J Digit Imaging (2013) 26:316–325
DOI 10.1007/s10278-012-9484-4

Tamper Localization and Lossless Recovery Watermarking Scheme with ROI Segmentation and Multilevel Authentication

Siau-Chuin Liew · Siau-Way Liew · Jasni Mohd Zain

Published online: 4 May 2012

Abstract Tamper localization and recovery watermarking scheme can be used to detect manipulation and recover tampered images. In this paper, a tamper localization and lossless recovery scheme that used region of interest (ROI) segmentation and multilevel authentication was proposed. The watermarked images had a high average peak signal-to-noise ratio of 48.7 dB and the results showed that tampering was successfully localized and tampered area was exactly recovered. The usage of ROI segmentation and multilevel authentication had significantly reduced the time taken by approximately 50 % for the tamper localization and recovery processing.

Keywords Lossless compression · Tamper localization · Recovery · Medical image · Watermarking

Introduction

To prevent counterfeiting, watermarking has been widely applied to paper material since its invention; for example, with paper money, passports, postage stamps, and other important documents. The watermark carries information about the object in which it is hidden to indicate authenticity and is usually hidden from normal view. It only becomes visible when the watermarked paper is held against a light. The risk of losing the data for authentication purposes is thus eliminated since the data is embedded within the digital content itself [1]. Watermarking can be also used in medical images to prevent unauthorized modification by authenticating the content of the image. The purpose of medical image security is to maintain privacy of the patient information in the image and to assure data integrity that prevents the image from being tampered with [2].

One of the requirements of an effective watermarking-based authentication system as defined by Liu and Qiu is the ability to identify manipulated areas, also known as localization, where the authentication watermark should be able to detect the location of manipulated areas, and thus verify other areas as authentic [3]. The tampered area can be recovered by retrieving the original pixel values stored on the image itself as part of the watermark. Tamper localization is useful for deducing the motive for the tampering and the legitimacy of any modification.

Guo and Zhuang proposed a reversible scheme with tamper localization based on difference expansion [4]. This scheme partitions an image into certain non-overlapping regions and appends the associated local authentication information directly into the watermark payload. It also introduces the concept of region of authentication (ROA) where ROA is a region used for integrity authentication; in other words, the area that needs to be protected. A ROA which can be flexibly defined by the user is partitioned into small regions as an image block or polygonal region in a multilevel hierarchical manner. A hashing function is used to produce digital signatures for each image block, which are then added to the watermark payload. To verify the authenticity of the image, the process begins by

S.-C. Liew (✉) · J. M. Zain
Faculty of Computer Systems and Software Engineering,
Universiti Malaysia Pahang,
Lebuhraya Tun Razak,
26300 Kuantan, Pahang, Malaysia
e-mail: liewsc@ump.edu.my

J. M. Zain
e-mail: jasni@ump.edu.my

S.-W. Liew
ConforMIS, Inc.,
11 North Ave.,
Burlington, MA 01803, USA
e-mail: siauway@gmail.com

comparing the signature for the whole image. If the initial verification process fails, the ROA is reconstructed. The signatures for the ROA are compared to detect any tampering. An interesting technique used in the tamper localization process produces an output image consists of shadings of the ROA. The shading reflects the level of confidence in the integrity of the ROA where light shadings correspond to high confidence values and dark shadings correspond to low confidence value. Ultrasound imaging is used as the quality of the watermarked image is crucial, especially for medical diagnoses. The perceptibility of the watermarked ultrasound image is not known since the distortion level of the watermarked image was not measured in the experiment.

Tan et al. also proposed a tamper localization watermarking scheme that uses pixel value modification to allow the watermark to be reversible [5]. Here the image is divided into 16×16 pixel blocks and a cyclic redundancy check (CRC) is computed for each block. Each CRC is embedded into its own block. In the event that the CRC cannot be embedded into its own block, the remaining bits are carried over to the next block. The watermarked image is verified by extracting the watermark and comparing the CRC of each block. Any mismatch of CRC values indicates tampering. The disadvantage of this scheme is that, in order to allow reversibility, all pixel values need to be increased by four pixel values during the embedding process to prevent bit overflow; thus, the maximum pixel value allowable in an image to be watermarked is constrained.

Wu proposed a scheme which embeds the watermark into the integer wavelet transform coefficients [6]. In addition to being reversible and robust against lossy compression at a low quality factor, this scheme is also able to localized tampering such as cropping and bit replacement. While this watermarking scheme might be able to identify the area of tampering, the tampered region cannot be recovered [4–8].

Yang and Shen apply hash function to image blocks and embedded the hash values into the least significant bits (LSB) of the corresponding blocks [9]. In their scheme, vector quantization is used to compress an image by producing an index table to be used for image recovery. The index table is embedded into the second and third LSB of each pixel. Each block of the image is authenticated using the embedded hash value. When tampering is detected, the index table is used to reconstruct an image. The tampered block is recovered using blocks from the reconstructed image. The limitation of this scheme, however, is reversibility.

Chiang et al. proposed a reversible tamper localization scheme with tampered region recovery capability [10]. Their scheme, based on a difference expansion scheme proposed by Tian, was modified to allow the watermark to be embedded into the transform domain by using the integer Haar wavelet transform [11]. In the modification, the image is first divided into blocks. The recovery information is generated by taking the average pixel value of each block and embedding it as a watermark. The watermark is encrypted before the embedding process for security. The whole image can be verified by comparing the retrieved average pixel value from the watermark with the current average pixel value of the image. Any mismatch indicates tampering. The tampered region can be localized to an accuracy of 4×4 pixels. The tampered block is then recovered using the average pixel value retrieved from the watermark. The disadvantage of this scheme is its complexity as it operates in the transform domain.

