EURASIP Journal on Applied Signal Processing 2004:13, 1965–1972

A New Repeating Color Watermarking Scheme Based on Human Visual Model

Chwei-Shyong Tsai

Department of Management Information System, National Chung Hsing University, Taichung 402, Taiwan
Email: tsaics@nchu.edu.tw

Chin-Chen Chang

Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 621, Taiwan
Email: ccc@cs.ccu.edu.tw

Received 26 November 2001; Revised 6 March 2004; Recommended for Publication by Yung-Chang Chen

This paper proposes a human-visual-model-based scheme that effectively protects the intellectual copyright of digital images. In the proposed method, the theory of the visual secret sharing scheme is used to create a master watermark share and a secret watermark share. The watermark share is kept secret by the owner. The master watermark share is embedded into the host image to generate a watermarked image based on the human visual model. The proposed method conforms to all necessary conditions of an image watermarking technique. After the watermarked image is put under various attacks such as lossy compression, rotating, sharpening, blurring, and cropping, the experimental results show that the extracted digital watermark from the attacked watermarked images can still be robustly detected using the proposed method.

Keywords and phrases: secret sharing, digital watermark, human visual model.

1. INTRODUCTION

With the improvement of telecommunications, more and more people process, transmit, and store digital media via Internet. However, problems such as illegal use, tampering, and forgery occur that not only violate copyright laws but also do harm to the monetary profits of the copyright owners. Therefore, the protection of the intellectual property for digital media has become an important issue. Recently, digital watermarking has successfully provided the methods to guard the intellectual property rights of digital media, and some excellent research results have been published [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18].

To effectively protect the copyright of the digital images, a successful digital watermarking technique must possess the following four characteristics [17, 18].

(1) Watermarking must not reveal any hint of the digital watermark; that is, the watermarked image must not visually differ from the host image. This achieves the goal of invisible embedding.

(2) The host image is unnecessary when verifying the copyright process that detects the watermark from watermarked image. This eliminates the complexity of the process and saves extra space for host image storage.

(3) Even if the embedding and verifying processes are known, unauthorized users still cannot remove and detect the digital watermark from the watermarked image, and this achieves the goal of secure embedding.

(4) When purposely enhancing the quality of the watermarked image or when damage occurs so that the watermarked image may be processed by some kind of operation such as lossy JPEG compression, blurring, sharpening, rotating, and cropping, the copyright verification procedure can still distinguish the identifiable digital watermark from the modified watermarked image, and this achieves the goal of robust embedding.

In this paper, the proposed watermarking technique uses color digital watermarking to provide a better visual effect. It combines the theory of visual cryptography and the technology of the human visual model to embed/extract watermarks. The main feature of visual cryptography is transforming secret message into transparencies (called shares) and sending the shares to message receivers. When recovering the secret message by stacking all transparencies, the receiver can obtain it without requiring any calculations. In addition, visual cryptography has proven to be perfectly secure. The proposed technique uses visual cryptography to produce a matching master watermark share and a shadow watermark share. The master watermark share is created according to the digital host image; on the other hand, the shadow watermark share is created based on the master watermark share and its related digital watermark. The master watermark share is open to the public, while the shadow watermark share is kept secret by the copyright owner. Human visual model technology is used to determine the number of bits that can be modified without decreasing the quality of the image. Thus the watermarked image created using the watermark embedding process to embed the digital watermark into the host image has such good quality that human vision cannot determine that message is contained inside. When identifying ownership, the watermark identification process can recover the embedded watermark by calculating the shadow watermark share given by the owner and the master watermark share derived from the watermarked image to ensure the legality of ownership.

In this paper, the proposed technique can create the matching shadow watermark share of each watermark according to different digital watermarks. Therefore, it is a multiple watermarking technique. The human visual model can be used to achieve the goal of invisible watermarking. Furthermore, the embedded watermark cannot be derived from the analysis using statistical methods and it is difficult to remove because of the perfect securely feature of visual cryptography.

