

A Copyright Protection Scheme for Still Images Based on Image Pinned

Field

Mn-Ta Lee¹ and Hsuan T. Chang², Member SPIE

¹Department of Electronic Engineering
Kao Yuan University
Kaohsiung, Taiwan, R.O.C.
mlee@cc.kyu.edu.tw

²Department of Electrical Engineering
National Yunlin University of Science and Technology
Yunlin, Taiwan, R.O.C.
htchang@yuntech.edu.tw

Abstract

Watermark embedding processes usually result in certain degradation in the digital multimedia contents. Hence, it is not suitable for valuable and sensitive digital multimedia contents. Therefore, schemes combining signature with digital watermarking-like techniques had been proposed in the literatures to conquer this challenge. Based on the general model for these combined schemes, a new scheme for image copyright protection by exploring the pinned field of the protected image is proposed in this paper. The pinned field explores the texture information of the images and can be used to enhance the watermark robustness. Experimental results show that the proposed scheme works well under different signal processing and geometric transformation attacks. On the other hand, while comparing with other related scheme in the literature, our proposed scheme also has better performance. Furthermore, the proposed scheme is robust to both the JPEG lossy compression and additive Gaussian noise as well.

Keywords: copyright protection, pinned field, content authentication, texture information, linear feedback shift register.

1. Introduction

In recent years, both the network and computer technologies have been growing very quickly. With the high speed network and the more powerful computers, there are many interesting and useful applications such as on-line games, blogs, e-learning, video on demand, e-map, etc. In these applications, many digital multimedia contents such as texts, images, audios, and videos are used. Due to the public and insecure environment of the Internet, many intruders intend to do malicious attacks on the digital multimedia contents stored in the servers. These malicious attacks may include illegal copying, tampering, modifying, and stealing of the digital multimedia contents. Therefore, how to provide useful methods for protecting digital multimedia contents from malicious attacks becomes an important issue.

Digital watermarking [1-5] is a major technique to protect the digital multimedia contents distributed on the Internet. By embedding the owner's watermarks such as logos, trademarks, seals, or copyright information into the digital multimedia contents without changing the perception of the digital multimedia contents, the owner can claim the ownership or intellectual property of the protected data. In realizing digital watermarking, the owner's watermarks could be embedded in the spatial or frequency domains of the digital multimedia contents. The owner's watermarks embedded in the spatial domain [6-10] are straightforward methods and have the advantages of low complexity and easy implementation. However, there are disadvantages. For example, the picture cropping operations may easily destroy the watermarks. The owner's watermarks embedded in the

frequency domain [11-14] are more robust than that embedded in the spatial domain. Embedding watermarks in the frequency domain, however, is time-consuming because all the pixel values of the cover image must be transformed into the corresponding frequency domain. The commonly used transforms include Fourier transform, the discrete cosine transform (DCT), and the discrete wavelet transform (DWT).

In designing a digital watermarking scheme for images, six essential properties must be satisfied [15]. First, the embedded watermark must be transparent. After the embedding process, the modification of the cover image must be inconspicuous and the embedded watermark must be perceptually invisible. The second property is robustness. The embedded watermark must be robust enough to resist the signal processing and geometrical attacks. The signal attacks may include blurring, additive noise, sharpening, and compression of images. The geometrical attacks may include scaling and cropping of images. The third property is unambiguity. The extracted watermark must be clear enough to identify the ownership of the cover image without ambiguity. The fourth property is security. Since the embedding algorithm is public, the security depends on keeping the key used in the algorithm secret. Without the secret key reserved by the image owner, the intruders cannot successfully extract the embedded watermark. The fifth property is blindness. The copyright can still be identified without the original cover image in the watermark verification phase, even if the protected image has been altered. The final essential property is the availability of embedding multiple watermarks. For legal distributions and users, the watermarking algorithms must allow the

image owner to embed additional watermarks in the cover image. These more recent watermarks must not interfere with the original watermarks

Watermark embedding usually results in slight degradation, which is not suitable for valuable and sensitive digital multimedia contents such as artistic, medical, and military images because some unsuitable analysis from these degraded images may be obtained. Therefore, how to conquer this disadvantage is a major challenge to most of digital watermarking techniques. Different from conventional watermarking schemes, some novel schemes combining the signature and digital watermarking-like techniques were proposed [15-19]. There are four major advantages in these schemes. First, these methods are lossless because they do not modify the protected image. Second, these methods don't need the original protected image during the authentication stage, so they can satisfy the blind properties of digital watermarking. Third, multiple-watermark embedding is possible. Finally, they can resist the counterfeit and copy attacks. A general model for these combining schemes is introduced in this paper.

Based on the general model mentioned above, we propose an image copyright protection scheme by using the pinned field of the cover image. The idea is that the robustness of watermarks could be enhanced by using the feature of the cover image. The pinned field reflects the texture information by evaluating the average pixel values at block boundaries of the images and can be used as the feature of the cover image to enhance the robustness of watermarks. Experimental results show that the proposed method can survive under different signal processing and geometric

transformation attacks, and also outperforms another related scheme in the literature, while comparing with the retrieval rate of the embedded watermark.

The rest of this paper is organized as follows: In section 2, the related works, including the general model for schemes, which combine signature with digital watermarking-like techniques, the determination of image pinned field, and the linear feedback shift register which is used to scramble the watermark, are described. The proposed novel image copyright protection scheme using the image pinned field is illustrated in Section 3. Experimental results for different types of image attacks and the comparison with other related scheme are presented in Section 4. The discussions about our scheme in the JPEG lossy compression and Gaussian noise attacks, which is a more significant consideration for the use of watermarks in many applications, are also given in Section 4. Finally, Section 5 concludes this paper.

2. Background

In this section, we briefly introduce the background of the proposed method. First, the general model of the copyright protection systems is reviewed. Then, the determination of the image pinned field is given. Finally, the linear feedback shift register (LFSR) scheme is introduced.

