	TDARWMI	TALLOR-RSMA	TDARWMI	TALLOR-RSMA		TDARWMI	TALLOR-RSMA
1	24,938	176,240	0.071	0.57	Salt and pepper	48.50	48.3
2	22,076	189,928	0.071	0.62	Cropping	49.61	48.5
3	69,300	157,560	0.022	0.51	50% added noise	52.970	49.0
Average	38,772	174,576	0.270	0.566	—	50.282	48.6

and recovery process. In case of any mismatch, it means the communicated image ROI has been tampered and recovery is essential. For example if h_1 is the hash value of original image, h_2 is the ROI hash value of the safely communicated image, and h_3 is the ROI hash value of the tampered image as shown in Figs. 14–16, respectively, then the comparison is easy. Figure 11 is the run time result of the TDARWMI scheme in the case of comparison of Figs. 14 and 16 when the ROI gets tampered. Figure 11(a) shows the original image, Fig. 11(b) shows the watermarked image, Fig. 11(c) shows the tampered image, and Fig. 11(d) shows the recovered image.

The comparison of h_1 and h_2 shown in Figs. 14 and 15 shows that the values are same before and after communication, which means there is no need of TDARWMI processing. The comparison of h_1 and h_3 shown in Fig. 16 shows that the values are different, meaning it is necessary to run the TDARWMI scheme because the ROI has been tampered and needs to be recovered as shown in Fig. 11.

2.5 Watermarked Image Accuracy Measurement

Perceptually, nondegradation of a watermarked image shows the reliable watermarking. A watermarked image degradation judgment can be carried out by the application of an engineering formula called PSNR. PSNR is measured in a unit called decibel (dB). The greater PSNR value indicates good quality of the image, while low value shows the low quality, meaning more degradation. Mean square error (MSE) is the difference

quantification of true and estimated image. MSE is a base for PSNR calculation and can be given by Eq. (4).

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I_o(i, j) - I_w(i, j)]^2, \quad (4)$$

where m, n are the number of rows and columns of the original image I_o , and I_w is the noise induced image due to watermarking. The PSNR can be calculated by the formula given in Eq. (5).

$$PSNR = 20 \cdot \log_{10} [\text{MAX}(I_o)] - 10 \log_{10} (MSE), \quad (5)$$

Fig. 13 Original US image sample 3.

$h_1=6e340b9c7b37a989ca544e6bb780a2c78901d3fb33738768511a30617afa01d$

Fig. 14 ROI hash of the original image before communication.

$h_2=6e340b9c7b37a989ca544e6bb780a2c78901d3fb33738768511a30617afa01d$

Fig. 15 ROI hash of safely communicated image.

$h_3=0e340b9c7b37a989ca544e6bb780a2c78901d3fb33738768511a30617afa01d$

Fig. 16 ROI hash of the tampered image. **Fig. 12** Original US image sample 2.

where MAX(Io) is the highest possible numeric value for a pixel of the original image, which is 255, because we are using 8-bit gray-scale US medical image. Table 2 shows the PSNR of the watermarked images. Three different US medical image samples were tested; compression ratio and PSNR values were recorded showing that our scheme is better than the TALLOR-RSMA scheme.

The experimental results show that if the image is truly recovered, then PSNR value remains high, and if it is not recovered accurately, then PSNR remains low, so the PSNR high values of TDARWMI show good image reconstruction quality.

3 Results and Discussion

The watermark was stored in an array, lossless compressed, and embedded into LSBs of the RONI part of the original image. The importance of compressed watermark insertion has been shown in Figs. 2–4 to keep the medical image distortion negligible. Selection of LZW as the watermark compression technique has been summarized in Table 1. During the string compression example, more bits reduction was noted, which ensures binary watermark compression using LZW technique to preserve the original qualities of watermarked medical image. Qualitative measurements of watermarked images are indicated by its calculated PSNR values. The embedding watermark size directly affects the PSNR value, which is evident from Tables 2 and 3. If we resize ROI from 70×115 to 160×240 , the PSNR values decrease as shown in Table 3. This depicts the reality that watermarking an image with heavy payload degrades its quality. Therefore, we need LZW as lossless compression technique to watermark the images with less number of bits to keep the image diagnostic quality standard. Table 1 shows that LZW is better than other compression techniques regarding PSNR. The average good compression ratio and PSNR values listed in Table 4 show good quality of watermarking capability of our scheme. One another proof of better performance of our scheme is that it takes same size ROI as TALLOR-RSMA uses as watermark but TDARWMI results are better for full watermark; our scheme includes ROI hash code in addition to watermark. Based on experimental results as summarized in Tables 1–4, we show that TDARWMI is better than TALLOR-RSMA for US medical images authentication, tamper detection, localization, and lossless recovery.