2. HUMAN VISUAL MODEL

In 1996, a human visual model for differential pulse code modulation (DPCM) was proposed by Kuo and Chen [19]. They took Weber's law [20] into consideration in their model. Later, they applied another scheme based on the model of vector quantization (VQ) image compression [21]. The purpose of the human visual model is to evaluate the sensitivity of the human eyes to a luminance against a background. To achieve this goal, a technique called contrast function in the gray-valued spatial domain (from 0 to 255) is used.

The two researchers constructed the contrast function $C(x)$ from the combination of a bright background and a dark one. Thus, there are two definitions of $C(x)$ according to the background B. Here B is the mean of the gray values in the background. For the bright background ($B \geq 128$), $C(x)$ is defined as follows:

$$C(x) = \begin{cases} \ln\left(\dfrac{c_1 \times (c_L - x)}{c_L \times (127.5 - (x - c_1))}\right), & 0 \leq x < 128, \\[2ex] \ln\left(\dfrac{(x - c_1) \times (x - c_H)}{c_1 \times (255 - c_H)}\right), & 128 \leq x \leq 255, \end{cases} \tag{1}$$

where c_1 is a constant and is equal to 127.5/2, $c_L = 128/(1-e^{-k})$, and $c_H = (128-255e^{-k})/(1-e^{-k})$. Here k is defined by $k = 2.5/(1 + e^{(255-B)/55})$.

The other definition of $C(x)$ for the dark background ($B < 128$) is

$$C(x) = \begin{cases} \ln\left(\dfrac{c_1 \times c_L}{127.5-(x-c_1) \times (c_L-x)}\right), & 0 \leq x < 128, \\[2ex] \ln\left(\dfrac{(x-c_1) \times (255-c_H)}{c_1 \times (x-c_H)}\right), & 128 \leq x \leq 255, \end{cases} \tag{2}$$

where c_1 is again a constant and is equal to 127.5/2, $c_L = -128e^k/(1 - e^k)$, and $c_H = (255 - 128e^k)/(1 - e^k)$. Here k is defined by $k = 2.5/(1 + e^{B/25})$.

In our proposed method, the contrast function is used to assess the sensitivity of an image block. The sensitivity of each pixel x in a block is measured via (1) or (2) based on the mean of the block (background). The evaluated sensitivity points out the number of bits of pixel x would be changed. It will be difficult for the ordinary human eye to notice the change.

3. THE PROPOSED WATERMARKING SCHEME

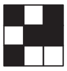
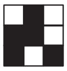
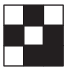
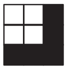
For a specific digital image in need of protection, the cooperative manufacturer and individuals (called participants) owning the image copyright embed their digital color watermarks into it. When using the proposed method to embed these digital watermarks, a permutation with pseudorandom number generator (PRNG) and a master watermark is first created. Then each matching shadow watermark share is created based on the corresponding digital watermark. The shadow watermark share is derived by combining the master watermark share and the information from its matching digital color watermark. Finally, the shadow watermark share is given to the related participant and kept privately for use in the future when declaring the legal copyright ownership. When one of the participants needs to identify the copyright, an unbiased third party will stack the master watermark share derived from the digital image as well as the permuted shadow watermark share from the possible copyright owner together and calculate both of them to recover the digital watermark possessing the copyright information. The proposed scheme can effectively identify the watermark to protect the intellectual property rights of the image.

3.1. *Watermark embedding process*

For the digital host image H needing protection and the digital watermark representing its copyright information W, H is a gray-value image and W is a color image. In the proposed method, the colors in W include white, red, green, and blue. We define H and W separately as follows:

$$\begin{aligned} H &= \{HP_{ij} \mid 0 \leq HP_{ij} \leq 255,\ 0 \leq i \leq N_1,\ 0 \leq j \leq N_2\}, \\ W &= \{WP_{uv} \mid WP_{uv} \in \{(255,0,0),(0,255,0), \\ &\qquad (0,0,255),(255,255,255)\}, \\ &\qquad 0 \leq u \leq M_1,\ 0 \leq v \leq M_2\}. \end{aligned} \tag{3}$$

TABLE 1: The generation rule of pattern P_{ij}.