2.1 The General Model

Figure 1 shows the block diagram of the general model for conventional copyright protection systems, which combine the signature with digital watermarking-like techniques. There are two main parts in the general model: the signature and the authentication procedures for generating an

encrypted digital signature and verifying the ownership of the digital content, respectively. In the signature procedure shown in Fig. 1(a), features of the digital content are extracted to increase robustness and reduce the dimensionality. First, some of the features extracted in the methods including the image-edge information [19], DCT [1] and DWT [15] are used. By using the significant features of the digital content, the robustness of watermarks could be enhanced. Second, the watermark is scrambled in order to survive under geometric attacks. Third, the features of digital content and the scrambled watermark are combined by using some function to form the content with verification attributes. Finally, by using the normal signature generation system with the owner's private key to sign the content with verification attributes, a digital signature can be generated. Two main groups of normal signature generation systems, direct and arbitrated, can be used to generate a digital signature. The main difference between the direct and the arbitrated signatures is that the later needs an arbitrator. The scrambled watermark is combined with the features of digital content to form the content with verification attributes, which is required in the authentication procedure to extract the watermark. Thus, the protected digital content is not disturbed because none of the protected digital content is modified. Therefore, it can be applied to artistic and medical digital contents and does not need the original protected digital content during the authentication procedure.

In the authentication procedure shown in Fig. 1(b), it is basically an inverse of the signature procedure. First, when the protected digital content is questioned, the same features are extracted.

Second, the normal signature verification system with the owner's public key is used to verify the owner's digital signature. If the verification result is correct, the content with verification attributes is validated. Third, the reverse combination operation is applied to the extracted features of the questioned digital content and the content with verification attributes, so a scrambled watermark is obtained. Finally, by reversing the scrambled process, the extracted watermark is obtained to demonstrate the copyright of the questioned digital content.

2.2 The Image Pinned Field

Meiri and Yudilevich [20] proposed the pinned sine transform (PST) for image coders. The PST, which is an approximation to the pinned Karhunen-Loeve transform (PKLT) [21], uses the properties of the block boundaries to partition an image into two fields, namely, the boundary field and the pinned field. The boundary field depends only on the block boundary and the pinned field vanishes at the boundaries. The pinned field partially represents the texture information of the image.

The PST divides the image X into non-overlapping blocks of size $k \times r$ pixels [22, 23]. A typical block $X_{m,n}$, where m and n are the indices of this block, is shown in Fig. 2. Each corner of this block is shared by four blocks and each boundary is shared by two blocks. The four corner coefficients are defined in Eq. (1).

$$\begin{aligned}
V_{11} &= \frac{X_{m,n}(1,1) + X_{m-1,n-1}(k,r) + X_{m-1,n}(k,1) + X_{m,n-1}(1,r)}{4} \\
V_{1r} &= \frac{X_{m,n}(1,r) + X_{m-1,n}(k,r) + X_{m-1,n+1}(k,1) + X_{m,n+1}(1,1)}{4} \\
V_{k1} &= \frac{X_{m,n}(k,1) + X_{m,n-1}(k,r) + X_{m+1,n-1}(1,r) + X_{m+1,n}(1,1)}{4} \\
V_{kr} &= \frac{X_{m,n}(k,r) + X_{m,n+1}(k,1) + X_{m+1,n}(1,r) + X_{m+1,n+1}(1,1)}{4}
\end{aligned} \tag{1}$$

The four boundary functions are defined in Eq. (2).

$$\begin{aligned}
V_{1x}(i) &= \frac{X_{m,n}(1,i) + X_{m-1,n}(k,i)}{2} \\
V_{kx}(i) &= \frac{X_{m,n}(k,i) + X_{m+1,n}(1,i)}{2} \\
V_{y1}(j) &= \frac{X_{m,n}(j,1) + X_{m,n-1}(j,r)}{2} \\
V_{yr}(j) &= \frac{X_{m,n}(j,r) + X_{m,n+1}(j,1)}{2}
\end{aligned} \tag{2}$$

As shown in Fig. 2, only one new corner V_{kr} and two new boundaries $V_{kx}(i)$ and $V_{yr}(j)$ are needed to be calculated for a new block in the sequential processing of blocks. The boundary field $B_{m,n}$ of block $X_{m,n}$ is obtained by the pinning function [20] and has the following form:

$$\begin{aligned}
B_{m,n}(j,i) &= V_{11} + (V_{1r} - V_{11})(i - \frac{1}{2})/r + (V_{k1} - V_{11})(j - \frac{1}{2})/k \\
&\quad + (V_{11} + V_{kr} - V_{k1} - V_{1r})(i - \frac{1}{2})(j - \frac{1}{2})/(kr) \\
&\quad + G_x(i) + (H_x(i) - G_x(i))(j - \frac{1}{2})/k \\
&\quad + G_y(j) + (H_y(j) - G_y(j))(i - \frac{1}{2})/r,
\end{aligned} \tag{3}$$

where

$$\begin{aligned}
G_x(i) &= V_{kx}(i) - (V_{k1} + \frac{V_{kr} - V_{k1}}{r}(i - \frac{1}{2})) \\
H_x(i) &= V_{1x}(i) - (V_{11} + \frac{V_{1r} - V_{11}}{r}(i - \frac{1}{2})) \\
G_y(j) &= V_{yr}(j) - (V_{1r} + \frac{V_{kr} - V_{1r}}{k}(j - \frac{1}{2})) \\
H_y(j) &= V_{y1}(j) - (V_{11} + \frac{V_{k1} - V_{11}}{k}(j - \frac{1}{2}))
\end{aligned} \tag{4}$$

are the pinned boundaries. The pinned field $P_{m,n}$ is then determined as

$$P_{m,n}(j,i) = X_{m,n}(j,i) - B_{m,n}(j,i). \tag{5}$$

Figure 3 shows an example of the pinned field of the PST. The sizes of the source Lena image and the non-overlapping blocks are 512×512 and 4×4 pixels, respectively. As shown in Fig. 3(b), the pinned field can partially represent the texture information of the source image.

2.3 The Linear Feedback Shift Register

LFSRs [24, 25] are a common method to produce pseudo-random sequences, also known either as pseudo-noise sequences or maximal length binary sequences. LFSRs have received great attention because they are widely used in the circuitries of data compression, encryption, communication, and error correction.