Osamah and Khoo proposed a scheme that consists of two types of watermarks [12]. The first watermark is embedded into a spatial domain and the second into a transform domain. The image is first divided into 16×16 pixel blocks. The first watermark consists of patient's data and the hash value of the region of interest (ROI). It is embedded into the ROI itself by using a modified difference expansion technique. An embedding map of the ROI is produced to form a second watermark together with compressed recovery information of the ROI and the average value of each block in the ROI. The second watermark is compressed and embedded into the region of non-interest (RONI) using a discrete wavelet transform technique. Tamper localization is done by comparing the average value of each block in the ROI with the retrieved average value from the watermark. Tampered blocks are recovered using the lossy compressed ROI. However, this scheme and others [9, 10, 13, 14] have a common disadvantage since the tampered area can only be approximately recovered, for example in the form of average intensity or lossy compression. The recovered image is only approximately identical to the original image and due to its poor quality; it may not be used for diagnosis purposes.

In a previously published paper [15], we proposed tamper localization and lossless recovery (TALLOR) scheme that allows exact recovery of tampered medical images. This scheme uses lossless compression to permit the tampered image to be recovered to its original state. The recovered medical image was identical to the original image and would still be useful for diagnosis purposes. The issue with this scheme was that lossless compression was used to compress the original image before being embedded as part of the watermark. Thus, more time was taken in the tamper localization and recovery process where the embedded watermark is decompressed and used to recover the tampered image. If the user requested the image be authenticated at the time of usage, this would lengthen the tamper localization and recovery processing. In this paper, we propose enhancements to our previous work in order to reduce the tamper localization and recovery time.

Materials and Methods

Our previously developed TALLOR scheme was specifically designed based on a common characteristic that can be found in most ultrasound images. Figure 1 shows an

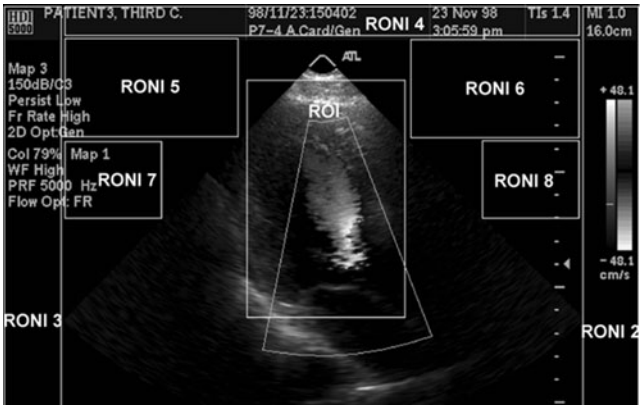

Fig. 1 Ultrasound image is divided into ROI and RONI

example of an ultrasound image where the ROI forms a triangle in the center of the image and the RONI is the black area outside of the triangle. The RONI usually contained descriptions for the image such as time, date, and measurements display. The RONI can be used to store watermarking information. The proposed enhancements are explained in the next section.

TALLOR with ROI Segmentation and Multilevel Authentication

Our initial testing using the technique in the TALLOR scheme revealed that a significant processing was taken to embed and retrieve the compressed ROI. We decided to further divide the ROI into segments with only the segments that were tampered