The interval of $\bar{x}_{ij}$	P_{ij}
$[0, 63]$	
$[64, 127]$	
$[128, 191]$	
$[192, 255]$	

Generally, the size of the watermark image is smaller than that of the host image. Thus let $M_1 < N_1$ and $M_2 < N_2$.

The proposed watermark embedding process mainly includes the master watermark share production procedure, the shadow watermark share production procedure, and the human-visual-based embedding procedure. The master watermark share production procedure generates master watermark share MS according to H, and the shadow watermark share production procedure combines MS and W to generate shadow watermark share SS. Note that in order to increase the security, a secret key SK is used to be the seed of PRNG and PRNG(SK) is applied to permute all pixels of W. And the inverse permutation is applied during the watermark verification process to reveal the original secret. Finally, the human-visual-based embedding procedure is used to generate watermarked image H'. We illustrate these three procedures in detail in the following subsections.

3.1.1. Master shadow share production

Because watermark image W is smaller than host image H, the proposed method divides H into many subimages of the same size H_i's, and lets every subimage H_i correspond to W. Here, let every H_i contain $n \times n$ pixels and $H = \{H_1, H_2, \dots, H_{\lfloor N_1/n \rfloor \times \lfloor N_2/n \rfloor}\}$. When mapping each subimage H_i to W, first H_i is divided into blocks HB_{ij}'s such that each HB_{ij} contains $q_1 \times q_2$ pixels, where $j = 1, 2, \dots, n \times n / q_1 \times q_2$, $q_1 = n/M_1$, and $q_2 = n/M_2$. Next, calculate the mean $\overline{X}_{ij}$ of each HB_{ij}, $0 \leq \overline{X}_{ij} \leq 255$. Then use the $\overline{X}_{ij}$ of each HB_{ij} to create a pattern P_{ij} according to a certain rule. Table 1 shows the rules of how to create P_{ij}. Every P_{ij} is 3×3 in size and contains 5 black pixels and 4 white pixels. We divide the range $[0, 255]$ in which all the possible values of $\overline{X}_{ij}$ may appear in 4 intervals, and define a specific P_{ij} for each interval. For example, if $\overline{X}_{ij} = 159$, the pattern to which HB_{ij} corresponds is defined by the interval $[128, 191]$.

After applying these rules to find the corresponding patterns for all blocks HB_{ij}'s in every H_i, the proposed method will combine all the patterns derived from H_i's to make up the master watermark share MS of H.

TABLE 2: An example of CT.

Color	No.
White	4
Red	3
Green	2
Blue	1

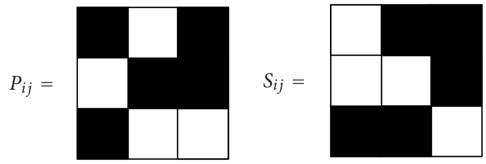


FIGURE 1: An example of P_{ij} and S_{ij}.

3.1.2. Producing shadow watermark share procedure

The size of shadow watermark share SS is the same as that of MS. Every P_{ij} in MS corresponds to a 3×3 pattern in SS defined as S_{ij}. P_{ij} and the pixel WP_{ij} in W collectively determine the generation method of S_{ij}. First, define a color referral table (CT) according to all of the color in W. In CT, every color in W is assigned a unique number. In the proposed method, the colors in W include white, red, green, and blue. Therefore, CT has 4 entries. Table 2 shows an example of CT.

We define CT(WP_{ij}) as the color number of the pixel WP_{ij} in CT. On the other hand, S_{ij} is a 3×3 black/white pattern built by making the number of black pixels appearing when S_{ij} and P_{ij} are both in the same position equal to CT(WP_{ij}). For example, if WP_{ij} is a red pixel, and P_{ij} is as shown in Figure 1 then CT(WP_{ij}) $= 3$. Thus the number of black pixels appearing when S_{ij} and P_{ij} are in the same position is 3. Therefore, S_{ij} can be constructed as in Figure 1.