An LFSR is a shift register with certain outputs modulo two added and the result fed back to the register at every clock cycle [26]. Figure 4 shows an N -stage LFSR consisting of N storage elements $s_1, s_2, s_3, \dots, s_{N-1}, s_N$. Let $s_i(t)$ denote the content of s_i after the t^{th} clock cycle. Then

$$s_i(t+1) = s_{i-1}(t) \quad \text{for } i = 2, 3, \dots, N \quad (6)$$

and

$$s_1(t+1) = \sum_{i=1}^N c_i s_i(t) \pmod{2}, \quad c_i \in \{0, 1\}. \quad (7)$$

An N -stage LSFR is characterized by an $N \times N$ matrix T_{SR} , which is called the global rule transition matrix. The construction of the matrix T_{SR} is based on the feedback dependence of the stages:

$$T_{SR} = \begin{bmatrix} c_1 & c_2 & c_3 & c_4 & \dots & \dots & c_{N-1} & c_N \\ 1 & 0 & 0 & 0 & \dots & \dots & 0 & 0 \\ 0 & 1 & 0 & 0 & \dots & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & \dots & \dots & 0 & 1 & 0 \end{bmatrix}_{N \times N}. \quad (8)$$

For an N -stage LFSR, it is always $c_N=1$. Let $S_{(t)} = [s_1(t), s_2(t), \dots, s_{N-1}(t), s_N(t)]^T$ denote the global output of the shift register after the t^{th} clock cycle. Then the global output of the next clock cycle, $s_{(t+1)}$, can be calculated as

$$S_{(t+1)} = T_{SR} \cdot S_t. \quad (9)$$

The global output state $S_{(t=k)}$ at the clock cycle $t=k$ can be directly obtained from the initial state $S_{(t=0)}$ using the relation

$$S_{(t=k)} = T_{SR}^k \cdot S_{(t=0)}. \quad (10)$$

The characteristic polynomial of the global rule transition matrix T_{SR} is given by

$$P_N(x) = \det(T_{SR} - x \cdot I), \quad (11)$$

where I denotes the identity matrix. It is easy to show that

$$P_N(x) = x^N + c_1x^{N-1} + c_2x^{N-2} + \dots + c_{N-1}x + 1. \quad (12)$$

An LFSR can produce a pseudo-random sequence if and only if its characteristic polynomial is a primitive polynomial [27]. By applying the LFSR scheme to scramble the watermark, the robustness can be enhanced furthermore.

3. The Proposed Scheme

The robustness of general watermarking schemes could be enhanced by using the features of the cover image for the verification purpose. Hence, we propose a novel digital signature-based scheme for protecting copyright of images using the image pinned field as the feature of the cover image to resist malicious attacks. The proposed scheme is based on the general model shown in Fig. 1. In the

signature procedure, the pinned field of the cover image is extracted as the feature. In the authentication procedure, the pinned field of the questioned image is also extracted and is used for further watermark reconstruction. These two procedures are subsequently described in the following subsections.

3.1 The Signature Procedure

Assume that the cover image C and the watermark T are grayscale images of size $W_c \times H_c$ and $W_t \times H_t$ pixels, respectively. The pinned field of the cover image C is first determined and the final objective is to generate a digital signature. Figure 5(a) shows the block diagram of the signature generation procedure. The main steps are described below:

- 1) By performing subsampling in the horizontal and vertical directions of the cover image, a down-scaled image is created. Through calculating the average values of the horizontal odd pixels with its neighbor pixels of the cover image, the width of the cover image is reduced to one half of its original size. This down-sampling operation is repeated until the width of the reduced image is as the same as that of the watermark T . The similar down-sampling operations are applied to the height of the cover image such that the height of the final image is as the same as that of the watermark T . Finally, the size of the reduced image will be same of the watermark T .

- 2) The down-scaled image is divided into non-overlapping blocks of size $k \times r$ pixels. Then, the pinned field of the down-scaled image is calculated in order to get the texture information of the cover image. The pinned field forms a feature image F' , which is robust to malicious attacks.

3) In order to survive under geometric attacks, the watermark T is scrambled by using the LFSR scheme, which generates a random sequence with a random seed R , to form a scrambled image T' , i.e.,

$$T' = \{ t'(j, i) = \text{LFSR}(t(j, i), R), 1 \leq j, j' \leq H_t, 1 \leq i, i' \leq W_t \}, \quad (13)$$

where “LFSR()” denotes the linear feedback shift register scrambling function and pixel $t(j, i)$ is scrambled to pixel $t'(j, i)$ in a random order.

4) An exclusive-or (XOR) operation is applied to the scrambled image T' and the feature image F' to create the signature image S' , i.e.,

$$S' = T' \text{ XOR } F'. \quad (14)$$

5) The signature image S' and the random seed R are then signed by using the normal signature generation system with the owner's private key PK to generate a digital signature DS' , i.e.,

$$DS' = \text{SIGN}(R, S', PK), \quad (15)$$

where “SIGN()” denotes the digital signature generation function which combines the one-way hashing function and a common RSA encryption scheme.

3.2 The Authentication Procedure

Given a questioned image, the authentication procedure is used to verify the ownership. The authentication procedure does not use the cover image and is similar to that of the signature procedure. Figure 5(b) shows the block diagram of the authentication procedure. The main steps are described as follows:

1) Derive a down-scaled image from the questioned image using the similar way described in the signature procedure.

2) Divide the down-scaled image into non-overlapping blocks of size $k \times r$ pixels. Then, the pinned field image F^* of the down-scaled image is determined to represent the feature of the questioned image.

3) Use the general signature verification system with the owner's public key UK to verify the digital signature DS' , i.e.,

$$YN^* = \text{VERI}(DS', UK), \quad (16)$$

where “VERI()” denotes the signature verification function used in the general RSA decryption scheme and YN^* is the verification result. If the verification result YN^* is correct, the signature image S' can be obtained by using the hashing function again and the random seed R is valid. Otherwise, the authentication procedure is terminated.

4) Apply the XOR operation to the signature image S' and the feature image F^* . The result forms a scrambled logo watermark T^* , i.e.,

$$T^* = S' \text{ XOR } F^*. \quad (17)$$

5) Inversely scramble the watermark T^* using the LFSR scheme with the seed R . Then the watermark image WT^* can be extracted, i.e.,

$$WT^*(j, i) = \{ \text{LFSR}^{-1}(T^*(j', i'), R), 1 \leq j, j' \leq H_t, 1 \leq i, i' \leq W_t \}, \quad (18)$$

where LFSR^{-1} denotes the inverse LFSR scrambling function. This reconstructed watermark image

WT^* is then used to verify the copyright of the questioned image.