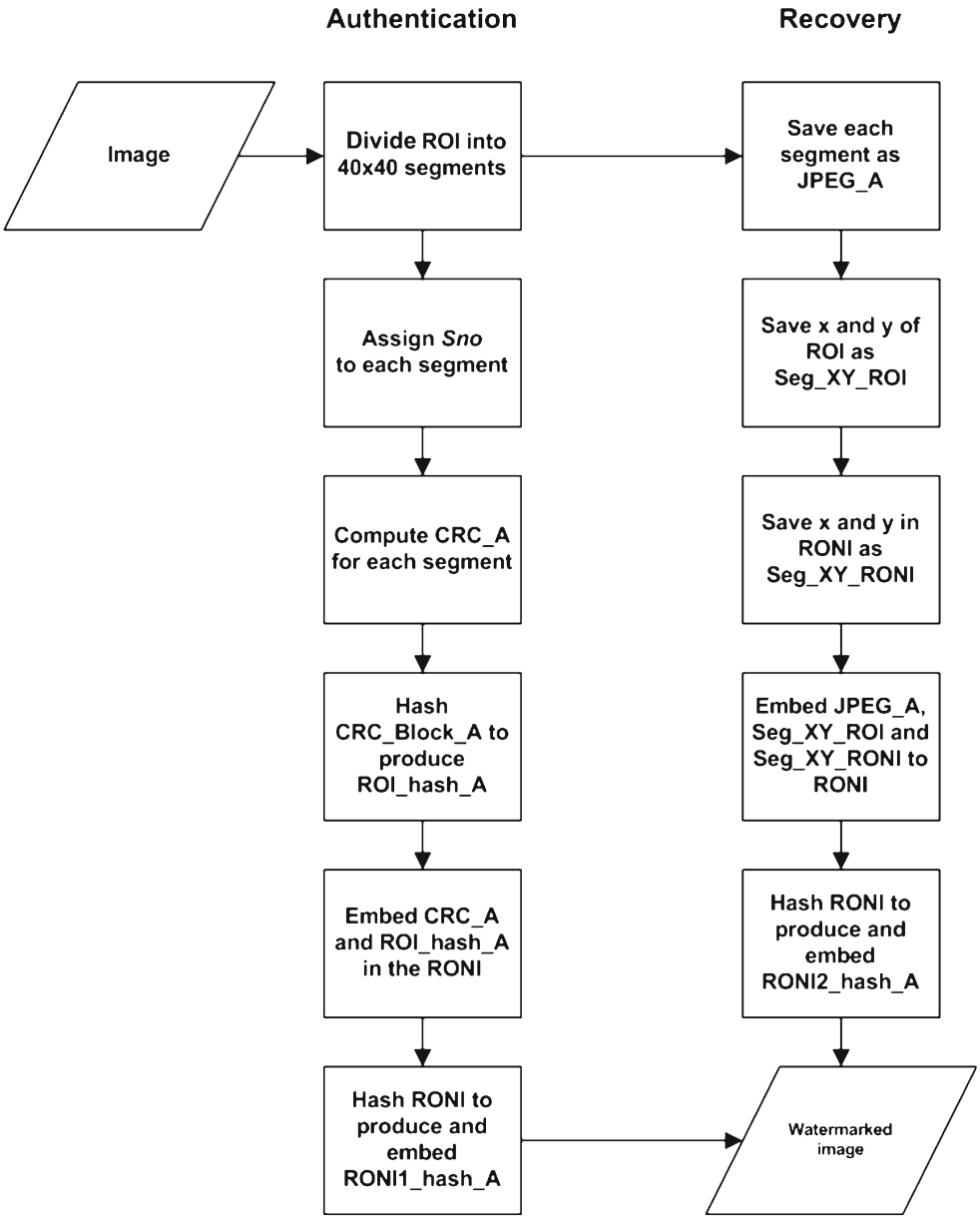

Fig. 2 The watermark generation and embedding process for the authentication and recovery information

with being retrieved from the RONI for recovery purposes. As the ROI was to be divided into segments, each segment would be authenticated individually. The authentication would be performed in a multilevel manner where only suspected segments would be examined further for tampering. Theoretically, these techniques would reduce the processing time.

Since the compressed ROI file contributed a major portion of the total watermark payload; therefore, additional

