A Hierarchical Fragile Watermarking with VQ Index Recovery

Chin-Feng Lee
Chaoyang University of Technology/ Department of Information Management, Taichung, Taiwan
Email: lcf@cyut.edu.tw

Kuo-Nan Chen, Chin-Chen Chang and Meng-Cheng Tsai

A National Chung Cheng University/ Department of Computer Science and Information Engineering, Chiayi, Taiwan
bFeng Chia University/ Department of Information Engineering and Computer Science, Taichung, Taiwan
Email: {kuonan.chen, alan3c, abc.gods}@gmail.com

Abstract—This paper proposes a hierarchical fragile watermarking scheme for image authentication with localization and recovery. Two phases are exploited for pixel-wise and block-wise authenticity. By applying the singular value decomposition (SVD), only a few pixels need to be modified to carry these watermark bits so we can produce high quality of the watermarked image and achieve the integrity verification of blocks. Pixel-wise tampering detection and recovery is also realized in this proposed scheme. Altered pixels in each block can be exactly localized using the authentication bits. Accordingly, unaltered pixels remain unchanged but only altered pixels need to be recovered. In the image recovery stage, instead of replacing the whole block identified as tampered, elements belonging to associated VQ codeword are restored for those altered pixels. In this way, the quality of recovered image is better than replacing whole altered block by a whole vector quantization block. The experimental results reveal that the average PSNR values of reconstructed images are higher than that of other schemes.

Index Terms—image authentication, fragile watermarking, tampering detection, tampering localization and recovery

I. INTRODUCTION

With the continuous innovation of digital and network technology, technology applications play an important role in many people’s lives. For example, mobile phones now have built-in digital cameras almost as a standard. After taking pictures, we can immediately transfer to the network and share them with friends through wireless networks. When digital information is shared with such case, the copyright protection of digital content is an important issue.

Image authentication has become an issue of considerable interest in recent years, and the literature related to image authentication schemes to ensure the integrity of images and to detect unauthorized modification has grown markedly. Many fragile watermarking or semi-fragile watermarking schemes have been proposed for authentication of image content [4-6, 8, 11, 15-16, 18, 20]. Fragile watermarking indicates when an authentic watermark (generally independent of the image data) is inserted so any attempt to alter the content of an image will also alter the watermark. The authentication process detects the distortions in the watermark such that the image’s regions that have been tampered with can be located. The difference between a fragile watermark and a semi-fragile watermark is related to how well modifications of images are tolerated. Semi-fragile watermarking schemes [8, 20] allow some specific modifications, depending on the watermarking approach used. Semi-fragile watermarking considers some common modifications made by image processing techniques, such as JPEG compression, noising, blurring, or filtering legitimate. However, for the majority of the applications in military or medical fields, even the slightest modifications have to be identified, and semi-fragile watermarks are too insensitive to be suitable in such application domains. In this paper, we aim to the research related to fragile watermarking schemes.

There are two categories of fragile watermarks: the block-wise [1-2, 4, 14-15, 17] approach and the pixel-wise [11, 13] approach. A host image is divided into blocks or pixels depending on which approach is adopted. Each block or pixel feature is created and then embedded into the host image as authentication information, which is later used to locate precisely any malicious alterations made to the image while verifying other areas of the images as authentic. In terms of computation complexity and execution efficiency, block-wise approaches are superior to pixel-wise approaches; however, the block-wise approach is not as sensitive to malicious manipulations as the pixel-wise approach and cannot locate exactly which pixel or pixels have been tampered with. With the block-wise approach, a pixel that has not been destroyed or manipulated may be considered an altered pixel because the block in which it is located is deemed to have been tampered with. In contrast, the pixel-wise approach more precisely locates the fake content, although, in some situations, the information derived from altered pixel values may coincide with the watermark itself. Therefore, pixel-wise approaches can not always localize the tampered pixels precisely.

In 2008, Wang et al. proposed a fragile watermarking scheme based on singular value decomposition (SVD) to ensure the integrity of biometric images [15]. The proposed scheme achieves a high quality watermarked
image by applying the whole biometric images, rather than dividing it into many sub-blocks. However, the method cannot locate the altered area precisely because the authentication information is correlated with the whole image, not parts of it, like blocks. Therefore, achieving a good balance between the quality of a watermarked image and the effectiveness of information detection is quite a challenging task.

