J Inf Process Syst, Vol.11, No.4, pp.601~615, December 2015
http://dx.doi.org/10.3745/JIPS.03.0044

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

# Secured Telemedicine Using Whole Image as Watermark with Tamper Localization and Recovery Capabilities

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

**Abstract**

Region of interest (ROI) is the most informative part of a medical image and mostly has been used as a major part of watermark. Various shapes ROIs selection have been reported in region-based watermarking techniques. In region-based watermarking schemes an image region of non-interest (RONI) is the second important part of the image and is used mostly for watermark encapsulation. In online healthcare systems the ROI wrong selection by missing some important portions of the image to be part of ROI can create problem at the destination. This paper discusses the complete medical image availability in original at destination using the whole image as a watermark for authentication, tamper localization and lossless recovery (WITALLOR). The WITALLOR watermarking scheme ensures the complete image security without of ROI selection at the source point as compared to the other region-based watermarking techniques. The complete image is compressed using the Lempel-Ziv-Welch (LZW) lossless compression technique to get the watermark in reduced number of bits. Bits reduction occurs to a number that can be completely encapsulated into image. The watermark is randomly encapsulated at the least significant bits (LSBs) of the image without caring of the ROI and RONI to keep the image perceptual degradation negligible. After communication, the watermark is retrieved, decompressed and used for authentication of the whole image, tamper detection, localization and lossless recovery. WITALLOR scheme is capable of any number of tampers detection and recovery at any part of the image. The complete authentic image gives the opportunity to conduct an image based analysis of medical problem without restriction to a fixed ROI.

**Keywords**

Lossless Recovery, Tamper Localization, Telemedicine, Watermarking, Whole Image, WITALLOR

## 1. Introduction

In the current era of image processing research, different security techniques, including cryptography, have been used for medical image security [1]. It has been observed that well-known cryptographic algorithms, such as AES, IDEA, and Triple-DES, are too weak to protect digital image contents in online digital communication systems. SHA-256 is a cryptographic hash function used to produce an image hash code for authentication without having tamper detection and recovery capabilities. Similarly, steganography is the inventory version of watermarking used for secret communication of special information in digital images [2]. Steganography is used only for


Manuscript received December 3, 2014; first revision June 30, 2015; accepted October 15, 2015; onlinefirst December 17, 2015.
**Corresponding Author:** Gran Badshah (gran16178@gmail.com)
* Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang, Malaysia (gran16178@gmail.com, {liewsc, jasni}@ump.edu.my, sunnyswa@hotmail.com)

communicating secret messages rather than giving any security to the contents of an image. The main common disadvantage of cryptography and steganography is that they have no capability of reversing the corrupted data to its original status. In case of data corruption they only report and might make a request for the same data retransmission. The retransmission wastes the system's precious time and causes possible repetitive corruption of the data. The watermarking technique does not require data retransmission in case of data corruption because the image carries information secretly as a watermark within itself in such a way that it can be used to preserve the image diagnostic and perceptual qualities. After the image communication the watermark can be extracted and used for data authentication, tamper localization, and lossless recovery [3,4]. Watermarking is a security technique that is applicable to any multimedia contents, including digital images and has the capability of copyright protection, controlling data duplication, tamper localization, and lossless recovery [5].

Teleradiology is one of the telemedicine applications used to store and forward medical images to remote destinations. These images may lose information due to noises and manipulations by hackers during communication, which is not tolerable in the case of medical images [6]. The affected data may become an obstacle in diagnostic analysis at the destination. Different watermarking techniques are available for image security, but are restricted to a specific part known as ROI. Considering only the ROI and the negligence of around parts makes the image based diagnosis weak. Therefore, complete data protection for a medical image is necessary in online distributed healthcare systems to make sure the complete image originality for effective diagnosis. The complete image protection in teleradiology gives an independent selection opportunity of ROI at the destination according to the physician's desire. The complete image protection can also solves the problem of ROI separation from RONI, which has been found problematic for most of medical images [7]. At destination, the authentication and recovery process make sure the originality of the communicating image. For authentication, a hash function is used to get the hash code of the communicated image and is compared to the authentication part of the extracted watermark. The tampered parts of the image are detected, localized and lossless recovered using the recovery part of the extracted watermark.

This paper is organized as follows: Section 2 discusses the watermarking related work already done. In Section 3, we propose WITALLOR watermarking scheme. Section 4 consists the discussion of the results and Section 5 concludes the paper.

