Journal of Digital Imaging

Tamper Detection and Recovery for Medical Images Using Near-lossless Information Hiding Technique

Jeffery H. K. Wu,[1,2] Ruey-Feng Chang,[3] Chii-Jen Chen,[4] Ching-Lin Wang,[4,5] Ta-Hsun Kuo,[4] Woo Kyung Moon,[6] and Dar-Ren Chen[7]

Digital medical images are very easy to be modified for illegal purposes. For example, microcalcification in mammography is an important diagnostic clue, and it can be wiped off intentionally for insurance purposes or added intentionally into a normal mammography. In this paper, we proposed two methods to tamper detection and recovery for a medical image. A 1024 × 1024 x-ray mammogram was chosen to test the ability of tamper detection and recovery. At first, a medical image is divided into several blocks. For each block, an adaptive robust digital watermarking method combined with the modulo operation is used to hide both the authentication message and the recovery information. In the first method, each block is embedded with the authentication message and the recovery information of other blocks. Because the recovered block is too small and excessively compressed, the concept of region of interest (ROI) is introduced into the second method. If there are no tampered blocks, the original image can be obtained with only the stego image. When the ROI, such as microcalcification in mammography, is tampered with, an approximate image will be obtained from other blocks. From the experimental results, the proposed near-lossless method is proven to effectively detect a tampered medical image and recover the original ROI image. In this study, an adaptive robust digital watermarking method combined with the operation of modulo 256 was chosen to achieve information hiding and image authentication. With the proposal method, any random changes on the stego image will be detected in high probability.

KEY WORDS: Medical image, image processing, image authentication

INTRODUCTION

Medical images are produced by a wide variety of imaging equipment, such as computed tomography (CT), magnetic resonance imaging, ultrasound, and so on. Now, these medical images generally are stored in digital forms on different types of storage media such as compact discs (CDs) and digital versatile discs (DVDs). A patient can keep a copy of his medical image in a CD instead of a hard copy film. However, the digital images are very easy to be modified by any image processing program in a computer. Hospitals, insurance companies, as well as patients might want to modify the image for various reasons. The tampered images may be used

[1]*From the Department of Medical Imaging, Chang-Hua Christian Hospital, Changhua, Taiwan.*

[2]*From the Department of Radiological Technology, Central Taiwan University of Science and Technology, Taichung, Taiwan.*

[3]*From the Department of Computer Science and Information Engineering, Graduate Institute of Biomedical Electronics and Bioinformatics, National Taiwan University, Taipei, Taiwan.*

[4]*From the Department of Computer Science and Information Engineering, National Chung Cheng, Chiayi, Taiwan.*

[5]*From the Department of Information Management, National Chin-Yi University of Technology, Taichung, Taiwan.*

[6]*From the Department of Diagnostic Radiology, College of Medicine, Seoul National University Hospital, Seoul, South Korea.*

[7]*From the Department of Surgery, Changhua Christian Hospital, 135 Nanhsiao Street, Changhua, 500, Taiwan.*

Correspondence to: Dar-Ren Chen, Department of Diagnostic Radiology, College of Medicine, Seoul National University Hospital, Seoul, South Korea, tel: +886-4-7238595; fax: +886-4-7228289;
e-mail: darren_chen@cch.org.tw

Online publication 28 March 2007
doi: 10.1007/s10278-007-9011-1

for illegal purposes. Therefore, how to protect a medical image, detect a tampered medical image, and even recover the original image are important and urgent topics in the current digital age.

Image authentication can be achieved by embedding a message into the image and that embedded message is derived directly from the image itself. When an image is tampered with, then the authentication message derived from the tampered image will be different from the original message. The authentication message can be called as a digital watermarking.[1–8] The digital watermarking should be hidden into the image. However, the information hiding technique generally introduces some amount of noninvertible distortion in the image. The distortion might cause some legal problems for medical images. Recently, some lossless hiding techniques are proposed in some papers.[9–13] In the lossless hiding techniques, the embedded images can be reversed into the original images without any distortion.

In general, only one authentication message is derived from the whole image. However, in this method, if an image is detected to be a tampered one, we do not have enough information to point out which region is modified. Hence, a block-based authentication technique is proposed for providing more detailed information. At first, a medical image is divided into several blocks, and the authentication message of each block is embedded into other blocks. Whether the block is tampered with can be checked by the message embedded in other blocks.

Another interesting topic is the recovery of the original image for the tampered block. Because the lossless information hiding method cannot embed too many data into the images, it is too difficult to recover all regions in an image with accepted image quality. At the first proposed method, only an approximate small image for each block is embedded into the image, and it is used to recovery a small image when a block is detected to be tampered with. However, the recovered image is not good enough, and the second method is proposed to embed the recovery information of only the most important region for diagnosis. In this paper, the physician could indicate a region of interest (ROI),[14] and the approximate image for this ROI is also embedded into other blocks for recovery usage. When the ROI is tampered with, the approximate image can be recovered from the information embedded in other blocks. For example, the microcalcification in an x-ray mammography is an important diagnostic clue. The microcalcification may be wiped off intentionally. In our proposed method, the white spots will be recovered in the recovered image. On the other hand, the microcalcification may be added intentionally into a normal mammography. This also can be detected by the proposed authentication approach.

In this study, the lossless information hiding technique based on robust spatial additive watermarks combined with modulo addition[9] was used to achieve the image authentication and to protect the medical image.

METHODOLOGY

Lossless Information Hiding Technique

Almost all current data-embedding methods have one common drawback that the original image is inevitably distorted due to data embedding. This distortion cannot be removed completely due to quantization, bit-replacement, or truncation. Although the distortion is often quite small and various perceptual models are used to minimize its visibility, the distortion might not be acceptable for medical images due to legal reasons.[15] Recently, some solutions had been proposed; for example, Fridrich et al.[9,11,12,15–17] have contributed a great deal of ideas. One of the methods is using the JBIG lossless compression scheme for compressing the bit-planes.[18–20] This method starts with decomposing an image into bit-planes. Then, the appropriate key bit-plane is compressed and used to hide the information. This key bit-plane is the lowest bit-plane satisfying the condition that the redundancies are more than the information that needs to be hidden. The embedded information might be obtained from calculating the whole image hash bits.

At last, the watermarked image including the processed bit-plane is protected with a secure scheme which is a special symmetric encryption scheme based on two-dimensional chaotic maps.[21] The verification procedure could be accomplished in the inverse order. There is a drawback that the stego image might include visible distortion due

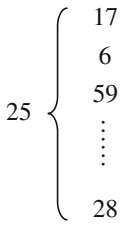

Fig. 1. The 25 six-bit symbols s_i displayed in decimal mode.

to the choosing of higher bit-plane in the method above. Another invertible authentication method using robust watermarks will be introduced and explained below.

The Main Art

The lossless authentication method based on the robust additive watermark in the spatial domain comes from the idea of modulo operation. In this method, the watermark payload is obtained from the hash of the original image at first, and then embedded to the original image with the robust watermarking technique including the modulo addition operation. The chosen watermarking scheme must be invertible; that is, the watermark could be exactly subtracted from most of the pixels with the exception of pixels truncated due to over- and underflow. The procedure of verification seems easy to be run in the inverse order. All we need is to extract the watermark payload from the stego image, to use the chosen watermarking scheme to obtain the verified image by subtracting the extracted payload, and to prove whether the extracted payload matches the hash of verified image.

Information Hiding Procedure

Honsinger et al. proposed the addition of modulo 256 as an invertible operation and chose the watermarking technique based on random phase spreading. The scheme provides sufficient capacity which must be at least equal to the length of hash $H(I)$, and it is highly robust to any changes in an image I. The procedure of information embedding is listed below:[9]

1. Calculate the hash of original image $H(I)$.
2. Use a robust watermarking technique to generate the watermark pattern $W(K,H(I))$, where W is a function of secret key K and the payload $H(I)$.
3. Get the watermarked image $I_w = I \oplus \alpha W$, where $\oplus$ is the modulo addition and α is the watermark strength.

Conceptually, the above watermarking technique seems to be a spatial method. However, in practice, it is a spread spectrum, frequency-based robust watermarking algorithm.[22] It could support sufficient capacity to hide information and could be explained with the running steps below.

Step 1: Calculate the hash bit-string, for example, $25 \times 6 = 150$ bits, from the original image I, and represent it using $M = 25$ six-bit symbols s_i as shown in Figure 1.