The following equation defines the creation of S_{ij}:

$$\sum_{p=1,q=1}^{p=3,q=3} S_{ij}(p,q) P_{ij}(p,q) = \text{CT}\left(WP_{ij}\right), \tag{4}$$

where

(1) $S_{ij}(p,q) = 1$ if the pixel that S_{ij} locates at pth row and qth column is black;

(2) $S_{ij}(p,q) = 0$ if the pixel that S_{ij} locates at pth row and qth column is white;

(3) $P_{ij}(p,q) = 1$ if the pixel that P_{ij} locates at pth row and qth column is black;

(4) $P_{ij}(p,q) = 0$ if the pixel that P_{ij} locates at pth row and qth column is white.

Many cases of S_{ij} can conform to the above equation, and any of them can be used arbitrarily. After all WP_{ij}'s and P_{ij}'s determine S_{ij}'s, the shadow watermark share SS is created.

Table 3: The thresholds of the 16 different contrast intervals.

Contrast intervals	Thresholds
$[-1, -0.975)$	16
$[-0.975, -0.85)$	13
$[-0.85, -0.625)$	10
$[-0.625, -0.5)$	8
$[-0.5, -0.375)$	6
$[-0.375, -0.25)$	5
$[-0.25, -0.125)$	4
$[-0.125, 0)$	3
$[0, 0.125)$	3
$[0.125, 0.25)$	4
$[0.25, 0.375)$	5
$[0.375, 0.5)$	6
$[0.5, 0.625)$	8
$[0.625, 0.75)$	8
$[0.75, 0.875)$	10
$[0.875, 1]$	10

3.1.3. Human visual model-based embedding

To enhance the robustness of this method, we adopt the theory of the human visual model to carry out the processing of watermark embedding. Due to the strong correlation between the creation of the master watermark share and the black means in the host image, the value of each pixel in HB_{ij} is mainly adjusted during the embedding process. The value that is closer to the mean $\overline{X}_{ij}$ is more desirable assuming that the image quality will not be affected. To measure the maximum change of each pixel without damaging the image quality, the contrast function $C(x)$ in Section 2 provides the best support. First, according to the viewpoint and experiment of the human visual model, we divide the range of $C(x)$ into 16 intervals and assign a specific threshold to each interval. When the value of the pixel is V, the contrast value of the pixel is $C(V)$, and the corresponding threshold of $C(V)$ is y, The adjusted pixel values V' and V should conform to the following inequality equation:

$$|V' - V| \le y. \tag{5}$$

Table 3 shows the thresholds for the 16 different contract intervals. Next, for each pixel V_{st} in HB_{ij}, calculate its contrast value $C(V_{st})$. Look up the value from Table 3 to obtain the corresponding threshold T for the contrast interval of $C(V_{st})$. Complete the process of adjusting V_{st} to V'_{st} based on the following equation:

$$V'_{st} = \begin{cases} \overline{X}_{ij} & \text{if } |\overline{X}_{ij} - V_{st}| \le T; \\ V_{st} - T & \text{if } |\overline{X}_{ij} - V_{st}| > T, V_{st} \ge \overline{X}_{ij}; \\ V_{st} + T & \text{if } |\overline{X}_{ij} - V_{st}| > T, V_{st} < \overline{X}_{ij}. \end{cases} \tag{6}$$

Once each pixel within all HB_{ij}'s has been adjusted, the watermarked image H' is available.

For example, it is assumed that HB_{ij}, a block in some subimage, is defined as

$$HB_{ij} = \begin{bmatrix} 170 & 161 & 161 & 160 \\ 161 & 161 & 160 & 161 \\ 161 & 162 & 161 & 161 \\ 162 & 161 & 161 & 152 \end{bmatrix}. \tag{7}$$

Therefore, from the formulas in human vision model, the background $B = \overline{X}_{ij} = 161$ from (1). Supposing the original pixel value $V_{st} = 170$ and $k = 0.3832$, $c_H = 143.96$ and $C(V_{st}) = -0.939$. Then $y = T(C(V_{st})) = T(-0.939) = 13$. Finally, from (6), $V'_{st} = \overline{X}_{ij} = 161$ and $T = 13$. We have $|\overline{X}_{ij} - V_{st}| = 9 < T$. Thus, the block is now

$$HB_{ij} = \begin{bmatrix} 161 & 161 & 161 & 160 \\ 161 & 161 & 160 & 161 \\ 161 & 162 & 161 & 161 \\ 162 & 161 & 161 & 152 \end{bmatrix}. \tag{8}$$