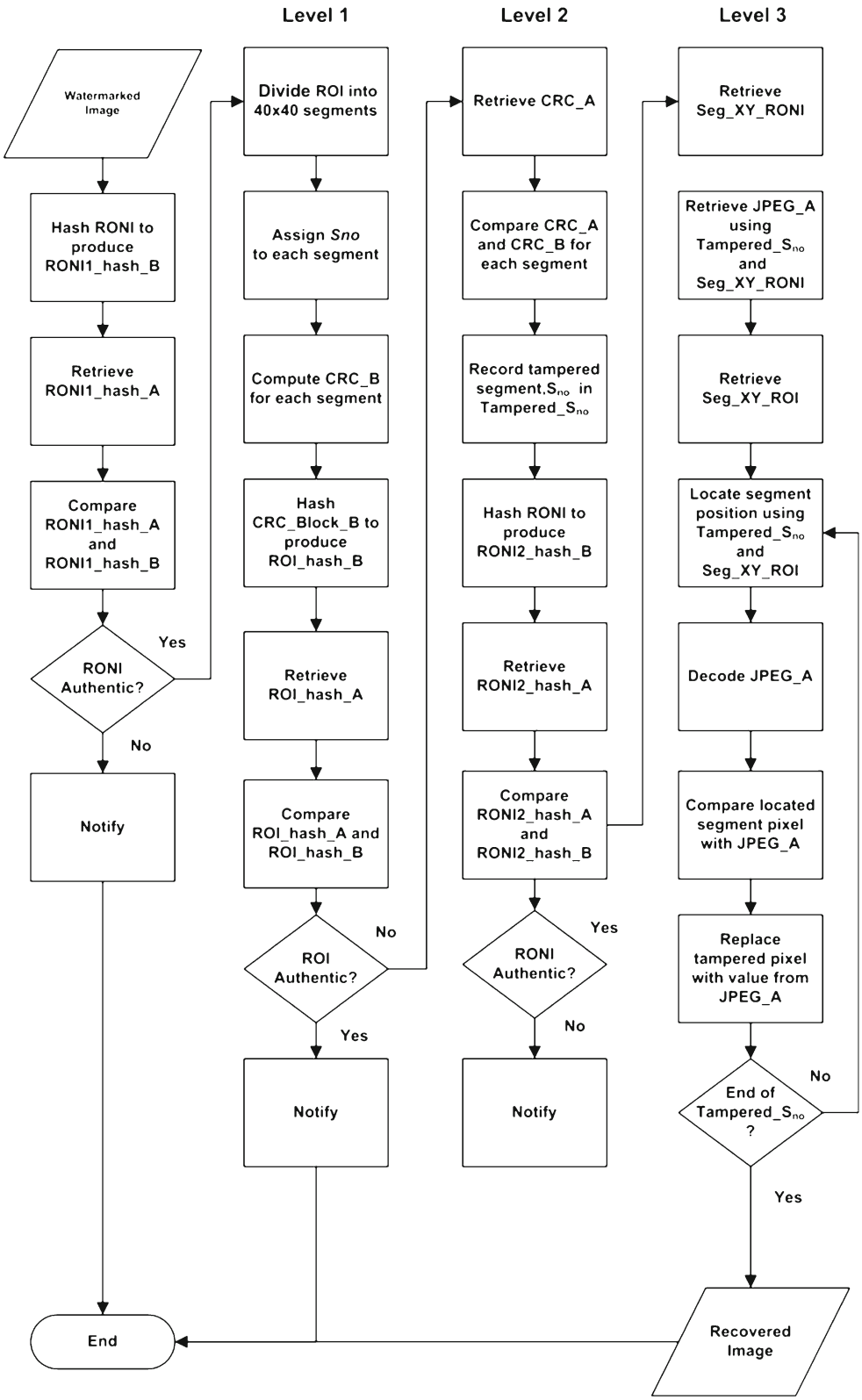

Fig. 3 The tamper localization and recovery process for all 3 levels

Table 1 The experiment results for all samples using TALLOR and TALLOR-RSMA

Total ROI bits=307,200

	TALLOR				TALLOR-RSMA			
Figure	Compression output (bits)	Compression ratio	PSNR (dB)	Total watermark payload (bits)	Compression output (bits)	Compression ratio	PSNR (dB)	Total watermark payload (bits)
Sample 1	180,704	0.59	48.1	180,960	176,240	0.57	48.3	177,008
Sample 2	190,680	0.62	48.0	190,936	189,928	0.62	48.5	190,696
Sample 3	156,248	0.51	48.9	156,504	157,560	0.51	49.0	158,328
Sample 4	221,976	0.72	47.9	222,232	231,160	0.75	47.6	231,928
Sample 5	179,616	0.58	48.8	179,872	188,424	0.61	47.8	189,192
Sample 6	188,288	0.61	48.6	188,544	195,488	0.64	48.2	196,256
Sample 7	173,920	0.57	48.6	174,176	179,864	0.59	48.6	180,632
Sample 8	209,264	0.68	47.5	209,520	218,448	0.71	47.4	219,216
Sample 9	166,736	0.54	49.6	166,992	176,848	0.58	50.4	177,616
Sample 10	100,040	0.33	51.5	100,296	112,048	0.36	51.3	112,816
Sample 11	174,840	0.57	48.3	175,096	182,720	0.60	48.5	183,506
Sample 12	180,960	0.59	48.0	181,216	183,896	0.60	48.3	184,682
Average		0.58	48.7			0.60	48.7	

payload from the authentication bits should be minimized and yet at the same time effective. Tan et al. had used a 16-bit CRC as the authentication bits for an image with non-overlapping blocks the size of 16×16 pixels, with CRC for each block computed and embedded in its own block [5]. In our enhanced scheme, CRC would be used to authenticate the segments of the ROI individually.

1. Image Preparation

   Our image was divided similar to the TALLOR scheme, with an ROI and eight RONI. But in our enhanced scheme, the ROI was further segmented into non-overlapping blocks of 40×40 pixels and the RONI divided into non-overlapping blocks of 2×2 pixels.

2. Watermark Generation and Embedding

   The watermark consisted of authentication and recovery information. The RONI was further divided into one area for authentication information embedding and one area for recovery information embedding. This allowed separate authentication for different types of information embedded in the RONI. The watermark was embedded in the LSB and second LSB of each pixel in the RONI.

   (a) Authentication

   Each of the 40×40 pixel segments in the ROI was assigned a segment number, $S_{\text{no}} \in \{1, 2, 3, ..., N_s\}$ where N_s equalled the total number of segments. The authentication bits were computed by producing 16-

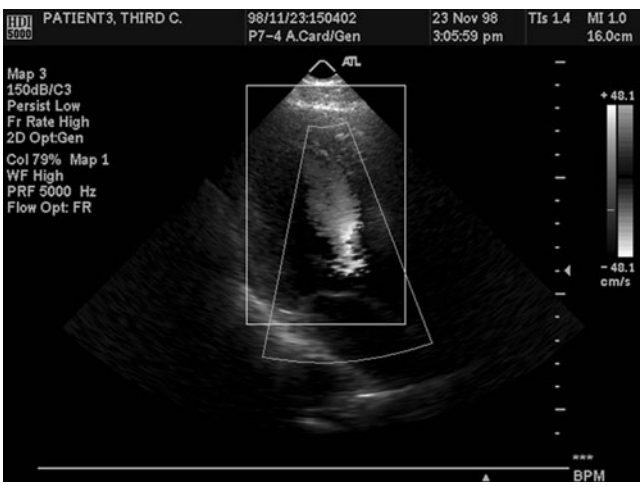

Fig. 4 Image of sample 1 with ROI highlighted

Fig. 5 Image of sample 7 with ROI highlighted

bit ITU-T CRC for each segment in the ROI, denoted as CRC_A. All of the CRC bits computed were gathered to form a single block, denoted as CRC_Block_A. A hash value for the ROI, denoted as ROI_hash_A, was generated by hashing CRC_Block_A with SHA-256. The authentication information was embedded in the designated area in the RONI. The RONI was hashed using SHA-256, producing a hash value, denoted as RONI1_hash_A.

(b) Recovery

Each segment in the ROI was saved in an individual JPEG file, denoted as JPEG_A, and identified by its segment number, S_{no}. The x and y coordinate, denoted as Seg_XY_ROI for each segment in the ROI, was saved. The x and y coordinate, where each JPEG file was embedded in the RONI, denoted as Seg_XY_RONI, was also saved. Both Seg_XY_ROI and Seg_XY_RONI were needed to allow speedy retrieval and recovery of ROI segments. The recovery information was embedded in the designated area in the RONI. The RONI where the embedding process occured was hashed using SHA-256 producing a hash value, RONI2_hash_A.

The summary of the watermark generation and embedding process described above is shown in Fig. 2.

3. Tamper Localization

We began the process of authentication by hashing the RONI where the authentication information was embedded using SHA-256 and produced a hash value denoted as RONI1_hash_B. The embedded RONI1_hash_A was retrieved and compared with RONI1_hash_B. A positive result indicated that the RONI where the authentication information was embedded had not been tampered with and the process of authenticating the ROI could begin.

The ROI was authenticated in three levels:

- Level 1: The ROI was divided into segments and numbered similar to the embedding process. CRC was computed for each segment denoted as CRC_B. The CRC bits were