## 2. Related Work

The recent improvements in information and communication technologies have enhanced the quality of healthcare services. New medical practices such as telemedicine have been introduced to make ease the medical services provision. Telemedicine has made possible the exchange of medical images and electronic healthcare records among the professionals and healthcare facilities centers all over the world [8]. Telesurgery, distant learning, telediagnoses, and teleradiology are the well-known healthcare applications of telemedicine. Teleradiology is used to communicate, store, share, and restore medical images in online healthcare environments that require strict security [9]. The three important requirements of integrity, confidentiality, and authentication must be fulfilled at the same time to provide the secured communication of medical images [10]. Integrity means that the image has not been altered at any level; confidentiality means that only the authorized users can access the image; and

authentication ensures that the image is associated with a unique patient who makes a claim from a correct source [11]. In this paper, the least significant bit (LSB) based spatial domain watermarking methodology has been used for complete image security. Our method is an updated version of ROI based tamper detection and a recovery watermarking scheme [12]. In this technique, only ROI information is embedded into RONI part of image at LSBs. Setting all of the LSBs to zero after watermark extraction is the main disadvantage of this scheme. This setting degrades the recovered image quality because all of the LSBs are not definitely zero before watermark embedding. As such, our aim is to guarantee the complete recovery of an image, to recover all the tampered parts to their original status and to make image secure from degradation. Although the insertion of additional data causes distortion in images and cannot be used for diagnostic purposes [13] but our method can recover the distorted image to original status. In our methodology first the whole image is compressed using the LZW technique and then randomly embedded into image at the same time without caring of ROI and RONI. At the destination, the watermark is extracted, decompressed and used for complete image authentication and lossless recovery.

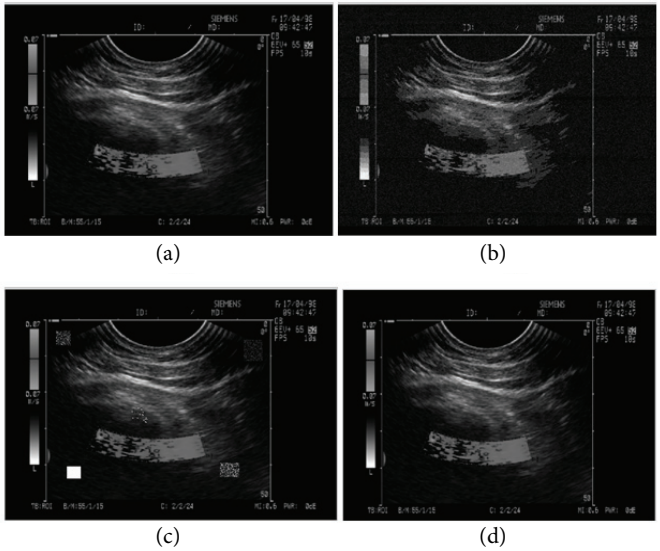
## 3. Proposed Methodology

In this paper, a new whole image authentication, tamper localization and lossless recovery (WITALLOR) scheme has been developed. Securing the entire image becomes possible if all of the image information is used as a watermark. For this purpose the complete image pixels data information and its hash code are combined to get a single watermark. The watermark is compressed using the LZW lossless compression technique [14]. LZW compression reduces the watermark bits to a lower number in such a way that can be easily encapsulated into an image at LSBs [15]. At destination, the extracted watermark is used for image authentication, tamper localization and lossless recovery. The hash part of the watermark is used for image authentication, while the pixel data information is used for tamper detection, localization and lossless recovery.

The WITALLOR scheme has the capability to locate and lossless recover the tampers occurred at any part of the image. It is easy to illegally modify medical images for non-mandatory purposes in order to deceive a non-protected system, such as the health insurance system of an organization, to approve fake medical records [16]. The ultrasound medical image shown in Fig. 1(c) has been tampered with using "ImageJ" software at five different sports (in the center and four corners) to test the WITALLOR scheme for authentication, tamper detection, localization and lossless recovery as carried out and shown in Fig. 1(d). Table 1 shows the noises that were added to the image and PSNR was used to measure the watermarked image quality.

**Table 1.** Details of noises added to image sample 1 as shown in Fig. 1(c)

| No. | Added noise | PSNR (dB) |
|---|---|---|
| 1 | 60% specified noise | 25 |
| 2 | Added noise | 25 |
| 3 | Salt and pepper noise | 25 |
| 4 | Cropped the image | 25 |
| 5 | 80% specified noise | 25 |



(a) (b)

(c) (d)

**Fig. 1.** (a) Ultrasound original image sample 1, (b) watermarked image, (c) tampered image, and (d) recovered image.

Image authentication is the process to know either the image has been tampered or not [17]. After the watermark extraction at destination, the hash code is separated from the image pixel data. The communicated image is hashed and the code is noted. Now the noted and extracted codes are compared; if the codes are same then the image is safe and has not been tampered. At this time there is no need to perform tamper detection and recovery process. If both the codes are not same to each other it means that the image has been tampered and needs the processes of tamper detection and recovery.

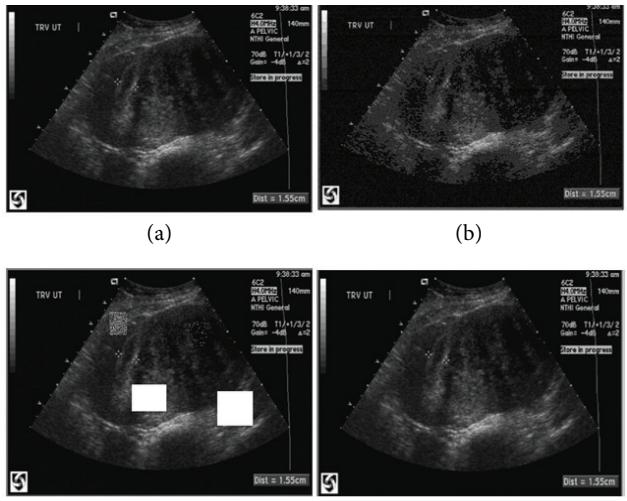
In this research, 10 different samples of ultrasound medical images shown in Figs. 1–10 were processed to check the proficiency of the WITALLOR scheme for tamper detection and recovery purposes. In each case, the original image was taken as the major part of watermark and compressed using the LZW lossless compression technique. The image was tempered by adding different noises, such as salt and pepper, adding noise by percentage and cropped the image for noise inducement. Each time tampers were successfully detected and lossless recovered. The results in Table 2 show that WITALLOR is an efficient scheme.

