Repairable Image Authentication Scheme

Yi-Hui Chen[1,2], Chih-Yang Lin[1,2], Wanutchaporn Sirakriengkrai[1], and I-Chun Weng[1]
(Corresponding author: Chih-Yang Lin)

Department of Computer Science and Engineering, Asia University[1]
500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
(Email: andrewlin@asia.edu.tw)
Department of Medical Research, China Medical University Hospital, China Medical University[2]
Taichung 40402, Taiwan

(Received May 16, 2013; revised and accepted Jan. 24 & Apr. 8, 2014)

Abstract

Nowadays, authentication mechanism is widely applied to digital images to verify whether the received image is not a fake. In this paper, we propose a self-authentication mechanism without any extra data to authenticate whether the area is modified by comparing the generated authentication code and hidden authentication code together. Also, the recovery ability is employed to the proposed scheme used to repair the modified area. In our experimental result, we show the positive result for the feasibility of the proposed scheme.

Keywords: Image authentication, located mechanism, recovery

1 Introduction

Image authentication is a mechanism to authenticate whether the areas is modified during transmission over the internet. The content of the image may be replaced with fake information, thus to identify the fake area even to recovery it after it is judged as an illegal place. One class of fragile watermarking method [2, 5, 10, 11, 12], the original image is separated into several small blocks; then, embeds the watermark into these blocks. While tempering the image, the matching between the content and the watermark in the corresponding block will be destroyed. As for pixel-wise fragile watermarking scheme [3, 4, 6, 7, 8, 9], this method the tampered pixels can be specified from the absence of the carried watermark. In other work [13], a hierarchical fragile watermarking mechanism, this method obtains the watermark data from pixels and blocks.

The receiver can identify the blocks inauthentic according to the watermark hidden in other blocks to locate the tampered pixels. The scheme [13] combined the advantages of block-wise and pixel-wise technique to find the detailed tampering pattern even though the modified area is too large. Some watermarking approach with content restoration is not feasible because the tampered area is too large to locate tampered pixels. In scheme [13], it has a limit that the tempered pixels cannot be restored if the percentage of tampered area is more than 6.6%. In scheme [1], the features of an image are obtained from the cryptographic hash function which only the owner can prove the rightful ownership with the pre-determined secret key. The scheme [1] can achieve the tampering detection for ownership protection, but it cannot recover the tampered areas.

In this paper, we proposed a self-authentication mechanism as well as recovery abilities for digital images. In the proposed scheme, the authentication codes for a digital image generated by itself with recovery data are to hides back into the original one. After that, receivers can extract the hidden data to check whether it is not a fake one. The fake area is detected and marked. Later on, the extracted recovery data could be used to repair the tampered area without any extra data.

2 Related Work

In this section, we introduce traditional (t, n)-threshold secret sharing.

Shamir *et al.* proposed the (t, n)-threshold secret sharing as shown in Equation (1), which the secret is treated as the parameter r_1 and the other parameters r_2, r_3, $\cdots$, r_t are chosen by random to construct a $(t-1)$-degree polynomials.

$$R(x_i) = r_1 + r_2 x_i + r_3 x_i^2 + \cdots + r_t x_i^{t-1}, \tag{1}$$

where the value of x_i is the ID of the i^{th} participant, and all x_i's are individual from each other. Hence, n participants will construct n $(t-1)$-degree polynomials, as shown in Equation (2).

$$\begin{cases} R(x_1) = r_1 + r_2 x_1 + r_3 x_1^2 + \cdots + r_t x_1^{t-1}, \\ \qquad \vdots \\ R(x_n) = r_1 + r_2 x_n + r_3 x_n^2 + \cdots + r_t x_n^{t-1} \end{cases} \tag{2}$$

