A Robust Authentication Scheme for Protecting Copyrights of Images and Graphics

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

Department of Computer Science and [†]
Information Engineering,
National Chung Cheng University,
Chaiyi, Taiwan, 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

March 26, 2001

[§] Responsible for correspondence:
Professor Min-Shiang Hwang
P. O. Box 55-67, Taichung, Taiwan 404, R.O.C.
Tel: 886-4-3323000ext4288
Fax: 886-4-3742337
Email: mshwang@mail.cyut.edu.tw

A Robust Authentication Scheme for Protecting Copyrights of Images and Graphics

Abstract

Watermarking techniques are primarily used for copyright protection. In this paper, a simple and robust watermark-like digital authentication scheme is proposed. This work has two major merits. First, the watermark used in the proposed authentication scheme is the same type used in the original image, e.g., grey level images. Second, the proposed scheme meets the requirements for watermarking techniques. Illegal users cannot perceive and break the watermark signed from the original image. Furthermore, the signed watermark is robust against attacks by many image altering algorithms, such as filtering, lossy compression, rotation, and scaling. The proposed scheme is not only suitable for ordinary natural images, but also for cartoon graphics.

Key Words: Digital watermarking, digital signature, digital authentication, torus automorphism, intellectual property right, time-stamping

1 INTRODUCTION

Because of the proliferation of the Internet, a huge amount of multimedia content is available over the network for any user to browse and download. Today, many traditional transactions are conducted over the Internet and new business applications are employed such as reading web newspapers, magazines, network audio, on-line pay-per-view, video on demand, on-line consulting, component-based software, virtual shopping, etc. Therefore, security and copyright issues have become increasingly important. Many security problems can be overcome using cryptography, but until now, copyright protection in the digital world has been lacking.

1.1 Digital Watermarking and Its Requirements

Digital watermarking is applicable to copyright protection. From a visual viewpoint there are two types of watermarking. The first is the visible embedded watermark. The primary advantage of the visible watermark is the ease of identification by the owner. The embedded watermark is also easier to remove using image processing techniques. The second type is the invisible embedded watermark. In order to achieve copyright protection, digital watermarking must satisfy the following requirements:

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. In general, a PSNR (peak signal-to-noise ratio) larger than or equal to 30 means that the quality of the modified image is acceptable.
2. The embedded watermark must be retrievable without using information from the original image. In other words, storing a duplicate copy should be avoided. This is not practical for a huge image database.
3. Similar to cryptography, the security of watermarking cannot be based upon the assumption that possible attackers do not know how the watermark was embedded into the image.
4. Even though the attack knows how the watermark image was embedded, only the copyright owner should possess a method to detect or remove the watermark from the watermarked image.
5. It must be possible to retrieve the watermark after multiple and various image processes, such as low-pass filtering, high-pass filtering, lossy compression, s-caling, cropping, etc., provided that the quality of the altered image is acceptable.

   For more information about digital watermarking, interested readers may consult [5, 10, 11, 15, 19, 23, 24].

From a conventional technical viewpoint, digital watermarking techniques can be classified into two categories. The first category embeds the watermark into the spatial domain [13, 20, 22]. In general, this method has a computing performance advantage, but the disadvantages are lower security and weaker robustness. The second category of watermarking technique embeds the watermark into the frequency domain [2, 4, 18]. This method transforms the original data into the frequency domain, which embeds the watermark after using the Fourier, Discrete Cosine, or Wavelet transformation. The proposed scheme belongs to the first category of watermarking techniques.

1.2 Time-Stamping

Time-Stamping (TS) [3, 8, 9] is a technique used to ascertain whether or not a piece of digital medium was created or signed at a certain time. TS is also a candidate as a copyright protection technique. Digital medium does not utilize time seals. In other words, the exact time that a certain medium is created cannot be obtained by examining the digital data. Since digital media can be easily reproduced, the rightful owner can use a TS to protect his copyright. An example of this is full text documentation. Most digital media, such as images, videos, and sounds, have characteristic allowable distortion. A pirate can utilize this characteristic to slightly modify a digital medium from the rightful owner. The modified medium could be wholly different from the original data in digital data style. It is very difficult to perceive the difference through human senses alone. Because of these differences, a pirate can claim that he is the rightful copyright owner of that medium. Time-Stamped messages for wholly different data cannot be used as strong evidence in court. This problem can be overcome by the robustness of watermark-like techniques.

1.3 Problems of Digital Watermarking

However, there are still problems in digital watermarking. One, as pointed out by Craver et al. [6, 7], is how to resolve the rightful ownership of the invisible watermarking scheme. Craver et al. argued that a watermarked image could allow multiple claims of ownership. In order to resolve this problem, Craver et al. proposed a watermarking scheme based on the concept of non-invertibility. Unfortunately, their scheme cannot be proven to be non-invertible. Until now, most of the proposed digital watermarking schemes involve only the owner's information, i.e., trademark, uniform commercial code, personal ID, etc. Moreover, in this process, the owner has complete control of the watermark embedding and the verification thereof. That is the essence of the problem demonstrated by Craver et al. In order to provide proper copyright protection, a trusted third party should be introduced. Voatzis and Pitas proposed a generic model for protecting copyrights [21], which also included a trusted registration authority. In addition, they pointed out that geometric attack, such as rotation and scaling, is an essential remaining problem for schemes that do not use original images in the watermark retrieval stage.