We used five LSBs of the manipulated pixels for watermark insertion into image and were found correct for the complete compressed image as watermark encapsulation. The watermark retrieval and reshaping to the image size for tamper detection and recovery were all accurately performed.

Before watermark compression for image sample 1, the image pixels were arranged in a single row array, from 1 to the image size 480×640 (1–307200). This array was divided into five equal segments (307200/5 = 61440 pixels). The image hash code was combined to the first segment; each segment was converted to binary and compressed separately to prevent the formation of binary long sequences for saving the watermark compression time. The compressed watermark is the combination of codes used to represent binary sequences. The maximum value of each translated code was checked and multiplied by an appropriate value to get the subsections of the watermark. The appropriate value here is the one that fully represents a maximum code in a binary format. All of the five compressed binary subsections of watermark were recombined as a single watermark to make ready for insertion into image.

There are different gray levels imaging systems such as 8-bits (0–255), 9-bits (0–511), 10-bits (0–1023), 11-bits (0–2047), 12-bits (0–4095), 13-bits (0–8191), 14-bits (0–16383), 15-bits (0–32767), and others. Table 3 shows that all the code values fall in the range of 15-bits so we represented every compressed element multiple of 15 to get its binary for embedding and decompression.

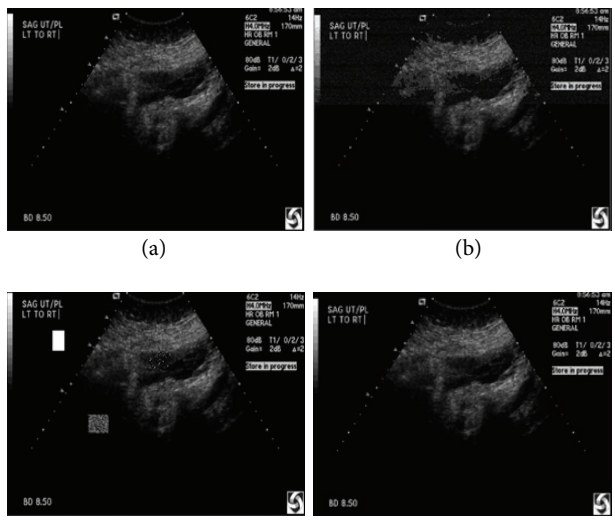
Fig. 1(a)–(d) show the original, watermarked, tampered and lossless recovered versions of the image sample 1, respectively. The WITALLOR scheme performs the same process for the remaining samples 2–10 in the same way, as shown in Figs. 2–10. The results in Table 2 show the successful performance of the WITALLOR scheme.




(a) (b)

(c) (d)

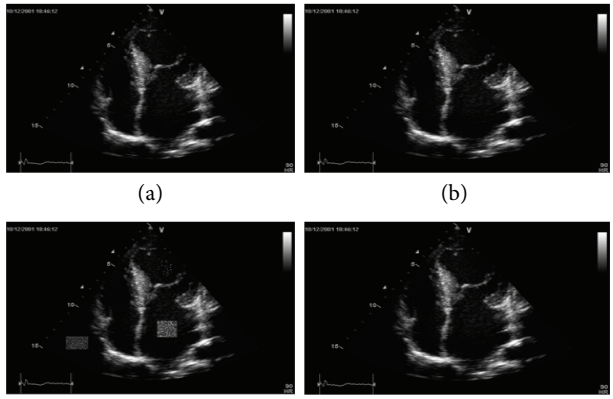
**Fig. 2.** (a) Ultrasound original image sample 2, (b) watermarked image, (c) tampered image, and (d) recovered image.




(a) (b)

(c) (d)

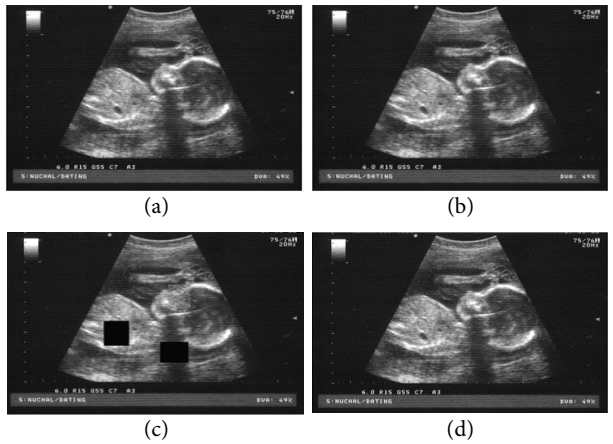
**Fig. 3.** (a) Ultrasound original image sample 3, (b) watermarked image, (c) tampered image, and (d) recovered image.