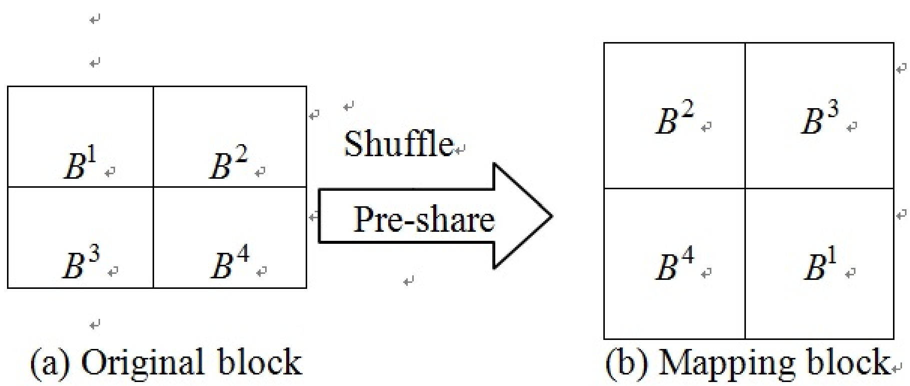


Figure 1: Illustration of a four-pixel block

The unknown messages r_1 can be resolved with the polynomial interpolation, shown in Equation (3), where t participants join to re-constructing procedure. The $(t-1)$-degree polynomial will be reconstructed.

$$\begin{aligned} R(x) &= R(x_1)(\frac{x-x_2}{x_1-x_2})(\frac{x-x_3}{x_1-x_3})\cdots(\frac{x-x_t}{x_1-x_t})+ \\ &\quad \vdots \\ &\quad R(x_t)(\frac{x-x_1}{x_t-x_1})(\frac{x-x_2}{x_t-x_2})\cdots(\frac{x-x_{t-1}}{x_t-x_{t-1}}). \end{aligned} \quad (3)$$

3 The Proposed Scheme

The proposed scheme consists of four procedures:

1) The secret sharing procedure;

2) The authentication generation procedure;

3) The authentication;

4) Secret reconstruction procedures and recovery of the inauthentic area.

First, the secret sharing procedure shows how the secret image is separated into shares. Second, the authentication codes generation procedure shows how to generate the authentication code and the recovery data. Third, the authentication and reconstruction procedures prove whether the image is authentic. If not, the inauthentic area will be marked and adjust the results of the authentication procedure. After that, the inauthentic area will be repaired during the last procedure.

3.1 Secret Sharing Procedure

Assume that the original image is the size of $n \times n$ pixels, where $n = 4$. Then divides original image into non-overlapping block with 2×2 pixels and pixels of the μ-th block are denoted as P_1^μ, P_2^μ, P_3^μ and P_4^μ where μ is the block ID, and $1 \leq \mu \leq \frac{n \times n}{16}$. The average value for the μ-th block, denoted as B^μ, i.e., $B^\mu = \sum_{i=1}^{4} P_i^\mu/4$. After that, a pre-shared key is used to shuffle the block positions shown in Figure 1(a) and 1(b) as the results before shuffled and after shuffled, respectively. For a given block the average value of mapping block is denoted as $\bar{B}^\mu$. B^μ and $\bar{B}^\mu$ are treated as a partner-block pair. For example, B^1 and B^2 are a partner-block pair in Figure 1. Next the value of is represented with a 7-based notation. For example, if $\bar{B}^\mu = 100$ and translated into 7-based notations as $(202)_7$, and the digits in $\bar{B}^\mu$ are denoted as $\bar{B_1}^\mu$, $\bar{B_2}^\mu$, and $\bar{B_3}^\mu$, respectively. That is, $\bar{B_1}^\mu = 2$, $\bar{B_2}^\mu = 0$, and $\bar{B_3}^\mu = 2$.

We reconstruct a formula with the values of $\bar{B_1}^\mu$, $\bar{B_2}^\mu$, and $\bar{B_3}^\mu$ as Equation (4).

