A Feature-Oriented Copyright Owner Detection Technique for Still Images *

Chin-Chen Chang †§ Kuo-Feng Hwang† Min-Shiang Hwang‡

Department of Computer Science and †
Information Engineering,
National Chung Cheng University,
Chaiyi, Taiwan 621, R. O. C.
Email: ccc@cs.ccu.edu.tw

Department of Information Management, ‡
Chaoyang University of Technology,
Wufeng, Taiwan, R.O.C.
Email: mshwang@mail.cyut.edu.tw

September 6, 2002

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC89-2213-E-324-025.

§Responsible for correspondence:
Professor Chin-Chen Chang
Chiayi, Taiwan 621, R.O.C.
Tel: 886-5-2720411ext6011
Fax: 886-5-2720859
Email: ccc@cs.ccu.edu.tw

A Feature-Oriented Copyright Owner Detection Technique for Still Images

Chin-Chen Chang, Kuo-Feng Hwang, Min-Shiang Hwang
Tel:886-5-2720411ext6011 Fax: 886-5-2720589
Email: ccc@cs.ccu.edu.tw

Abstract

This paper presents a copyright owner detection technique for images and graphics. A digital time-stamped signature for this copyright identification technique is also introduced in this work. The secret key, used to detect the watermark, is generated from the extracted features of the host images in the proposed scheme. The proposed algorithm enables the successful detection of watermarks under several attacks, such as filtering, lossy compression, cropping, rotating and so on. In particular, our method is not only suitable for ordinary natural images, but can also be applied to cartoon graphics. Furthermore, the proposed scheme can be applied to no distortion allowed images, such as medical images.

KeyWords: Digital watermarking, intellectual property right, digital signature, time-stamping

1 INTRODUCTION

Digital watermarking techniques are primarily applicable to intellectual property right protection. The idea of watermarking technique is to embed an indelible watermark to identify uniquely the source of an image. We call the watermarked images as the protected images. Conventionally, digital watermarking has been categorized into ”steganography” or information hiding [**?**]. Steganography has been defined as ”the technique of hiding messages in innocuous forms; for example, writing a secret message with invisible ink in an ordinary letter.”

To date, the existing digital watermarking techniques can be classified into two categories from technical viewpoint. In the first category, the watermark is embedded into the spatial domain [**?**, **?**, **?**, **?**, **?**]. In the second category, the watermarking technique embeds the watermark into the frequency domain [**?**, **?**, **?**, **?**], which is the transformed data by Fourier, discrete cosine, or wavelet transformation and so on. In this paper, we propose an entirely new technique for copy right protection which is wholly different from these two categories. In our scheme, the original image is not necessary to be modified when the secret key, for watermark detection at later, is generated. In the schemes of the above two categories, however, the original image is necessary to be modified when the watermark embedding stage is accomplished.

Digital watermarking must satisfy the following requirements to protect copyright.

1. The quality of the watermarked image must be very high. In other words, the embedded watermark in a modified original image, should be perceptually invisible.

2. The original image is not necessary at watermark retrieving stage. In other words, storing of a duplicate copy should be avoided as it is not practical for a huge image database.

3. Similar to cryptography, the details of algorithm is open to the public.

4. Except the copyright owner, no other person should be able to detect or remove the watermark from the watermarked image.

5. For trading reason, one image should be embedded unlimited number of watermarks. Moreover, it is necessary to hold the quality of watermarked images.

6. It should be possible to retrieve the watermark even after multiple and various image processes, such as low-pass filtering, high-pass filtering, lossy compression, rotating, cropping and so on.

There are some problems in invisible digital watermarking systems. The major problem is the rightful claim of ownership of the invisible watermarking technique. Craver et al. pointed out this problem in [**?**]. They argued that a watermarked/protected image could allow multiple claims of ownership. Today, most of the existed watermarking techniques involve only the owner's watermark. Moreover, the owner has complete control over the watermark embedding and its detection process. That is the essence of the problem demonstrated by Craver et al. To solve this problem, a trusted third party should be introduced. Voatzis and Pitas proposed a generic model for protecting copyrights [**?**], which also included a trusted registration authority. In addition, they pointed out that geometric attacks, such as rotation and scaling, is a remaining problem of watermarking techniques that do not use original images for watermark retrieving.