Step 2: Generate 25 sequences of pseudo-random numbers whose length is equal to $N_m + 64$, as shown in Figure 2, and uniformly distributed in $[-1,1]$, where N_m is three-tenth of the total number of image pixels. The secret key determines the seed of pseudo-random number generator (PRNG).

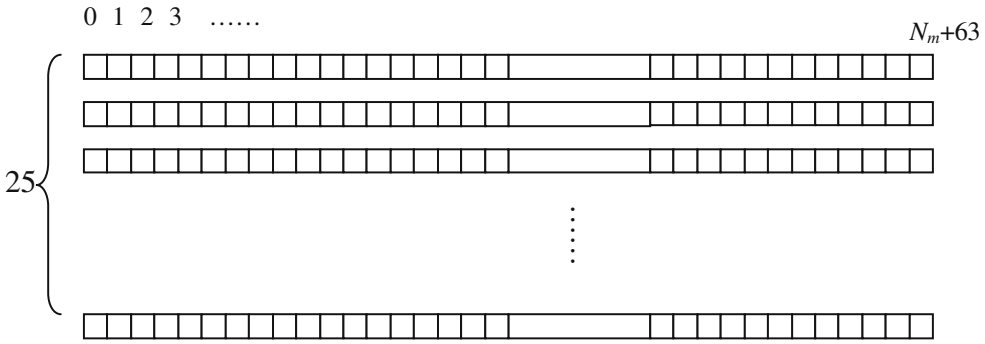

Fig. 2. The 25 sequences of random numbers with length N_m + 64 and uniformly distributed in [−1,1].

Step 3: Synthesize 25 new sequences of pseudo-random numbers η^i whose length is equal to N_{m} for each symbol s_i. For example, if $s_i = k$, then from the kth element to the $(N_{\mathrm{m}} + k - 1)$th element of the ith source sequence of pseudo random numbers are chosen as elements of new sequence numbers η^i as shown in Figure 3.

Step 4: Calculate the spread spectrum signal S.

$$S(n) = \sqrt{\frac{3}{M}} \sum_{i=1}^{M} \eta^i(n), \text{ where } n = 1, 2, \ldots, N_m,$$

where S is an approximate Gaussian with zero mean and unit standard deviation.

Step 5: Use S as the middle 30% of the DCT coefficients in the zigzag pattern.

Step 6: Calculate the stego image (watermarked image) I'

$$I' = I \oplus DCT^{-1}(\alpha S),$$

where α is an image independent watermark strength.

As mentioned above, when the frequency-based robust watermarking algorithm embeds the information with the form of $DCT^{-1}(\alpha S)$, the hiding information will be spread and added to all pixels of the image in random.

Integrity Verification Procedure

The procedure of information extracting and image verification is listed below:[9]

1. Extract the watermark payload H' from the watermarked image I_{w}.
2. Generate the watermark pattern $W' = W(K, H')$.
3. Obtain the verified image $I' = I_w - \alpha W'$.
4. Compare the hash of I', $H(I')$, with the extracted payload H'.

In the above steps, the process of extracting payload must be handled carefully. It depends on a correlation operation between the sequence random numbers and the DCT coefficients of the stego image. The running steps are listed to clarify the course.

Step 1: Calculate the DCT coefficients of stego image I', DCT(I'), and extract the middle N_{m} DCT coefficients with the zigzag order. Note that the stego image I' may be tampered with.

Step 2: Generate 25 sequences of random numbers whose length is equal to $N_{\mathrm{m}} + 64$ and uniformly distributed in $[-1,1]$. The secret key determines the seed of PRNG.

Step 3: For each sequence, all 64 segments of length N_{m} are correlated with the middle N_{m} DCT coefficients. The largest value

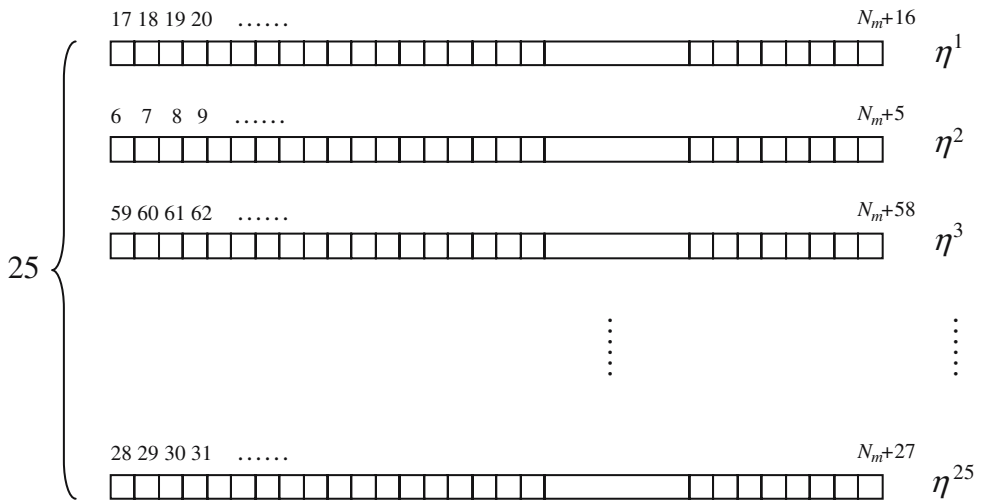

Fig. 3. The 25 new sequences random numbers η^i of length N_m.

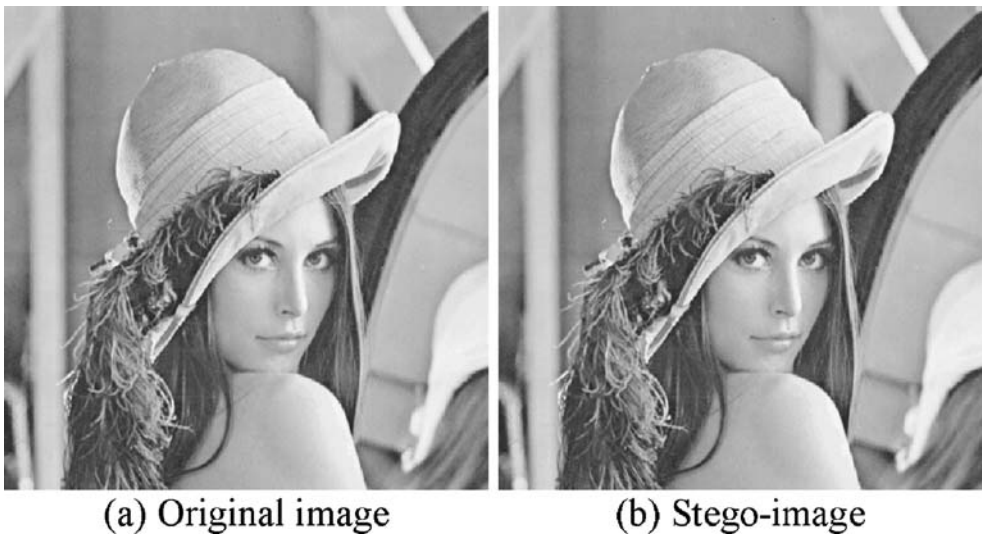

Fig. 4. Image Lenna with 512 × 512 pixels. PSNR = 52.29 dB. Some 36.28% of the total pixels were changed.

of the correlation determined the encoded symbol s_i.

Step 4: Synthesize 25 sequences of random numbers with symbol s_i, and rebuild the spread spectrum signal S.

Step 5: Get the recovery image X from the operations of inverse DCT and subtraction.

$$X = I' - DCT^{-1}(\alpha S)$$

Step 6: Calculate the hash bit-string, 25×6 bits, from the recovery image Y, $H(X)$. If the symbol s_i and the $H(X)$ are matched, then the recovery image X is the same with original image I losslessly. Otherwise, image X is deemed nonauthentic, and the stego image had been tampered with.