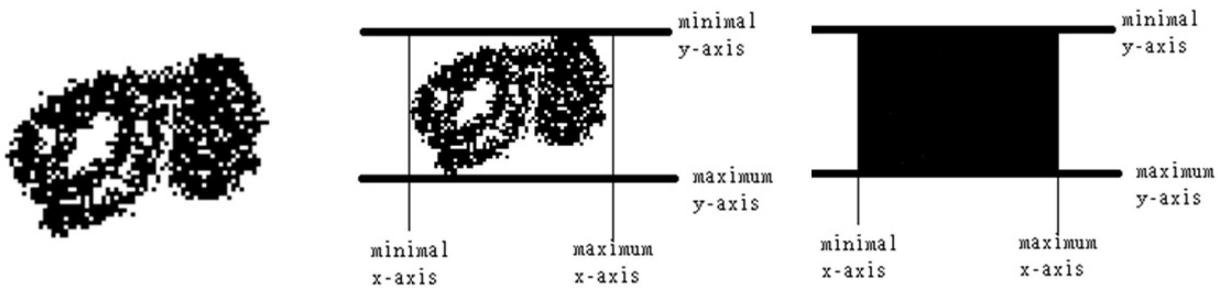
$$R_B(x_i) = \bar{B_1}^\mu + \bar{B_2}^\mu x_i + \bar{B_3}^\mu x_i^2 \bmod 7. \quad (4)$$

Here, the notation i means the i-th input value and μ is the block ID. Assume that x_1, x_2, and x_3 are 2, 3, and 5, respectively. If $\bar{B_1}^\mu$, $\bar{B_2}^\mu$, and $\bar{B_3}^\mu$ are 2, 0, 2, the formula are built through Equation (1) as $R_B(x_i) = 2 + 0x_i + 2x_i^2 \bmod 7$. Then we input the predefined value of x_1, x_2, and x_3 to be as 2, 3, and 5 and input into Equation (1) to get the value of $R_B(x_1 = 2)$, $R_B(x_2 = 3)$, and $R_B(x_3 = 5)$ as 3, 6, and 3, respectively.

Later on, we translate $R_B(x_1 = 2)$, $R_B(x_2 = 3)$, and $R_B(x_3 = 5)$ into binary bit streams and depicted as A_{b1}^μ, A_{b2}^μ and A_{b3}^μ. For example, while the values of $R_B(x_1 = 2)$, $R_B(x_2 = 3)$, and $R_B(x_3 = 5)$ are 3, 6, and 3, the values of A_{b1}^μ, A_{b2}^μ and A_{b3}^μ will be $(011)_2$, $(110)_2$, and $(011)_2$, respectively. After that, we embed the generated shares into original image by replacing the least three significant bits of pixels P_1^μ, P_2^μ and P_3^μ with the values of A_{b1}^μ, A_{b2}^μ, A_{b3}^μ, and A_{b4}^μ to generate the stego-pixels. After embedding, stego-pixel values are 163, 150 and 171, and depicted as $\bar{P_1}^\mu$, $\bar{P_2}^\mu$, $\bar{P_3}^\mu$ and $\bar{P_4}^\mu$.

3.2 The Authentication Generation Procedure

In this procedure, we describe how to generate the authentication codes for block B^μ. The authentication



(a) Authentication detection results (b) The area of authentication detection results (c) Inauthentic area adjustment

Figure 2: Adjustment method of the authentication results

codes generated for the block B^μ is denoted as A^μ. The given block B^μ contains four pixels, i.e., P_1^μ, P_2^μ, P_3^μ and P_4^μ. Let four pixels be a group, and each pixel must be transformed into a binary stream. For example, when $P_1^\mu = 161$, $P_2^\mu = 146$, $P_3^\mu = 170$, and $P_4^\mu = 86$, then translated into a binary bit stream as $(10100000)_2$, $(10010010)_2$, $(10101010)_2$, and $(01010110)_2$, respectively. Later on, we keep the five most significant bits of P_i^μ and represented as $P_{i,1}^\mu$, $P_{i,2}^\mu$, $P_{i,3}^\mu$, $P_{i,4}^\mu$, and $P_{i,5}^\mu$, for $i = 1$ to 4. For example, the most five significant bits of P_i^μ are presented by $P_{1,1}^\mu$, $P_{1,2}^\mu$, $P_{1,3}^\mu$, $P_{1,4}^\mu$, and $P_{1,5}^\mu$ as 1, 0, 1, 0, and 0, respectively. The authentication must be generated with Equation (5) and the values of A_1^μ, A_2^μ, A_3^μ, A_4^μ, and A_5^μ must be generated with Equation (6), for $j = 1$ to 5, "$\oplus$" means XOR (Exclusive OR) operation.