(a) (b)

(c) (d)

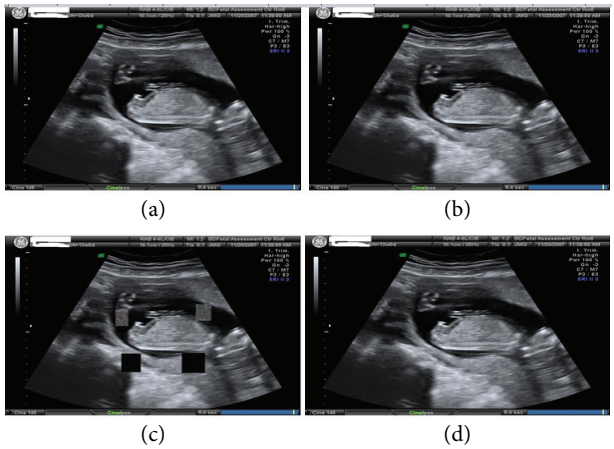
**Fig. 4.** (a) Ultrasound original image sample 4, (b) watermarked image, (c) tampered image, and (d) recovered image.



(a) (b)

(c) (d)

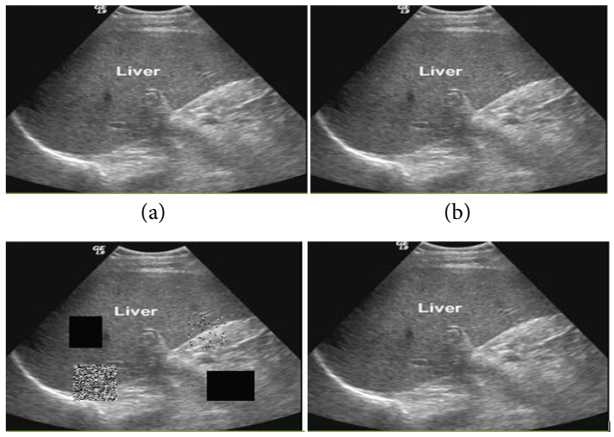
**Fig. 5.** (a) Ultrasound original image sample 5, (b) watermarked image, (c) tampered image, and (d) recovered image.



(a) (b)

(c) (d)

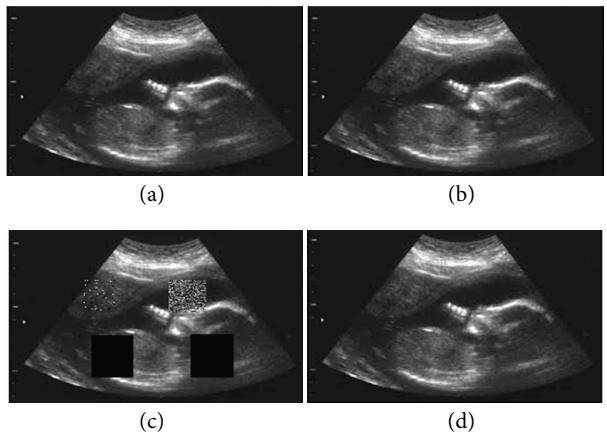
**Fig. 6.** (a) Ultrasound original image sample 6, (b) watermarked image, (c) tampered image, and (d) recovered image.




(a) (b)

(c) (d)

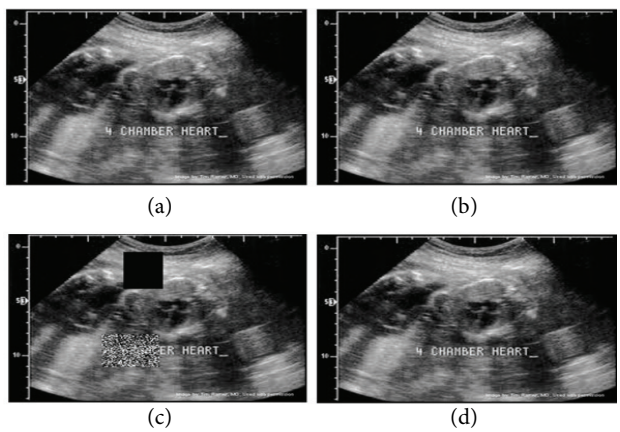
**Fig. 7.** (a) Ultrasound original image sample 7, (b) watermarked image, (c) tampered image, and (d) recovered image.