4. Experimental Results

In this section, the experiments of applying the signal processing and geometric transformation attacks on the proposed scheme are performed to verify the robustness of the proposed method. Many sets of the cover and watermark images are used in our experiments. However, only two sets are used to demonstrate the results. Figures 6(a) and 6(b) show the cover and the corresponding watermark images in Sets 1 and 2, respectively. All the cover and the watermark images are grayscale with sizes 512×512 and 64×64 pixels, respectively. The comparison between the proposed scheme and another related scheme in the literature is also given in this section.

4.1 Results under attack environments

The peak signal-to-noise ratio (PSNR) is used to evaluate the quality of the attacked images of the same size $W_c \times H_c$ pixels. The PSNR is defined as

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\frac{1}{H_c W_c} \sum_{j=1}^{H_c} \sum_{i=1}^{W_c} |C(j,i) - A(j,i)|^2} \quad \text{dB}, \quad (19)$$

where $C(j,i)$ and $A(j,i)$ denote the grayscale values of the cover image C and the attacked image A at the pixel coordinate (j,i) , respectively. In addition, the similarity measurement between the original watermark T and extracted watermark T' is evaluated to estimate the robustness of the proposed copyright protection scheme under different attacks. The similarity is evaluated by the use of the watermark retrieval rate (RR), which is the percentage of the correct pixels recovered and is defined as

$$RR = \frac{\sum_{j=1}^{H_T} \sum_{i=1}^{W_T} T(j,i) \text{ XOR } T'(j,i)}{H_T W_T}, \quad (20)$$

where $T(j,i)$ denotes the grayscale value of the $(j,i)^{\text{th}}$ pixel in the original watermark T . It is obvious that the higher RR is, the higher similarity between the original and the extracted watermarks can be obtained. Furthermore, the average retrieval rate (ARR) is used to evaluate the practicability of a copyright protection scheme for common attacks and is defined as

$$ARR = (\sum_{i=1}^{NA} RR) / NA, \quad (21)$$

where “ NA ” denotes the number of examined attacks.

In the proposed signature procedure, the cover image is down-scaled at first. Then, the pinned field of the down-scaled cover image is evaluated and used to generate a feature signature. The pinned field of the down-scaled cover image is obtained by dividing the down-scaled cover image into non-overlapping blocks of size 4×4 pixels. For examples, Figs. 7(a) and 7(b) show the pinned field of the down-scaled cover image and the generated signature, respectively, for Set 1. Figures 7(c) and 7(d) show the pinned field of the down-scaled cover image and the generated signature, respectively, for Set 2.

Here the various attacks used in the experiments are summarized as follows:

Attack 1) Image blurring: A Gaussian filter with 9×9 kernel coefficients is applied to the cover image and thus a blurring image is obtained.

Attack 2) Quarter cropping: A quarter cropping operation is applied to the cover image to obtain a quarter cropping image.

Attack 3) Surround cropping: A surround cropping operation is applied to the cover image to obtain a surround cropping image.

Attack 4) Additive noise: While digital images are transmitted on the Internet, they may be interfered with Gaussian noise. Hence, the additive Gaussian noise with a zero mean value and the variance value 0.01 is applied to the cover image.

Attack 5) JPEG lossy compression: Images are usually compressed before transmission or storage, so the watermark should be robust to compression schemes. JPEG is one of the most efficient compression techniques. A JPEG lossy compression function in MATLAB with quality factor 95 is applied to the cover image to generate a compressed image.

Attack 6) Scaling: The cover image is resized to 256 x 256 pixels at first and then is enlarged to 512 x 512 pixels.

Attack 7) Sharpening: A linear mapping is applied to the cover image to generate a sharpened image.

Attack 8) Median filtering: The median filtering operation is often used to reduce the “salt and pepper” noise in images. It is a nonlinear operation. A median filter with 9 x 9 kernel coefficients is used to the cover image to generate a filtered image.

Attack 9) Average filtering: The average filtering operation blurs an image, especially in the edge part. An average filter with 9 x 9 kernel coefficients is applied to the cover image to generate a blurred image.

Tables 1 and 2 show the experimental RR results of the watermarks extracted from the proposed method under different attacks for Sets 1 and 2, respectively. These attacks include applying signal processing schemes and geometric transformation on the cover images. From these experiments, the retrieved watermark is still recognizable even though the PSNR value of the attacked image is low. As shown in Tables 1 and 2, all the RR values are greater than 0.84, which mean that the recovered watermarks are highly correlated with the original one. Therefore, embedding the watermark into the pinned field of the cover image is an efficient way and is robust to different types of attacks.

4.2 Comparison with another related scheme

The proposed method is compared with Chen's method [15]. The key idea of Chen's scheme is to use the DWT technology to extract low-frequency components of the copyright image. The low-frequency components can survive with little loss under significant attacks, based on the observation that human eyes are more sensitive to low-frequency components than high-frequency components. In Chen's scheme, the cover image is decomposed at first to obtain the 3-level LL subband, representing the low-frequency components of the copyright image, by using the 3-level wavelet transformation. Then, the 3-level LL subband and the watermark image are used to generate a verification key, i.e., the feature signature. Since the feature signature contains the low-frequency components of the copyright image, their scheme is robust to different kinds of attacks. Tables 3 and 4 show the comparison results between the proposed and Chen's methods on image Sets 1 and 2, respectively. In both tables, the proposed method significantly improves the RR values under the

attacks of the quarter- and surround-cropping operations from Chen's method. As for the other operations, the RR results of the proposed method are very close to that of Chen's method.

4.3. More discussions

Consider the six essential properties mentioned in Section 1. The experiment results show that the proposed method satisfies these six essential properties. First, our method owns the transparency because it does not modify the cover image. Second, the proposed method is robust because all the RR values under different attacks are greater than 0.84, which represent that the retrieved watermarks are highly correlated with the original watermark. Third, our method is secure because it is based on the signature procedure. Fourth, the retrieved watermark images are clear enough according to the experimental results. Therefore, the unambiguity has been satisfied. Fifth, our method does not need the original image during the authentication procedure. Hence, it satisfies the blind property. Finally, the owner can utilize other logo images to generate different signature images, so it allows multiple watermarks.

In the above six properties, the robustness is a more significant consideration in many different applications. Since images are usually compressed before the transmission or storage, the watermarking schemes should be robust to compression schemes. JPEG is one of the most common compression techniques, so the performances of the proposed method under different quality factors in JPEG compression are examined. On the other hand, images are usually transmitted through the Internet and might be interfered by the additive Gaussian noise. The performances of the proposed

method attacked by the additive Gaussian noise with different variance values are investigated.