$$A^\mu = A_1^\mu \times 2^4 + A_2^\mu \times 2^3 + A_3^\mu \times 2^2 + A_4^\mu \times 2 + A_5^\mu \mod 8. \quad (5)$$

$$A_j^\mu = P_{1,j}^\mu \oplus P_{2,j}^\mu \oplus P_{3,j}^\mu \oplus P_{4,j}^\mu. \quad (6)$$

For example, with Equation (6), $A_1^\mu = 1 \oplus 1 \oplus 1 \oplus 0 = 1$; and thus $A_1^\mu = 1$, $A_2^\mu = 1$, $A_3^\mu = 0$, $A_4^\mu = 0$, and $A_5^\mu = 1$, respectively. Through Equation (5), A^μ is equal to 1 (i.e., $A^\mu = 25 \bmod 8 = 1$). Then A^μ transform into a 3-bit binary stream, denoted as $A_{b4}^\mu = (001)_2$. Finally, we embed the generated authentication codes into the pixel P_4^μ by replacing the least three significant bits of pixel P_4^μ with the value of A_{b4}^μ to generate the stego-pixels. After embedding, the fourth pixel value of the block B^μ is changed as 81, which is depicted as $\bar{P_4}^\mu$.

3.3 Authentication Procedure

In this procedure, we describe the way to extract the hidden information and to authenticate whether the secret image is an authentic one. The watermarked image is the size of $n \times n$ pixels then divided into non-overlapping blocks with size of 2×2 pixels a block. For a given block, four pixels in the μ-th block are denoted as $\bar{P_1}^\mu$, $\bar{P_2}^\mu$, $\bar{P_3}^\mu$, and $\bar{P_4}^\mu$, where μ is the block ID.

For a given pixel $\bar{P_i}^\mu$, we keep the five most significant bits and represented as $\bar{P_{i,1}}^\mu$, $\bar{P_{i,2}}^\mu$, $\bar{P_{i,3}}^\mu$, $\bar{P_{i,4}}^\mu$, and $\bar{P_{i,5}}^\mu$, for $i = 1$ to 4. For example, if $\bar{P_1}^\mu = 163$, the binary bits stream will be $(10100)_2$. Therefore, the most five significant bits are presented by $\bar{P_{i,1}}^\mu$, $\bar{P_{i,2}}^\mu$, $\bar{P_{i,3}}^\mu$, $\bar{P_{i,4}}^\mu$, and $\bar{P_{i,5}}^\mu$ as 1, 0, 1, 0, and 0, respectively. The authentication code must be generated with Equation (5). Then, we can extract the hidden authentication codes by the last three bits pixel of the block. We compare the generated authentication codes with the extracted authentication codes together to check whether they are the same. If true, it judged as an authentic block; otherwise, inauthentic.

There is a risk that some pixels are not detected as inauthentic pixel as shown in Figure 2(a). Thus, the biggest area covers all the possible inauthentic pixels to adjust the authentication results. That is, the most minimal and most maximum x-axis and y-axis are recorded. The pixels located at the range from the minimal x-axis to the maximum x-axis and also in the range of minimum y-axis and maximum y-axis are treated as inauthentic pixels. As shown in Figure 2, Figure 2(a) is the original authentication results. The minimal and maximum x-axis and y-axis are found as shown in Figure 2(b). All the pixels locate at the range of the minimal and maximum x-axis and y-axis are treated as inauthentic pixels as shown in Figure 2(c).

3.4 Reconstruction Procedure

The pixels $\bar{P_1}^\mu$, $\bar{P_2}^\mu$, $\bar{P_3}^\mu$, and $\bar{P_4}^\mu$ are transformed into a binary streams, individually. Next, we get the last three bits of the transformed binary stream and then transform the 3-bit binary stream into three decimal digits as the returned values of $\bar{R_B}(x_1 = 2)$, $\bar{R_B}(x_2 = 3)$, and $\bar{R_B}(x_3 = 5)$. Finally, the values of $\hat{B_1}^\mu$, $\hat{B_2}^\mu$, and $\hat{B_3}^\mu$ can be obtained with Equation (7). The mean value of the mapping block, denoted as $\hat{B}^\mu$ is obtained with Equa-