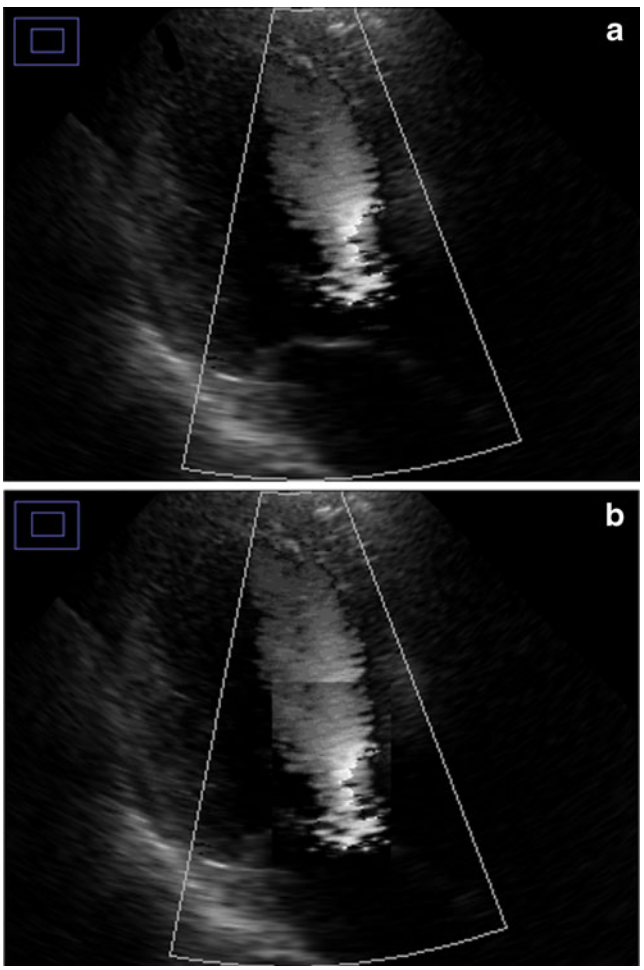

Fig. 6 **a** Magnified ROI of watermarked sample 1, **b** magnified ROI of sample 1 tampered with cloning

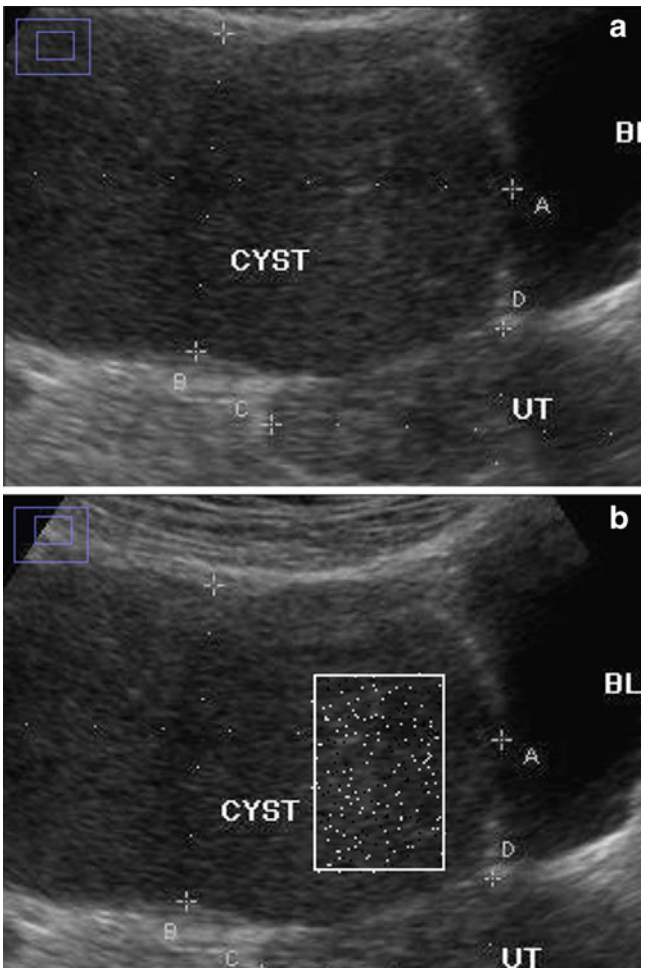

Fig. 7 **a** Magnified ROI of watermarked sample 6, **b** magnified ROI of sample 6 tampered with salt and pepper noise as highlighted

gathered as a block, CRC_Block_B and hashed using SHA-256, producing hash value, ROI_hash_B. ROI_hash_A was retrieved and compared with ROI_hash_B. A positive result indicated that the ROI was authentic and the process of authentication would end. Otherwise, the authentication process would proceed to the next level.

- Level 2 : In the level 2 authentication process, we expected at least one segment of the ROI to have been tampered with. Each segment was authenticated by comparing its retrieved CRC_A from the RONI and the current CRC bits, CRC_B. The tampered segments were recorded in a list denoted as Tampered_S_{no}, using segment number, S_{no}. At the next level, tampered pixel were localized and recovered. The RONI where the recovery information was embedded was hashed, producing a hash value denoted as RONI2_hash_B. The embedded hash value, RONI2_hash_A was retrieved and compared with RONI2_hash_B. When both hash values were equal, then we concluded that the embedded recovery information was authentic.
- Level 3: We retrieved Seg_XY_RONI which stores the location of the JPEG file for each segment. By knowing the location of each JPEG file and reference to Tampered_S_{no}, we were able to perform direct retrieval of only the desired JPEG files. The exact location of the tampered segment in the ROI was known by referring to the embedded Seg_XY_ROI. The retrieved JPEG file, JPEG_A was decoded and compared pixel by pixel with the tampered segment in the ROI. The tampered pixels were localized and recovered using the pixel values from JPEG_A.

The summary of the tamper localization and recovery process described above is shown in Fig. 3.