(a) (b)

(c) (d)

**Fig. 8.** (a) Ultrasound original image sample 8, (b) watermarked image, (c) tampered image, and (d) recovered image.




(a) (b)

(c) (d)

**Fig. 9.** (a) Ultrasound original image sample 9, (b) watermarked image, (c) tampered image, and (d) recovered image.

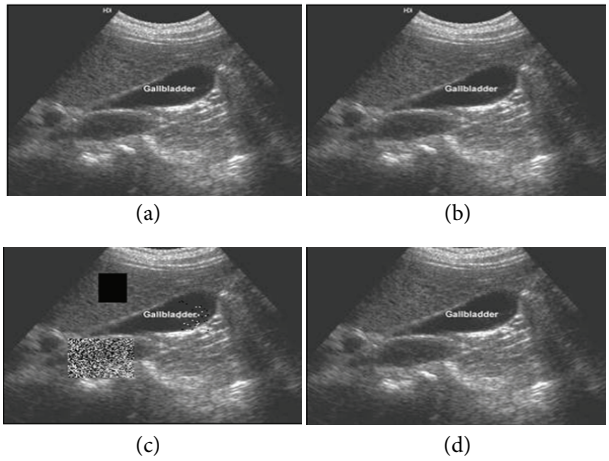



**Fig. 10.** (a) Ultrasound original image sample 10, (b) watermarked image, (c) tampered image, and (d) recovered image.

**Table 2.** WITALLOR watermarking scheme application on ten samples

| Sample no. | Total number of bits | LZW compressed watermark bits | Compression ratio | PSNR of watermarked image (dB) | PSNR in terms of recovery |
|---|---|---|---|---|---|
| 1 | 2457600 | 1470900 | 0.598511 | 24.8961 | Lossless recovered |
| 2 | 2457600 | 1536000 | 0.625 | 14.2380 | Lossless recovered |
| 3 | 2457600 | 667125 | 0.271454 | 14.4590 | Lossless recovered |
| 4 | 2457600 | 667120 | 0.271452 | 23.5562 | Lossless recovered |
| 5 | 3886920 | 1526000 | 0.392599 | 24.2314 | Lossless recovered |
| 6 | 1550000 | 956000 | 0.616774 | 23.4321 | Lossless recovered |
| 7 | 1516000 | 816000 | 0.538259 | 22.5647 | Lossless recovered |
| 8 | 152389 | 50500 | 0.331389 | 25.4512 | Lossless recovered |
| 9 | 154164 | 93400 | 0.605848 | 24.7634 | Lossless recovered |
| 10 | 1551296 | 142300 | 0.09173 | 26.2346 | Lossless recovered |
| Average | 1864117 | 792534 | 0.434302 | 22.38267 | - |

**Table 3.** WITALLOR watermarking scheme results for watermark preparation of ultrasound medical image sample 1

| Segment no. | Number of bytes | Number of compressed bytes | Max element of compressed bytes | Number of equivalent binary values |
|---|---|---|---|---|
| 1 | 61440 | 14287 | 14240 | 14287×15 = 214305 |
| 2 | 61440 | 26811 | 26732 | 26811×15 = 402165 |
| 3 | 61440 | 26986 | 26847 | 26986×15 = 404790 |
| 4 | 61440 | 24564 | 24511 | 24564×15 = 368460 |
| 5 | 61440 | 5412 | 5412 | 5412×15 = 81180 |
| Total | 307200 (image size) | 98060 | - | 1470900 (watermark) |

The tabulated results in Table 2 show that the lossless recovery of tampered images was successful, as can be seen from the PSNR values. The PSNR calculating formula was activated between the original and recovered images. It shows that the WITALLOR watermarking scheme provides 100% efficiency.

## 3.1 Watermark Compression and Embedding into Image

For LZW compression, first the watermark is converted to binary and stored in a single row array. This conversion results in a series of unique binary sequences, which help the watermark good compression. During compression, every unique sequence is replaced by a decimal number, which is called a decimal code. A string array named as dictionary is created and initialized to two stings (i.e., '0' and '1'). There are only two unique values in the watermark binary stream, otherwise the dictionary values can vary in the case of English sentence compression. Here, the combinations of binaries from a binary stream give different repeating sequences, which result in new strings. The resultant unique strings are inserted in the dictionary and a decimal code is allotted to every string. The allotted decimal codes are stored into another defined array called codes table. LZW Algorithm 1 checks the availability of the newly constructed strings in the dictionary. In case of uniqueness, the strings and the allotted codes are inserted in the dictionary and codes table respectively. This process of unique strings formation, codes allocation and insertions continue until the whole watermark is compressed. As the result, the code table values collectively give the compressed watermark. Algorithm 1 explains the step-by-step process of watermark lossless compression. The final dictionary and codes table are used for watermark lossless decompression after the watermark extraction at the destination.

**Algorithm 1.** Binary watermark lossless compression using the LZW technique

1. Convert the whole image watermark to binary
2. Initialize Dictionary={'0', '1'}
3. Unique String formation = get the first binary from the whole image watermark binary
4. WHILE access the succeeding available binary from the binary stream and continue
5. Succeeding-binary = Get the next binary
6. IF String + Succeeding-binary exists in the Dictionary then
7. String = String + Succeeding-binary
8. ELSE
9. Assign decimal code to the String and insert in the Codes Table
10. Add String + Succeeding-binary to the Dictionary
11. String= Succeeding-binary
12. END of IF
13. END of WHILE
14. Output the final Dictionary and Codes Table

## 3.2 Watermark Extraction, Decompression, Image Authentication, Tamper Localization, and Lossless Recovery

At the destination, watermark is retrieved from the communicated image and decompressed through the LZW Algorithm 2. First, the extracted watermark is divided into the image pixel information and its

hash. The hash part is reconverted to 64-bytes hexadecimal code and the pixel data is resized to the size of the original image. The hash code and image pixel data are used for image authentication, tamper localization and recovery respectively.