Digital media can easily be distorted by a pirate. The pirate can made a modified copy of the original look and thus claim himself/herself the rightful owner of the copyright. One of the solution to resolve the forging problem is to use Time-Stamping technique [**?**, **?**]. Time-Stamping technique is used to ascertain whether a digital media was created or signed at a certain time and like most of digital signature techniques [**?**, **?**], it is based on public-key cryptosystems in which forging can be avoided. But for a fully or partially modified data the differences cannot be detected by the naked eye and, moreover, Time-

Stamping cannot be a strong evidence to prove in a court. On the other hand, digital watermarking technique can overcome this problem. In the proposed algorithm, we used Time-Stamping only to ascertain that a watermark was embedded at a certain time. This mechanism can conquer the problem pointed out by Craver et al.

Digital cartoon graphics have significant differences from ordinary natural images. Cartoon graphics are usually without complicated color and texture variations. Therefore, cartoon graphics can be repainted using similar colors without affecting the meaning of original image. These features of cartoon graphics make it more difficult to embed watermarks. In a word, this is another challenge for digital watermarking techniques.

In this paper, we propose a new robust watermarking detection technique for digital images and graphics. We simply used the exclusive-or operator to generate a secret key for watermark retrieving. This secret key is determined from the watermark, the extracted feature of the original image, and a seed of the pseudo-random number generator. In addition, a trusted third party or time-stamp service (TSS) signed a time-stamp for this generated secret key. At verification stage, we can verify whether a watermark was embedded at certain time by the signed time-stamp when this secret key can retrieve watermark successfully.

The rest of this paper is organized as follows. Some related works are reviewed in Section 2. Section 3 demonstrates the detailed algorithm of our method. Section 4 deals with the experimental results of the proposed digital watermarking technique. The discussions and security analyses of our scheme are shown in Section 5. Finally, Section 6 presents the conclusions of the present work.

2 RELATED WORKS

Langelaar et al. [**?**] presented two watermarking techniques for images. Their first scheme embeds watermark into the Y-image (luminance, [**?**]) of color images. A watermark consists of a few hundred bits. Each bit of watermark is embedded into a block $\mathbf{B}(8 \times 8)$ of luminance values. The blocks are non-overlapping and tile the image without gaps. For watermark embedding, a quality threshold T, and the embedding-levels k_0, and k_{max} are determined by degree against JPEG compression. Therefore, the DCT coefficients of block $\mathbf{B}$ is needed for T, k_0, and k_{max}. Unfortunately, the inventors only demonstrated that this scheme enables to resist lossy compression (JPEG) attack in their experimental results.

Caronni [**?**] proposed a method which embeds a watermark (bitstream) in the luminance values of an image. The original image is partitioned into blocks. Every block pixels are incremented by a certain factor to encode a '1' and left unaltered to encode a '0'. To retrieve watermark, the luminance of each pixel in the watermarked image is subtracted from the original one. If the mean of block pixels differences exceeds a certain threshold, the corresponding bit is taken as '1', otherwise as '0'. This method is resistant to JPEG compression with quality parameter set to 30%. A disadvantage of this method is that the watermark retrieving requires original images. As mentioned in Section 1, the practice is limited on this condition.

Hsu and Wu [**?**] proposed an image watermarking technique based on DCT. To embed a watermark (binary image) into a host image by selectively modifying the middle-frequency DCT coefficients. According to their experimental results, this method can resist lossy compression (JPEG) and cropping attacks. However, it is uncertain whether it will survive under other attacks, such as rotation, low-pass filtering, and high-pass filtering and so on. Moreover, like Caronni's scheme the drawback of Hsu and Wu's scheme is that the original image is required for watermark retrieving.

Su et al. [**?**] proposed a watermarking technique based on wavelet-transform, called TAWS (threshold-adaptive watermarking scheme). TAWS has capability to embed an invisible watermark into several kinds of images. Contrast to other existing schemes, cartoons and maps are especially suitable for this scheme. To embed watermarks, TAWS selects a couple of perceptually significant wavelet-transform coefficients within the same sub-band. The inventors' experimental results demonstrate that the quality of watermarked images are higher ($PSNR > 40$). Moreover, they also shows that TAWS protects against various lossy compression attacks, such as JPEG and SPIHT. Unfortunately, TAWS did not consider the "repaint" attack for cartoons. According to the characteristics of cartoons, a pirate can easily repaint/replace some colors of cartoons with other colors to destroy the embedded watermark. However, it is uncertain whether TAWS will survive under this kind of attack.