Note that the image independent watermark strength α can be used to control the variation of pixels between original and stego images. Choosing a weaker one can reduce the difference between the original image and the stego image, but it might cause fatal failure in the procedure of verification. Choosing a stronger one would increase the successful verification rate, but visible distortion might be introduced into the stego image. In our

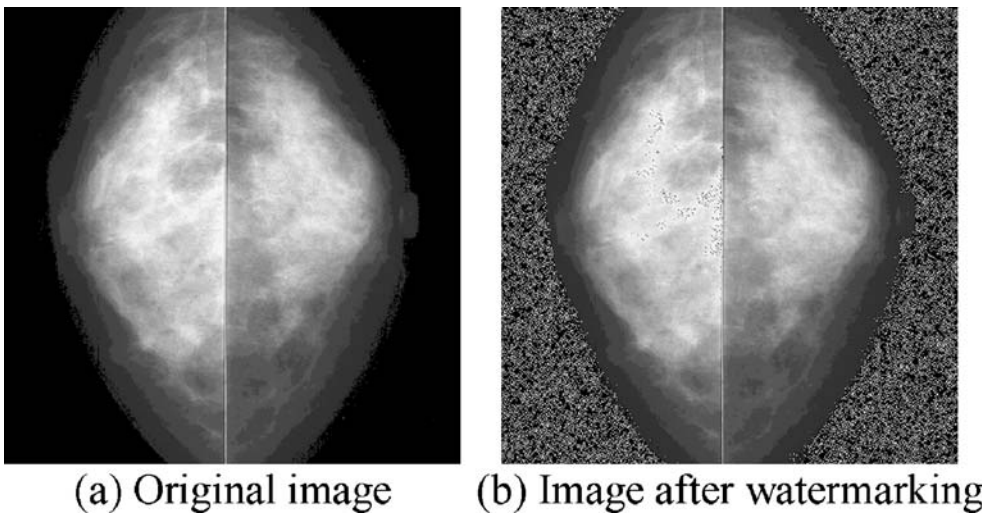

Fig. 5. A breast x-ray image with 512 × 512 pixels; PSNR = 11.61 dB with 18,237 flipping pixels.

experiences, the image of 512×512 pixels may select the watermark strength $\alpha = 1$ to satisfy the procedure of verification. For larger images, the smaller value α could be chosen.

Advantage

The above robust watermarking technique satisfies the image authentication requirements.[23–30] It has the property that the stego image is very close to the original image and the artifact is almost invisible. That is to say, the visions of original image and the stego image coming from adding or subtracting small grayscale in each pixel could hardly be made out of the difference between them practically as shown in Figure 4.

Also, it has the ability to accomplish the lossless authentication with the stego image only; moreover, the authorship can be declared with the secret key K. If the stego image is authentic, the original image could be obtained from it. That is, the medical image can be protected with this information hiding technique, and any tampering in the medical image would be detected. It seems that the work was done well until now, but we need to point out the drawback of the method.

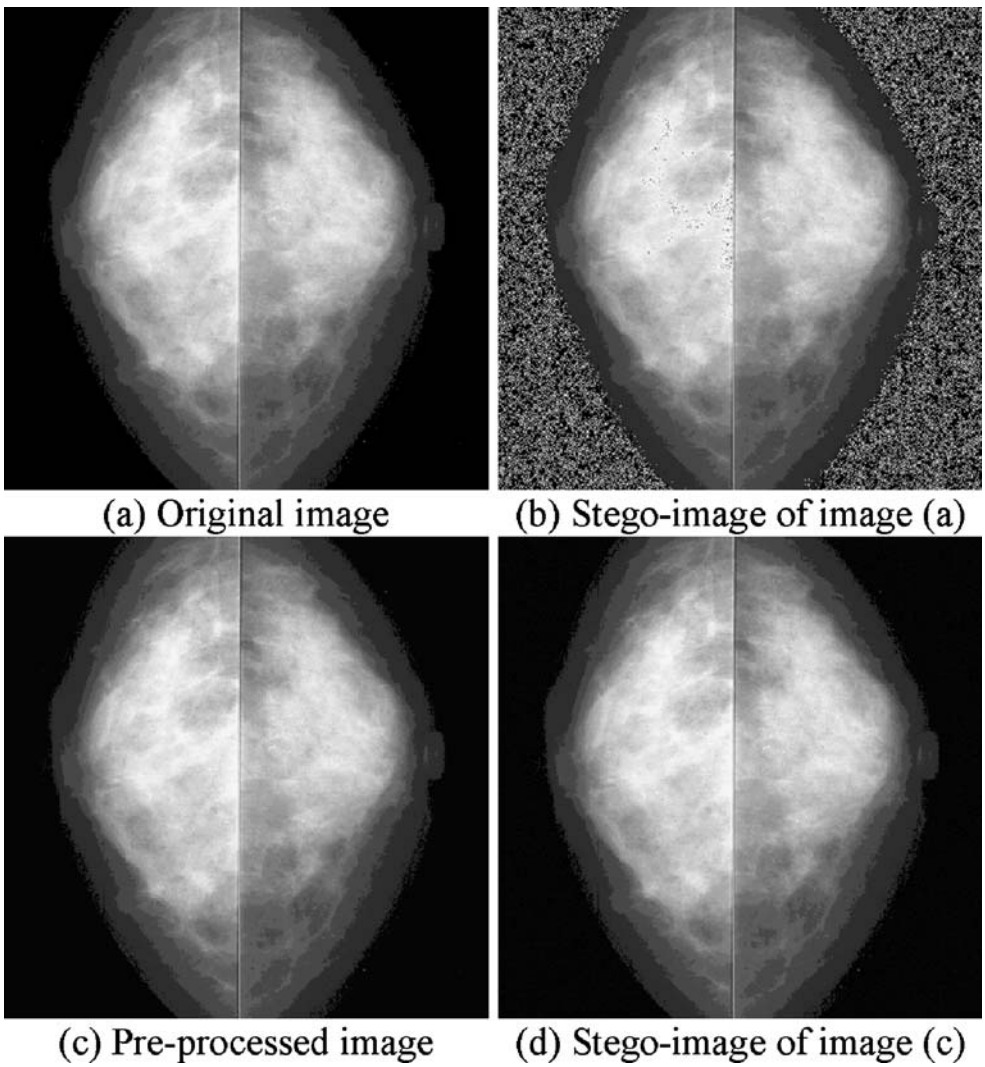

Fig. 6. An x-ray image with 512×512 pixels. PSNR between (a) and (b) is 11.61 dB, including 18,237 flipping pixels. The preprocessed image is forced the grayscale range from 2 to 253, PSNR between (a) and (c) is 46.36 dB, 1,859 pixels are moved from the brightest value, and 97,453 pixels are moved from the darkest value. The image (d) was taken from the preprocessed image with the robust watermarking technique, PSNR between (c) and (d) is 52.36 dB, and no flipping pixels exist.

When the pixels of medical image are close to the gray level of 255 or 0, it might cause the pixels changing from 255 to 0 or from 0 to 255 through the operation of modulo 256, which is called the flipping pixel. In general, the case will not occur frequently and can be solved with a preprocessing before the procedure of verification, but when we concern about the information hiding of medical image, it will become a serious problem. The flipping pixels will be all over the area of border as shown in Figure 5 because of sheets of black areas and the most bright pixels in the central area. It will affect the authentication process and cause an error. The solution to solve the problem will be given in the next section.

TAMPER DETECTION AND RECOVERY

The block-based information hiding technique is proposed to detect tampering and recover the original information from a tampered medical image. As mentioned in the previous section, the