Let the protected Elaine and Boat images be compressed using JPEG with different quality factors. Figure 8(a) shows the RRs between the embedded and extracted watermarks under different quality factors. As observed from the graphs, the embedded watermark can be exactly extracted even though the quality factors are as low as 30 to 40. By reducing the image quality more, our scheme still can extract the embedded watermark. For example, with the quality factor four it is able to extract the embedded watermark with $RR=79.8\%$. Figure 8(b) shows the RRs for the variance values between zero and 0.1. All the RR values are greater than 72%, which means that the extracted watermark is still recognizable even when the variance value is 0.1. Therefore, the proposed method is robust to both the JPEG compression and additive Gaussian noise.

5. Conclusions

A novel image copyright protection scheme using the image pinned field is proposed in this paper. The image pinned field partially reflects the global texture information of the image and can be used to enhance the watermark robustness. The experimental results demonstrate that the proposed method can resist and survive under different signal processing and geometric transformation attacks. Comparing with Chen's scheme, our scheme achieves significant improvements on image cropping operations. The average RR values are also comparable with that of Chen's method. Furthermore, the performances under different quality factors for JPEG compression attacks and different variance values for Gaussian noise attacks have been examined

more thoughtfully.

6. Acknowledgment

This work was partially supported by National Science Council, Taiwan under the contract number NSC 98-2221-E-224-042.

References

- [1] C.T. Hsu and J.L. Wu, "Hidden digital watermarks in images," *IEEE Trans. Image Processing*, **8**(1), pp. 58–68, 1999
- [2] C.I. Podilchuk and E.J. Delp, "Digital watermarking: algorithms and application," *IEEE Signal Process. Mag.* **18**(4), pp. 33–46, 2001
- [3] M.D. Swanson, M. Kobayashi, and A.H. Tewfik, "Multimedia data embedding and watermarking technologies," *Proc. IEEE*, **86**(6), pp.1064–1087, 1998.
- [4] B.R. Macq and I. Pitas, "Special issue on watermarking," *Signal Process.*, **66**(3), pp. 281–282, 1998.
- [5] S.H. Low, N.F. Maxemchuk, and A.M. Lapone, "Document identification for copyright protection using centroid detection," *IEEE Trans. Commun.*, **46**(3), pp. 372–383, 1998.
- [6] I. Pitas and T.H. Kaskalis, "Applying signatures on digital images," in *Proc. IEEE Nonlinear Signal and Image Processing*, pp. 460–463, June 1995.
- [7] O. Bruyndonckx, J.J. Quisquater, and B. Macq, "Spatial method for copyright labeling of digital

- images,” in Proc. IEEE Nonlinear Signal and Image Processing, pp. 456–459, June 1995.
- [8] D.C. Wu and W.H. Tsai, “A steganographic method for images by pixel-value differencing,” *Pattern Recognition Lett.*, **24**(9-10), pp.1613–1626, 2003.
- [9] Y.H. Yu, C.C. Chang, and Y.C. Hu, “Hiding secret data in images via predictive coding,” *Pattern Recognition*, **38**(5), pp. 691–705, 2005.
- [10] M.U. Celik, G. Sharma, A.M. Tekalp, and E. Saber, “Lossless generalised-LSB data embedding,” *IEEE Trans. Image Processing*, **14**(2), pp. 253–266, 2005.
- [11] E. Koch and J. Zhao, “Toward robust and hidden image copyright labeling,” in Proc. IEEE Nonlinear Signal and Image Processing, pp. 452–455, June 1995.
- [12] I.J. Cox, J. Kilian, T. Leighton, and T. Shammoon, “Secure spread spectrum watermarking for multimedia,” Tech. Rep. 95-10, NEC Res. Inst., Princeton, NJ, 1995.
- [13] H.T. Chang, C.-C. Hsu, Chia-H. Yeh, and D.F. Shen, “Image authentication and tampering localization based on watermarking embedding in wavelet domain,” *Optical Engineering*, **48**(5), 057002, 2009
- [14] H.T. Chang and C.L. Tsan, “Image watermarking by use of digital holography embedded in DCT domain,” *Applied Optics*, **44**(29), pp. 6211–6219, 2005
- [15] T.H. Chen, G. Horng, and W.B. Lee, “A publicly verifiable copyright-proving scheme resistant to malicious attacks,” *IEEE Trans. Industrial Electronics*, **52**(1), pp. 327–334, 2005
- [16] C.C. Chang, K. F. Hwang, and M.S. Hwang, “Robust authentication scheme for protecting

- copyrights of images and graphics,” IEE Proc. - Vis. Image Signal Proc., **149**(1), pp. 43–50, 2002
- [17] C.C. Chang and J.C. Chuang, “An images intellectual property protection scheme for gray-level images using visual secrete sharing strategy,” Pattern Recognition Letters, **23**(8), pp. 931–941, 2002
- [18] W.B. Lee and T.H. Chen, “A publicly verifiable copy protection technique for still images,” J. Sys. Softw., **62**(3), pp. 195–204, 2002
- [19] C.C. Chang and P.Y. Lin, “Adaptive watermark mechanism for rightful ownership protection,” J. Sys. Softw., **81**(7), pp. 1118–1129, 2008
- [20] A.Z. Meiri and E. Yudilevich, “A pinned sine transform image coder,” IEEE Trans. Commun., **29**(12), pp. 1728–1735, 1981
- [21] A.Z. Meiri, “The pinned Karhunen-Loeve transform of a two dimensional Gauss-Markov field,” Proc. SPIE, **87**, pp. 155, 1976
- [22] A.T.S. Ho, X. Zhu, and Y.L. Guan, “Image content authentication using pinned sine transform,” EURASIP Journal on Applied Signal Processing, **14**, pp. 2174–2184, 2004
- [23] X. Zhu, A.T.S. Ho, and P. Marziliano, ”A new semi-fragile image watermarking with robust tampering restoration using irregular sampling,” Signal Processing: Image Communication, **22**(5), pp. 515–528, 2007
- [24] K. Zeng, C.H. Yang, D.Y. Wei, and T.R.N. Rao, “Pseudo-random bit generators in stream-cipher cryptography,” IEEE Computer, **24**(2), pp. 8–17, 1991
- [25] C.A. Chen and S.K. Gupta, “BIST test pattern generators for two-pattern testing: theory and design

algorithms,” *IEEE Trans. Computers*, **45**(3), pp. 257–269, 1996

[26] I. Kokolakis, I. Andreadis, and Ph. Tsalides, “Comparison between cellular automata and linear feedback shift registers based pseudo-random number generators,” *Microprocessors and Microsystems*, **20**(10), pp. 643–658, 1997

