A Certificate-based Watermarking Scheme for Colored Images *

Nan-I Wu† Chung-Ming Wang† Chwei-Shyong Tsai‡ Min-Shiang Hwang‡

Institute of Computer Science †
National Chung Hsing University
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.
rocjfk2000@yahoo.com.tw
Department of Management Information Systems ‡
National Chung Hsing University
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.
Email:mshwang@nchu.edu.tw
Tel:886-4-22855401

February 19, 2008

*

‡Responsible for correspondence: Prof. Min-Shiang Hwang

A Certificate-based Watermarking Scheme for Colored Images

Abstract

In recent years, much of the research energy within the field of digital watermarking has been focused on techniques that depend on a third party, called the Image Certification Authority (ICA), to enhance the digital image copyright protection. However, in order to record the embedding locations of the watermark bits, in the design of most of these schemes, a secret key has to be generated after embedding one watermark into the cover image. As a result, there wind up to be quite some bunches of secret keys for the user to keep if large numbers of watermarked images are involved, which of course means a lot of inconvenience. In this paper, we propose a novel watermarking method to solve this problem. Also depending on the ICA for copyright protection, our new method makes a difference by providing the user with the power to process masses of digital image watermarking tasks by using just one PRivate-key (PRK). The results of our extensive experiments have proven both the capability of the proposed technique as an efficient management mechanism and the robustness of it against various image processing attacks such as JPEG compression, low-pass filtering and high-pass filtering as well as noise contamination.

Keywords: Copyright protection, watermarking, private-key, robustness

1 Introduction

Due to the incredibly rapid advancement of digital communication networks such as the Internet, wireless telecommunication systems, and global mobility networks, people nowadays get to obtain easy accesses to digital images of all kinds, and powerful software is as a result more often used to tamper or copy the contents of the digital images legally or illegally. Under such circumstances, how to make sure that the ownership of digital images is under proper protection has become an important topic of research. So far, there have been two major streams of technologies widely studied that deal with problems of digital image ownership protection-the cryptosystem and digital watermarking. With the cryptosystem, the integrity of digital images can be absolutely confirmed, and the ownership of images can be verified when the contents of the digital images have not been modified. However, in common everyday applications, it is only reasonable to allow slight image processing because that is what actually happens in real-life situations. In other words, the cryptosystem does not seem to be a very common option. Digital watermarking, on the other hand, is a data hiding technique that primarily deals with the embedding of meaningful patterns such as trademarks, seals, or logos into digital images. It can efficiently help verify the ownership of an image when the image content has been slightly altered. The major challenge a watermarking scheme has to face is the establishment of the robustness against various image processing attacks.

Generally speaking, watermarking techniques can be classified into two categories: spatial domain techniques and frequency/transform domain techniques. Spatial domain methods directly modify the pixel values in the contents of the digital images. Quite a few well-accepted watermarking methods belong to this type. For example, Lin [13] proposed a robust transparent watermarking system that can resist various image attacks by hiding watermark bits in the edge areas. Besides, Liu and Chen [14] presented a two-layer watermarking scheme that can resist both high and low frequency destruction. In addition, in [16], there is a spatial watermarking technique focused on buyer authentication. Also, Wong et al. [20] presented a secret and public key image watermarking scheme that uses a hash function to embed the watermark in the least significant bit of each pixel. To add up, Pei and Guo [17] proposed a high-capacity watermarking technique based on minimal-error bit searching and least-mean square filtering for halftone images. On the other hand, frequency/transform domain techniques embed the watermark bits into digital images by modifying the coefficients generated after transformation processes such as discrete fourier transform (DFT), discrete cosine transform (DCT) and discrete wavelet transform (DWT). In general, compared with spatial domain methods, frequency domain techniques are capable of offering higher level robustness. However, this security advantage has to be earned at a cost: a larger storage space demand. In the literature concerned, many brilliant frequency domain watermarking methods can be found. For example, Cox et al. [6] presented a watermarking scheme based on spread spectrum that inserts the watermark bits into the DCT coefficients. A similar scheme based on the concept of subsampling was proposed by Chu [5] to recover watermarks without the original images. However, Cox et al.'s and Chu's schemes are, according to Das et al. [7, 8], insecure under the single watermarked copy attack. To improve the robustness of Cox's scheme, Lu et al. [15] proposed a cocktail watermark to fix this flaw. In their scheme, the human visual system (HVS) is used to obtain better image quality after watermark embedding. Wong et al. [19] presented three blind multiple watermarking techniques for different purposes that embed watermark bits in the DCT coefficients. In addition, based on mean quantization watermarking, the method proposed by [3] functions by altering the DWT coefficients. In deal with high resolution pictures such as medical images, Giakoumaki et al. [9] utilize their watermarking technqiue to embed four types of watermarks into the wavelet coefficients. Besides these two types of watermarking methods, there are also mixed methods that embed watermarks in both the spatial domain and the transform domain at the same time [10, 18].