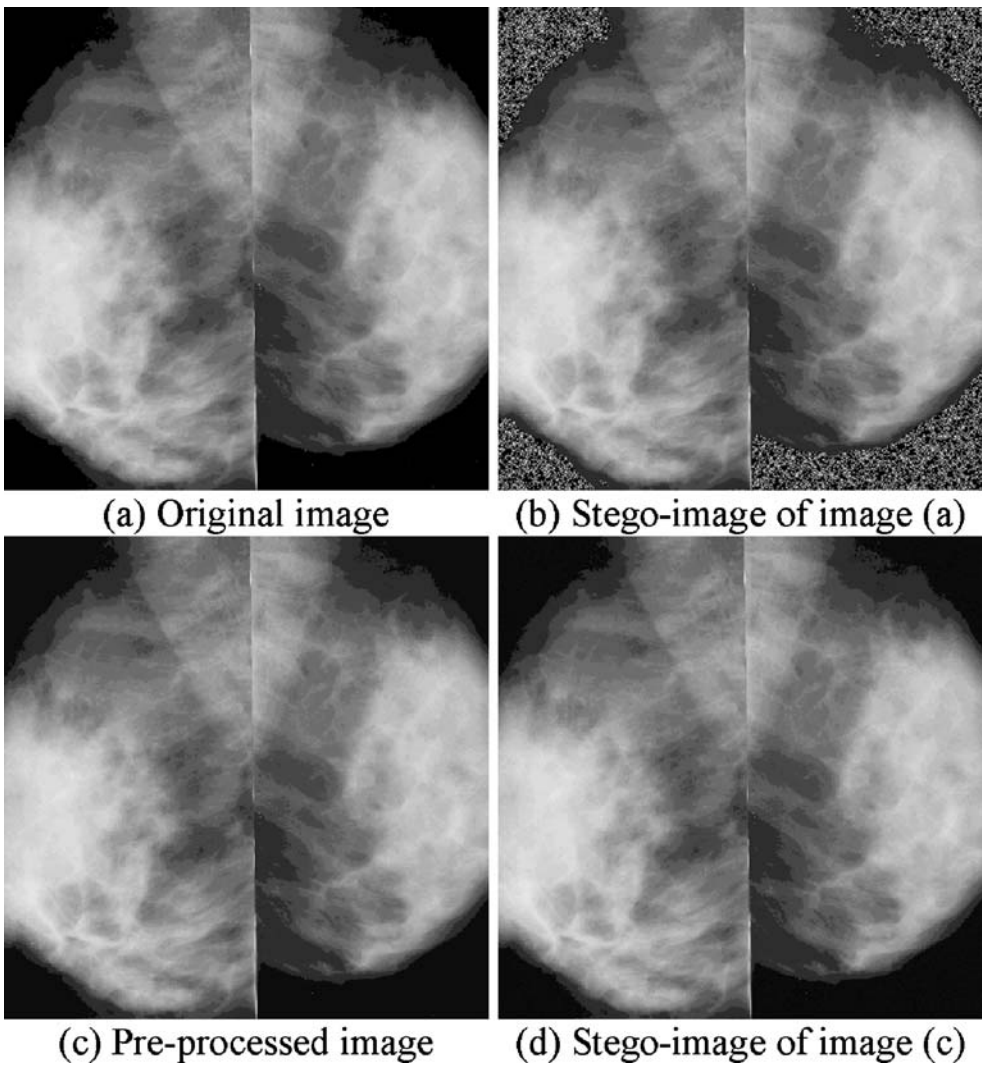

Fig. 7. An x-ray image with 512 × 512 pixels. PSNR between (a) and (b) is 16.10 dB, including 6,492 flipping pixels. The preprocessed image is forced the grayscale range from 3 to 252, PSNR between (a) and (c) is 47.33 dB, 1 pixel is moved from the brightest value, and 35,269 pixels are moved from the darkest value. The image (d) was obtained from the preprocessed image with the robust watermarking technique, PSNR between (c) and (d) is 52.38 dB, and no flipping pixels exist.

flipping pixels in the stego image were an obvious distortion and might cause a fatal error in the verification procedure. This problem must be solved at first to ensure the correctness of tamper detection; consequently, the concept of near lossless is proposed in this paper. Moreover, two block-based information hiding methods are designed to detect the tampered area. One has the ability to recover all blocks, whereas the other one has the ability to recover only a selected region where a physician will be interested.

Near-lossless Embedding

To avoid the flipping pixels from occurring in the stego image, the idea was proposed that if the gray levels of pixels at extremes of gray-level range could be moved some levels from the end to the central value, then it might be guaranteed that the flipping pixels would not appear through information hiding or modulo addition operation. For instance, almost the difference between the original image and the preprocessed image could

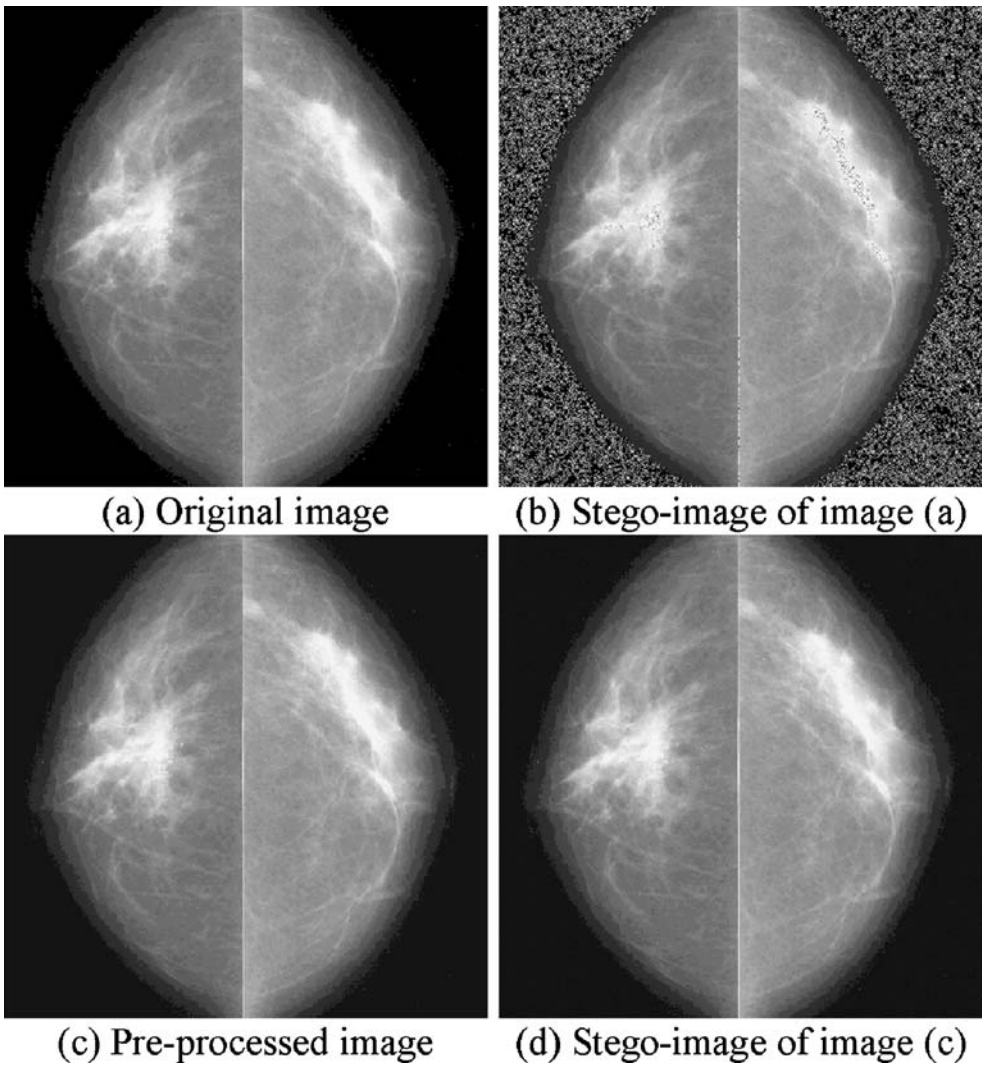

Fig. 8. An x-ray image with 512 × 512 pixels. PSNR between (a) and (b) is 12.18 dB, including 15,989 flipping pixels. The preprocessed image is forced the grayscale range from 5 to 250, PSNR between (a) and (c) is 38.86 dB, 2,389 pixels are moved from the brightest value, and 86,945 pixels are moved from the darkest value. The image (d) was obtained from the preprocessed image with the robust watermarking technique, PSNR between (c) and (d) is 52.39 dB, and no flipping pixels exist.

not be distinguished, and flipping pixels were removed from the stego image as shown in Figures 6, 7, and 8.

Using the information hiding technique on the preprocessed image, it is clear that the artifact is almost invisible, and the ability of invertible authentication is held because of no flipping pixels. Although the preprocessed and original images are very similar, and the lossless property was kept when the preprocessed image had been watermarked and extracted, but still there are some pixels changed between the preprocessed image and the original one. Therefore, the modified method was called as the near-lossless information hiding technique due to the preprocessing procedure.

Algorithm to Detect and Recover Tampered Block

The algorithm to detect the tampering in an image was proposed by some authors.[29–33] Most of them have only the tamper detection without the recovery capability. According to the discussion in the previous section, two new block-based tamper detection and recovery methods were developed. The tamper detection is based on the robust watermarking combined with modulo addition. By checking each block of stego image being authenticated or not, the lossless original block will be restored or the tampered block will be found. On the other hand, the information hiding technique needs to be modified to embed more information about another block for recovery besides the hash value of an original block for authentication. To embed the recovery information efficiently, the image block was transferred to the JPEG-encoded bit-string.[34–37] For each block, using the hash value and JPEG bit-string, the tamper detection and recovery could be done simultaneously.