Table 1: Visual qualities of the five test images

Images	Visual qualities		
	PSNR of watermarked image	PSNR of modified Image	PSNR of recovery image
Barbara	38.13	27.05	35.82
Baboon	38.58	25.03	39.09
Boats	38.13	29.26	30.06
Cartoon	37.71	23.34	30.12
Goldhill	38.13	25.92	30.20

tion (8).

$$\begin{aligned}
\hat{B_1}^{\mu} &= [\frac{1}{(x_1-x_2)(x_1-x_3)}] \times \bar{R_B}(x_1) + \\
&\quad [\frac{1}{(x_2-x_1)(x_2-x_3)}] \times \bar{R_B}(x_2) + \\
&\quad [\frac{1}{(x_3-x_1)(x_3-x_2)}] \times \bar{R_B}(x_3) \bmod 7 \\
\hat{B_2}^{\mu} &= [\frac{(x_2+x_3)}{(x_1-x_2)(x_1-x_3)}] \times \bar{R_B}(x_1) + \\
&\quad [\frac{(x_1+x_3)}{(x_2-x_1)(x_2-x_3)}] \times \bar{R_B}(x_2) + \\
&\quad [\frac{(x_1+x_2)}{(x_3-x_1)(x_3-x_2)}] \times \bar{R_B}(x_3) \bmod 7 \\
\hat{B_3}^{\mu} &= [\frac{x_2 x_3}{(x_1-x_2)(x_1-x_3)}] \times \bar{R_B}(x_1) + \\
&\quad [\frac{x_1 x_3}{(x_2-x_1)(x_2-x_3)}] \times \bar{R_B}(x_2) + \\
&\quad [\frac{x_1 x_2}{(x_3-x_1)(x_3-x_2)}] \times \bar{R_B}(x_3) \bmod 7
\end{aligned} \tag{7}$$

$$\hat{B}^{\mu} = \hat{B_1}^{\mu} \times 7^2 + \hat{B_2}^{\mu} \times 7 + \hat{B_3}^{\mu}. \tag{8}$$

For example, the pixel values in the four-pixel block are represented as $\bar{P_1}^{\mu} = 163$, $\bar{P_2}^{\mu} = 150$, $\bar{P_3}^{\mu} = 171$, and $\bar{P_4}^{\mu} = 81$, respectively. Later on, we can get the values of $\bar{R_B}(x_1 = 2)$, $\bar{R_B}(x_2 = 3)$, and $\bar{R_B}(x_3 = 5)$ as 3, 6, and 3, respectively. Finally, with Equation (7), we can calculate the values of $\bar{B_1}^{\mu}$, $\bar{B_2}^{\mu}$, and $\bar{B_3}^{\mu}$ as 2, 0, and 2, respectively, and $\hat{B}^{\mu} = 100$. Then, we reshuffle the mean values back to be the original block location. Finally, we duplicate the mean value of block to expend to four pixels in the block to generate a new image WI.

If the block located at (i, j)-position is judged an inauthentic block, the four pixel values of the block are all replaced with the values of the pixels located at (i, j)-axis of WI'.

4 Experimental Results

In this section, we show our experimental results and the performances of our proposed scheme. Five grayscale images with size 256×256 pixels are as test images in the experiments, which are named "Barbara", "Baboon", "Boat", "Cartoon", and "Gold Hill". The visual quality measured by PSNR (peak-signal-to noise ratio) is used to evaluate the visual qualities between the original images and the watermarked images as listed in Table 1.

To measure the authentication and recovery abilities, five examples modified images are shown in Figures 3(a)-(e). After the authentication and reconstruction method, the located areas are shown in Figures 3(f)-(j), where the modified area is marked with black color. After recovery procedure, the recovery results are illustrated in Figures 3(k)-(o). The visual qualities of the recovery image are good to recognize what the original look like with naked eyes even the modified area is up to 50% (see Figure 3(l)).

5 Conclusion

In this paper, we proposed a self-authentication mechanism with recovery ability for digital images. With the proposed system, the image is authenticated whether the area is modified by comparing the generated authentication code and hidden authentication code together. Moreover, this scheme can reconstruct the secret image. In the experimental results, the proposed scheme shows the positive results to confirm its feasibility.

Acknowledgments

This work was supported by the Ministry of Science and Technology of Taiwan under Grant No. 103-2221-E-468-017.