We have introduced time-stamping techniques to our watermarking scheme to ascertain the watermark is embedded at certain time. Some time-stamping schemes are reviewed below. Haber and Stornetta [**?**] proposed a linking time-stamping protocol in 1991. A trusted third party or TSS signs the current time t_n to the n-th submitted document X_n as

$$s = sig_{TSS}(n, t_n, ID_n, X_n, L_n). \tag{1}$$

Here t_n is the current time, ID_n is the identification of the submitter, and L_n is the linking information, which is defined as below:

$$L_n = (t_{n-1}, ID_{n-1}, X_{n-1}, H(L_{n-1})). \tag{2}$$

Here $H(\cdot)$ denotes a one-way hash function [**?**, **?**]. This scheme has some complications with practical implementation. Firstly, TSS must to store each values of L_n. Secondly, it's time consuming to verify the signed time-stamp. Haber et al. have proposed two improved schemes in [?] and [?]. Buldas et al. [?] proposed a binary-linking mechanism of time-stamping technique. For their scheme, Buldas and Laud [?] showed that the size of a time-certificate is bounded by $4\log_2 N$, where N is the number of time-stamps issued. In [?], M. Just pointed out some failures of time-stamping protocol proposed previously. In addition, M. Just emphasized that the importance and difficulty in implementing a secure protocol even if there existed secure underlying algorithms.

To date, most of the proposed schemes commonly use a secret key, chosen by the owner, to embed watermark into host images. A right secret key will retrieve the rightful watermark back later on. In the proposed scheme, the secret key is determined by the original image, the watermark and a seed of pseudo-random number generator. The details of the proposed algorithm will be described in next section.

3 THE PROPOSED SCHEME

In contrast to traditional digital watermarking techniques, our scheme has primarily two different features. Firstly, the protected image is same as original image. Secondly, the secret key K, used to retrieve the watermark, is determined using the original image, the watermark, and a seed of pseudo-random number generator.

The secret key K has the same dimensions as the watermark's. After the secret key K is generated, a signed time-stamp for K through a trusted third party as K_s is required. The signed time-stamp K_s stands for K, which was generated at a certain time t. Consequently, when K enables to retrieve the watermark, K_s represents the exact time t, the original image was produced. In other words, K, t and K_s will be the evidences to identify the rightful intellectual property right (IPR) owner. The details of the proposed algorithm are described following.

Key Generation Algorithm

The original image O requires β bit(s) per pixel, and the watermark W is a binary image. Original image O is defined as following:

$$O = \{o_{i,j} \mid 0 \le o_{i,j} \le 2^{\beta} - 1\}. \quad (3)$$

Here $0 \le i \le O_H - 1, 0 \le j \le O_W - 1$ and O_H and O_W are the original image's height and width, respectively. The watermark W is defined as below.

$$W = \{w_{i,j} \mid w_{i,j} \text{ is } 0 \text{ or } 1\}. \quad (4)$$

Here $0 \le i \le W_H - 1, 0 \le j \le W_W - 1$, W_W is the watermark's width and W_H is the watermark's height.

First, a block set $\mathcal{B}$ is selected from O according to a pseudo-random number generator. $\mathcal{B}$ is produced and defined as follows.

$$\mathcal{B} = \{b_{m,n} \mid m = 0, 1, \ldots, W_H - 1, n = 0, 1, \ldots, W_W - 1\}, \quad (5)$$

$$b_{m,n} = \begin{bmatrix} o_{i,j} & o_{i,j+1} & \cdots & o_{i,j+w-1} \\ o_{i+1,j} & o_{i+1,j+1} & \cdots & o_{i+1,j+w-1} \\ \cdots & \cdots & \cdots & \cdots \\ o_{i+h-1,j} & \cdots & \cdots & o_{i+h-1,j+w-1} \end{bmatrix}. \quad (6)$$

Here $0 \le i \le O_H - 1$ and $0 \le j \le O_W - 1$. h and w are block's height and width, respectively. Note that we used $h = \frac{O_H}{W_H}$ and $w = \frac{O_W}{W_W}$ in our experiments. The blocks $b_{m,n}$ allow mutual overlapping. The coordinate (i, j) for block $b_{m,n}$ is determined by the pseudo-random number generator $Rand(\cdot)$ as follows.

$$(i, j) = Rand(s, m, n). \tag{7}$$

Here s is the seed of random number generator $Rand(\cdot)$, $m = 0, 1, \ldots, W_H - 1, n = 0, 1, \ldots, W_W - 1$. The seed s is a part of secret key to detect watermark. Consequently, a highly secret pseudo-random number generator is required. Hwang et al. [**?**] have been using one-way hash functions to form a highly secured pseudo-random number generator. Their scheme is recommended to introduce here $Rand(\cdot)$.