4 Conclusion

Image security is an important part of online digital image processing. Medical image authenticity is very important in teleradiology for an accurate decision making process. If medical image data is manipulated, then there should be a reliable mechanism to detect, locate, and recover the altered data. Watermarking technique is capable of providing security to medical images using data hiding techniques, but excessive data embedding degrades the image perceptual and diagnostic qualities. There should be a mechanism to keep the degradation under control and ensure tamper detection, localization, and lossless recovery. Therefore, the watermark is lossless compressed to reduce the number of bits and to embed into image RONI at LSBs to keep the diagnostic part (ROI) free of degradation. ROI is small in size but the most informative part of the image, enough for medical decision making. Different compression techniques are used to compress watermark, but LZW is selected as the best one on the basis of good

compression ratio and more bits reduction. In this work, we have developed TDARWMI, a new watermarking scheme for ROI tamper detection, localization, and lossless recovery of medical images security in teleradiology. ROI and its SHA-256 function calculated hash value are combined as watermark in the binary form and lossless compressed using LZW technique. The compressed watermark is embedded into the first and second LSBs of RONI. Our TDARWMI scheme shows better performance as compared to TALLOR-RSMA watermarking scheme used previously for ultrasound medical image watermarking. The tamper detection and recovery restriction to a specific part of image ROI is the main limitation of this scheme.

Acknowledgments

We thank Universiti Malaysia Pahang (www.ump.edu.my) for funding this research under Grant No. GRS, 110336, FSKKP. The digital images used in this research were downloaded from the Internet.

References

1. M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proc. IEEE* **86**(6), 1064–1087 (1998).
2. J. D. Newell, Jr. and C. A. Kelsey, *Digital Imaging in Diagnostic Radiology*, Churchill Livingstone, New York (1990).
3. M. Holliman and N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes," *IEEE Trans. Image Process.* **9**(3), 432–441 (2000).
4. H. K. Maity and S. P. Maity, "Joint robust and reversible watermarking for medical images," in *Procedia of Second Int. Conf. on Communication, Computing and Security*, Vol. 6, pp. 275–282 (2012).
5. G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Signal Process. Mag.* **17**(5), 20–46 (2000).
6. I. J. Cox et al., "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.* **6**, 1673–1687 (1997).
7. S. Voloshynovskiy et al., "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks," *IEEE Commun. Mag.* **39**(8), 118–126 (2001).
8. S. Radharani and M. Valarmathi, "A study on watermarking schemes for image authentication," *Int. J. Comput. Appl.* **2**(4), 24–32 (2010).
9. P. W. Wong, "A watermark for image integrity and ownership verification," in *Proc. IS&TPIC Conf.*, pp. 374–379 (1998).
10. C. W. Wu et al., "Fragile imperceptible digital watermark with privacy control," *Proc. SPIE* **3657**, 79 (1999).
11. M. Wu and B. Liu, "Watermarking for image authentication," in *Int. Conf. on Image Processing*, pp. 437–441 (1998).
12. D. Anand and U. C. Niranjana, "Watermarking medical images with patient information," in *Proc. of the 20th Annual Int. Conf. of the IEEE Engineering in Medicine and Biology Society*, Vol. 2, pp. 703–706 (1998).
13. H. H. Larijani and G. R. Rad, "A new spatial domain algorithm for gray scale images watermarking," in *Int. Conf. on Computer and Communication Engineering*, pp. 157–161 (2008).
14. C. I. Podilchuk and Z. Wenjun, "Image-adaptive watermarking using visual models," *IEEE J. Sel. Areas Commun.* **16**(4), 525–539 (1998).
15. W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images," *IEEE Trans. Image Process.* **8**(11), 1534–1548 (1999).
16. J. M. Zain and A. R. M. Fauzi, "Medical image watermarking with tamper detection and recovery," in *28th Annual Int. Conf. of the IEEE Engineering in Medicine and Biology Society*, pp. 3270–3273 (2006).
17. J. M. Zain and A. R. Fauzi, "Evaluation of medical image watermarking with tamper detection and recovery (AW-TDR)," in *Conf. Proc. of IEEE Engineering in Medicine and Biology Society*, pp. 5662–5665 (2007).