In order to lift up the efficiency of the verification procedure and to offer stronger protection to the copyright of images, watermarking systems based on the cryptosystem have been proposed [1, 2, 4, 11, 12]. Lee and Chen [12] proposed a publicly verifiable copyright protection technique where everyone can verify the existence of the watermark by using a public-key but cannot remove the watermark without using the private-key even if he/she has the public-key. Nevertheless, with their scheme, one secret key must be stored in one digital image after the embedding of the watermark because this secret key, which has a great length, records all the embedding locations. In fact, the length of the secret key depends on the size of the watermark logo. This way, when there are many watermarked images to keep, there will be a large number of secret keys to store and protect. Such a task is of course a heavy burden on the image owners. The same problem occurs in [11], where three secret keys must be kept by the image owner after one watermark gets embedded into one digital image.

In this paper, we shall propose an efficient watermarking technique to hide binary watermarks into color images. In the design of our new scheme, an Image Certification Authority (ICA) is a necessary part responsible for the enhancement of the verification efficiency and for the reduction of the heavy load of secret keys. With the help of the ICA, the proposed method requires the image owner to keep only one PRK even if there are a huge number of digital image watermarking tasks to do. In our scheme, the spatial domain of channels R, G and B is where the watermark is directly hidden, and one watermark bit is embedded into the same location on the three channels. To improve the survivability of the watermark and the quality of the watermarked image, the robustness coefficients of channels R, G and B are distinct in our scheme. Besides that, a majority mechanism is used to decide which one the real watermark bit is after extracting the hidden bits from channels R, G and B. That is to say, the proposed scheme can identify the damaged channel and thus can probably help repair it if only one channel has been destroyed. Besides that, the idea of hiding watermarks in color images comes with another advantage–to allow multi-watermark embedding. For example, suppose there are three watermarks, namely the name of the image owner, the registered serial number, and the registration date, to be embedded into a digital image. In this case, with our new scheme, we can readily embed the name into channel G, embed the registered serial number into channel R, and embed the registration date into channel B.

The remainder of this paper is organized as follows. In the next Section, we shall present the proposed watermarking algorithm. Then, in Section 3, we shall offer our experimental results to demonstrate the robustness of the new scheme. Finally, a brief conclusion will be given in Section 4.

2 The proposed method

In our scheme, for each image to hold a watermark (or watermarks), an application has to be made at the Image Certification Authority (ICA) to get a Certificate (CT) before the user can proceed with the watermark embedding procedure. In general, the content of CT included the name of applicant, application date, the serial number of CT, and the annotation section. In order to enhance the security of the embedding location of watermark bit and protect the original watermark bits. The bits must be encrypted by image owner's PRivate Key (PRK) and the encrypted data is incorporated with the content of CT by putting them in the annotation section. When the embedding procedure is accomplished, the CT must be delivered back to the ICA and then to be issued. The embedding and extracting algorithms of the proposed scheme will be presented in Sections 2.1 and 2.2 respectively.

2.1 Embedding Algorithm

Assume I is a color image with $M \times N$ pixels which consists of channels R, G and B. We divide the three channels into a set of $n \times n$ (n is odd) non-overlapping sub-blocks. In general, the size of the sub-block has an influence on the robustness of the watermark. Each watermark bit can be embedded into one sub-block by modifying the values of the sub-block's middle pixel and the other pixels. Let's define m as the middle pixel value and u as the mean value of the other pixels. For example, suppose we have a 3×3 sub-block as shown in Figure 1. In this case, P_5 is the middle pixel value m and the mean value of the other pixels can be computed by $\mu = (P_1+P_2+P_3+P_4+P_6+P_7+P_8+P_9)/8$. In order to control the balance between the robustness and image quality, the robustness coefficient value 'T' must be used. In this paper, we shall use different robustness coefficient values for channels R, G and B: T_R is the robustness coefficient value of channel R, T_G is for channel G, and T_B is for channel B. Basically, the visual effect to modify the R, G, and B channel is different in terms of the human visual sensitivity. In addition, the B channel has the larger tolerance to be modified than that of other channels. For these reasons, the robustness coefficient value T_B used in our scheme is the largest value. T_R and T_G are the secondly and minimal, respectively. The other advantage to adopt varied robustness coefficient is that the whole survival rate of watermark bit can be enhanced. The detailed procedure of the embedding algorithm is as follows:

1. Divide channels R, G and B into a set of $n\times n$ non-overlapping sub-blocks respectively.

2. Random select the sub-block for embedding watermark bit. All embedding locations and original watermark bits must be encrypted by PRK.