[27] S. Lin and D.J. Costello, *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, N. J: Prentice Hall, 1983

Author Biographies



Mn-Ta Lee was born in Tainan County, Taiwan, Republic of China (ROC). He received the B.S. degree in Electronic Engineering from National Taiwan University of Science and Technology, Taiwan, R.O.C., in 1991, the M.S. degree in Electronic Engineering from National Taiwan University of Science and Technology, Taiwan, R.O.C., in 1993. Since 1993, he has been with the Department of Electronic Engineering at Kao Yuan University, Taiwan, R.O.C., where he is currently a lecturer. His research interests include information security, optical information processing/computing, steganography, multimedia security, artificial intelligence, and image processing.



Hsuan T. Chang was born in Tainan County, Taiwan ROC. He received his B.S. degree in Electronic Engineering from National Taiwan University of Science and Technology, Taiwan, in 1991, and M.S. and Ph.D. degree in Electrical Engineering (EE) from National Chung Cheng University (NCCU), Taiwan, in 1993 and 1997, respectively. He was an adjunct lecturer in Department of Automation in National Yun-Lin Polytech Institute from 1993 to 1994 and a visiting researcher at Laboratory for Excellence in Optical Data Processing, Department of Electrical and Computer Engineering, Carnegie Mellon University, from 1995 to 1996. Dr. Chang was an assistant professor in Department of Electronic Engineering in Chien-Kuo University of Technology, Changhua, Taiwan, from 1997 to 1999, an assistant professor in Department of Information Management, Chaoyang University of Technology, Wufeng, Taiwan, from 1999 to 2001, and an assistant professor and associate professor in EE Department of National Yunlin University of Science and Technology (NYUST), Douliu, Taiwan, from 2001 to 2002 and 2003 to 2006, respectively. He currently is a full professor in EE Department and Chairman of Graduate School of Communication Engineering of NYUST. He was also an adjunct assistant professor in Graduate Institute of Communications Engineering of NCCU from 2000 to 2003. Dr. Chang was a visiting scholar in Institute of Information Science, Academia Sinica, Taiwan and in EE department, University of Washington, Seattle from 2003/7 to 2003/9 and 2007/8 to 2008/3, respectively.

Dr. Chang's interests include multimedia signal processing, optical information processing, and medical image processing. He has published more than 160 journal and conference papers in the above research areas. He was the recipient of the visiting research fellowship from Academia Sinica, Taiwan in 2003, and the excellent research award for new faculty in NYUST in 2005. He served as the reviewer of several international journals. He served as the conference chair of 2005 Workshop on Consumer Electronics and Signal Processing held in Taiwan and was an invited speaker, session chair, and program committee in many domestic and international conferences. Dr. Chang is Senior Member of Institute of Electrical and Electronics Engineers (IEEE), International Society for Optical Engineering (SPIE), Optical Society of America (OSA), Asia-Pacific Signal and Information Processing Association (APSIPA), Taiwanese Association of Consumer Electronics (TACE), and The Chinese Image Processing and Pattern Recognition (IPPR) Society.

Table 1. The attacked images, the corresponding PSNR values, the retrieved watermark images, and the corresponding RR values.



















	Image Blurring	Quarter Cropping	Surround Cropping
Attacked Image			
PSNR (dB)	38.47	13.69	12.43
Retrieved watermark image			
RR	99.54%	87.74%	84.99%
	Additive noise	JPEG	Scaling
Attacked Image			
PSNR (dB)	20.07	36.52	27.07
Retrieved watermark image			
RR	91.60%	99.80%	99.44%
	Sharpening	Median filter	Average filter
Attacked Image			
PSNR (dB)	20.16	29.8	26.06
Retrieved watermark image			
RR	99.66%	96.48%	95.68%

Table 2. The attacked images, the corresponding PSNR values, the retrieved watermark images, and the corresponding RR values.



















	Image Blurring	Quarter Cropping	Surround Cropping
Attacked image			
PSNR (dB)	37.68	13.72	12.29
Retrieved watermark image			
RR	97.53%	86.38%	85.30%
	Additive noise	JPEG	Scaling
Attacked image			
PSNR (dB)	20.10	36.96	19.48
Retrieved watermark image			
RR	87.50%	98.05%	91.21%
	Sharpening	Median filter	Average filter
Attacked image			
PSNR (dB)	20.50	23.84	22.79
Retrieved watermark image			
RR	98.00%	89.14%	90.55%

Table 3. The RR comparison results for Set 1 images.

Operation	Type	Specification	Proposed	Chen's
			RR	RR
Blurring	Gaussian filter	9 x 9	99.54%	99.88%
Quarter cropping		25%	87.74%	78.52%
Surround cropping		26%	84.99%	71.04%
Additive noise	Gaussian noise	mean=0 variance=0.01	91.60%	97.75%
JPEG compression		Quality factor=95	99.80%	99.98%
Scaling			99.44%	99.85%
Sharpening	linear mapping		99.66%	99.93%
Median filtering	nonlinear filter	9 x 9	96.48%	98.61%
Average filtering	linear filter	9 x 9	95.68%	97.12%
Average RR			94.99%	93.63%

Table 4. The RR comparison results for Set 2 images.

Operation	Type	Specification	Proposed	Chen's
			RR	RR
Blurring	Gaussian filter	9 x 9	97.53%	97.90%
Quarter cropping		25%	86.38%	66.63%
Surround cropping		26%	85.30%	59.38%
Additive noise	Gaussian noise	mean=0 variance=0.01	87.50%	95.70%
JPEG compression		Quality factor=95	98.05%	98.27%
Scaling			91.21%	95.61%
Sharpening	linear mapping		98.00%	98.12%
Median filtering	nonlinear filter	9 x 9	89.14%	94.31%
Average filtering	linear filter	9 x 9	90.55%	92.72%
Average RR			91.52%	88.74%

Figure Captions:

Figure 1. Block diagrams of the general model for conventional schemes combining signature with digital watermarking-like techniques: (a) the signature procedure; (b) the authentication procedure.