As previously mentioned, watermarking techniques are used to protect the copyright of digital medium. Trading behavior is very common in everyday life. Consequently, how to deal with the transaction of intellectual property is another problem. As we know from existing watermarking techniques, this problem has not been dealt with in most of the proposed methods. To embed multiple watermarks into the digital medium is one of the solutions. In other words, both the seller's and buyer's watermarks are embedded into the traded medium at the same time. Nevertheless, the previous embedded watermark cannot be guaranteed to survive after the next watermark is embedded. Authentication systems have mostly been applied to electronic commerce (EC). Applying the authentication system here should be a solution to solve the above problem.

As discussed above, utilizing the robustness of watermarking techniques along with TS is applicable to copyright protection. Consequently, we attempt to develop a watermark-like authentication scheme to overcome the previously mentioned problems. Note that the authentication scheme is like a watermark in purpose rather than in methodology.

Digital cartoons and map graphics have significant differences from ordinary natural images. Cartoon and map images do not possess complicated color and texture variations. This unique feature makes it difficult to embed watermarks. Moreover, these images can be easily repainted using other colors without affecting the original purpose. That is another challenge for copyright protection techniques. This challenge is what motivated us to research this topic.

1.4 Organization of This Paper

In this paper, we propose a new digital authentication scheme for the copy protection of images. We simply use the torus automorphism to construct a matrix which records the mapping rule from the watermark into the original image. The mapping rule is later used to compute a watermark from a protected image. The details of the proposed scheme can be found in Section 4. Section 2 reviews some digital watermarking and digital time-stamping schemes. Section 3 demonstrates the torus automorphism theorem, which will be used in the proposed scheme. Section 4 describes the details of this work. Section 5 shows the experimental results of the proposed digital authentication scheme. Finally, Sections 6 and 7 present the discussions and conclusions of this paper.

2 RELATED WORKS

Voatzis and Pitas first introduced the theory of torus automorphism to digital watermarking [22]. A watermark is chaotically mixed using torus automorphism and superimposed onto a host image. In fact, the watermark is embedded within the least significant bits (LSB) of the host image. Hence, the watermark can be destroyed easily. In [20], Voatzis and Pitas proposed another scheme also based upon torus automorphism. They concluded that this algorithm is robust against JPEG lossy compression up to 15:1 and for 5×5 average filters (blurring). Furthermore, the embedded watermark can be detected using statistical hypothesis testing when large modifications have been rendered upon the watermarked image.

In 1997, Langelaar et al. [14] proposed two watermarking techniques for images. Their first scheme embeds a watermark into the Y-channel (luminance) of color images. A watermark is a bit string (containing approximately a few hundred bits). Each watermark bit is hidden into a non-overlapped block $\mathbf{B}(8 \times 8)$ of luminance values. To embed the watermark, a quality threshold T, and the embedding-levels (k_0 and k_{max}) are determined by the degree of the JPEG compression ratio. In their experiments, the authors only demonstrated that their scheme is able to resist JPEG compression attacks.

Hsu and Wu [12] proposed an image watermarking technique based on DCT. A watermark (binary image) is embedded into a host image by selectively modifying the middle-frequency DCT coefficients. Multiple watermarks can also be embedded into a host image. The inventors claim that this algorithm is robust against lossy compression (JPEG) and cropping attacks. However, it is uncertain whether it is robust against other attacks, such as rotation, low-pass filtering, high-pass filtering, etc. In addition, the primary drawback of Hsu and Wu's scheme is that the original image is required to retrieve the watermark. As mentioned in Section 1, this is not practical for a large image database.

Su et al. proposed a digital watermarking technique based on wavelet-transformation [18], called TAWS (threshold-adaptive watermarking scheme). TAWS can embed an invisible watermark into various kinds of images. Cartoons and map graphics are especially suitable for this process. TAWS selects a few of perceptually significant wavelet-transformation coefficients within the same sub-band for watermark embedding. TAWS has demonstrated higher quality (PSNR $>$ 40) watermarked images in the inventors' experiments. Moreover, their experimental results also showed that TAWS protects against various lossy compression attacks, such as JPEG and SPIHT. Unfortunately, TAWS did not consider the "repaint" attack for cartoon graphics. Using the characteristics of cartoon graphics to destroy an embedded watermark, a pirate can easily repaint/replace cartoon graphics with other colors. Consequently, the capability of TAWS against this kind of attack is uncertain.

Haber and Stornetta [8] proposed a linking time-stamping protocol. A trusted third party (Time-Stamping Service, 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 identifier of the submitter, and L_n is the linking information, which is defined as follow:

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

Here $H(\cdot)$ is a one-way hash function [16, 17]. This scheme has some problems with practical implementation. For more information and improved schemes, please refer to [3, 9].

3 TORUS AUTOMORPHISM

Torus automorphism is a dynamical system. Briefly, a dynamical system is one whose state s changes with time t. When t is discrete, a dynamical system can be presented as $s_{t+1} = f(s)$, $t \in \mathbf{Z}$, which is an iteration of function f. A two-dimensional torus automorphism is depicted here. It can be considered a spatial transformation of a plane region. This transformation is performed using a 2×2 matrix $\mathbf{A}$ with wholly constant elements. A state or point $s' = (x', y')$ is given from $s = (x, y)$ by Equation (3).

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod 1. \tag{3}$$

Here $|\mathbf{A}|$ denotes the determinant of $\mathbf{A}$. In Equation (3), $a_{ij} \in \mathbf{Z}$, $|\mathbf{A}| = 1$, and $\mathbf{A}$ has eigenvalues $\lambda_{1,2} \in R - \{-1, 0, 1\}$. The detailed characteristics of $\mathbf{A}$ are described in [1] and [22]. A set of points $\{s_0, s_1, s_2, \ldots\}$ is an orbit $\mathcal{O}$ of the system. The initial point $s_0 = (x_0, y_0)$ classifies $\mathcal{O}$ into two categories. When both x_0 and y_0 are rational, $\mathcal{O}$ is periodic at every R times ($s_R = s_0$). R is called "recurrence time". If x_0 and/or y_0 are irrational, $\mathcal{O}$ is infinite. Our research involves the first category where the initial point is always rational.