The Method with Ability to Recover All Blocks

In this method, the tamper detection and recovery can be accomplished for all blocks. At first, the image is divided into several blocks; the procedure of information hiding is executed for each block to get the stego image. Then, the stego image might be sent around for some purposes. When the physician needs to check whether the stego image had been tampered with, he should execute the integrity verification procedure on the stego image. If all of the blocks are authenticated, it can be announced that the stego image is not tampered with; moreover, the original image would be acquired from the stego image only and was lossless. Otherwise, if some of the blocks could not pass the verification and are unauthentic, the tampered blocks will be pointed out. Therefore, the JPEG bit-string was extracted from the corresponding blocks to recover the tampered one. The algorithm is lined up now.

Algorithm for information hiding:

1. Divide the original image into blocks.
2. For each block I_i:
   - 2.1 Calculate the hash bits $H(I_i)$ of block I_i.
   - 2.2 Get the JPEG bits of block I_j, $G(I_j)$, where block I_j is the farthest block away from block I_i.
   - 2.3 Use the robust watermarking technique to generate a watermark pattern W_i which is a function of secret key K and the payload $H(I_i) + G(I_j)$ only, $W_i = W(K, H(I_i) + G(I_j))$.
   - 2.4 Get the embedded block $I_{wi} = I_i \oplus \alpha W_i$.
3. Combine all blocks I_{wi} to form the stego image.

Algorithm for tamper detection and recovery:

1. Divide the stego image into blocks.
2. For each block I_{wi}:
   - 2.1 Extract watermark payload P_i' from I_{wi}.
   - 2.2 Separate P_i' to H_i' and G_j'.
   - 2.3 Generate the watermark pattern W_i'.
   - 2.4 Subtract W_i' from I_{wi} to obtain $I_i' = I_{wi} - \alpha W_i'$.
   - 2.5 Compare the hash of I_i', $H(I_i')$ with H_i' to decide whether block I_{wi} was tampered with.
3. If all blocks I_i' were not tampered with, combine all of them to form the original image lossless. Else, if block I_j' was tampered with, recover the block with G_j'.

It is important that when the JPEG bit-string is picked up, it must be kept at the same size carefully in each block. Rewriting the procedures to get the JPEG bit-string from blocks and rebuilding JPEG image from bit-string are need-

ed. In this method, each tampered block in the stego image could be detected and recovered with the compressed form. In our experiences, detecting the tampered block is clever, but the recovered block is disagreeable when the tampered area is quite small. The unacceptable situation is caused by the embedded information capacity. For the limit of embedding capacity, the excessive compression method was used, and then the recovery image did not have enough image quality. Hence, another method is proposed in the next section.

The Method with Ability to Recover ROI

A physician concerns about the most interesting area like the microcalcification in mammography because microcalcification is the earliest sign of breast carcinomas.[38] The area with microcalcification can be called as the ROI. In this proposed method, the original medical image is divided into several blocks too, but only the recovery information of ROI is embedded. That is to say, only the most important recovery information will be hidden in the stego image; hence, the compression rate can be reduced on ROI, and the compressed information will be separated and embedded into blocks except the block with ROI. When the ROI was tampered with, it would be detected and could be recovered more clearly.

For the reason of stability, the feature of ROI must be kept in every block. The JPEG bit-string of ROI must scatter over all blocks excluding the block with ROI, and the size of the hiding information in each block needs to be of fixed value. The algorithm must be much smarter when the procedure of recovering the tampered ROI is executed. It separates all blocks, excluding the one with ROI, into three parts in accordance with the distance away from the block with ROI. When some blocks around the ROI were tampered with too, we could still recover the ROI from the rest of the parts. Therefore, it is needed that the length of JPEG bit-string can be variable when the JPEG image is rebuilt. Now, the algorithm is listed below.

Algorithm for information hiding:

1. Select ROI.
2. Get its JPEG bit-string and cut the bit-string to fixed-length segments.
3. Divide the original image into blocks.
4. For each block I_i excluding the block with ROI:
   - 4.1 Calculate the hash bits $H(I_i)$.
   - 4.2 Get the JPEG bit-string segment S_i which includes the coordinate of ROI.
   - 4.3 Use the robust watermarking technique to generate a watermark pattern W_i.
   - 4.4 Get the block $I_{wi} = I_i \oplus \alpha W_i$.
5. Combine all blocks I_{wi} and the block with ROI to form the stego image.

Algorithm for tamper detection and recovery:

1. Divide the stego image into blocks.
2. For each block I_{wi}:
   - 2.1 Extract watermark payload P_I' from I_{wi}.
   - 2.2 Separate P_i' to H_i' and S_i'.
   - 2.3 Generate the watermark pattern W_i'.
   - 2.4 Subtract W_i' from I_{wi} to obtain $I_i' = I_{wi} - \alpha W_i'$.
   - 2.5 Compare the hash of I_i', $H(I_i')$ with H_i' to decide whether block I_{wi} was tampered with.
3. If all blocks I_i' were not tampered with, combine all of them to form the original image lossless.
4. Else, if the block with ROI was tampered with, collect S_i' of the other blocks which are authentic, and combine all of the bit-strings to recover the ROI.
5. Else, if the block without ROI was tampered with, point it out.

For medical images, the method is more powerful in persuasiveness when the ROI was tampered with. The tampered ROI can be recovered very closely to the original one. It must be mentioned that it is necessary to rewrite the programming code for the JPEG procedure to fit the special need. Also, it might be noted that if there is no any tampered area detected, the medical image could be obtained as lossless. If there is any tampered area to be detected, generally, it would be the block of ROI, the region of ROI will be rebuilt, and the other blocks are also invertible if they were not tampered with.

EXPERIMENTS AND RESULTS

In this section, the experimental results will be shown and discussed in detail. During the

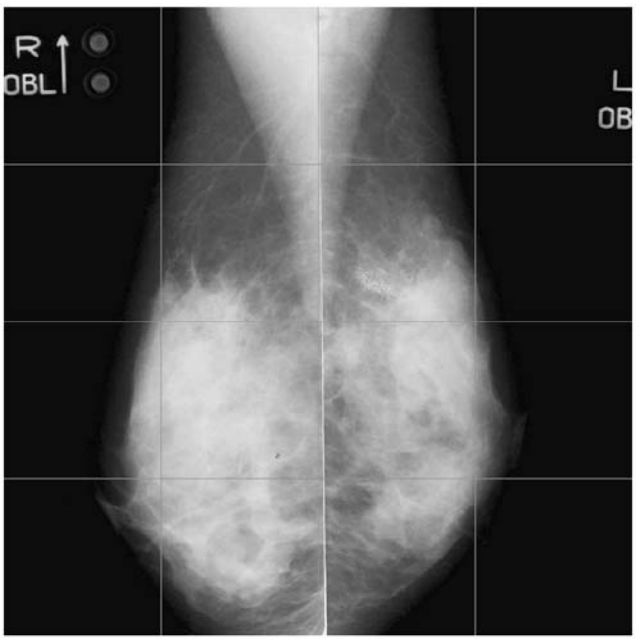

Fig. 9. An x-ray mammography with size of 1,024 × 1,024 pixels preprocessed by forcing the grayscale to a range from 3 to 252 in advance. The image is divided into 16 blocks.

experiments, an x-ray mammogram with image size of 1,024 × 1,024 pixels was chosen to test the ability of tamper detection and recovery. The image had been processed by forcing its grayscale to a range from 3 to 252 in advance, and divided it into 16 blocks. Each block size is 256×256 pixels as shown in Figure 9. This study was approved by the local ethics committee, and informed consent was obtained from all included patients.

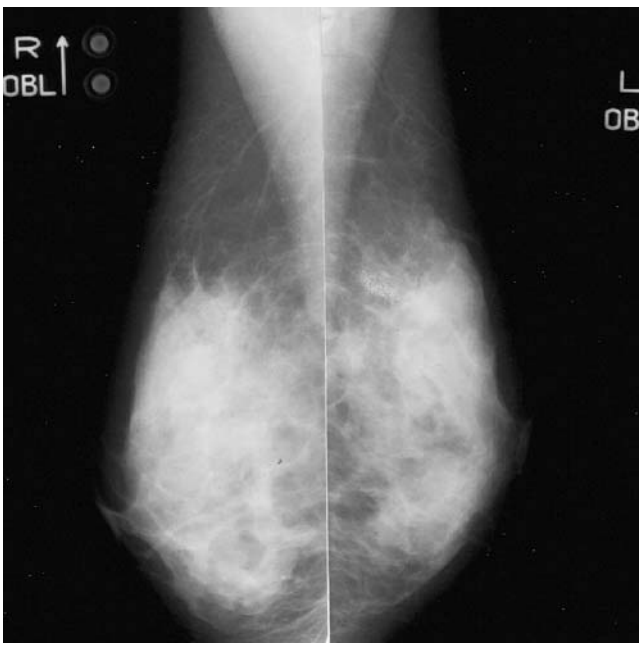

Fig. 10. Stego image. There are 602,908 pixels changed, 41 flipping pixels, and PSNR = 48.82 dB.