Next, we extract each block's feature through a feature function $F(\cdot)$. For instance, $F(\cdot)$ could be the function which calculates the variance or mean of its input block and gives the output. We define the block feature $v_{m,n}$ of block $b_{m,n}$ as

$$v_{m,n} = F(b_{m,n}). \tag{8}$$

Here $m = 0, 1, \ldots, W_H - 1$ and $n = 0, 1, \ldots, W_W - 1$. After block feature $v_{m,n}$ is obtained, we transform $v_{m,n}$ to a temporary key T through a transform function $Tran(\cdot)$. The main purpose of $Tran(\cdot)$ is make T's elements have the same value domain with watermark's. T is defined as

$$T = \{t_{m,n} |\, t_{m,n} \text{ is 0 or } 1\}, \tag{9}$$

$$t_{m,n} = Tran(v_{m,n}). \tag{10}$$

Here $m = 0, 1, \ldots, W_H - 1$ and $n = 0, 1, \ldots, W_W - 1$. It is clear that T has the same dimensions as watermark's. In our experiments, the block feature $v_{m,n}$ is transformed through a threshold A. A is defined as follows.

$$A = \frac{\sum_{m=0}^{W_H-1}\sum_{n=0}^{W_W-1} v_{m,n}}{W_H \times W_W}. \tag{11}$$

Note that the transform function may be modified according to the characteristics of feature function $F(\cdot)$. Now, we define the transform function $Tran(\cdot)$ as follows.

$$Tran(v_{m,n}) = \begin{cases} 0, & \text{if } v_{m,n} \leq A, \\ 1, & \text{if } v_{m,n} > A. \end{cases} \tag{12}$$

Here $m = 0, 1, \ldots, W_H - 1$ and $n = 0, 1, \ldots, W_W - 1$. Finally, the secret key K is constructed by

$$K = T \oplus W. \tag{13}$$

Here $\oplus$ is the exclusive-or operator. The key generation procedure is finished when the secret key K is generated. Note that the original image does not get modified, even if the key generation stage is accomplished. For watermarks detection at later stage, the image owner has to keep K as well as s secretly.

After the secret key K is generated, the time-stamp K_s for K is signed by a trusted third party or TSS using its private key as

$$K_s = sig_{TSS}(h(O), t, K). \tag{14}$$

Here $h(\cdot)$ denotes a public known collision free and one-way hash function [**?**], t is the time while K_s is signing. Involving $h(O)$ in K_s is useful when an owner has several similar images. This mechanism can avoid the case that claiming the ownership of some similar images by using a set $\{t, K$ and $K_s\}$.

Watermark Detection Algorithm

The processes to detect watermark from a protected image are similar to the key generation processes except the final step (Equation 13). We can obtain the retrieved watermark W' using a temporary key T, and the secret key K. As mentioned above, the pseudo-random number generator seed is a part of secret key to retrieve watermarks. If a right seed is introduced, the right temporary key T is obtained. In addition, the watermark can be retrieved if correct secret key K is used. W' is obtained using

$$W' = T \oplus K. \tag{15}$$

The retrieved watermark W' is equal to W if the protected image is same as original image. On the other hand, if the protected image has been modified, there maybe a little difference between W' and W. To verify if the secret key K was indeed generated at certain time t, we can use the public key of TSS with the original image O and the time-stamp K_s.

Figure 1 shows the procedures of key generation and watermarks detection. In next section, we will show the experimental results for the proposed algorithm.

4 EXPERIMENTAL RESULTS

The robustness of the proposed scheme was subjected to various attacks. The experimental results from Blurring, JPEG, Sharpening, Rotation and Cropped attacks are demonstrated as follows. Note that all altering algorithms were performed using ”Photoshop”, which was published by the Adobe Company. Figure 2(a) shows the original image of ”Lena” (8 bits/pixel, 512×512), Figure 2(b) and Figure 2(c) are the watermarks (64×64) of ”National Chung Cheng University (CCU)” and ”PlayBoy Company (PB)”, respectively.