Inspired by Voyatzis and Pitas [22], a one-parameter torus automorphism is introduced as follows. This system was applied in our scheme.

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \bmod N. \tag{4}$$

Here $(x_i, y_i) \in [0, N-1] \times [0, N-1]$ and $k \in [1, N-1]$. The recurrence time R depends upon the parameters k and N and the initial point (x_0, y_0). R was analyzed in [22] and it is concluded that in most cases R is equal to $N-1$ or $N+1$ when N is prime. There are other conditions which make R irregular. The system (4) is used to provide location information through A^n. The location information consists of the watermark's elements approximately mapped to the host image's. A complete description of our scheme will appear in the next section. Note that a pseudo-random number generator can also be utilized to provide the location information, but the torus automorphism provides a more convenient way to implement our scheme.

4 THE PROPOSED SCHEME

The primary idea of the proposed scheme is to determine a mapping rule to go from the watermark's elements to the original image's elements. This rule is recorded as a matrix P, called a secret key, which has the same dimensions as the watermark. The recorded matrix P is used to later compute the watermark. Furthermore, the signed P as P_s, through a trusted third party or TSS, will be the evidence used to identify the rightful intellectual property right (IPR) owner. The algorithm for the proposed scheme is described in the first subsection. The next subsection depicts the extended methods.

4.1 The Algorithm

Both the original image O and the watermark W require β bit(s) per pixel. Note that in our experiments β equals 8. O and W are defined as follows:

$$O = o_{i,j},\ i = 1, 2, \ldots, O_H,\ j = 1, 2, \ldots, O_W,\ 0 \leq o_{i,j} \leq 2^{\beta} - 1, \tag{5}$$

$$W = w_{i,j},\ i = 1, 2, \ldots, W_H,\ j = 1, 2, \ldots, W_W,\ 0 \leq w_{i,j} \leq 2^{\beta} - 1. \tag{6}$$

Here O_H and O_W are the original image's height and width, respectively. W_W is the watermark's width and W_H is the watermark's height. The system parameters of the torus automorphism are k and N. The criterion for choosing k and N creates the "recurrence time" $R \geq 2^{\tau}$, but it is not essential. Here τ is the length of P's elements. The tth matrix A^t is defined as follows:

$$A^t = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix}^t \bmod N. \tag{7}$$

$P = \{p_{i,j} | i = 1, 2, \ldots, W_H, j = 1, 2, \ldots, W_W\}$, is constructed by

$$p_{i,j} = t,\ \text{such that}\ \left|O_{A^t_{i,j}} - w_{i,j}\right| = \min_{0<n<2^{\tau}} \left(\left|O_{A^n_{i,j}} - w_{i,j}\right|\right). \tag{8}$$

Here $0 < t < 2^{\tau}$; $i = 1, 2, \ldots, W_H$; $j = 1, 2, \ldots, W_W$; and $O_{A^t_{i,j}}$ is defined as follows:

$$O_{A^t_{i,j}} = o_{i',j'}, \tag{9}$$

and

$$(i', j') \;=\; (i, j) \times A^t \bmod (O_H, O_W). \tag{10}$$

Briefly, $O_{A^t_{i,j}}$ is one pixel value of the original image at coordinate (i', j'). Here (i', j') is determined by A, t, and (i, j). After P is constructed, the key generation process is completed. Clearly, the protected image is the same as the original image in the proposed scheme. In other words, the original image has never been modified even though the image is protected. The image owner sends P to TSS to get a time-stamp P as P_s. P_s is used as a evidence to identify that the secret key P was generated from the image O at a certain time. The image owner has to keep k, N, and P_s secret.

The image owner's watermark W' can be computed by

$$w'_{i,j} \;=\; O_{A^{p_{i,j}}_{i,j}},\; i = 1, 2, \ldots, W_H,\; j = 1, 2, \ldots, W_W. \tag{11}$$

Note that the computed watermark W' is different from the original watermark W. The distortion is caused by Equation 8. However, the distortion is acceptable as shown in our experiments.

4.2 Extended Methods

In this subsection, we extend the proposed algorithm to achieve two goals. The first goal is to increase the quality of the computed watermark. Improving the robustness of the proposed scheme is the second goal.

Since the secret key is the mapping between the watermark and the original image, all of the pixel values in the watermark refer to that of the original image using the location information P. According to this characteristic, the brightness (histogram) of the watermark can be adjusted to be close to the original image's brightness before the embedding process. The quality of the computed watermark will be improved. Moreover, it is unnecessary to modify the proposed algorithm. In Section 5, we compare the computed watermarks before adjustment with the watermarks after adjustment. The quality of the adjusted watermark is better (see Table 1).

In order to resist a cropping attack in which pirates crop a major portion of the original image, we need to modify the embedding area of our scheme. The simplest method is to use a rectangle $\Re$ to enclose the major/important portion of the original image. $\Re$ is defined as

$$\Re \quad = \quad \{(\rho_x, \rho_y),\ (\rho_w, \rho_h)\}. \tag{12}$$

Here $\Re$ is a subset of O, which is enclosed from (ρ_x, ρ_y) to (ρ_w, ρ_h), where $1 \leq \rho_x \leq O_W$, $1 \leq \rho_y \leq O_H$, $1 \leq \rho_w \leq O_W$, $1 \leq \rho_h \leq O_H$, $\rho_x < \rho_w, \rho_y < \rho_h$.