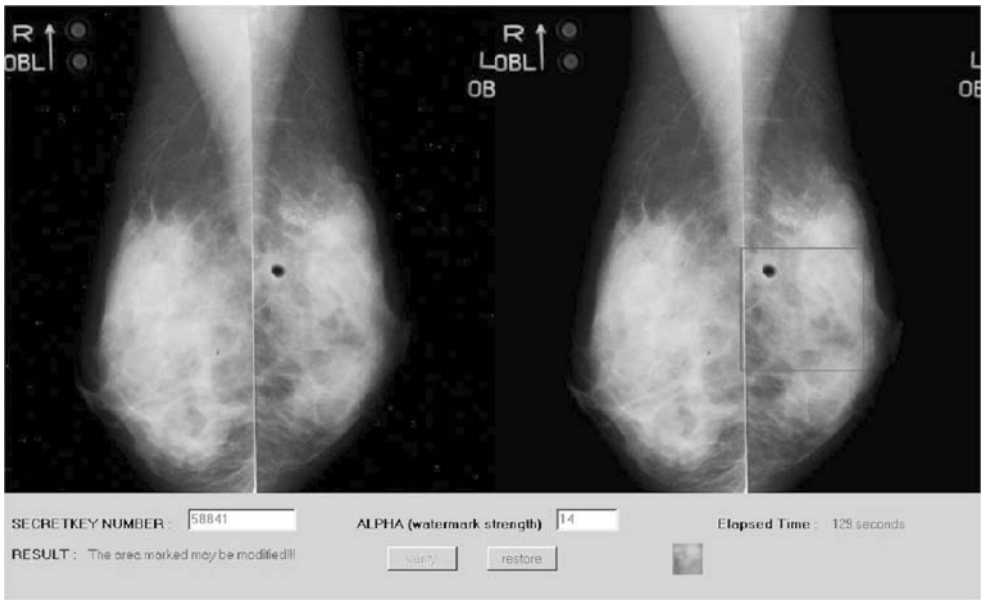

Fig. 11. The *left image* is the stego image with a tampered black spot, and the *right one* is the verification result. The tampered block is pointed out and restored with a smaller image shown below.

All Block Recovery

For each block, the robust watermarking was executed to obtain the stego image as shown in Figure 10. It can be found that the stego image is very close to the original image with peak signal-to-noise ratio (PSNR) of 48.82 dB, and there are 41 flipping pixels almost in the dark background. To avoid failure in authentication, a scheme of preprocessing was executed first at the procedure of verification. The scheme checks each pixel in stego image and its neighborhoods to decide

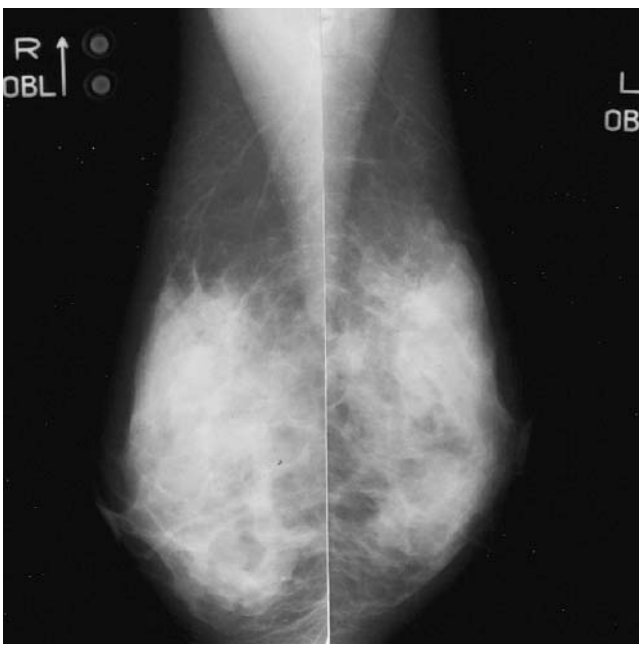

Fig. 12. Tampered image. The microcalcification was removed from the area of *upper-right side*.

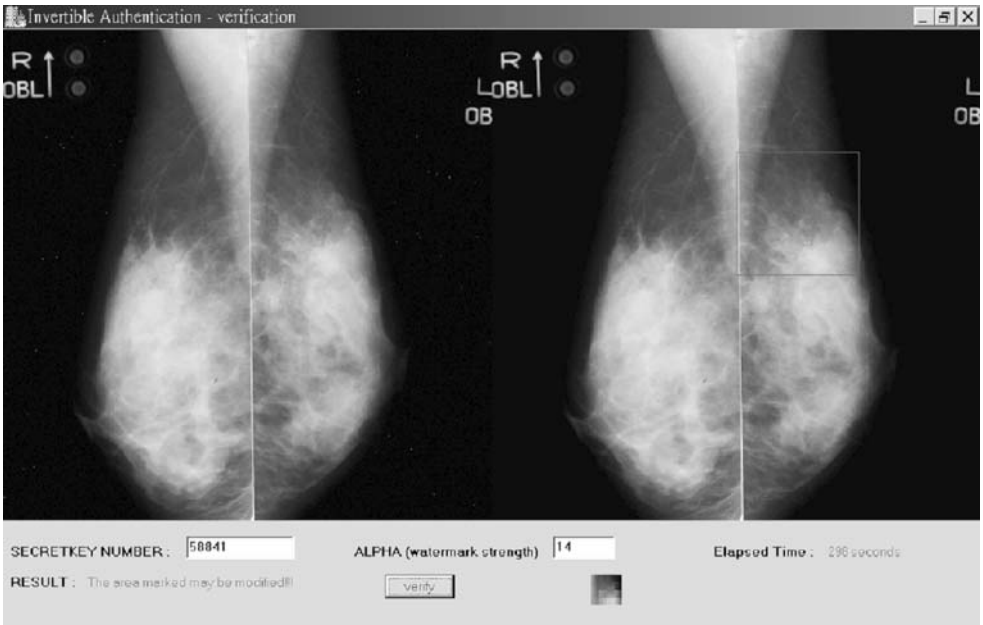

Fig. 13. In the *left tampered image,* the microcalcification was wiped off. The tampered block was pointed out and restored within a smaller image of size 32×32 pixels as shown below. It is hard to make out the original existing white spots.

whether the pixel is a flipping pixel. The value of flipping pixel was turned over to guarantee that the payload would be extracted correctly during the correlation operation. Then, the influence of small quantity of flipping pixels will be removed.

If all blocks are authentic during the verification procedure, it can be announced that the verified image is the same as the original one. Otherwise, the tampered block that does not pass the authentication would be detected. In the first

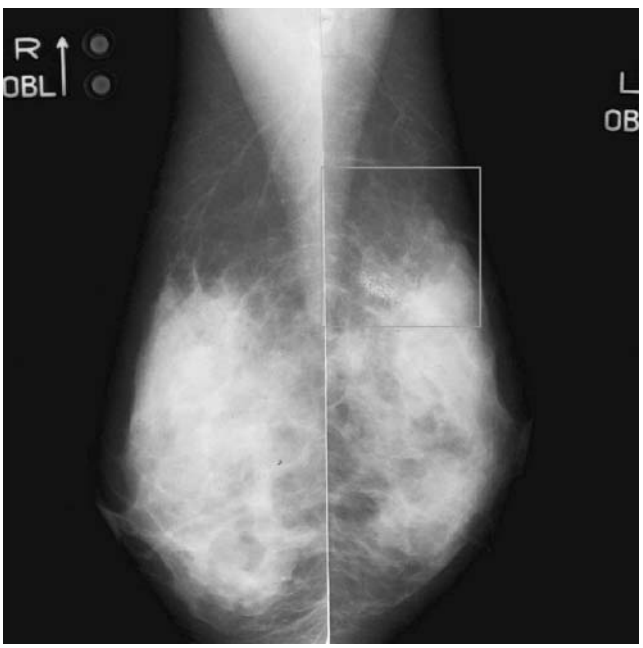

Fig. 14. The block with microcalcification will be assigned as ROI.

test case, a black spot is added on the stego image as shown on the left side of Figure 11.