Figure 2. The dual-field decomposition in PST for a typical image block.

Figure 3. The pinned field decomposition in the PST of the Lena image: (a) the source image; (b) the corresponding pinned field.

Figure 4. Block diagram of the LFSR operation.

Figure 5. The systematic block diagrams of the proposed method: (a) the signature procedure; (b) the authentication procedure.

Figure 6. Test images and watermarks for (a) Set 1 and (b) Set 2.

Figure 7. (a) The pinned field of the down-scaled image for Set 1; (b) the corresponding signature image for Set 1; (c) the pinned field of the down-scaled image for Set 2; (d) the corresponding signature image for Set 2.

Figure 8. The RR results under the attacks of (a) JPEG compression and (b) the additive Gaussian noise.

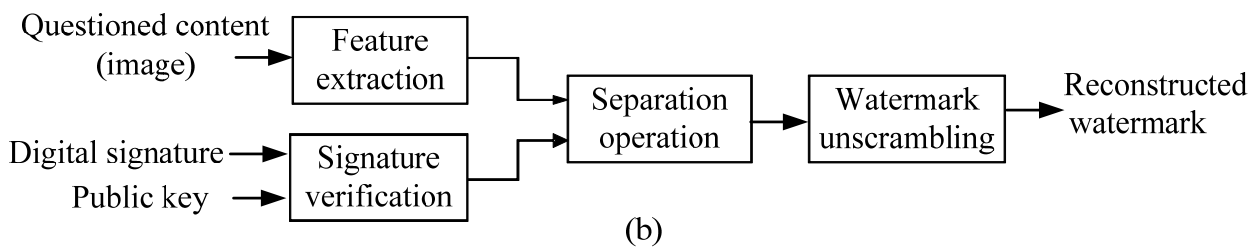
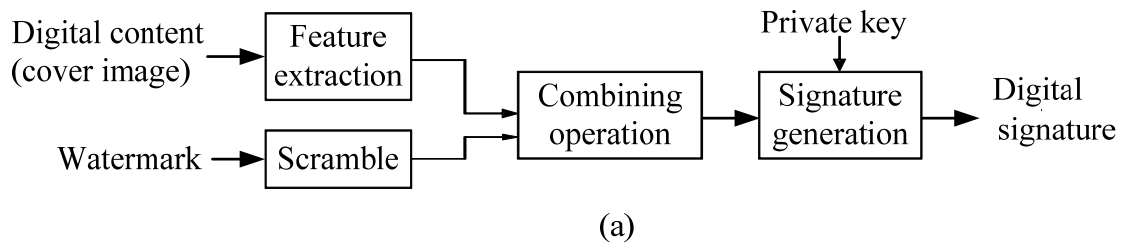


Figure 1. Block diagrams of the general model for conventional schemes combining signature with digital watermarking-like techniques: (a) the signature procedure (b) the authentication procedure.

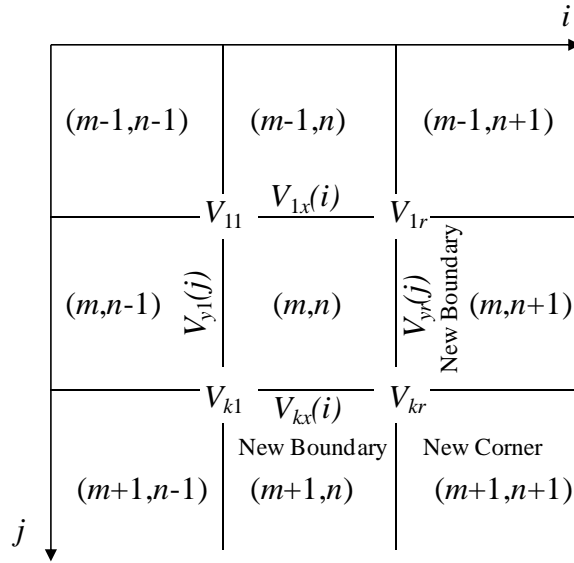


Figure 2. The dual-field decomposition in PST for a typical image block.

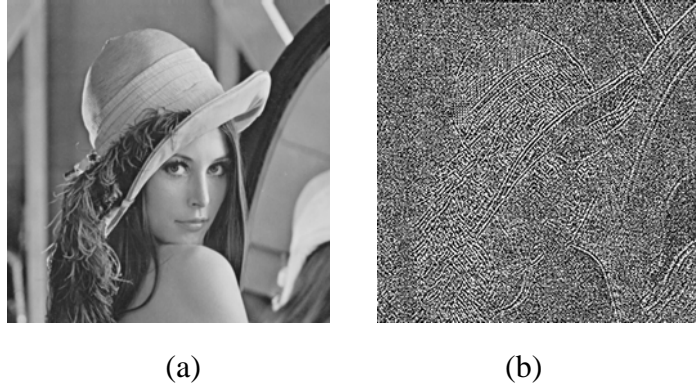


Figure 3. The pinned field decomposition in the PST of the Lena image: (a) the source image (b) the corresponding pinned field.

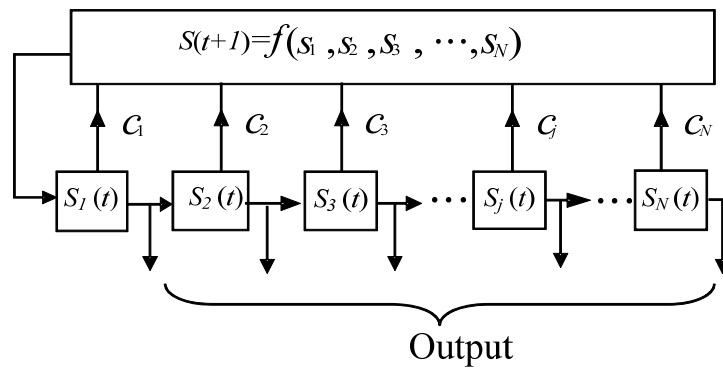


Figure 4. Block diagram of the LFSR operation.