If an authorized receiver finds that a host image has been tampered with, he or she can ask for the image to be retransmitted, but the retransmission cost is an issue. To address the problem of retransmission cost, image reconstruction is kind of a solution. Research on self-recovering schemes [17, 19] includes that proposed by Yang and Shen [17], in 2010, a VQ index table image-recovering scheme in which an index table produced by VQ compression is embedded into the host image four times to enhance the quality of image reconstruction. Codewords within the index table are embedded multiple times to increase the validity of block reconstruction.

This paper proposes a hierarchical fragile watermarking scheme with VQ index recovery. An SVD fragile watermarking scheme is employed such that each pixel associated with watermark bits can be adopted for pixel-wise authentication. If an image has been changed, the image content and the watermark corresponding with the altered blocks will not pass the verification, so the altered areas can be detected. After localizing the altered pixels within a block, valid pixels are kept unchanged. As for those altered pixels, they can be perfectly restored using the information from two copies of VQ index table.

II. RELATED WORKS

This section introduces an image recovery scheme using a VQ index table proposed by Yang and Shen [17], and a hierarchical fragile watermarking scheme proposed by Zhang and Wang [18].

a) Recover the tampered image based on vector quantization (VQ) indexing

In 2010, Yang and Shen [17] proposed an image recovery scheme using VQ indexing. When VQ is performed, an index table associated with the original image is produced. Using a secret key, the indices are randomly embedded into the second and third least-significant-bit planes of the original image four times. For example, assume that a 512×512 image is divided into 4×4 blocks and that a VQ codebook has a size of 256=25, where each index can be represented by an 8-bit string, so the size of an index table is 128×128 after vector quantization compression has been performed. For the index table to be embedded into 2-LSB2 and 3-LSB planes of the host image, the total required embedding space is 128×128×8. The total embeddable space for the 2-LSB and 3-LSB planes of the host image is 512×512×2 in bits. Therefore, the index table can be embedded four times to increase the reliability of the index after image has been reconstructed. Each index value \( x \), which is an encoding correlated with an image block, can be represented in eight bits, i.e., \( x = x_0 \times x_1 \times x_2 \times x_3 \times x_4 \times x_5 \times x_6 \times x_7 \) and be embedded into the 2-LSB and 3-LSB planes of four selected pixels. Fig. 1 illustrates the index value to be embedded into four pixels.

b) Fragile watermarking scheme using a hierarchical mechanism

Zhang and Wang [18] proposed a hierarchical fragile watermarking scheme that can verify and locate which pixels have been tempered with. There are two kinds of information for the hierarchical detection scheme: pixel-derived and block-derived watermarks.

For the pixel authentication, the pixel-derived watermark can be created as follows. The first to the third least-significant-bit (LSB) planes in the host image are employed to embed the watermark data, and the first to the fifth most-significant-bit (MSB) planes are kept unchanged for watermark generation. The watermark generating steps are as follows:

1. Denote the host image as \( M \times N \) and the number of pixels in the host image as \( n = M \times N \). Each pixel \( p_n \) can be represented as eight bits, i.e., \( p_n = b_{n,0}, b_{n,1}, ..., b_{n,7} \). Equation (1) shows that the five most significant bits of pixel \( p_n \) are multiplied by a pseudo-random binary matrix \( A_n \) to produce \( V \) authentication bits. Therefore, the total number of authentication bits for the host image is \( n \times V \).

\[
\begin{bmatrix}
a_{n,1} \\
a_{n,2} \\
\vdots \\
a_{n,5}
\end{bmatrix} = \begin{bmatrix}
b_{n,0} \\
b_{n,1} \\
\vdots \\
b_{n,7}
\end{bmatrix} \mod 2^V
\]  

where \( n = 1, 2, ..., M \times N \), the size of pseudo-random binary matrix \( A_n \) is \( V \times 5 \); \( [ a_n ] = [ a_{n,1}, a_{n,2}, ..., a_{n,V} ] \) is a vector of \( V \times 1 \) and \( V \) is a multiple of five.

2. Apply a secret key to pseudo-randomly divide \( n \times V \) authentication bits into a series of subsets, each subset containing \( K \) bits, where \( K = 2V/5 \). Then, the sum of \( K \) authentication bit values in each subset, called authentication-sum, is calculated. Perform modulo operation on the authentication-sum by 2 to get a sum-bit.