References

[1] C. C. Chang, Y. H. Hu, and T. C. Lu, "A watermarking-based image ownership and tampering authentication scheme," *Pattern Recognition Letters*, vol. 27, pp. 439-446, 2006.

[2] C. C. Chang, T. S. Nguyen, and C. C. Lin, "Reversible image hiding for high image quality based on histogram shifting and local complexity," *International Journal of Network Security*, vol. 16, no. 3, pp. 208-220, 2014.

[3] Y. H. Chen, P. Prangjarote, and C. Y. Lin, "Self-verifiable secret sharing scheme with locatability for halftone Images," *International Journal of Network Security*, vol. 17, no. 3, pp. 246-250, 2015.

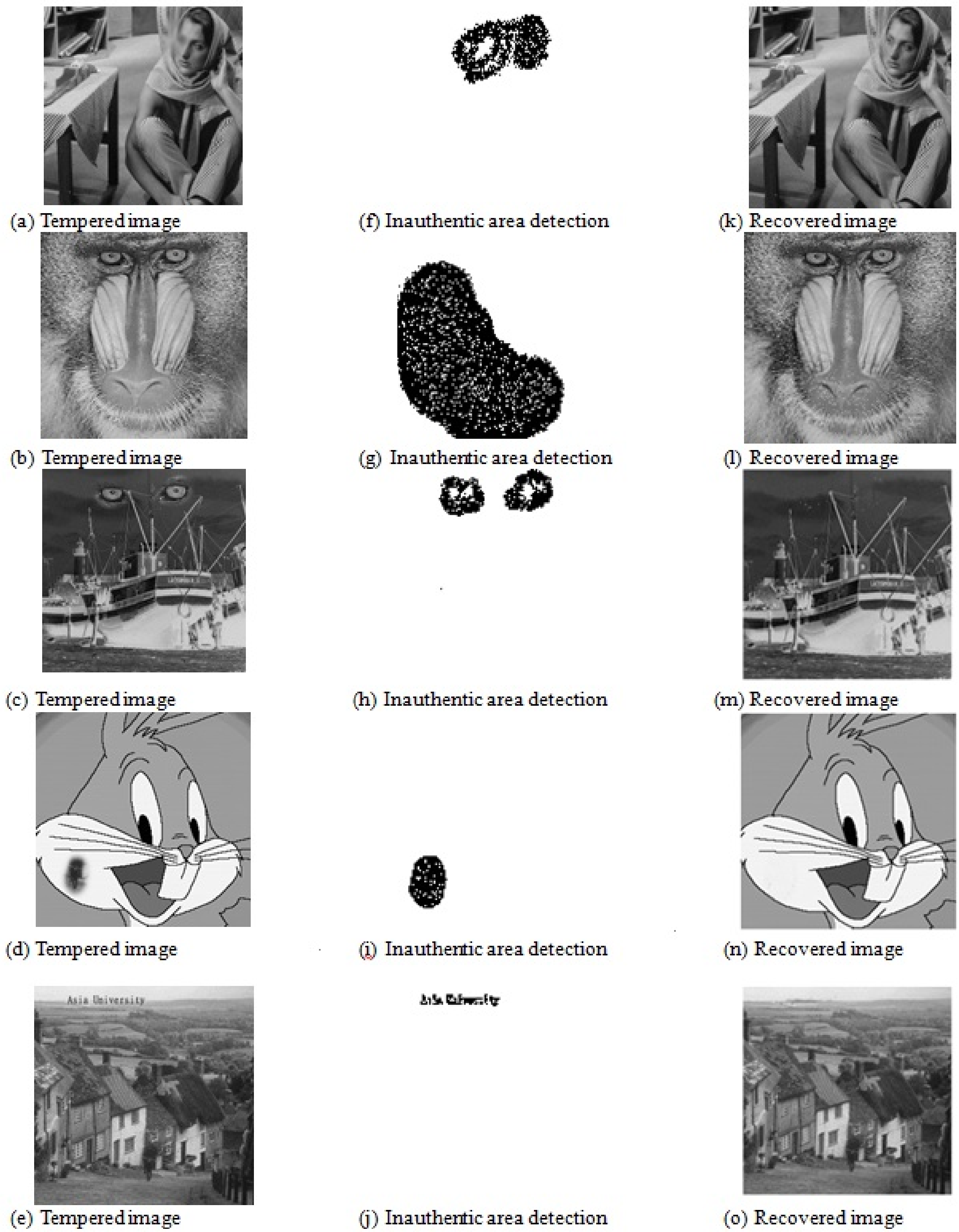


Figure 3: The tempered images and their corresponding recovery result

[4] H. He, J. Zhang, and H. M. Tai, "A wavelet-based fragile watermarking scheme for secure image authentication," in *Proceedings of the 5th International Workshop Dig. Watermarking*, vol. 4283, pp. 422-432, 2006.

[5] B. Karthikeyan, S. Ramakrishnan, V. Vaithiyanathan, S. Sruti, and M. Gomathymeenakshi, "An improved steganographic technique using LSB replacement on a scanned path image," *International Journal of Network Security*, vol. 16, no. 1, pp. 14-18, 2014.

[6] S. H. Liu, H. X. Yao, W. Gao, and Y. L. Liu, "An image fragile watermark scheme based on chaotic image pattern and pixel-pairs," *Applied Mathematics and Computation*, vol. 185, no. 2, pp. 869-882, 2007.

[7] H. Lu, R. Shen, and F. L. Chung, "Fragile watermarking scheme for image authentication," *Electronics Letters*, vol. 39, no. 12, pp. 898-900, 2003.

[8] P. D. Sheba Kezia Malarchelvi, "A semi-fragile image content authentication technique based on secure hash in frequency domain," *International Journal of Network Security*, vol. 15, no. 5, pp. 355-362, 2013.

[9] S. S. Sujatha and M. Mohamed Sathik, "A novel DWT based blind watermarking for image authentication," *International Journal of Network Security*, vol. 14, no. 4, pp. 223-228, 2012.

[10] S. Suthaharan, "Fragile image watermarking using a gradient image for improved localization and security," *Pattern Recognition Letters*, vol.25, pp. 1893-1903, 2004.

[11] D. Wang, C. C. Chang, Y. Liu, G. Song, Y. Liu, "Digital image scrambling algorithm based on Chaotic sequence and decomposition and recombination of pixel values," *International Journal of Network Security*, vol. 17, no. 3, pp. 322-327, 2015.