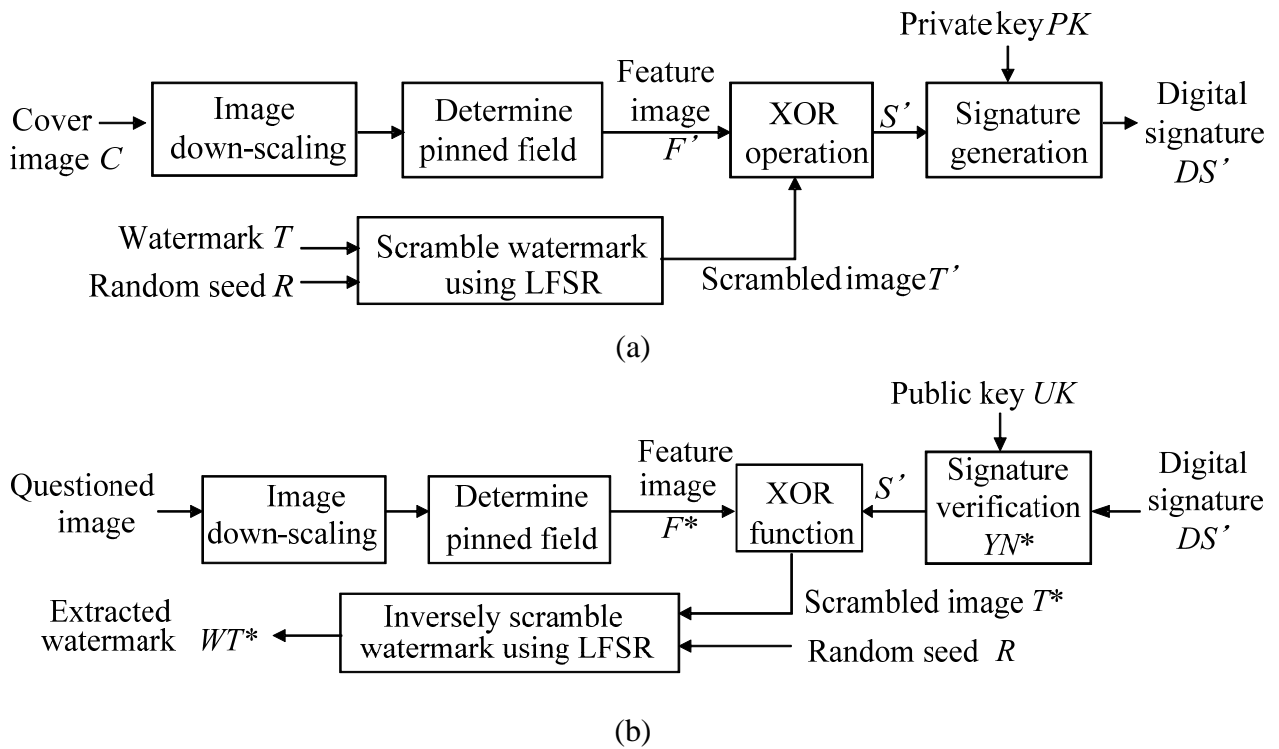


Figure 5. The systematic block diagrams of the proposed method: (a) the signature procedure; (b) the authentication procedure.



(a)



(b)

Figure 6. Test images and watermarks for (a) Set 1 and (b) Set 2.

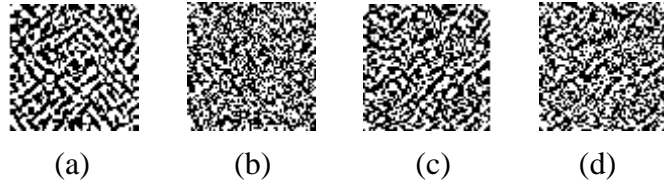
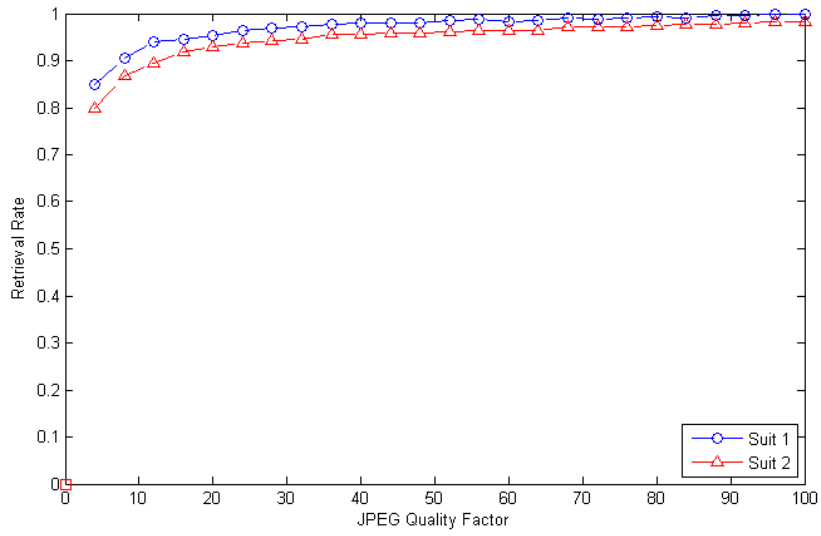
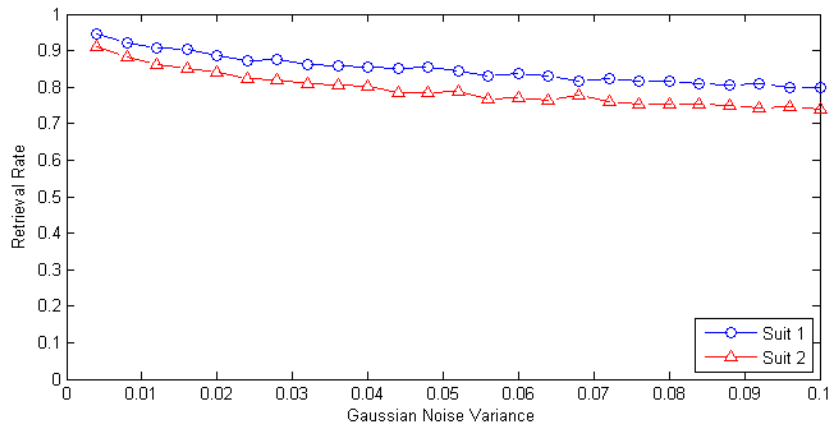


Figure 7. (a) The pinned field of the down-scaled image for Set 1; (b) the corresponding signature image for Set 1; (c) the pinned field of the down-scaled image for Set 2; (d) the corresponding signature image for Set 2.



(a)



(b)

Figure 8. The RR results under the attacks of (a) JPEG compression and (b) the additive Gaussian noise.