3. Divide \( n \) host pixels into non-overlapping blocks where the size of each block is \( 8 \times 8 \); assume that \( M \) and \( N \) are multiples of 8.
4. For each block, the first, second and third least-significant-bit (LSB) planes are employed to embed the watermark; accordingly, the embedding capacity within a block is 8 × 8 × 3 = 192 bits. Randomly select 160 positions to be replaced by the pixel-derived watermark so the remaining of embeddable space is 32 bits.

5. Perform a hash function by feeding the first to fifth most-significant-bits (MSB) of each pixel and the 160 sum-bit obtained in the previous step to generate 32 hash-bits, which then become a block-derived watermark.

For more details of pixel-derived and block-derived watermark embedding, Fig. 2 is to show watermark embedding procedure for an 8 × 8 host block.

The embedding space, i.e., 1-LSB, 2-LSB and 3-LSB planes of the block is 64 × 3 bits. The pixel-derived watermark is composed of 160 sum-bits and the block-derived watermark is made up of 32 hash-bits.

On the receiver side, the procedure to locate pixels that have been tampered with is made up of two stages: first, identify the altered blocks, and then locate the altered pixels in those blocks. If the hash of the 320 MSBs and 160 sum-bits in a block is not identical to the 32 hash-bits hidden in the same block, the block is judged as “tampered with.” After identifying the blocks that have been tampered with, the watermark hidden in the rest of the blocks are used to find the exact locations of the altered pixels.

III. PROPOSED SCHEME

In this paper, a hierarchical watermark embedding procedure is presented in three phases. The first phase contains two tasks: encode an index table associated with a given grayscale image using a vector quantization compression technique and embed the index table twice into the original image. This phase is performed so the altered areas of watermarked image can be recovered after they have been detected and located. The second and third phases of the procedure embed watermarks into the intermediate image derived from the first phase. In these two embedding phases, watermark data are derived from pixels and blocks. An authorized receiver can first locate the altered blocks using the block-derived watermarks and then use the pixel-derived watermarks hidden in the other unaltered blocks to locate the altered pixels. By spreading the pixel-derived watermarks extensively over the host pixels, these authentication data can be used to identify which pixels are tampered with because they will lack the watermark information they should have carried.

Fewer block-derived watermarks generated by the SVD operation on the host blocks can reduce image distortion and improve the ability to locate altered blocks.

A. VQ index embedding

The first phase computes index values of an image using the VQ technique and embeds the obtained index table into the original image for the purpose of image recovery. For a host image composed of \( M \times N \) pixels divided into non-overlapping blocks of 4 × 4 pixels, the total index values within an index table associated with that image are \((M \times N)/16\). If we assume there are 256 codewords in a codebook; with each codeword associated with an 8-bit index value, the total size for an index table is \( 8 \times ((M \times N)/16) = (M \times N)/2 \) in bits. For security considerations, these indices are rearranged into a random sequence \( R_s \) by a secret key \( Key_s \) and carried by the second least-significant-bit (2-LSB) plane of a host image. Because the size of generated indices is half of the whole embedding space, each index value can be embedded twice in order to enhance the recovery ability. In this phase of VQ index embedding, an intermediate image \( I_{VQ} \) is generated. Fig. 3 shows the steps for VQ index embedding.

The intermediate image acts as an input to the watermarking embedding procedure in the second phase of the procedure.

B. Two-phase watermark embedding

Two phases are exploited for pixel-wise and block-wise authenticity respectively.

According to the first phase of VQ index embedding, an intermediate image is generated and acts as an input to the second phase of the embedding procedure. For each intermediate pixel, first generate five authentication bits by applying (1), where \( V \) is five and \( A_n \) is a 5-by-5 pseudo-random binary matrix so there are \( 5 \times M \times N \) authentication bits in total for the intermediate image \( I_{VQ} \). Use a secret key \( Key_v \) to rearrange these authentication bits as a random sequence \( R_v \), select every five bits from \( R_v \) as a group, and calculate a sum-bit for each group. There are \((5 \times M \times N)/5\) sum-bits that will be embedded into the first LSB (1-LSB) plane of the intermediate image \( I_{VQ} \).