First, we used a Blurring algorithm and JPEG compression to alter the original image. The altered results are shown in Figure 3(a) and Figure 3(b), respectively. Note that, a 5×5 neighborhood median was used for the Blurring algorithm [**?**]. The lowest quality parameter of JPEG was used in the above altered image. The feature function is the block-mean which is used in the following experiments. In other words, the feature of each selected block is its mean. The block's height and width both are 8 (512/64) pixels, respectively. Figure 3(c) is the retrieved watermark of ”CCU” from Figure 3(a), and Figure 3(d) shows the retrieved watermark of ”Play Boy” from Figure 3(a). Figure 3(e) and Figure 3(f) are retrieved watermarks from Figure 3(b).

Next, the original image was rotated one degree in clockwise direction as shown in Figure 4(a) (resized to 521×521). The other modified image, using the Sharpening algorithm, is shown in Figure 4(b). Figures 4(c), 4(d) and Figures 4(e), 4(f) are retrieved watermarks from Figures 4(a) and 4(b), respectively. In particular, we can directly retrieve the watermark from the rotated image. In other words, for watermark retrieving, it is not necessary to resize the size of the rotated image to the original ones. Furthermore, if resizing of the rotated image returns to the original ones, the higher ratio of retrieved watermarks can be obtained.

A cartoon graphic ”Bunny” was also used in our experiment. We used the block-variance as the feature function in this experiment. The block's height and width both are 4 (256/64) pixels, respectively. Figure 5(a) is the original graphic of ”Bunny”, Figure

5(b) shows a repainted image of "Bunny". Both the face and background of "Bunny" were replaced with other grey levels. The retrieved watermarks from original image of "Bunny" are shown in Figures 5(c) and 5(d). In particular, Figures 5(c) and 5(d) show that the retrieved watermarks from unmodified images are stable (same as original watermarks). Figures 5(e) and 5(f) demonstrate the retrieved watermarks from Figure 5(b), the repainted image.

Figure 6(a) is a cropped left-top corner of "Lena". The block-variance is the feature function in this experiment, too. Figures 6(b) and 6(c) demonstrate the retrieved watermarks respectively belonging to "CCU" and "PB" are recognizable. In other words, the proposed digital watermarking technique enables to overcome the crop attack.

Finally, the retrieved watermarks under different host images are shown in Table 1. The experimental results demonstrate that the retrieved watermarks are recognizable under various attacks.

5 DISCUSSIONS AND SECURITY ANALYSES

Table 2 shows comparisons between the feature-based copyright detection method and some traditional watermarking schemes. The main difference is the focus on the watermarked/protected image. In traditional watermarking schemes, the watermarked image is different from the original image. Both images are the same in the proposed method. Furthermore, the experimental results show that the proposed method can resist several attacks. In particular, the 'repaint' attack for cartoon images. The second characteristic of this work is that the feature function can vary with the properties of the original images. Later in this paper we will state the candidates for this feature function.

The security of the proposed algorithm depends upon the domain of the seed s. In general, $1,024$ bits are enough for a watermarking system. On the other hand, the secret key length $|K|$ is according to the size of watermark. For $|K| \geq 1024$ bits, the watermark's size should be larger than or equal to 32 by 32. In fact, the larger watermarks size is, the higher security of the proposed scheme will be. Nevertheless, the memory space requirement increases.

As mentioned above, the required storage space for the secret keys K depends upon the watermark size. In general, the signed time-stamp K_s has limited length. However, the extra space requirement caused by embedding a watermark is practical in the proposed algorithm. For example, if the length of K_s is 1,024 bits and the size of the watermark is 64×64, the extra space equals 4,096+1,024=5,120 bits. In contrast to lost intellectual property, the cost for the extra space is worthwhile.

We previously mentioned that the main feature of the proposed algorithm is that the protected image remains the same as the original host image. This characteristic makes the proposed scheme easily applicable to any undistorted images. Furthermore, there is no time limit for embedding the watermark. In other words, the copyright can be traded and traced any number of times through the secret key K and its time-stamp K_s. In addition the quality of the protected image will still be as good as the original. However, there are strong probabilities that the same secret key can be used for two or more similar images, if there are two similar images belonging to two different owners. The proposed scheme can identify exactly who is the original copyright owner, because the time associated with the pirate's time-stamp will always be later than the owner's time-stamp. However, if there are two similar images that are actually created by two different individuals, our method will xreate some confusion. Fortunately, the probability of this situation is very small in the real world. To overcome this problem, the TSS must keep an original copy to identify the actual copyright owner.