Results

Using an Intel i3 computer with a 2.93 GHz processor and 4 GB RAM, we determined that 12 different eight-bit monochrome grayscale Digital Imaging and Communications in

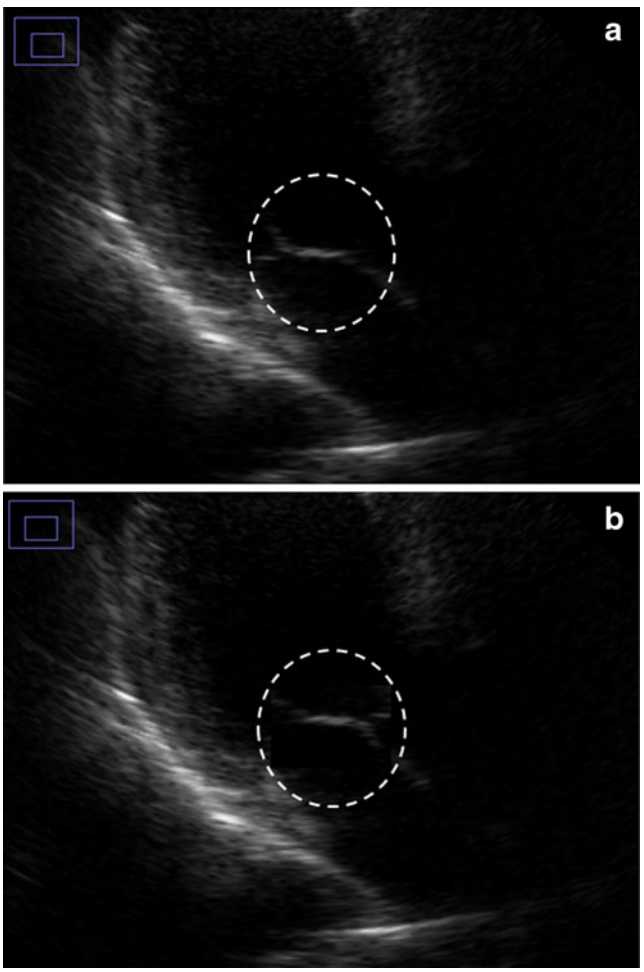

Fig. 8 **a** Magnified ROI of watermarked sample 3, **b** magnified ROI of sample 3 tampered by rotating the highlighted area by 180°

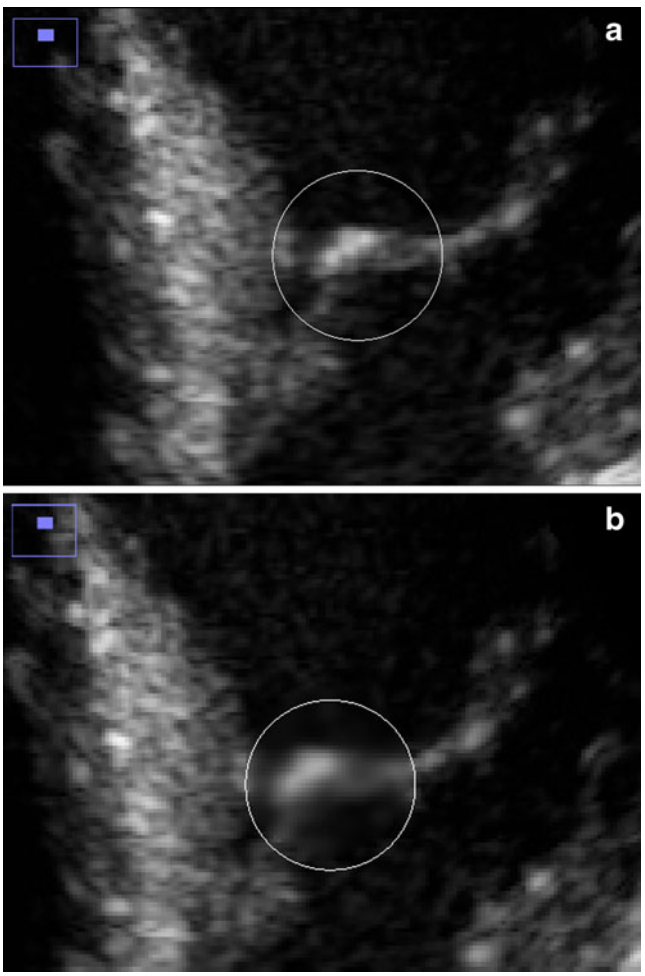

Fig. 9 **a** Magnified ROI of watermarked sample 12, **b** magnified ROI of sample 12 tampered by smoothing the highlighted area

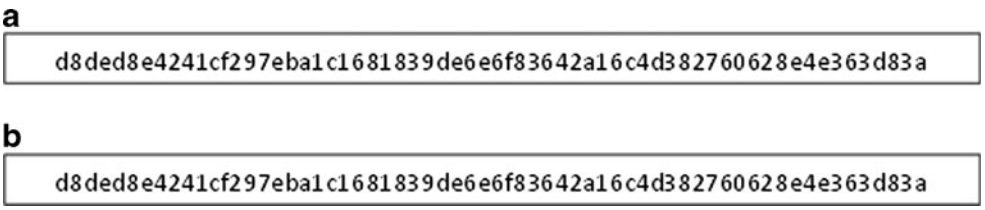

Fig. 10 **a** Hash value from the ROI of the original image of sample 1, **b** hash value from the ROI of the recovered image of sample 1

Medicine format ultrasound images, measuring 640×480 pixels, were watermarked. The ROI had a size of 160×240 pixels and was losslessly compressed. The details of the experiment results for TALLOR and TALLOR-ROI Segmentation and Multilevel Authentication (RSMA) scheme are shown in Table 1. The average compression ratio and peak signal-to-noise ratio (PSNR) achieved for TALLOR were 0.58 and 48.7 dB, respectively. The TALLOR-RSMA scheme achieved an average compression ratio and PSNR of 0.60 and 48.7 dB, respectively. This result showed that the TALLOR-RSMA scheme was as effective as the TALLOR scheme in terms of compression ratio and PSNR. Figures 4 and 5 show the images of samples 1 and 7 with the ROI highlighted.