For security considerations, a secret key \( Key_v \) is applied to generate a sequence of embedding positions that indicate which intermediate pixels will carry the sum-bits. The watermarked image can thus be obtained by embedding the authentication sum-bits into the intermediated image \( I_{VQ} \).
Let $I_{\text{VQ,Rc}}$ stand for the watermarked image that carries the pixel-derived watermarks. Fig. 4 illustrates the pixel-derived watermark generation and presents the watermarked image $I_{\text{VQ,Rc}}$.

In the third phase, block-wise fragile watermark scheme based on SVD is presented to ensure the integrity and authenticity of the watermarked image $I_{\text{VQ,Rc}}$.

First, divide the image $I_{\text{VQ,Rc}}$ into 4-by-4 non-overlapping blocks. To generate the block-wise watermark associated with a block $B$, a secret key $Key_B$ is used to choose a masking block, which is a partner of block $B$, and the watermark corresponding to block $B$ is embedded into the masking block. Determine 9 pixels and set the first, second and third LSBs of those pixels as zeroes. Then, $B'$ is denoted as a masking block corresponding to block $B$, with three LSBs of nine pixels set as zeroes. To increase the security, 16 pixels in block $B'$ are shuffled using another secret key $Key_{E}$, and the shuffled block is denoted as $SB'$. Then calculate the singular values for these two blocks, i.e., $B'$ and $SB'$; each block will produce four singular values. To represent each singular value in a binary representation, multiply each singular value by a sensitive factor $\alpha$ and round it to an integer. Then perform a modulo-2 operation on this integer to produce an SVD-bit. Let four SVD-bits be denoted as $b_i, \ i=0,1,2,3$ for block $B'$ and another four SVD-bits $s_{bi}, i=0,1,2,3$ for block $SB'$. The sensitive factor $\alpha$ is adjustable; in most cases, the bigger the $\alpha$, the more sensitive the fragile watermarking performance. In Wang et al.'s scheme, they had more discussions about the sensitive parameter $\alpha$.

A flag bit $F$ is generated by (2) to detect whether the block can be destroyed by a cut-and-paste attack.

$$F = b_i \oplus b_i \oplus b_i \oplus b_i \oplus s_{b_i} \oplus s_{b_i} \oplus s_{b_i} \oplus s_{b_i} \oplus 1,$$  \hspace{1cm} (2)

where $b_i$ and $s_{bi}$ are SVD bits for blocks $B'$ and $SB'$, respectively; $0 \leq i \leq 3$.

A nine-bit watermark associated with each block is embedded into another block, also called masking block, and if the block is damaged, the embedded block-wise watermark can be extracted to perform the altered block localization. Each nine-bit watermark contains one flag bit $F$ and eight SVD-bits: $b_i$ and $s_{bi}, \ i=0,1,2,3$, for block $B'$ and block $SB'$, respectively. In a corresponding masking block, nine pixels are randomly selected and these nine watermark bits are hidden into the third LSB of those nine randomly chosen pixels. When all blocks have been dealt with, an image $I_{\text{VQ,Rc,SVD}}$ is the produced as shown in Fig. 5.

We remarked here that a flag bit is created and embedded for block authentication. In a situation in which a block has suffered a block-cut attack, all pixels within that destroyed block become zeros, implying that the SVD bits associated with that fake block are also computed as zeroes. At this time, the flag bit can function as a verifier against such a fake block.

C. Tampering detection and recovery

This section introduces how to verify an image’s integrity. The procedure contains three phases: block-wise tampering detection, pixel-wise tampering detection and pixel restoration.

For a given watermarked image $I_{\text{VQ,Rc,SVD}}$, in the proposed scheme, the top-down detection concept of hierarchical mechanism is employed. The regions that have been tampered with are first detected with a block-wise mechanism, and then the original pixels in the tampered regions are classified into two categories: altered pixels and unaltered pixels.

![Flowchart of block-wise watermark generation and embedding.](image)

Figure 5. Flowchart of block-wise watermark generation and embedding.
Finally, the index table is extracted from the normal pixels to recover the altered pixels in the way that the altered pixels are replaced by the mapped elements at the vector quantization block. In this way, the quality of recovered image is better than replacing whole altered block by a whole vector quantization block.