Next, the copyright owner must register the shadow watermark share *SS* with the certification authority in order to prevent copyright forgery. In our proposed scheme, the certification authority uses a public-key cryptosystem such as RSA, signs the time-stamp registration in *SS* with his own private key, and generates time-stamped shadow watermark share SS^T. After receiving SS^T, the owner will keep it a secret. Then, the watermarked image can be distributed to the public. As for the forged copyright, it can be easily identified since the time stamp of the fake time-stamped shadow watermark share is dated after that of SS^T belonging to the owner.

3.2. Watermark verification

After obtaining the secret key *SK* from the person declaring the copyright ownership and the time-stamped shadow watermark share SS^T, the arbitrator can carry on the process of watermark verification. First, use *SK* and H' and execute the procedure for watermark share production to obtain the master watermark share *MS*. Then, stack *MS* and *SS*. For each 3×3 pattern P_{ij} in *MS* and the corresponding 3×3 pattern S_{ij} in *SS*, recover the watermark pixel WP_{ij} according to (4) and the inverse permutation of the PRNG process. After all P_{ij}'s and S_{ij}'s are processed, the restored color watermark W' is available. The arbitrator compares W' and the digital watermark W registered by the person declaring the copyright ownership.

If the suspected image belonged to the legal copyright owner, the revealed image W' stacked by *MS* and SS^T should be the target watermark W in optimal. But the incoming tested image may be damaged by malicious or unavoidable distortions and there may be errors on the result image. Thus if W is related to W', the declarer is a legal copyright owner; otherwise, the declarer is a copyright violator.

Figure 2: Original image of Lena (512 × 512).

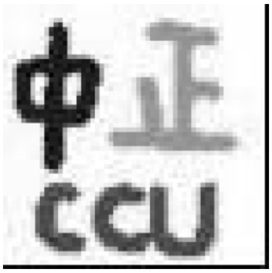


Figure 3: Watermark of National Chung Cheng University (64 × 64).

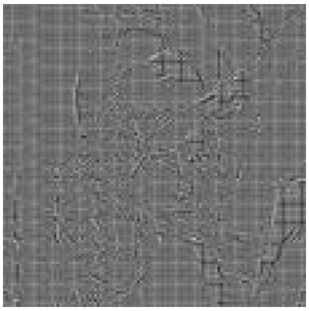


Figure 4: Master watermark share (384 × 384, without PRNG process).

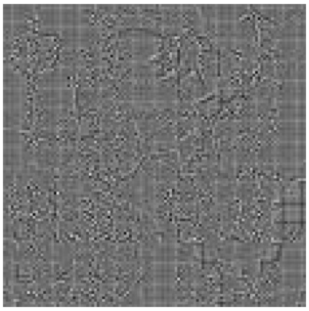


Figure 5: Shadow watermark share (384×384, without PRNG process).

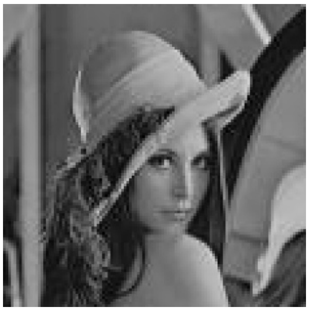


Figure 6: Watermarked image of Lena (512 × 512); PSNR = 33.45 dB.

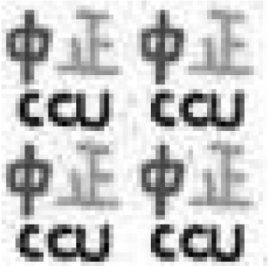


Figure 7: Recovered repeating watermark (128 × 128).