Equation (9) can now be redefined as follows:

$$O_{A^t_{i,j}} \quad = \quad o_{i'',j''}. \tag{13}$$

Here $(i'', j'') = (\rho_x, \rho_y) + A^t \times (i, j) \bmod (\rho_w - \rho_x, \rho_h - \rho_y), 1 \leq i'' \leq O_H, 1 \leq j'' \leq O_W$. Note that $\Re$ is determined by the image owner; ρ_x, ρ_y, ρ_w, and ρ_h must be kept for watermark computing. Indeed, the proposed scheme in the previous subsection is a special case of this extended method where $\Re = \{(1, 1),\ (O_w, O_h)\}$.

5 EXPERIMENTAL RESULTS

In our experiment, the parameters of the torus automorphism are $k = 32$ and $N = 1117$. Figure 1(a) shows the original image of "Lena" (512×512), Figure 1(b) and Figure 1(c) are watermarks (64×64) of "National Chung Cheng University" and "Honey", respectively. The size of the watermark is $32,768$ $(64 \times 64 \times 8)$ bits. We used τ=4 bits to construct matrix P. The robustness of the proposed scheme was subjected to various attacks. The experimental results from Blurring, JPEG, Rotating, and Shear attacks are demonstrated as follows. Note that all altering algorithms were performed using "Photoshop", which was published by the Adobe company.

The altered images using a Blurring algorithm and JPEG compression are shown in Figure 2(a) and Figure 2(b), respectively. Figure 2(c) shows the computed watermark (Figure 1(b)) from Figure 2(a), and Figure 2(d) shows the computed watermark (Figure 1(c)) from Figure 2(a). Figure 2(e) and Figure 2(f) are computed watermarks from Figure 2(b).

Next, the original image is rotated 1 degree (clockwise) as Figure 3(a) (Resized to 521×521). The other modified image using the Shear algorithm is shown in Figure 3(b). Both of these two alterations are geometric distortions. The key feature of the Shear technique lowers the PSNR but produces a higher visual quality. Figure 4 shows the parameters of the Shear algorithm. Figures 3(c), 3(d) and Figures 3(e), 3(f) are computed watermarks from Figures 3(a) and 3(b), respectively.

A cartoon graphic was also used in our experiment. Figure 5(a) shows the original graphic of "Bunny", Figure 5(b) is a repainted image of "Bunny". Both the face and background were replaced with other grey levels. The computed watermarks from Figure 5(a) are shown in Figures 5(c) and 5(d). Figures 5(e) and 5(f) demonstrate the computed watermarks from Figure 5(b). Note that the quality of the retrieved watermark will be improved using our extended methods.

The extended methods are implemented and experimented with as follows. First, the watermark's (Figure 1(b)) grey level is adjusted to close to that of "Lena"'s (Figure 1(a)). Figures 6(a) and 6(b) demonstrate the histograms of "Lena" and the watermark of "National Chung Cheng University". Figure 6(c) is the adjusted watermark. Figure 6(d) shows the histogram of the adjusted watermark. Comparisons of the computed watermarks and their PSNR under various attacks are shown in Table 1. The quality of the computed watermarks is improved.

The second extension method shrinks the area for computing the watermark. Let $\Re = \{(125, 50), (370, 435)\}$, $\tau = 8$ bits, $k = 32$, and N=1117. After P is constructed, a major portion of "Lena" (around Lena's face) is cropped and pasted onto another picture. Figure 7(a) demonstrates the processed image. The computed watermark from the processed image is shown in Figure 7(b). Note that the approximate coordinates $\Re$ are needed to compute the watermark from the cropped and pasted picture. This is not feasible in practice. However, the purpose of this experiment is to prove that possessing the exact coordinates of $\Re$ is not necessary. We have examined several values of $\Re$ for the computing watermark. The range between $\{(120, 45), (365, 430)\}$ and $\{(130, 55), (375, 440)\}$ is workable. Therefore, if there are some mechanisms that can be applied to estimate the appropriate coordinates using case cropping, the second extension method will be more practical.

Finally, the computed watermarks under different host images and several values of τ are shown in Table 2. The experimental results show that the computed watermarks are recognizable under various attacks.

6 DISCUSSIONS

A watermark can be a trademark (image), uniform commercial code, personal ID, etc. The advantage of using an image, particularly a grey level image, is intuitive recognition. Moreover, a slight distortion of the image is allowable. Therefore, using images as a watermark is recommended. Our efforts in this work have achieved this.

Table 2 shows that τ, which is greater than or equal to four, is suitable for larger ($\geq 512 \times 512$) images, $\tau \geq 6$ is suitable for smaller images and cartoon graphics. If storage is not taken into account, $\tau = 8$ is suggested. The requirement for storage space is dependent on the watermark size and τ. The extra space required to compute a watermark is practical in the proposed scheme. For example, let $\tau = 8, W_w = 64,$ and $W_h = 64$, the extra space equals 4 KB. The ratio of extra space to host image (512×512 bytes) is 1.56 percent. In comparison with the consequences of the loss of intellectual property, the cost of the extra space is worthwhile.

Table 3 shows comparisons between the robust digital authentication system and some traditional watermarking schemes. The main differences are listed as follows. First, in traditional watermarking schemes, the protected image is different from the original image, but they are exactly the same in the proposed method. Second, the type of watermark can be a grey level image of the proposed scheme, but a binary image of the others. Furthermore, as shown in the experimental results, the proposed method can resist several attacks. In particular, it can resist the "repaint" attack for cartoon images.