The first phase is SVD-based block verification. The image \( I_{ori} \) is divided into 4-by-4 non-overlapping blocks. For a block to be verified, first find its masking block with a secret key \( \text{key}_b \). In the masking block, determine 9 pixels whose third LSBs (3-LSB) have carried block-wise watermark bits. Accordingly, there are nine block-wise watermark bits, i.e., a flag bit \( \text{ef} \) and eight SVD bits, \( \text{eb}_i \) and \( \text{sh}_i \), for \( i = 0, 1, 2, 3 \). Extract nine block-wise watermark bits and clear the 3-LSBs of nine pixels as zeroes. Next, determine whether the extracted flag bit \( \text{ef} \) is equal to 1; if \( \text{ef} = 1 \), then block \( B \) has not suffered from a cut-paste attack; otherwise, block \( B \) will be located as a block that has been tampered with. In addition, verify whether the extracted 9 bits \( \text{eb}_i \parallel \text{sh}_i \parallel \text{ef} \) are equal to the watermark bits \( b_i \parallel s_i \parallel F \) of block \( B \). If they are not equal, then block \( B \) is identified as altered; otherwise, it is considered to be unaltered. The next task is to identify which pixels within the altered block have been altered.

Let \( p' \) be a pixel in an altered block. Apply (1) to obtain five authentication bits, which are denoted as \( a_{ut_1}, a_{ut_2}, a_{ut_3}, a_{ut_4}, \) and \( a_{ut_5} \), respectively. Reversing to the pixel-wise watermark-embedding procedure, a secret key \( \text{key}_w \) is used to determine every cluster to which each authentication bit belongs. Each cluster is comprised of five authentication data that can produce a sum-bit corresponding to each cluster. Assume that each authentication bit \( a_{ut_i} \) is associated with a sum-bit, \( s_i' \), for \( i = 1, 2, 3, 4 \) and 5. A secret key \( \text{key}_c \) helps to identify the pixels in which the five sum-bits have been hidden. Extract the sum-bits from 1-LSBs of those pixels and use them to verify whether the pixel \( p' \) is fake or not.

For a given altered block with \( k \) pixels that have been modified, the following pixel restoration using VQ index values is employed. We know that each VQ index is associated with a codeword in a codebook, and that each codeword is a vector of 16 elements, where each element is a pixel of the image. For a block that has been identified as altered, its codeword index which has been embedded twice, can be extracted. Through the index, a codeword vector can be obtained from the codebook. Therefore, \( k \) fake pixels within that tampered block can be replaced with \( k \) codeword elements.

IV. EXPERIMENTAL RESULTS

Two general characteristics of fragile watermark technique are its ability to detect the altered location and its ability to retain image quality. In addition, the quality of recovered image is another important issue. Simulations of the proposed scheme are performed in order to determine the scheme’s detection capability, watermarked image quality and recovered image quality.

A. Tampering detection capability

Common image processing attacks such as cut, salt-and-pepper noise, and text-adding are performed to evaluate the capacity of the proposed scheme for detecting tampering. Fig. 6 shows that the proposed scheme can exactly detect any modifications to the watermarked image.

Figs. 6(a), (b) and (c) show images are attacked and Figs. 6(d), (e) and (f) present the detection results by the proposed scheme. Fig. 6(a) shows that the image “Sailboat” has been cut with a square. In Fig. 6(b), salt-and-pepper noise is added to the image “Pepper”; In Fig. 6(c), several lines are randomly drawn on the face of image “Lena.” Figs. 6(d), (e) and (f) reveal that the proposed scheme precisely locates out the altered areas.

After an altered block has been determined, we can also distinguish the actual altered pixel in that block. Fig. 10 shows that the text “CCU” has been added at the center of the image “Sailboat.” In order to illustrate the altered area clearly, a binary image is employed in which a white pixel indicates an altered pixel and vice versa. Figs. 7(b)-(c) show the altered block by block-wise localization and Figs. 7(d)-(e) show the result of tamper pixel detection. Another simulation on image “Lena” is shown in Fig. 8(a) in which the text “copyright” is added at the top-right of the image. Figs. 8(b)-(c) show the altered block by block-wise localization and Figs. 8(d)-(e) show the result of altered pixel detection. The enlarged black-and-white images in Figs. 7(c) and 8(c) show that the images are modified from a block-wise viewpoint. The enlarged black-and-white images of Figs. 7(e) and 8(e) show that the proposed scheme has the ability to locate the altered pixels in a pixel-wise manner.