The proposed method can correctly detect the tampered block including the black spot; moreover, the tampered block will be recovered with the smaller image size of 32×32 pixels, which shows the original block without a black area indistinctly as shown on the right side of Figure 11. In this test case, it can prove that the black spot did not exist really from the smaller recovered block.

However, in some cases, the results may not be so fortunate in the recovery procedure. For example, when the very small and meaningful drops like microcalcification are wiped off, as shown in Figure 12, it can be detected by the proposed method but the recovery 32×32 image is too small to recognize the original drops of microcalcification as shown in Figure 13. This is because the lossless information hiding technique cannot embed too much data. Hence, another method coming from the concept of ROI is proposed to solve the problem.

It must be also mentioned that if an x-ray mammogram without any microcalcification was tampered with some white spots, the tampered block could be detected by the verification proce-

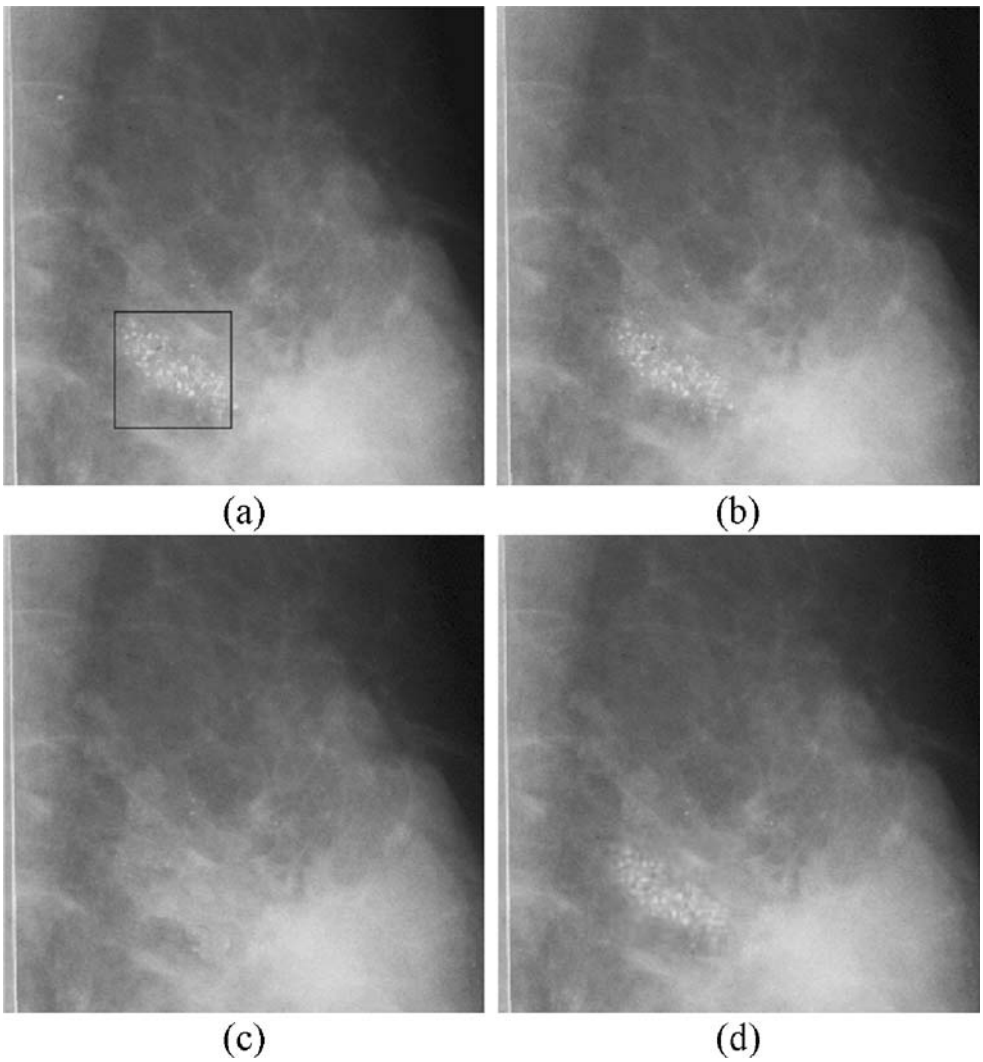

Fig. 15. (a) Original image block. A physician selects the ROI of size 64×64 pixels before running the information embedding. The region includes visible microcalcification. (b) Stego image block. PSNR is 49.05 dB between original image and stego image. There are 603,758 pixels changed, and 38 flipping pixels in the whole stego image. (c) Tampered block. The microcalcification is wiped off. (d) Put the recovered region back to the tamper block. It can convince anybody on the existence of microcalcification.

dure and restored roughly. However, in general, the recovered block is too obscure to be recognized.

ROI Recovery

From the above experiment and discussion, for the medical image like an x-ray mammogram, there are some regions that are important for diagnosis, and these regions should be recovered with better image quality. For example, because the microcalcification is the earliest sign of breast carcinomas, the microcalcification region should be highly protected. This particular important area is called ROI and needs to be protected especially.

In the first test case, the microcalcification ROI of 64×64 pixels was selected by a physician, and this ROI is the region that will be tampered with high probability as shown in Figure 14.

This ROI will be transferred to the JPEG bit-string and embedded into other blocks excluding itself. Only the most important block is displayed at each step in Figure 15. It shows that the recovery result is clear enough to indicate that the microcalcification had been wiped off and it exists actually.

In the second test, the tampered stego image with white spots is pretended to be some microcalcification in mammography, as shown in Figure 16, and might be used for illegal purposes. It can be detected by the proposed method too, but the most concerned message embedded is the information about ROI, and during the verification procedure, it will be found that the block with ROI cannot be tampered with as shown in Figure 17.

The robust watermarking procedure has a property that more information could be hidden for larger image blocks. Hence, the block size could not be too small, and the size of 256×256 is selected. At the same time, the quantity of hiding information should not be too large to avoid failure in the verification procedure. In our experience, 102 bits could be embedded into a block with size 256×256. There are 37 bits used for the image verification; the rest of 65 bits are used to embed the recovery information. Normally, these 65 bits are not enough to hide the JPEG bit-string of a block. It is feasible to run the embedding procedure with more loops. At each iteration, 65 bits could be embedded, and more other bits could be added with several iterations. But it must be considered that more iterations might cause more flipping pixels and spend more time to run the procedure. Although reducing the gray-level range could resist the growth of flipping pixels, but it loses the properties of near lossless and makes the variation visible. Furthermore, the problem of time

Fig. 16. The marked block was tampered with some added white spots. It does not exist in original image.

Fig. 17. The *left tampered image* has the added white spots. The tampered block was pointed out, and the block with ROI was also shown. The system will show that the most important area was not tampered.

cost is another death wound. To balance the efficiency and embedding ability, the number of watermarking loops in the experiments is three. It supplies enough information to be embedded, is more efficient in running time, and keeps the property of near lossless.

Another question concerned is the choosing of watermark strength α. The image size will influence the choosing of α value. When the robust watermarking mechanism applies to the block size of 256×256, the α value with 14 is satisfied. The variation of pixels between the original and stego images is controlled under the range from -2 to 2.

DISCUSSION

In this study, an adaptive robust digital watermarking method combined with the operation of modulo 256 was chosen to achieve information hiding and image authentication. With the method, any random changes on the stego image will be detected in high probability. It is also lossless (or invertible) when the stego image is authentic, that is to say, the embedded images could be restored to their original forms without any distortion. It is well done for the ordinary images such as natural scenes; however, we are concerned about the medical images that will bring us the flipping pixel problem due to the modulo operation on the brightest and darkest pixels which are generally existed in medical images with the style of large piece.

To avoid the influence of flipping pixels, the method of forcing the medical image's gray levels under the range from 3 to 252 was used. Because of this reduction of the gray-level range, the original lossless technique becomes the near-lossless information hiding one. For medical images, it is still acceptable because the original image and the process one are almost the same. If the medical images do not use all the gray levels that the file format supports, then this reduction of gray-level range is not required. For example, most CT images are stored in 16-bit format but they only use the values from 1,000 to $-1,000$. That is, for these images, the flipping pixel problem will not occur. If the images do not have the flipping pixel problem after the embedding procedure, then the proposed hiding technique is still a lossless one.