4. EXPERIMENTAL RESULTS

As shown in Figure 2 in our experiments, the image size of a given gray-valued host image Lena was 512 × 512 pixels. In Figure 3, a 64 × 64 color digital copyright image must be cast into the host image. First, in our method, Lena is permuted by the secret key and then partitioned into 2 × 2 blocks, where each block contains 256 × 256 pixels. We divide each 4 × 4 subblock into groups according to sequence after calculating the mean value of each subblock. The next steps to generate a master watermark share are composed of patterns of 3 × 3 pixels. According to the mean value of each subblock and Table 1, each pattern of the master watermark share can then be constructed. A generated 384 × 384 master watermark share is shown in Figure 4.

Next, our shadow watermark share production procedure is utilized to combine the generated master watermark share and digital watermark image; then the shadow watermark share is generated (as shown in Figure 5). Finally, the watermarked image with PSNR = 33.45 dB, shown in Figure 6, can be generated by applying the human visual model.

The authorized owner keeps the shadow watermark share secret. When identification is required, the arbitrator obtains the secret key from the person claiming the authorized ownership and uses our master watermark share production procedure to retrieve a master watermark share of Lena. After stacking the shadow watermark share with the master watermark share and performing the proposed copyright verification procedure, the arbitrator will recover the digital watermark, as shown in Figure 7.

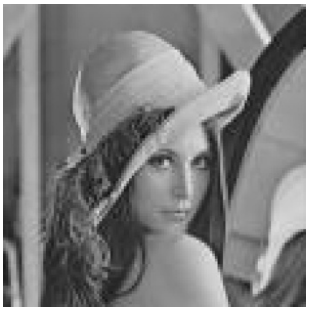


Figure 8: Reconstruction of JPEG compression of Lena.

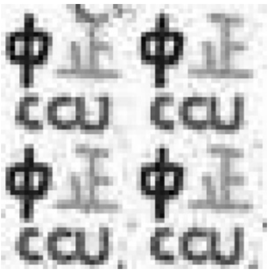


Figure 9: Recovered watermark from Figure 8.

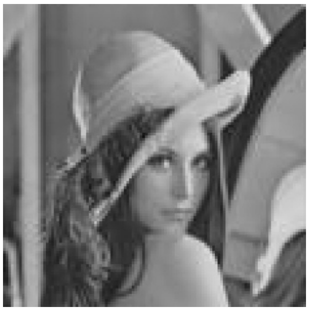


Figure 10: Blurred image of Lena.

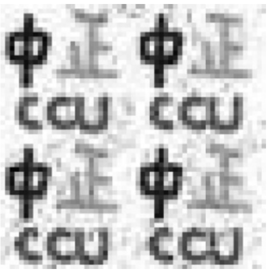


Figure 11: Recovered watermark from Figure 10.

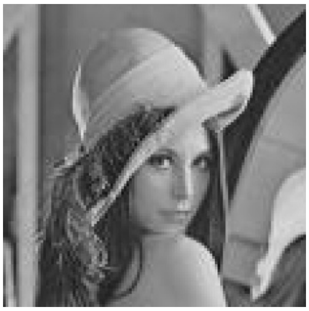


Figure 12: Rotated image of Lena.

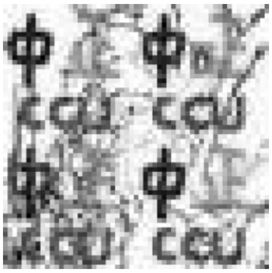


Figure 13: Recovered watermark from Figure 12.

In our method, the master watermark share is not available to illegal users without the secret key. Furthermore, because the shadow watermark share must be generated by both the master watermark share and the digital watermark, an illegal user cannot obtain the ownership's shadow watermark share. The security of our proposed scheme relies on the secret key that is used in master watermark production share. Thus, different host images use different secret keys to create different master watermark shares of host images; and different images, if they have the same digital watermark, will still have different corresponding shadow watermark shares. Therefore, it is very difficult for an attacker to retrieve the copyright information using statistical methods and to fake ownership.

In order to prove the robustness of the copyright protection technique proposed in our method, we simulate various kinds of attacks on watermarked image Lena in our experiments. Figures 8, 10, 12, 14, and 16 show the results of JPEG lossy compression attacks with a compression factor of 80, blurring, rotating, cropping, and sharpening attacks, respectively. The digital watermarks under various kinds of attacks can still be clearly recovered. The results of the recovered repeating watermarks are shown in Figures 9, 11, 13, 15, and 17, respectively.