18. O. M. Al-Qershi and B. E. Khoo, "Authentication and data hiding using reversible ROI-based watermarking scheme for DICOM images," in *Proc. of Int. Conf. on Medical Systems Engineering*, pp. 829–834 (2009).
19. O. M. Al-Qershi and K. Bee Ee, "ROI-based tamper detection and recovery for medical images using reversible watermarking technique," in *IEEE Int. Conf. on Information Theory and Information Security*, pp. 151–155 (2010).
20. S. C. Liew and J. M. Zain, "Reversible medical image watermarking for tamper detection and recovery," in *3rd IEEE Int. Conf. on Computer Science and Information Technology*, pp. 417–420 (2010).
21. S. C. Liew, S. W. Liew, and J. M. Zain, "Tamper localization and lossless recovery watermarking scheme with ROI segmentation and multilevel authentication," *J. Digit. Imaging* **26**(2), 316–325 (2013).
22. E. Watanabe and K. Mori, "Lossy image compression using a modular structured neural network," in *Proc. of IEEE Signal Processing Society Workshop*, pp. 403–412 (2001).
23. H. Vilas et al., "New approaches for image compression using neural network," *J. Intell. Learn. Syst. Appl.* **3**, 220–229 (2011).
24. B. Jennifer and L. Annie, "Supplement to chapter 3 of the science of digital media—digital image processing," 2007, <http://csweb.cs.wfu.edu/~burg/nsf-due-0340969/worksheets/DitheringWorksheet.pdf> (16 December 2015).
25. G. Badshah et al., "Watermark compression in medical image watermarking using Lempel-Ziv-Welch (LZW) lossless compression technique," *J. Digit. Imaging* **28**(5), 1–10 (2015).
26. G. Badshah et al., "Importance of watermark lossless compression in digital medical image watermarking," *Res. J. Recent Sci.* **4**, 75–79 (2015).
27. N. Mark et al., "LZW data compression," 1989, <http://marknelson.us/1989/10/01/lzw-data-compression/> (16 December 2015).
28. F. D. Martino and S. Sessa, "Fragile watermarking tamper detection with images compressed by fuzzy transform," *Inf. Sci.* **195**, 62–90 (2012).
29. S. Wong et al., "Radiologic image compression—a review," *Proc. IEEE* **83**(2), 194–218 (1995).
30. G. Badshah et al., "Secured telemedicine using whole image as watermark with tamper localization and recovery capabilities," *J. Inf. Process Syst.* **11**(4), 601–615 (2015).

Gran Badshah received his bachelor and master degrees in computer science from the University of Peshawar, Pakistan, in 1998 and 2003, respectively. Recently, he has completed his PhD in the research area of digital image security using watermarking technique from University Malaysia Pahang. His research interests include digital watermarking, image processing, as well as cloud data security. He has published more than 15 articles as primary and coauthor in different journals and conferences.

Siau-Chuin Liew received his bachelor's degree in information technology from the University of Southern Queensland, Australia, in 2003. He did his master's degree in strategic business IT from the University of Portsmouth, United Kingdom, in 2006. He completed his PhD in computer science from UMP, Malaysia, in 2011. Currently, he is a senior lecturer at the Faculty of Computer Systems and Software Engineering, UMP; his research interests include image processing and signal processing.

Jasni Mohamad Zain received her bachelor's degree in computer science from the University of Liverpool, England, United Kingdom, in 1989 and her PhD from Brunel University, West London, United Kingdom, in 2005. She started her career as a tutor in 1997 at the University of Technology Malaysia. Currently, she is a professor and dean of the Faculty of Computer Systems and Software Engineering at UMP since 2008. She has a patent file for digital watermarking (PI 2008047).

Mushtaq Ali received his bachelor's degree in computer science from the University of Peshawar, Pakistan, in 2003. He completed his master's degree from Hazara University, Mansehra, Pakistan, in 2006. Currently, he is pursuing his PhD candidature at UMP. He started his career as an IT-instructor at Pak Swiss Technical Training Center, Mingora Swat, Pakistan, in 2007. His research interests include mobile computing, efficiency of mobile devices, cloud security, and watermarking of digital images.