In the conventional lossless authentication method, only one authentication message derived from the whole image is used. The drawback of

using a message for the whole image is that we cannot know which region is tampered with when an image is detected to be a tampered one. In this study, two block-based methods are proposed for providing more detailed information. In the first method, a medical image is divided into several blocks; the authentication message and a small recovery block of each block are embedded into other blocks. Whether a block is tampered with could be checked by its authentication message and be recovered by the recovery information embedded in other blocks. Each block's recovery information is transferred to the JPEG bit-string and embedded into another block. Due to the limitation of the number of embedding bits, only several JPEG bits can be embedded. In the verification procedure, if all blocks pass the examination, we can announce that the stego image cannot be changed at any pixel. Furthermore, a near-lossless image could be obtained directly from the stego image without the original one. Note that any change in watermarked image will be detected and can be recovered from other blocks containing their JPEG information.

In experiments, the recovered image block is too small and not clear. It may be only useful in the case with bigger tampered area but helpless when somebody changed the small pieces, like the microcalcification of an x-ray mammography image. Accordingly, another method, which highly protects the ROI, is proposed. Because the lossless information hiding method cannot embed too much data, it is too difficult to recover any regions in a medical image with good quality. In the second method, only the ROI selected by a physician has the recovery information. That is, only the ROI can be recovered when it is tampered. An ROI is an important region for diagnosis in medical images, and it needs to be protected especially. The ROI was transferred to the JPEG form with lower compression rate and simultaneously embedded into each block excluding the block with ROI.

When an ROI is tampered with, the approximate image will be obtained from other blocks. In this study, microcalcifications can be detected, and the white spots will be recovered in the approximate image. Microcalcifications can also be added intentionally into a normal mammogram. This also can be detected but not recovered by our proposed authentication approach. The second method contains the concept of ROI, and it seems reasonable for medical images because the physician and those who want to tamper the medical images will concentrate on these areas generally. In the proposed method, only one square ROI is considered. It might be developed in the future to make the ROI selection more flexible, such as more than one region can be selected or any type of shapes can be chosen.

REFERENCES

1. Hsu C-T, Wu J-L: Multiresolution watermarking for digital images. IEEE Trans Circuit Syst–II 45:1097–1101, 1998

2. Podilchuk CI, Zeng W: Image-adaptive watermarking using visual models. IEEE J Sel Areas Commun 16:525–539, 1998

3. Pitas I: A method for watermark casting on digital images. IEEE Trans Circuits Syst Video Technol 8:775–780, 1998

4. Wei ZH, Qin P, Fu YQ: Perceptual digital watermark of images using wavelet transform. IEEE Trans Consum Electron 44:1267–1272, 1998

5. Hsu C-T, Wu J-L: Hidden digital watermarks in images. IEEE Trans Image Process 8:58–68, 1999

6. Lee C-H, Lee Y-K: An adaptive digital image watermarking technique for copyright protection. IEEE Trans Consum Electron 45:1005–1015, 1999

7. Ng KS, Cheng LM, Cheng LL, Wang MK: Adaptive watermarking by using pixel position shifting technique. IEEE Trans Consum Electron 45:1057–1064, 1999

8. Hwang M-S, Chang C-C, Hwang K-F: A watermarking technique based on one-way hash functions. IEEE Trans Consum Electron 45:286–294, 1999

9. Fridrich J, Goljan M, Du R: Invertible authentication. In: Proceedings of SPIE Photonics West, Security and Watermarking of Multimedia Content III. San Jose, CA, 2001, pp 197–208

10. Celik MU, Sharma G, Tekalp AM, Saber E: Reversible data hiding. In: IEEE International Conference on Image Processing. Rochester, NY, 2002, pp 157–160

11. Goljan M, Fridrich J, Du R: Distortion-free data embedding. In: The 4th Information Hiding Workshop. Pittsburgh, Pennsylvania, 2001, pp 27-41

12. Fridrich J, Goljan M, Du R: Invertible authentication watermark for JPEG images. In: Information Technology: Coding and Computing. Las Vegas, Nevada, 2001, pp 223–227

13. Vleeschouwer CD, Delaigle J-F, Macq B: Circular interpretation of bijective transformations in lossless watermarking for media asset management. IEEE Trans Multimedia 5:97–105, 2003

14. Gokturk SB, Tomasi C, Girod B, Beaulieu C: Medical image compression based on region of interest, with application to colon CT images. In: Annual Reports of the Research Reactor Institute, Kyoto University. Istanbul, Turkey, 2001, pp 2453–2356

15. Fridrich J, Goljan M, Du R: Lossless data embedding—new paradigm in digital watermarking. J Appl Signal Process 185–196, 2002

16. Fridrich J, Goljan M, Du R: Lossless data embedding for all image formats. In: Proceedings of SPIE Security and Watermarking of Multimedia Contents. San Jose, CA, 2002, pp 572–583

17. Du R, Fridrich J: Lossless authentication of MPEG-2

video. In: IEEE International Conference on Image Processing. Rochester, NY, 2002, pp 889–892

18. Welch TA: A technique for high-performance data-compression. IEEE Comput 17:8–19, 1984

19. Weinberger MJ, Rissanen JJ, Arps B: Applications of universal context modeling to lossless compression of gray-scale images. IEEE Trans Image Process 5:575–586, 1996

20. Shen L, Rangayyan RM: Lossless compression of continuous-tone images by combined inter-bit-plane decorrelation and JBIG coding. J Electron Imaging 6:198–207, 1997

21. Fridrich J: Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurc Chaos 8:1259–1284, 1998

22. Herrigel A, Ruanidh JO, Petersen H, Pereira S, Pun T: Secure copyright protection techniques for digital images. In: Information Hiding Workshop. Portland, Oregon, 1998, pp 169–190

23. Friedman GL: The trustworthy digital camera—restoring credibility to the photographic image. IEEE Trans Consum Electron 39:905–910, 1993

24. Schneider M, Chang S-F: A robust content based digital signature for image authentication. In: IEEE International Conference on Image Processing. Lausanne, Switzerland, 1996, pp 227–230

25. Queluz MP: Towards robust, content based techniques for image authentication. In: IEEE Workshop on Multimedia Signal Processing. Los Angeles, CA, 1998, pp 297–302

26. Wong PW, Memon N: Secret and public key image watermarking schemes for image authentication and ownership verification. IEEE Trans Image Process 10:1593–1601, 2001

27. Bhattacharjee S, Kutter M: Compression tolerant image authentication. In: IEEE International Conference on Image Processing. Chicago, IL, 1998, pp 435–439

28. Lu C-S, Liao H-YM: Multipurpose watermarking for image authentication and protection. IEEE Trans Image Process 10:1579–1592, 2001

29. Yu G-J, Lu C-S, Laio H-YM: Mean-quantization-based fragile watermarking for image authentication. Opt Eng 40:1396–1408, 2001

30. Kundur D, Hatzinakos D: Digital watermarking for telltale tamper proofing and authentication. Proc IEEE 87:1167–1180, 1999

31. Podilchuk CI, Delp EJ: Digital watermarking: algorithms and applications. IEEE Signal Process Mag 18:33–46, 2001

32. Lin ET, Podilchuk CI, Delp EJ: Detection of image alterations using semi-fragile watermarks. In: Proceedings of SPIE Security and Watermarking of Multimedia Contents. San Jose, CA, 2000, pp 152–163

33. Tefas A, Pitas I: Image authentication and tamper proofing using mathematical morphology. In: Proceedings of European Signal Processing Conference (EUSIPCO 2000), Tampere, Finland, 2000, vol 3, pp 1681–1684

34. Lee YL, Kim HC, Park HW: Blocking effect reduction of JPEG images by signal adaptive filtering. IEEE Trans Image Process 7:229–234, 1998

35. Han Y-H, Leou J-J: Detection and correction of transmission errors in JPEG images. IEEE Trans Circuits Syst Video Technol 8:221–231, 1998

36. Konstantinides K, Bhaskaran V, Beretta G: Image sharpening in the JPEG domain. IEEE Trans Image Process 8:874–878, 1999

37. In J, Shirani S, Kossentini F: On RD optimized progressive image coding using JPEG. IEEE Trans Image Process 8:1630–1638, 1999

38. Cheng H-D, Lui YM, Freimanis RI: A novel approach to microcalcification detection using fuzzy logic technique. IEEE Trans Med Imag 17:442–450, 1998