In Table 4, the second row lists the retrieval rate of a master watermark share, which stands for the ratio of the number of accurate pixels to all of the pixels of the master watermark share in copyright retrieval. The experimental results show that the retrieval rate of our method is above 80%, which means that the ownership can be retrieved robustly.

An excellent feature of our copyright protection technique is that only the host image is required when the digital watermark is retrieved. In addition, multiple watermarks can be independently cast into an image by using the proposed technique.

TABLE 4: The bit correct rates of extracted color watermarks of different images under various attacks.

Images	Attacks				
	JPEG compression (quality 90%)	Blurring (2-radius pixel)	Rotating (degree 1)	Cropping (cut up left quarter)	Sharpening
Lena	98.92%	92.86%	88.57%	80.17%	97.53%
F14	98.38%	93.25%	87.85%	84.55%	96.77%
Barbara	98.69%	92.10%	82.81%	81.92%	97.62%

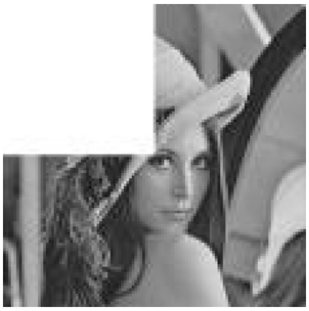


FIGURE 14: Cropped image of Lena.

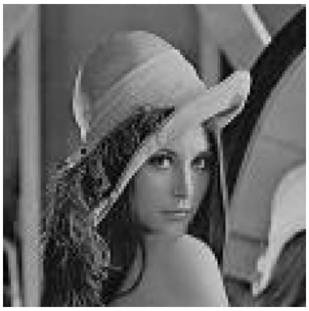


FIGURE 16: Sharpened image of Lena.

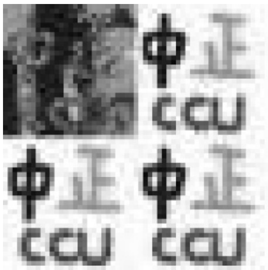


FIGURE 15: Recovered watermark from Figure 14.

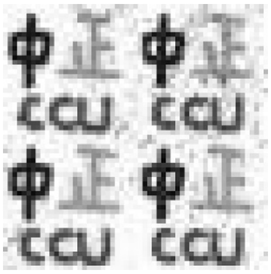


FIGURE 17: Recovered watermark from Figure 16.

5. CONCLUSIONS

Combining the theory of the visual secret sharing scheme and the viewpoint of the human visual model, this paper proposes a new watermarking scheme to embedding the digital color watermark into a digital grey-level host image. The proposed method applies the theory of the visual secret sharing scheme along with its security feature to produce the master watermark share and the shadow watermark share for color watermarks. The shadow watermark share is kept secret by the copyright owner. On the other hand, the human visual model can be used to detect the sensitivity of each pixel in the host image so that the master watermark share is effectively embedded into the host image without reducing the image quality. Our method not only can effectively embed and detect the watermark but it also can prevent the forgery of ownership. Furthermore, the qualities of security, invisibility, robustness, and multiple embedding are provided in the embedded watermark.

ACKNOWLEDGMENTS

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by National Science Council, Taiwan, under contract no. NSC92-2213-E-025-004.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, no. 3/4, pp. 313–336, 1996.

[2] A. G. Bors and I. Pitas, "Image watermarking using DCT domain constraints," in *Proc. IEEE International Conference on Image Processing (ICIP '96)*, vol. 3, pp. 231–234, Lausanne, Switzerland, September 1996.

[3] C.-C. Chang and C. S. Tsai, "A technique for computing watermarks from digital images," *Informatica*, vol. 24, no. 3, pp. 391–396, 2000.

[4] C.-C. Chang and K.-F. Hwang, "A digital watermarking scheme using human visual effects," *Informatica*, vol. 24, no. 4, pp. 505–511, 2000.