For watermark extraction, the modified LSBs of the communicated image, modified during the watermark encapsulation are accessed for the retrieval of all hidden bits. At the completion of bits retrieval, all of the bits are converted back to the decimal codes. The decimal codes that equaling the binary sequences, as already stored in the dictionary are accessed for watermark decompression. The accessed binary sequences are recombined to get back the watermark in form of a binary stream. The watermark decompression process is started from a null string definition, as shown in Algorithm 2. At the start, the first code equaling string is accessed and stored as a string. Then, the second code equaling string is accessed and concatenated to the first accessed one. In the same way, the third code equaling string is concatenated to the previously combined string and this process goes on until the watermark complete decompression. Ultimately, all of the codes and their equaling strings are accessed and a single row binary stream is obtained as a lossless decompressed watermark. After watermark lossless decompression, it exists as it was before compression without any bit loss. Algorithm 2 describes the step-by-step process of LZW lossless decompression.

**Algorithm 2.** Binary compressed watermark decompression using the LZW technique

```
String= Null
Access the first code from the code table
String=String + the first code equaling string in the Dictionary
Counter=1
While there are still Codes to process Do
    Counter= Counter+1
    Next-string= Access the Counter code equaling the string in the dictionary
    String=String + Next-string
    Output String
End While
```

Algorithm 2 works to decompress the watermark using the code table and dictionary values. As the second step of decompression, the first element of the dictionary is accessed on the basis of the first element of the code table and is concatenated to the null string. Then, the process of decompression goes ahead in a loop and the third dictionary string is accessed using the third code from the code table. At watermark decompression, the watermark is divided into authentication and recovery parts for authentication, tamper localization and recovery operations.

## 3.3 Image Authentication

The watermarked image hash value is calculated before and after communication, as shown in Figs. 11 and 12. By comparison, if both the values are the same, this means that the image has not been

tampered and there is no need to carry out WITALLOR processing for recovery. If both the values do not match each other then it means the image has been tampered and needs recovery, as done for image sample 1 shown in Fig. 1(d).

**1f620832414583892bf2a9f226f7274892ef3c6931a074144dd86818e62a814b3**

**Fig. 11.** Sample 1 image hash before watermarking.

**3b9e407e9accf5fb340c2f2642d624ea3e004f1bc1f00981c59b8819f08df4f7**

**Fig. 12.** Sample 1 image hash after watermark extraction.

This is clear that both of the values do not match each other, which means the image has been tampered and recovery is required. This process is repeated for all the other samples too. If the image has not been tampered and has safely communicated, then both of the hash values will be same, as shown in Figs. 13 and 14. There is no need to run the WITALLOR scheme further and the image safely communication is reported, as shown in Fig. 15.

**h1=6e340b9cffb37a989ca544e6bb780a2c78901d3fb33738768511a30617afa01d**

**Fig. 13.** Sample 1 image hash before communication.

**h2=6e340b9cffb37a989ca544e6bb780a2c78901d3fb33738768511a30617afa01d**

**Fig. 14.** Sample 1 image hash after communication.

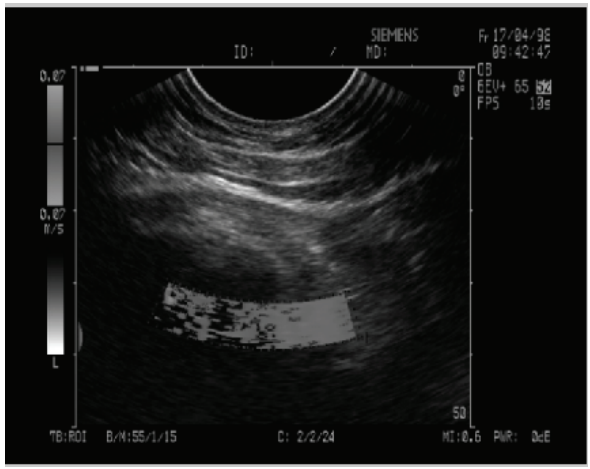



**Fig. 15.** Sample 1 image safely communicated without any tamper.

## 3.4 Tamper Detection and Lossless Recovery

If the communicated image is not found authentic, then the image needs to be recovered. The recovery must be lossless because the recovered image may be used for diagnostic purposes [18,19]. The

extracted watermark pixel data part, which is also called the recovery part, is used for this operation. The watermark recovery part is the information of the complete original image in pixel format. Before starting tamper detection and recovery process, the recovery part is first resized to the size of the original image. The resized part is compared in a 1:1 mapped format to the image. The tamper detection is started at the first pixel of the image. The first value is compared to the first pixel of the image; the second pixel value is compared to the second pixel and so on. The 1:1 mapped comparison is completed between the recovery part of the watermark and the image. During the comparison, if both of the values are different then the differed pixels are noted as tampered pixels and are replaced by the watermark recovery part corresponding pixels. All of the comparisons and recoveries are completed in the same way and the image is restored to its original status. For image sample 1 the tampered image shown in Fig. 1(c), tampered by adding different type tampers as tabulated in Table 1 has been recovered as shown in Fig. 1(d). To know about the qualities of the tampered and recovered images, the PSNR value is calculated as shown in Tables 1 and 2. WITALLOR uses two defined functions: one calculates the PSNR of the watermarked image and the other calculates PSNR value for the recovered image. Function defines how much the image is degraded; otherwise it signals that the recovered image is same as the original one.