The watermarked images for all samples were tampered using ImageJ. Samples 1, 5, and 9 were tampered by cloning an area measuring 60×90 pixels. Figure 6 shows the tampering done on sample 1. Samples 2, 6, and 10 were tampered by adding salt and pepper noise in the ROI, with the tampered area measuring 60×90 pixels. Figure 7 shows the tampering done on sample 6. We next tampered samples 3, 7, and 1 by rotating a portion of the ROI by 180°. Figure 8 shows the tampering done on sample 3. Samples 4, 8, and 12 were tampered by smoothing an area within the ROI. Figure 9 shows the tampering done on sample 12.

We recovered tampered samples successfully using TALLOR and TALLOR-RSMA scheme. Further testing was done to verify the content of the recovered images. The ROI of the original image and recovered image were hashed using SHA-256. The hash values from the ROI of the original image and recovered imaged were compared for all samples. The results showed that hash values were equal, indicating that the content of the ROI of the recovered image was identical to the ROI of the original image. Figure 10 shows the hash values from sample 1.

The processing time taken for the tamper localization and recovery for the TALLOR and TALLOR-RSMA schemes had an average time of 28.5 and 14.2 s, respectively as shown in Table 2. A standard *t* test performed on the data collected showed that the value of *p* was less than 0.0001, indicating that the difference is statistically significant (Figs. 11, 12, 13, and 14).

Table 2 Tamper localization and recovery processing time in seconds

Figure	Tampering	TALLOR	TALLOR-RSMA
Sample 1	Cloning	28.0	14.1
Sample 2	Salt and pepper	27.8	13.9
Sample 3	Rotation	21.3	9.6
Sample 4	Smoothing	36.7	12.8
Sample 5	Cloning	25.4	12.4
Sample 6	Salt and pepper	29.0	14.0
Sample 7	Rotation	23.5	11.5
Sample 8	Smoothing	31.2	15.4
Sample 9	Cloning	31.5	18.1
Sample 10	Salt and pepper	21.0	16.4
Sample 11	Rotation	33.9	18.4
Sample 12	Smoothing	32.0	13.3
	Average	28.5	14.2

Discussion and Conclusion

In our TALLOR-RSMA scheme, which is the enhancement of the TALLOR scheme, the quality of the watermarked images is high, with the average PSNR of 48.7 dB for the proposed scheme. This high PSNR indicated low distortion in the watermarked image. The TALLOR-RSMA achieved an average compression rate of 0.60, comparable to the TALLOR scheme. For all samples, the tampered ROI was localized and recovered with 100 % success. The recovered images were identical with the original images. This was verified when we compared the hash values from the original and recovered images. The quality of the recovered area was high where the pixels values were retrieved from the JPEG file

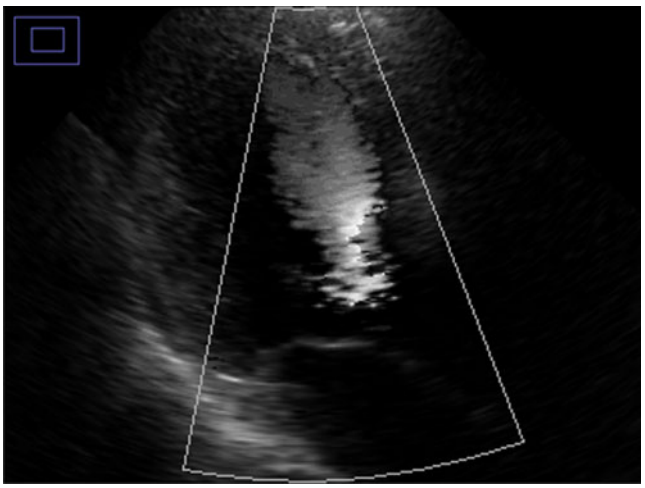

Fig. 11 Recovered image of sample 1

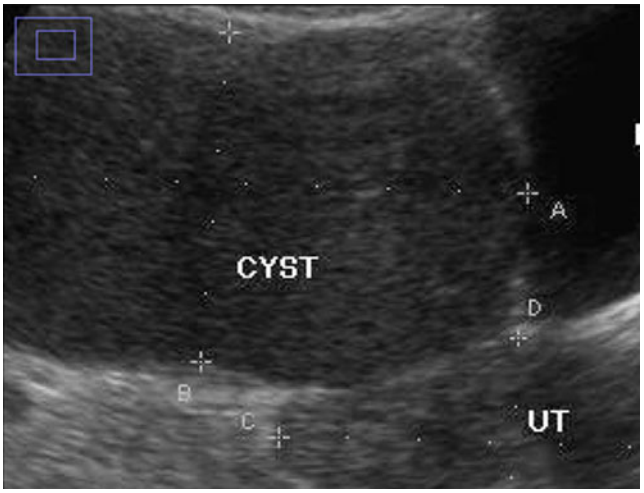

Fig. 12 Recovered image of sample 6

which had been losslessly compressed. The pixel values were the exact values originated from the nontampered ROI. Due to its high quality, the recovered ROI may be used for diagnoses purposes.

The method we used in the TALLOR-RSMA scheme proved effective in reducing the tamper localization and recovery average processing time by approximately 50 % compared with the TALLOR scheme as shown in Table 2. This reduction for TALLOR-RSMA is considered to be statistically significant based on the *t* test performed. A user may retrieve a watermarked image from the server and request it to be authenticated. A watermarked image may be tampered intentionally and unintentionally. If the image has been found to be tampered, the recovery of the image will take place. As a result, the use of ROI segmentation and multilevel authentication in the TALLOR-RSMA scheme during the tamper detection and recovery process can significantly reduce the time a user waits as well as save expensive server computing time.