[5] C.-C. Chang and H. C. Wu, "A copyright protection scheme of images based on visual cryptography," to appear in *The Imaging Science Journal*.

[6] T. S. Chen, C.-C. Chang, and M. S. Hwang, "A virtual image cryptosystem based upon vector quantization," *IEEE Trans. Image Processing*, vol. 7, no. 10, pp. 1485–1488, 1998.

[7] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[8] I. J. Cox and J. P. M. G. Linnartz, "Some general methods for tampering with watermarks," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 587–593, 1998.

[9] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 573–586, 1998.

[10] M. S. Hwang, C.-C. Chang, and K.-F. Hwang, "A watermarking technique based on one-way hash functions," *IEEE Transactions on Consumer Electronics*, vol. 45, no. 2, pp. 286–294, 1999.

[11] C. T. Hsu and J. L. Wu, "Hidden digital watermarks in images," *IEEE Trans. Image Processing*, vol. 8, no. 1, pp. 58–68, 1999.

[12] M. Kutter, F. Jordan, and F. Bossen, "Digital watermarking of color images using amplitude modulation," *Journal of Electronic Imaging*, vol. 7, no. 2, pp. 326–332, 1998.

[13] S. Low and N. Maxemchuk, "Performance comparison of two text marking methods," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 561–572, 1998.

[14] N. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology (Eurocrypt '94)*, A. De Santis, Ed., vol. 950 of *Lecture Notes in Computer Science*, pp. 1–12, Springer-Verlag, Berlin, 1995.

[15] R. Ohbuchi, H. Masuda, and M. Aono, "Watermarking three-dimensional polygonal models through geometric and topological modifications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 551–560, 1998.

[16] G. Voyatzis and I. Pitas, "Protecting digital image copyrights: a framework," *IEEE Computer Graphics and Applications*, vol. 19, no. 1, pp. 18–24, 1999.

[17] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proceedings of the IEEE*, vol. 86, no. 6, pp. 1064–1087, 1998.

[18] R. B. Wolfgang and E. J. Delp, "A watermark for digital image," in *Proc. IEEE International Conference on Image Processing (ICIP '96)*, vol. 3, pp. 219–222, Lausanne, Switzerland, September 1996.

[19] C. H. Kuo and C. F. Chen, "A prequantizer with the human visual effect for the DPCM," *Signal Processing: Image Communication*, vol. 8, no. 5, pp. 433–442, 1996.

[20] T. G. Stockham Jr., "Image processing in the context of a visual model," *Proceedings of the IEEE*, vol. 60, no. 7, pp. 828–842, 1972.

[21] C. H. Kuo and C. F. Chen, "A vector quantization scheme using prequantizers of human visual effects," *Signal Processing: Image Communication*, vol. 12, no. 1, pp. 13–21, 1998.

Chwei-Shyong Tsai was born in Changhua, Taiwan, on September 3, 1962. He received the B.S. degree in applied mathematics in 1984 from National Chung Hsing University, Taichung, Taiwan. He received the M.S. degree in computer science and electronic engineering in 1986 from National Center University, Chungli, Taiwan. He received the Ph.D. degree in computer science and information engineering in 2002 from National Chung Cheng University, Chiayi, Taiwan. From August 2002, he was an Associate Professor in the Department of Information Management at National Taichung Institute of Technology, Taichung, Taiwan. Since August 2004, he has been an Associate Professor in the Department of Management Information System at National Chung Hsing University, Taichung, Taiwan. His research interests include image authentication, information hiding, and cryptography.

Chin-Chen Chang was born in Taichung, Taiwan, on November 12, 1954. He received his B.S. degree in applied mathematics in 1977 and his M.S. degree in computer and decision sciences in 1979 from National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D. in computer engineering in 1982 from National Chiao Tung University, Hsinchu, Taiwan. From 1983 to 1989, he was among the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. Since August 1989, he has worked as a Professor in the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. Dr. Chang is a Fellow of IEEE and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, and the Phi Tau Phi Society of the Republic of China. His research interests include computer cryptography, data engineering, and image compression.