B. Watermark image quality

The simulation results were evaluated using the peak signal-to-noise ratio (PSNR), which is expressed as follows:

\[
\text{PSNR} = 10 \times \log_{10} \frac{255^2}{MSE},
\]

where

\[
MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{ij} - X'_{ij})^2,
\]

and \( M \) and \( N \) are the width and length of the image, respectively, and \( X_{ij} \) and \( X'_{ij} \) are the pixel values of the original image and the watermarked image, respectively. The fifteen images displayed in Fig. 9 are used as test images in the simulations.

Table 1, which presents the quality of the watermarked images, shows that the proposed scheme yields more stable and higher PSNR values, with an average PSNR of 39.6dB greater than those obtained by using the algorithm of Yang and Shen.
Figure 6. Image attacks and detection results

Figure 7. Comparison of block-wise and pixel-wise detection for image “Sailboat.”

Figure 8. Comparison of block-wise and pixel-wise detection for “Lena”

C. Recovery image quality

In this section, we compare Yang and Shen’s scheme [17] with our proposed scheme in terms of recovered image quality. Yang and Shen’s scheme detects an altered block and recovers it by extracting the index value from unaltered parts of the image using a vector quantization recovery scheme. Although the recovered image seems the same as the original one to the human eyes, we can zoom in to the recovered region and observe that that region is not very smooth. The pixel recovery procedure of proposed scheme can first identify which pixels are unaltered and then keep the unaltered pixels unchanged, even though they are located in a block which is detected as a tampered block. Vector quantization recovery is used restore those altered pixels.

Several simulations are conducted to compare the performance of Yang and Shen’s scheme with the proposed recovery scheme. In Fig. 10(a), a line is added at the left edge of the letter “H”; Fig. 10(b) shows a 500% magnification of the recovered part using Yang and Shen’s scheme, and Fig. 10(c) shows the 500% magnification of the recovered part using the proposed scheme. Fig. 11(a) shows modifications of the Sailboat image, and Fig. 12(a) shows a cross symbol on the Boat image. Figs. 11(b) and 11(c) show the 500% magnification of the recovered part of Yang and Shen’s scheme and our proposed scheme; comparing to the red regions in the two images, the region using our recovery scheme is smoother than that of Yang and Shen’s
scheme. In Fig. 12(b), the rope in the red region is more blurred than that in Fig. 12(c). We also measure the PSNR values of the magnified regions: Fig. 11(b)’s PSNR value is 37.1 dB, Fig. 11(c)’s is 38.8 dB, Fig. 12(b)’s is 37.3 dB and Fig. 12(c)’s is 39.4 dB. We test fifteen images, as presented in Fig. 9, by sketching a large cross symbol on the center of those images. Fig. 13(a) is the test image “Lena,” and Fig. 13(b) shows the cross drawn on the Lena image, which is an altered region of 128×128 pixels. The recovered results for the altered region using Yang and Shen’s scheme and the proposed scheme are shown in Figs. 13(c) and (d), respectively. Both recovered images present the same as the original one to the human eyes. However, the image PSNR values for the scheme of Yang and Shen and the proposed scheme are 36.0 dB and 37.9 dB respectively. As for the other fourteen test images, the image PSNR values of proposed scheme are all greater than those of Yang and Shen’s scheme. Table 2 illustrates the two schemes’ performance in terms of recovered image quality for all fifteen test images. For all recovered images, the experimental results shows that the proposed scheme has higher PSNR values and achieves superior performance in image reconstruction.

![Figure 10](image1.png)
(a) text H
(b) 500% Zoom-in
(c) 500% Zoom-in

Figure 10. Enlarged letter “H”: (a) a segment line is added on the left of the original letter “H”; image recovered using (b) Yang and Shen’s scheme (c) proposed scheme.

![Figure 11](image2.png)
(a) Sailboat
(b) 500% Zoom-in
(c) 500% Zoom-in

Figure 11. (a) A modifications on image “Sailboat”; enlarged image recovered by (b) Yang and Shen’s scheme (c) proposed scheme.

![Figure 12](image3.png)
(a) Boat
(b) 500% Zoom-in
(c) 500% Zoom-in

Figure 12. (a) A cross added on image “Boat”; enlarged image recovered by (b) Yang and Shen’s scheme (c) proposed scheme.

![Figure 13](image4.png)
(a)
(b)
(c)
(d)

Figure 13. Comparison of image recovery of image “Lena” for the tampered region.