The security of the proposed scheme depends upon the domain of k and N. In general, $1,024$ bits are enough for a watermarking system. Furthermore, using variant k or N for an individual image, the security can be improved. Inspired by Voyatzis and Pitas [22], a more complex dynamical system (different automorphisms) can be introduced to improve the security of the proposed scheme. The signed time-stamp P_s of the copyright owner is the main evidence to prove the copyright ownership in the proposed scheme. A pirate can still produce a valid secret key P' and obtain a corresponding time-stamp P'_s from TSS. However, the time embedded in P'_s is always later than that of P_s unless P'_s can be forged. The time-stamp P_s is produced using a public-key cryptosystem, such as RSA [17]. Consequently, to forge an illegal time-stamp is as difficult as breaking a public-key cryptosystem.

Since the computation of the proposed scheme is very simple, the complexity of the key generation algorithm depends on W_H, W_W and τ (at most 8). Moreover, a look-up table can be substituted for A^p. In contrast to frequency domain techniques, the performance of the proposed method is very high. Furthermore, other types of images, such as the RGB color image, are also suitable because the proposed algorithm does not depend upon the image format.

The main feature of the proposed scheme is that the quality of the protected image is very high. In fact, the protected image is the same as the original host image. This characteristic is applicable to images in which distortion is not allowable, e.g., medical images. Furthermore, the potential to trade the protected images is unlimited. In other words, the copyright can be traded and traced unlimited times through P and P_s. By applying the linking time-stamping protocol [3, 9], we can trace the trading history. No matter how many times the image is traded, the image quality is still as good as the original one. Moreover, there is also no size limit for host images. Even through the size of the host image is equal to the watermark, the proposed algorithm is still workable. Consequently, a watermark can be computed multiple times from various portions of the host image, and the robustness can be improved. This characteristic makes it more practical for copyright protection.

7 CONCLUSIONS

A new robust digital authentication technique is proposed in this paper. The proposed scheme can compute the watermark of the owner from the protected images. Our method satisfies most of the requirements of digital watermarking. The fact that the protected image remains the same as the original one is the main difference between our scheme and digital watermarking. This method is robust against various attacks as shown by the experimental results. To properly provide copyright protection, a time-stamping technique is introduced in this work. Furthermore, two extended methods are proposed to improve the quality of the computed watermark. Future work will include applications to audio, video, DVD, full text, etc. to increase the utilization of the proposed scheme.

References

[1] Arrowsmith, D. K. and Place, C. M.: 'An Introduction to Dynamical Systems' (Cambridge Univ. Press, 1990)

[2] Bors, A. G. and Pitas, I.: 'Image watermarking using dct domain constraints,' Proceedings of 1996 IEEE International Conference on Image Processing (ICIP'96), 1996, **3**, pp. 231–234

[3] Buldas, A., P. Laud, H. L., and Villemson, J.: 'Time-stamping with binary linking schemes,' *Advances in Cryptology - CRYPTO'98*, 1998, pp. 486–501

[4] Cox, I. J., Kilian, J., Leighton, F. T., and Shamoon, T.: 'Secure spread spectrum watermarking for multimedia,' *IEEE Transactions on Image Processing*, 1997, **6**, (12), pp. 1673–1687

[5] Cox, I. J., Miller, M. L., and McKellips, A. L.: 'Watermarking as communications with side information,' *Proceedings of the IEEE*, July 1999, **87**, (7), pp. 1127–1141

[6] Craver, S., Memon, N., Yeo, B.-L., and Yeung, M.: 'Can invisible watermarks resolve rightful ownership?' *Proc. SPIE Stroage and Retrieval for Still Image and Video Databases V*, 1997, **SPIE 3022**, pp. 310–321

[7] Craver, S., Memon, N., Yeo, B. L., and Yeung, M. M.: 'Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications,' *IEEE Journal on Selected Areas in Communications*, 1998, **16**, (4), pp. 573–586

[8] Haber, S. and Stornetta, W. S.: 'How to time-stamping,' *Journal of Cryptology*, 1991, **3**, (2), pp. 99–111

[9] Haber, S. and Stornetta, W. S.: 'Secure names for bit-strings,' Proceedings of 4th ACM Conference on Computer and Communications Security, 1997, pp. 28–35

[10] Hartung, F. and Kutter, M.: 'Multimedia watermarking techniques,' *Proceedings of the IEEE*, July 1999, **87**, (7), pp. 1079–1107

[11] Hernandez, J. R. and Perez-Gonzalez, F.: 'Statistical analysis of watermarking schemes for copyright protection of images,' *Proceedings of the IEEE*, July 1999, **87**, (7), pp. 1142–1166

[12] Hsu, C. T. and Wu, J. L.: 'Hidden digital watermarks in images,' *IEEE Trans. on Images Processing*, January 1999, **8**, (1), pp. 58–68

[13] Kutter, M., Jordan, F., and Bossen, F.: ‘Digital watermarking of color images using amplitude modulation,’ *Journal of Electronic Imaging*, 1998, **7**, (2), pp. 326–332

[14] Langelaar, G. C., Lubbe, J. C. A., and Lagendijk, R. L.: ‘Robust labeling methods for copy protection of images,’ Proceedings of SPIE Electronic Imaging ’97, Storage and Retrieval for Image and Video Database V, San Jose, CA, 1997, pp. 298–309

[15] Petitcolas, F. A. P., Anderson, R. J., and Kuhn, M. G.: ‘Information hiding-a survey,’ *Proceedings of the IEEE*, July 1999, **87**, (7), pp. 1062–1078

[16] Rivest, R. L.: ‘The MD5 message digest algorithm,’ *RFC 1321*, April 1992

[17] Schneier, B.: ‘Applied Cryptography’ (WILEY, 1996), 2nd edition

[18] Su, P.-C., Kuo, C.-C. J., and Wang, H.-J. M.: ‘Blind digital watermarking for cartoon and map images,’ Proceedings of SPIE, 1999, **3657-31**