[12] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image autheticaation and ownership verification," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1593-1601, 2001.

[13] X. Zhang and S. Wang, "Fragile watermarking scheme using a hierarchical mechanism," *Signal Processing*, vol. 89, no. 4, pp. 675-679, 2009.

Yi-Hui Chen received B.S. and M.S. degrees in information management from the Chaoyang University of Technology in 2001 and 2004, respectively. In 2009, she earned her Ph.D. degree in computer science and information engineering at the National Chung Cheng University. From 2009 to 2010, she worked with Academia Sinica as a post-doctoral fellow. Later, she worked at IBM's Taiwan Collaboratory Research Center as a Research Scientist. She is now an assistant professor with the Department of Applied Informatics and Multimedia, Asia University. Her research interests include image processing, watermarking, steganography, and XML techniques.

Chih-Yang Lin received the B.S. degree in computer science and information engineering from Tung-Hai University, Taichung, in 1998, the master degree in information management from National Chi-Nan University, Nantou, in 2000. In 2006, he received a Ph.D. degree from Dept. Computer Science and Information Engineering at National Chung-Cheng University, Chiayi. After graduated, he servered in Advanced Technology Center of Industrial Technology Research Institute of Taiwan (ITRI) from 2007 to 2009. Then, he joined the Institute of Information Science (IIS), Academia Sinica, as a postdoctoral fellow. Currently, he is an Assistant Professor in the Department of Computer Science and Information Engineering, Asia University. His research interests include computer vision, digital rights management, image processing, and data mining.

Wanutchaporn Sirakriengkrai received B.S. degree in Humanities from Bangkok University in 2010. Now, she is a master degree student in computer science at Asia University. Her research focus on image processing and image authentication.

I-Chun Weng studied Computer Science and Information Engineering at Asia University. Her research interests focus on image processing and computer vision.