## 4. Results Discussion

The watermark lossless compression at half of its size tabulated in Table 3, shows that LZW lossless compression technique performance is very good. Checking WITALLOR for image sample 1, the image was tampered using ImageJ software at five different places. The image was tampered from left to right and top to bottom, 60% specified noise addition of standard deviation, simple added noise, salt and pepper noise, cropped the image and specified added noise 80% as tabulated in Table 1. During the tamper detection and recovery process, the tampers were localized at specified positions and lossless recovery was carried out, as shown in Fig. 1(d). Noises added to the image for tampering purposes, degrade the image as the PSNR value is 25 dB shown in Table 1. The 25-dB PSNR value means that the image is highly degraded. The recovery of this degraded image is 100%, as shown in Table 2. The recovered image is perceptually identical to the original one, as can be compared from Fig. 1(a) and (d). This means that the image has been completely recovered. The same processes were repeated for all of the other samples. The PSNR values of the recovered images listed in Table 2 show the good performance of WITALLOR as the values are more than 30 and lossless because the original and the recovered images are perceptually the same.

## 5. Conclusions

In this paper, we used 10 different samples of ultrasound medical images for experiments. All of the samples were grayscale 8-bit images. In each case, the whole image was used as the major part of watermark, compressed and embedded into image at the LSBs. The watermark bits were perfectly retrieved and used for successful authentication and lossless recovery of the image. The average PSNR values of more than 40 dB of watermarked and recovered images indicate the good quality of

watermarked and recovered images, as shown in Table 2. The PSNR of recovered images shows the exact and lossless recovery of tampered images for the original diagnostic capabilities of medical images. The more bits reduction during watermark compression and a good compression ratio of less than one show the good compression capability of the LZW technique. The security of the complete image makes free the user from defining only a specific part important as ROI, while leaving the rest of image at risk. Sometimes, incorrectly defining the ROI by missing some important data around can make the watermarking scheme useless. The wrong selection of ROI can directly affect the exact or lossless recovery of the image. If the important area is not perfectly recovered it can devalue the treatment process, which could lead to a non-recoverable loss. The WITALLOR watermarking scheme can be made more effective by repeatedly applying the LZW algorithm to the compressed watermark data. Theoretically we can say that the repetitive application of LZW algorithm to watermark for compression will results effectively in bits reduction and image watermarking with a less number of bits.

## References


[1] J. X. Chen, Z. L. Zhu, and H. Yu, "A fast chaos-based symmetric image cryptosystem with an improved diffusion scheme," *Optik - International Journal for Light and Electron Optics,* vol. 125, no. 11, pp. 2472-2478, 2014.

[2] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727-752, 2010.

[3] J. Pan, J. Zheng, and G. Zhao, "Blind watermarking of NURBS curves and surfaces," *Computer-Aided Design,* vol. 45, no. 2, pp. 144-153, 2013.

[4] F. Y. Shih and Y. T. Wu, "Robust watermarking and compression for medical images based on genetic algorithms," *Information Sciences,* vol. 175, no. 3, pp. 200-216, 2005.

[5] N. Wang and C. Men, "Reversible fragile watermarking for 2-D vector map authentication with localization," *Computer-Aided Design,* vol. 44, no. 4, pp. 320-330, 2012.

[6] J. C. Garcia-Alvarez, H. Fuhr, and G. Castellanos-Dominguez, "Evaluation of region-of-interest coders using perceptual image quality assessments," *Journal of Visual Communication and Image Representation*, vol. 24, no. 8, pp. 1316-1327, 2013.

[7] M. M. Abd-Eldayem, "A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine," *Egyptian Informatics Journal*, vol. 14, no. 1, pp. 1-13, 2013.

[8] B. Davie, V. Florance, A. Friede, J. Sheehan, and J. E. Sisk, "Bringing health-care applications to the internet," *IEEE Internet Computing*, vol. 5, no. 3, pp. 42-48, 2001.

[9] F. J. McEvoy and E. Svalastoga, "Security of patient and study data associated with DICOM images when transferred using compact disc media," *Journal of Digital Imaging*, vol. 22, no. 1, pp. 65-70, 2009.

[10] R. Norcen, M. Podesser, A. Pommer, H. P. Schmidt, and A. Uhl, "Confidential storage and transmission of medical image data," *Computers in Biology and Medicine*, vol. 33, no. 3, pp. 277-292, 2003.

[11] L. O. M. Kobayashi, S. S. Furuie, and P. S. Barreto, "Providing integrity and authenticity in DICOM images: a novel approach," *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, no. 4, pp. 582-589, 2009.

[12] O. M. Al-Qershi and B. E. Khoo, "ROI-based tamper detection and recovery for medical images using reversible watermarking technique," in *Proceedings of IEEE International Conference on Information Theory and Information Security (ICITIS)*, Beijing, China, 2010, pp. 151-155.