Anyone else can apply our algorithm to construct his/her secret key even though the image is stolen from others. A pirate can also forge a time-stamp K'_s to make the signing time earlier than the original owner's. After that, with the help of his/her secret key, the pirate steals the image successfully. Nevertheless, since the signed time-stamp K_s' is produced by a public-key cryptosystem, such as RSA. Consequently, to forge an illegal time-stamp K_s' is as difficult as breaking a public-key cryptosystem.

The interesting issue of the proposed algorithm is to find better feature functions as well as transform functions. For the feature function, we suggest some alternate methods. For example, the indices of vector quantization (VQ) techniques [**?**, **?**], the centroid of feature blocks, the block-harmonic-mean and so on. A frequency domain transformer also can be the feature function. For example, extract the significant coefficients of DCT or wavelet transform as the block feature. For transform function, another method can be considered with the help of relationship between the adjacent block features. For example, if the current block feature is greater than previous block feature, the transformed bit is taken as '1', or as '0'. By comparing all the blocks a temporary key can be generated. However, it needs to be confirmed.

6 CONCLUSIONS

A new feature-oriented copyright owner detection technique was proposed in this paper. The presented technique can retrieves watermarks from various kinds of images and graphics and also saves images from distortion. In addition, as the experimental results show, this method can resist various attacks, such as blurring, sharpening, lossy compression, cropping and rotation. In particular, cropping and rotating attacks are entirely difficult problem in traditional watermarking system before this work. Time-stamping technique has also been introduced in this work to protect copyright.

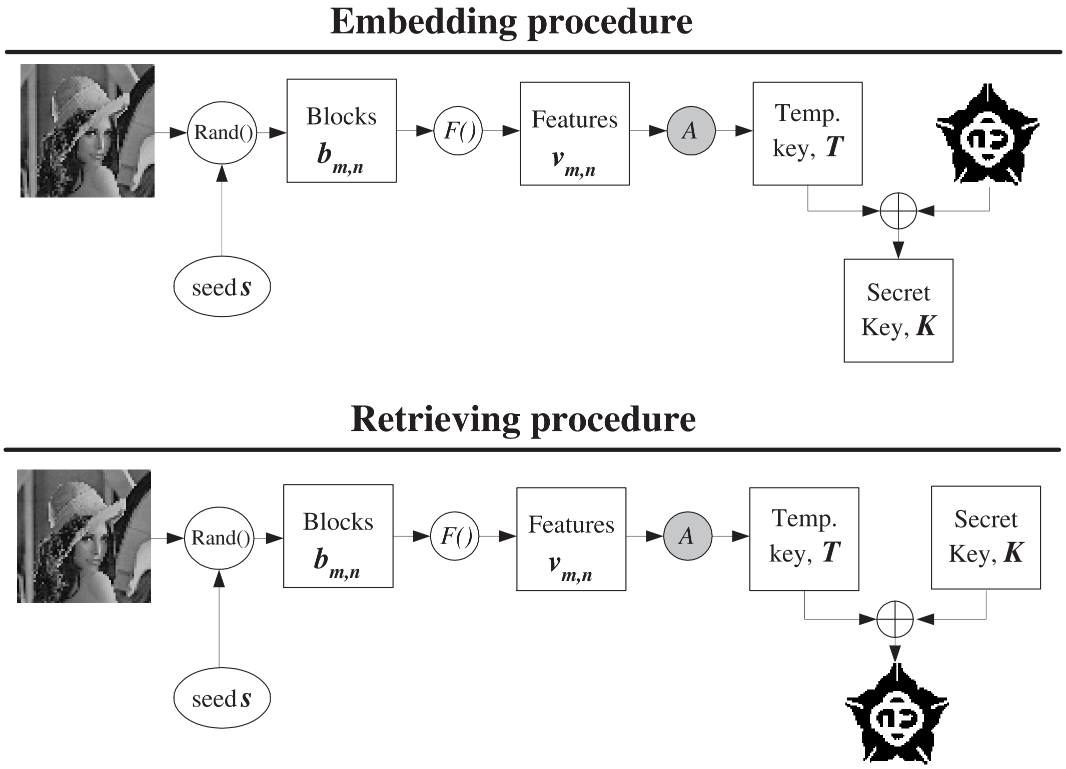
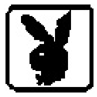