<table>
<thead>
<tr>
<th>Test images</th>
<th>Image PSNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yang and Shen’s</td>
</tr>
<tr>
<td>F16</td>
<td>34.5</td>
</tr>
<tr>
<td>Baboon</td>
<td>36.1</td>
</tr>
<tr>
<td>Barbara</td>
<td>34.9</td>
</tr>
<tr>
<td>Boat</td>
<td>34.4</td>
</tr>
<tr>
<td>Elaine</td>
<td>35.6</td>
</tr>
<tr>
<td>Family</td>
<td>34.3</td>
</tr>
<tr>
<td>Girl</td>
<td>36.3</td>
</tr>
<tr>
<td>Gold Hill</td>
<td>35.9</td>
</tr>
<tr>
<td>Lena</td>
<td>36.0</td>
</tr>
<tr>
<td>Pepper</td>
<td>35.1</td>
</tr>
<tr>
<td>Sailboat</td>
<td>35.0</td>
</tr>
<tr>
<td>Stream and Bridge</td>
<td>33.6</td>
</tr>
<tr>
<td>Tiffany</td>
<td>37.0</td>
</tr>
<tr>
<td>Toys</td>
<td>34.5</td>
</tr>
<tr>
<td>Zelda</td>
<td>37.0</td>
</tr>
<tr>
<td>Average</td>
<td>35.3</td>
</tr>
</tbody>
</table>

V. CONCLUSIONS

This paper proposes a hierarchical fragile watermarking scheme for image authentication with localization and recovery. Using SVD watermarking, a few authentication bits associated with a block are produced, so only a few pixels need to be modified to carry these watermark bits, with the result that the quality of the watermarked image remains high at 39.6 dB. Moreover, an attack relative to the block-cut results in the pixel value becoming zeroes. Through the pixel-level detection of tampering, the image recovery stage needs only to recover the altered pixels instead of replacing the whole block. In the experimental results, several attacks are simulated, such as cut-paste and added text on the image. With our pixel recovery scheme, the altered block is not restored by using a VQ codeword vector on the whole block. Pixels are identified as fake or not, and authentic pixels are retained while on the fake pixels are replaced. From the experimental results, the average PSNR values of reconstructed images are higher using our scheme than those when using Yang and Shen’s scheme.

REFERENCES

of the IEEE International Conference on Image Processing


Chin-Feng Lee received his Ph.D. degree in Computer Science and Information Engineering from National Chung Cheng University, Taiwan. She is currently an Associate Professor of Information Management at Chaoyang University of Technology, Taiwan.

Her research interests include database design, data mining, image processing, and information hiding.

Kuo-Nan Chen received his B.S degree in Information Engineering and Computer Science from Feng Chia University and his MS degree in Educational Measurement and Statistics from National Tsing Hua University. Currently, he is a Ph.D. student in Computer Science and Information Engineering at National Chung Cheng University, Taiwan. His research interests include image data hiding technologies.

Chin-Chen Chang received his Ph.D. degree in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. During the academic years of 1980-1983, he was on the faculty of the Department of Computer Engineering at the National Chiao Tung University.

From 1983-1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From August 1989 to July 1992, he was the head of, and a professor in, the Institute of Computer Science and Information Engineering at the National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the dean of the college of Engineering at the same university. From August 1995 to October 1997, he was the provost at the National Chung Cheng University. From September 1996 to October 1997, Dr. Chang was the Acting President at the National Chung Cheng University. From July 1998 to June 2000, he was the director of Advisory Office at the Ministry of Education of Taiwan. He is currently a Fellow of IEEE and a Fellow of IEE, UK. And since his early years of career development, he consecutively won Outstanding Youth Award of Taiwan, Outstanding Talent in Information Sciences of Taiwan, Acer Dragon Award of the Ten Most Outstanding Talents, Outstanding Scholar Award of Taiwan, Outstanding Engineering Professor Award of Taiwan, Chung-Shan Academic Publication Awards, Distinguished Research Awards of National Science Council of Taiwan, Outstanding Scholarly Contribution Award of the International Institute for Advanced Studies in Systems Research and Cybernetics, Top Fifteen Scholars in Systems and Software Engineering of the Journal of Systems and Software, and so on. Professor Chang’s specialties include, but not limited to, data engineering, database systems, computer cryptography and information security.

Meng-Cheng Tsai received his MS degree in Computer Science from Chinese Culture University, Taiwan. His research interests include image data hiding technologies.