[19] Swanson, M. D., Kobayashi, M., and Tewfik, A. H.: ‘Multimedia data-embedding and watermarking technologies,’ *Proceedings of IEEE*, 1998, **86**, (6), pp. 1064–1087

[20] Voyatzis, G. and Pitas, I.: ‘Embedding robust watermarks by chaotic mixing,’ Proceedings of 13th International Conference on Digital Signal Processing (D-SP’97), 1997, **1**, pp. 213–216

[21] Voyatzis, G. and Pitas, I.: ‘Protecting digital-image copyrights: A framework,’ *IEEE Computer Graphics and Applications*, 1999, **19**, (1), pp. 18–24

[22] Voyatzis, G. and Pitas, I.: ‘Chaotic mixing of digital images and applications to watermarking,’ Proceedings of European Conference on Multimedia Applications, Services and Techniques (ECMAST ’96), May 1996, **2**, pp. 687–695

[23] Wolfgang, R. B., Podilchuk, C. I., and Delp, E. J.: ‘Perceptual watermarks for digital images and video,’ *Proceedings of the IEEE*, July 1999, **87**, (7), pp. 1108–1126

[24] Yeung, M. M.: ‘Digital watermarking,’ *Communications of the ACM*, July 1998, **41**, (7), pp. 30–33

Table 1: Comparison before and after adjusting watermark

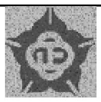
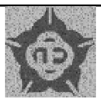
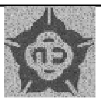
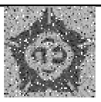
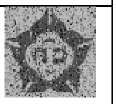
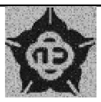
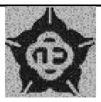
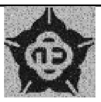
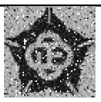
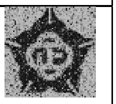
Attacks	Original	Blurring	JPG	Rotating	Shear
Original mark					
PSNR(dB)	13.48	13.32	13.42	11.27	11.26
Adjusted mark					
PSNR(dB)	22.21	20.88	21.93	15.27	15.78

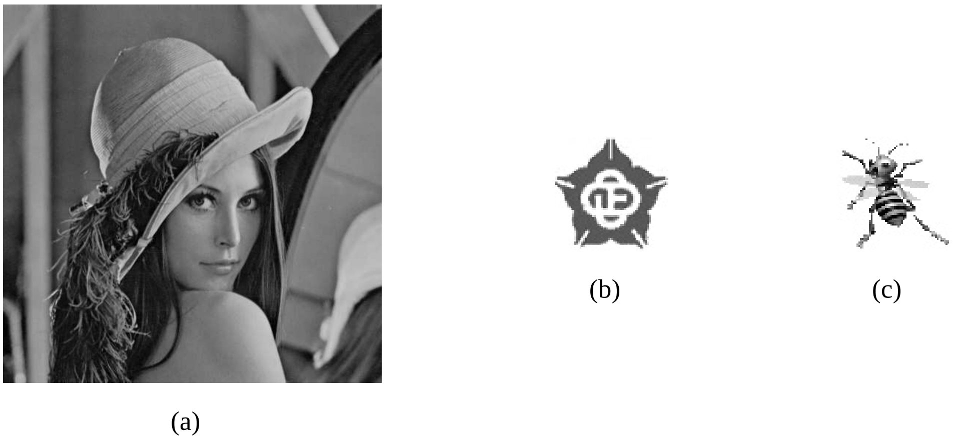
Table 2: All of the PSNR values obtained by using the first extended method to compute watermarks from various host images under different τ

Host image	τ(bits)	Original	Blurring	JPEG	Rotating	Shear
Lena (512×512) and watermark (Fig.6(c))	2	13.24	13.02	13.18	11.56	11.67
	3	17.56	17.03	17.46	13.68	13.87
	4	22.21	20.88	21.93	15.27	15.78
	5	27.38	24.34	26.48	16.14	16.72
	6	32.18	26.32	30.05	16.52	16.73
	7	36.28	27.15	32.20	16.37	16.35
	8	49.10	27.30	33.40	15.91	16.10
Barbara (512×512) and watermark (Fig.6(c))	2	13.71	13.24	13.64	11.52	11.80
	3	19.74	17.64	19.48	13.87	14.06
	4	25.69	20.55	24.76	14.59	15.34
	5	32.77	22.07	29.40	15.10	16.26
	6	39.01	22.42	31.05	14.95	16.16
	7	44.72	22.31	31.62	14.83	16.39
	8	49.70	22.32	31.73	14.72	16.39
Bunny (256×256) and watermark (Fig.1(b))	2	12.44	10.98	9.79	9.76	12.44
	3	15.37	14.09	15.29	10.72	10.97
	4	18.18	15.84	17.92	11.26	11.56
	5	21.00	17.10	20.38	11.58	12.01
	6	24.43	18.03	22.87	11.97	12.27
	7	27.63	18.50	24.83	12.18	12.34
	8	28.91	18.62	25.52	12.21	12.36

Table 3: Comparisons between the proposed technique and some traditional watermarking schemes

	Voatzis & Pitas [20]	Langelaar etc. [14]	Hsu & Wu [12]	TAWS [18]	Proposed scheme
Frequency/Spatial domain	Spatial	Spatial	Frequency (DCT)	Frequency (Wavelet)	Spatial
Protected image V.S. Original image	Modified	Modified	Modified	Modified	Unchanged
Type of watermark	Binary	Bit string	Binary	Binary	Grey level
Original image for watermark detection	No	Yes	Yes	No	No
Robustness	JPEG Blurring	JPEG	JPEG Cropping	JPEG SPHIT	JPEG Blurring Sharpening Rotation Repainted
Multiple claims problem [6]	Undescribed	Undescribed	Undescribed	Undescribed	Time-Stamping with TTP