[13] S. Das and M. K. Kundu, "Effective management of medical information through ROI-lossless fragile image watermarking technique," *Computer Methods and Programs in Biomedicine*, vol. 111, no. 3, pp. 662-675, 2013.

[14] G. Badshah, S. C. Liew, J. M. Zain, S. I. Hisham, and A. Zehra, "Importance of watermark lossless compression in digital medical image watermarking," *Research Journal of Recent Sciences,* vol. 4, no. 3, pp. 75-79, 2015.

[15] G. Badshah, S. C. Liew, J. M. Zain, and M. Ali, "Watermark compression in medical image watermarking using Lempel-Ziv-Welch (LZW) lossless compression technique," *Journal of Digital Imaging*, 01 October 2015. http://dx.doi.org/10.1007/s10278-015-9822-4.

[16] D. Coppersmith, F. C. Mintzer, C. P. Tresser, C. W. Wu, and M. N. Yeung, "Fragile imperceptible digital watermark with privacy control," in *Proceedings of SPIE 3657: Security and Watermaking of Multimedia Contents*. Bellingham, WA: Interntional Society for Optics and Photonics, 1999.

[17] S. C. Liew, S. W. Liew, and J. M. Zain, "Tamper localization and lossless recovery watermarking scheme with ROI segmentation and multilevel authentication," *Journal of Digital Imaging,* vol. 26, no. 2, pp. 316-325, 2013.

[18] A. Al-Haj and A. Amer, "Secured telemedicine using region-based watermarking with tamper localization," *Journal of Digital Imaging*, vol. 27, no. 6, pp. 737-750, 2014.

[19] G. Badshah, S. C. Liew, M. Z. Jasni, and T. Herawan, "Tamper localization and recovery medical image watermarking," in *Proceedings of International Conference on Computational Science and Information Management (ICoCSIM-2012)*, Medan, Indonesia, 2012, pp. 266-270.

**Gran Badshah** http://orcid.org/0000-0002-1060-580X

He received his Bachelor degree in Computer Science and Mathematics subjects from the University of Peshawar Pakistan in 1998. He was awarded Master in Computer Science from the University of Peshawar, in 2003. In December 2015, he completed his Ph.D. from Faculty of Computer Systems and Software Engineering, at University Malaysia Pahang, Malaysia. He started his career as an IT-instructor in 2003 at Federal Administered Tribal Area (FATA), in Govt. College of Management Sciences (GCMS) Khar, Bajour Agency. During his service period 2006-2011, he holed the posts of Assistant Programmer (AP) and Data Control Assistant (DCA) at the offices of Executive District Officer Finance and Planning at Dir Upper and Lower Districts of Khyber-Pakhtunkhwa Province of Pakistan. He has published more than 15 refereed articles in different journals and conferences. He has been actively presenting papers in national and international conferences. His research interests include digital watermarking, image processing, and battery efficiency of mobile devices as well as cloud data security.

**Siau-Chuin Liew** http://orcid.org/0000-0001-5020-7921

He received his Bachelor degree in Information Technology from University of Southern Queensland, Australia, in 2003. He did his Master in Strategic Business IT from University of Portsmouth, United Kingdom, in 2006. He completed his Ph.D. in Computer Science from Universiti Malaysia Pahang, Malaysia, in 2011. He started his career as a lecturer at Informatics College and Shahputra University College. Currently, he is a Senior Lecturer at Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang since July 2011. His research interests include image processing, signal processing as well as in Picture Achieving and Communications Systems. He has six postgraduate students under his supervision. He has published at least 27 refereed articles as main and co-author in different journals and conferences.

**Jasni Mohamad Zain** http://orcid.org/0000-0003-2072-1510

She received her Bachelor degree in Computer Science from University of Liverpool, England, UK in 1989 and Ph.D. from Brunel University, West London, UK in 2005. She started her career as a tutor in 1997 at University of Technology Malaysia (UTM). Currently she is Professor and Dean of Faculty of Computer Systems and Software Engineering at University Malaysia Pahang since 2008. She has been actively presenting papers and keynote address in national and international conferences. Her research interests include digital watermarking, image processing as well as data and network security. She has graduated eight PhDs and six Masters by research under her supervision and published more than 100 refereed articles. She has a patent file for digital watermarking (PI 2008047).

**Mushtaq Ali** http://orcid.org/0000-0002-4928-3166

He received his Bachelor degree in Computer Science from University of Peshawar, Pakistan in 2003. He completed his Master from Hazara University Mansehra Pakistan, in 2006. Currently he is pursuing his Ph.D. Candidature at University Malaysia Pahang (UMP). He started his career as an IT-Instructor at Pak Swiss Technical Training Center Mingora Swat Pakistan in 2007. He held last position as Network Administrator at AL-Khayrin Group Trading & Construction W.L.L, Doha Qatar in 2012. His research interests include Mobile Computing, Battery & Processing Efficiency of Mobile Devices, Cloud Security, and Watermarking of digital images. He has published 3 refereed articles as a main & co-author in different Journals. He presented 3 papers in national & International conferences.