Figure 1: Procedures of key generation and watermarks detection

(a)

(b)



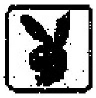
(c)

Figure 2: (a)Original image of ”Lena” (512 × 512), (b)Watermark of ”National Chung Cheng University (CCU)” (64 × 64), (c)Watermark of ”Play Boy (PB)” (64 × 64)

(a) PSNR=29.62dB

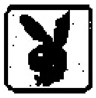
(b) PSNR=34.07dB

(c) R=99.22%



(d) R=99.09%

(e) R=99.63%



(f) R=99.68%

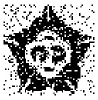
Figure 3: (a)Blurred image of ”Lena”, (b)Reconstructed JPEG image, (c)A retrieved watermark from Figure 3(a), (d)Another retrieved watermark from Figure 3(a), (e)A retrieved watermark from Figure 3(b), (f)Another retrieved watermark from Figure 3(b)

Table 1: The ratio of the retrieved watermarks (”CCU” and ”PB”) from several attacks using various host images

Image		Blurring	JPEG	Sharpening	Rotating	Cropping
Lena	PSNR (dB)	29.62	34.07	23.10	NA	10.29
	CCU/PB (%)	99.22/99.09	99.63/99.68	98.90/98.95	87.50/88.45	94.82/95.75
Barbara	PSNR (dB)	23.41	31.29	17.15	NA	11.42
	CCU/PB (%)	99.15/99.02	99.56/99.54	96.68/96.44	87.72/87.16	90.36/93.69
Airplane	PSNR (dB)	26.38	31.65	21.18	NA	14.18
	CCU/PB (%)	98.97/99.05	99.56/99.61	98.58/98.80	91.04/91.14	93.51/93.99

(a) Resized to 521×521

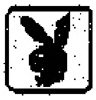
(b) PSNR=23.10dB



(c) R=87.50%

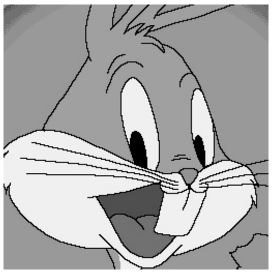
(d) R=88.45%

(e) R=98.90%

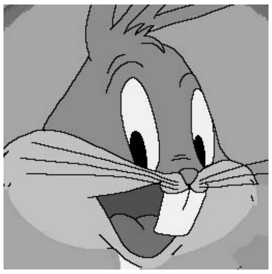


(f) R=98.95%

Figure 4: (a)Rotated one degree image of "Lena", (b)Sharpened image of "Lena", (c)A retrieved watermark from Figure 4(a), (d)Another retrieved watermark from Figure 4(a), (e)A retrieved watermark from Figure 4(b), (f)Another retrieved watermark from Figure 4(b)

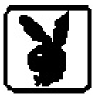


(a) 256×256

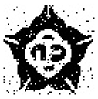


(b) PSNR=18.68dB

(c) R=100.0%



(d) R=100.0%

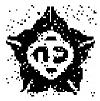


(e) R=96.12%

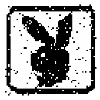
(f) R=96.41%

Figure 5: (a)Original graphic of "Bunny", (b)Repainted graphic of "Bunny", (c)A retrieved watermark from Figure 5(a), (d)Another retrieved watermark from Figure 5(a), (e)A retrieved watermark from Figure 5(b), (f)Another retrieved watermark from Figure 5(b)

(a) PSNR=10.29dB



(b) R=94.82%



(c) R=95.75%

Figure 6: (a)Cropped image of "Lena", (b)Retrieved watermark of "CCU", (c)Retrieved watermark of "Play Boy"

Table 2: Comparisons between the proposed technique with some traditional watermarking schemes

	Hsu & Wu [?]	TAWS [?]	Langelaar etc. [?]	Caronni [?]	feature-based
frequency/spatial domain	freq. (DCT)	freq. (Wavelet)	spatial	spatial	freq./spatial
protected image V.S. original image	modified	modified	modified	modified	unchanged
original image for watermark detection	Yes	No	Yes	Yes	No
Robustness	JPEG, Cropping	JPEG, SPHIT	JPEG	JPEG	JPEG, Blurring, Sharpening, Cropping, Rotation, Repainted
consider multiple claims problem [?]	Undescribed	Undescribed	Undescribed	Undescribed	Time-Stamping with TTP