List of Figures

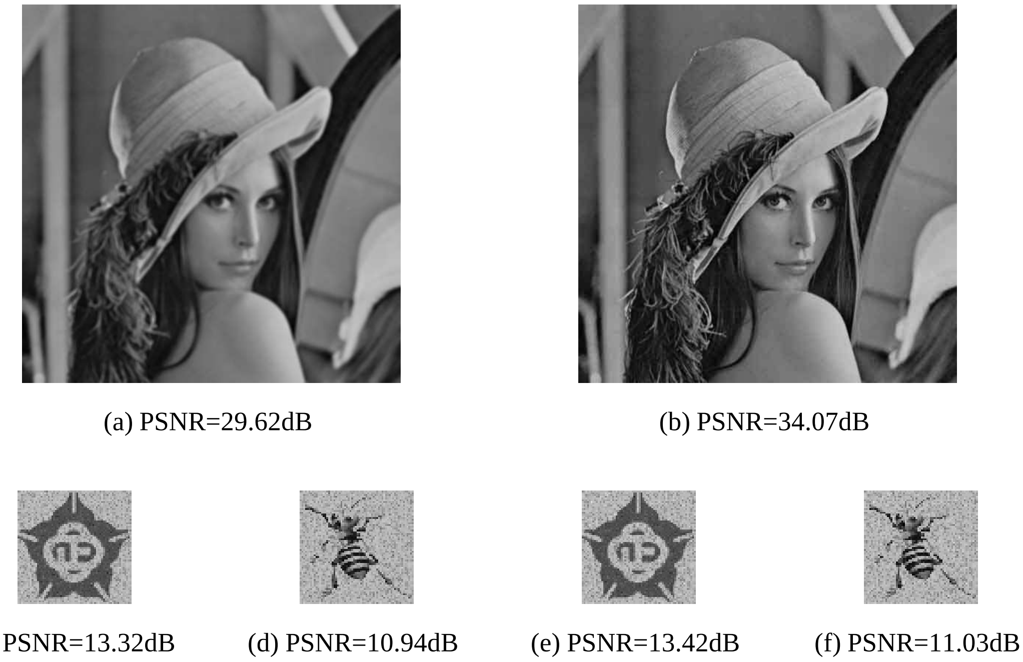


(a)

(b)

(c)

Figure 1: (a)Original image of “Lena” (512×512), (b)Watermark of “National Chung Cheng University” (64×64), (c)Watermark of “Honey” (64×64)



(a) PSNR=29.62dB

(b) PSNR=34.07dB

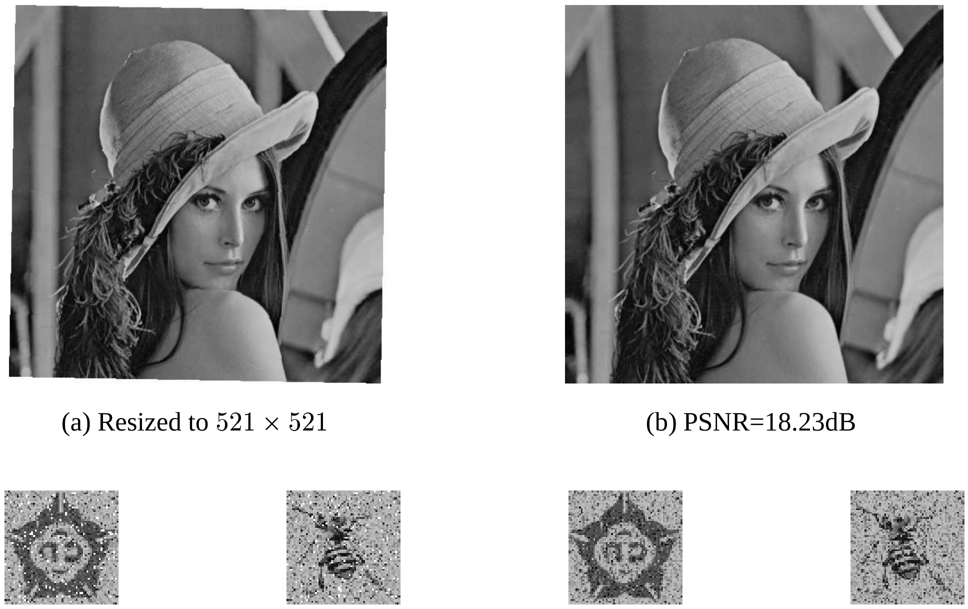
(c) PSNR=13.32dB

(d) PSNR=10.94dB

(e) PSNR=13.42dB

(f) PSNR=11.03dB

Figure 2: (a)Altered image from “Lena” using a Blurring algorithm, (b)Reconstructed JPEG image, (c, d)Computed watermark from Figure 2(a), (e, f)Computed watermark from Figure 2(b)



(a) Resized to 521×521

(b) PSNR=18.23dB

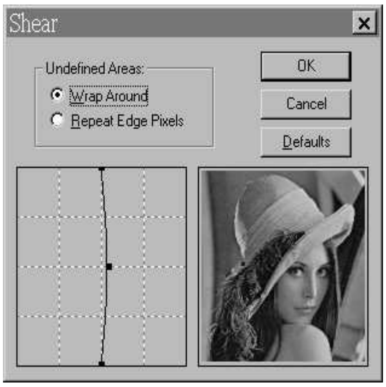
(c) PSNR=11.27dB

(d) PSNR=9.52dB

(e) PSNR=11.26dB

(f) PSNR=9.29dB

Figure 3: (a)Rotated 1 degree image from “Lena”, (b)Altered image by Shear algorithm, (c, d)Computed watermark from Figure 2(a), (e, f)Computed watermark from Figure 2(b)