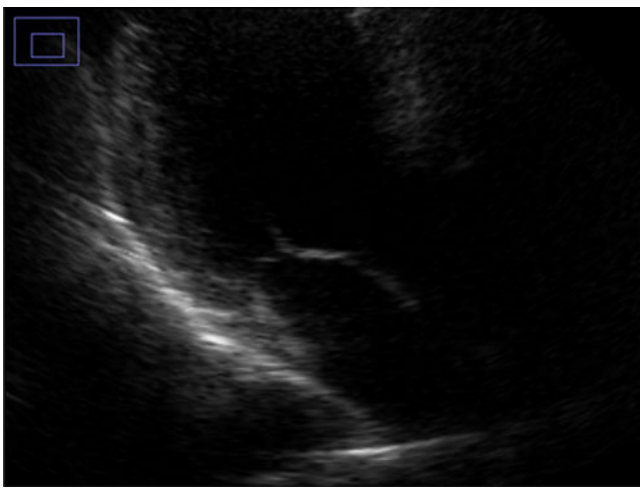

Fig. 13 Recovered image of sample 3

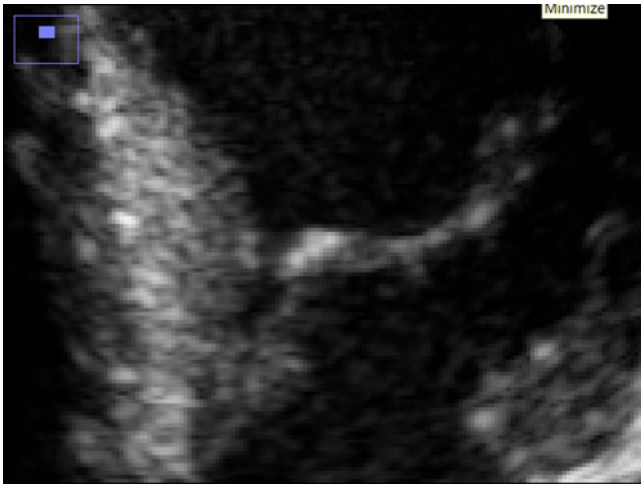

Fig. 14 Recovered image of sample 12

For the purpose of comparison, we used a tamper localization and recovery scheme for medical images proposed by Osamah and Khoo previously described with available data and similar functions to our proposed watermark scheme [12]. The data provided by Osamah and Khoo were based on an experiment performed on an ultrasound image [12]. The comparison details in Table 3 show that our TALLOR-RSMA scheme is better in terms of embedding capacity and PSNR. The tamper localization accuracy of our proposed scheme is at one pixel compared with 16×16 pixels in the Osamah and Khoo scheme. The recovered ROI produced by our scheme is also of better quality due to exact recovery achieved, where as only approximate recovery was achieved by the Osamah and Khoo scheme. Our proposed scheme maintains the originality of the ROI where the watermark is embedded in the RONI. By contrast, the compared scheme embeds part of the watermark in the ROI, which needs to be reversed later on.

Because our proposed scheme was designed based on the characteristics of the ultrasound images, it cannot be used

Table 3 Comparison of TALLOR-RSMA scheme with Osamah and Khoo scheme

	Osamah and Khoo [12][a]	TALLOR-RSMA (sample 1)
Image size	576×768.8 bit	640×480.8 bit
Watermark size (bits)	136,780	177,008
Embedding capacity (bits per pixel)[b]	0.31	0.58
PSNR (dB)	36.7	48.3
Localization accuracy (pixel)	16×16	1
ROI recovery	Approximate	Exact

[a] Ultrasound image

[b] Embedding capacity=watermark size/image size

for images from other modalities. For future work, however, the TALLOR-RSMA scheme could be further developed for the use of multiframe ultrasound images and other modalities. Other lossless compression such as arithmetic encoding, Huffman code, and JPEG2000 could be tested to achieve better compression rate allowing larger ROI to be defined.

References

1. Cox IJ, Miller ML, Bloom JA: Digital watermarking. Morgan Kaufmann, San Francisco, 2002
2. Cao F, Huang H-K, Zhou X-Q: Medical image security in a HIPAA mandated PACS environment. Comput Med Imaging Graph 27:185–196, 2003
3. Liu T, Qiu Z-D: The survey of digital watermarking-based image authentication techniques in Proceedings of the 6th International Conference on Signal Processing. 2002
4. Guo X, Zhuang T: Lossless watermarking for verifying the integrity of medical images with tamper localization. J Digit Imaging 22 (6):620–628, 2009
5. Tan C-K, Ng C, Xu X, Poh C-L, Yong L-G, Sheah K: Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability. J Digit Imaging 24(3):528–540, 2011
6. Wu X: Reversible semi-fragile watermarking based on histogram shifting of integer wavelet coefficients in Proceedings of Inaugural IEEE-IES Digital EcoSystems and Technologies Conference. 2007
7. Liu Y, Mei L, Liu Q, Jiang X: A high-tamper localization capability of image authentication algorithm in Proceedings IEEE International Conference on Computer Science and Automation Engineering. 2011
8. Guo J, Qiu W, Li P: Fragile watermarking scheme with pixel-level localization. commun comput inf sci 228(1):109–115, 2011
9. Yang C-W, Shen J-J: Recover the tampered image based on VQ indexing. Signal Process 90(1):331–343, 2010
10. Chiang K, Chang K, Chang R, Yen H: Tamper detection and restoring system for medical images using wavelet-based reversible data embedding. J Digit Imaging 21:77–90, 2008
11. Tian J: Reversible data embedding using a difference expansion. IEEE Trans Circuits Syst Video Technol 13(8):890–896, 2003
12. Osamah M, Khoo B-E: Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. J Digit Imaging 24:114–125, 2011
13. Wu JHK, et al: Tamper detection and recovery for medical images using near-lossless information hiding technique. J Digit Imaging 21(1):59–76, 2008
14. Zain JM, Fauzi ARM: Medical image watermarking with tamper detection and recovery in Proceedings of the 28th IEEE EMBS Annual International Conference. 2006
15. Liew S-C, Zain JM: Tamper localization and lossless recovery watermarking scheme. Commun Comput Inf Sci 179(1):555–566, 2011