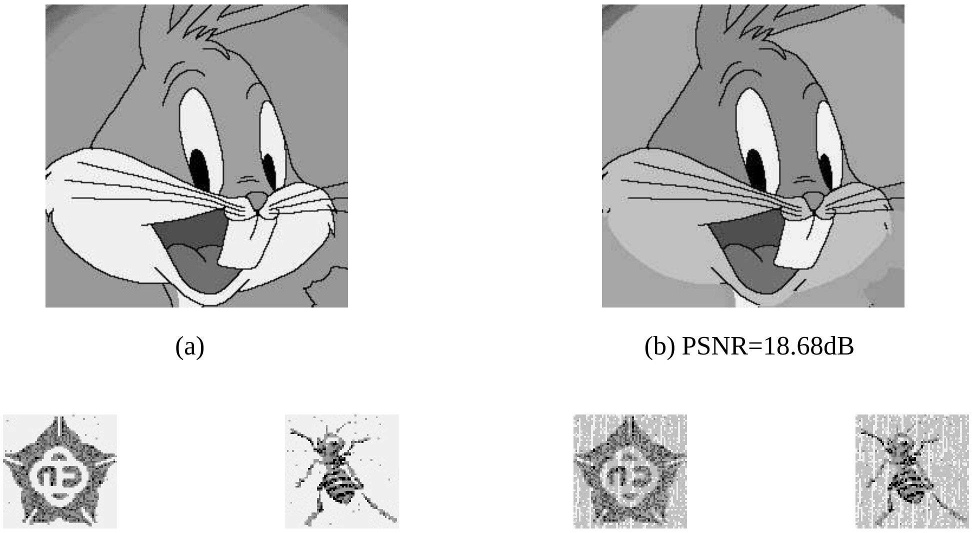
Shear

Undefined Areas:

● Wrap Around

○ Repeat Edge Pixels

Figure 4: The parameter of the Shear algorithm



(a)

(b) PSNR=18.68dB

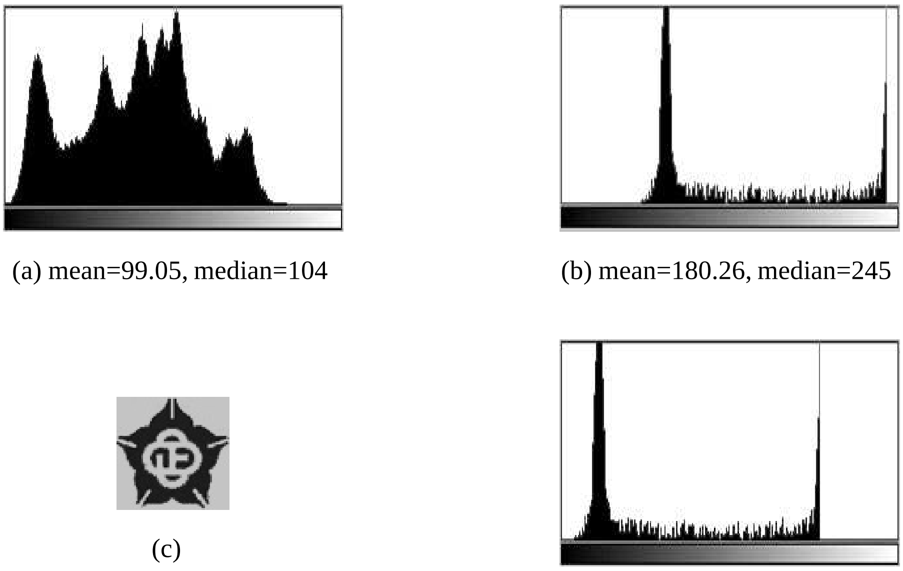
(c) PSNR=18.18dB

(d) PSNR=20.04dB

(e) PSNR=14.28dB

(f) PSNR=13.73dB

Figure 5: (a)Original image of “Bunny”(256×256), (b)Image of repainted “Bunny”, (c, d)Computed watermark from Figure 5(a), (e, f)Computed watermark from Figure 5(b)



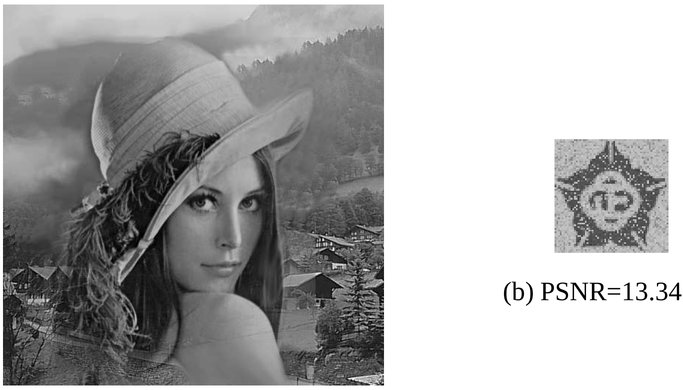
(a) mean=99.05, median=104

(b) mean=180.26, median=245

(c)

(d) mean=129.26, median=194

Figure 6: (a)Histogram of “Lena” (Figure 1(a)), (b)histogram of original watermark(Figure 1(b)), (c)adjusted watermark, (d)histogram of adjusted watermark



(b) PSNR=13.34dB

(a) PSNR=14.43dB

Figure 7: (a)“Lena” cropped and pasted to another picture, (b)Computed watermark from Figure 7(a)