3. Set the robustness coefficient values T_R, T_G and T_B for channels R, G and B respectively. And in the next Step, T represents T_R, T_G and T_B when channels R, G and B are chosen to hide the watermark respectively.

4. Modify m and u for watermark embedding by following the algorithm below:

   If ($W_k = 1$) and (m - $\mu \geq$ T)

   No Modify

   Else

$$(m, u) = (m + \lceil |(m - u) - T|/2 \rceil, u - \lfloor |(m - u) - T|/2 \rfloor). \tag{1}$$

   If ($W_k = 0$) and (μ - $m \geq$ T)

   No Modify

   Else

$$(u, m) = (u + \lceil |(u - m) - T|/2 \rceil, m - \lfloor |(u - m) - T|/2 \rfloor). \tag{2}$$

   In Equation 1 and 2, we can adjust the u value by subtracting or adding the pixel values $P_1, P_2, P_3, P_4, P_6, P_7, P_8,$ and P_9, respectively. When the first watermark bit has been embedded on channel R, the same location on channels G and B are also chosen to embed the first watermark bit.

5. Read the next watermark bit and repeat Step (4) until the whole watermark has been embedded.

P1	P2	P3
P4	P5	P6
P7	P8	P9

Figure 1: A sub-block of sized 3×3

2.2 Extracting Algorithm

When the image owner wants to recover the watermark to prove the ownership of the image, the original CT and PRK must be used again to indicate all the embedding positions and extract the original watermark bit. The detailed extracting algorithm is as follows:

1. Divide channels R, G and B into a set of $n \times n$ non-overlapping sub-blocks respectively.

2. Use of the image owner PRK and the ICA's CT to obtain all the embedding locations.

3. Compute the middle pixel value 'm' and the mean value 'μ' of the sub-block.

4. Recover the watermark bit by comparing 'm' with 'μ' according to the following algorithm:

   If $m \geq \mu$,

   the watermark bit '1' is extracted

   Else

   the watermark bit '0' is extracted.

5. Read the next watermarked sub-block and repeat Steps (3) $\sim$ (4) until all the watermark bits are extracted.

When the first watermark bit is extracted from channel R, the watermark bit hidden on channels G and B can also be extracted by using the proposed extracting algorithm. Further more, we can confirm the watermark bits extracted by utilizing the majority voting mechanism.

3 Experimental Results and Comparsion

In this section, some experimental results are presented to test the robustness of our scheme. In our experiments, the color image “Lena” as shown in Figure 2(a) with the size is 255 × 255. The watermark “Apple” is a binary image with the size is 32 × 32 as shown in Figure 2(b). Each channel of the color image were divided into 85 × 85 non-overlapped sub-block with the size is 3 × 3 respectively and set the robustness coefficient values T_R=9, T_G=7 and T_B=11 respectively. We use the peak signal-to-noise ratio (PSNR) to evaluate the image quality after embedding watermark. And use the normalized correlation (NC) to evaluate the quality of the extracted watermark. The PSNR and NC are individually defined as follows:

$$PSNR = 10log_{10}\frac{255^2}{MSE}dB$$

and

$$MSE = (\frac{1}{M \times N})\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(\alpha_{ij} - \beta_{ij})^2$$

$$NC = \frac{\sum_{i=1}^{M_W}\sum_{j=1}^{N_W}[W(i,j) \cdot W'(i,j)]}{\sum_{i=1}^{M_W}\sum_{j=1}^{N_W}[W(i,j)]^2}$$

$\alpha_{\mathrm{i,\ j}}$ is the original image pixel which the coordinate is (i, j) and $\beta_{\mathrm{i,\ j}}$ is the watermarked image pixel which the coordinate is (i, j). The M and N represented the size of the color image. The $W(i,\ j)$ is the original watermark without any destruction, and $W'(i,\ j)$ is the watermark by extracting from the attacked watermarked image. The M_W and N_W represented the size of the watermark.

- Experiment 1 — No Attacks:

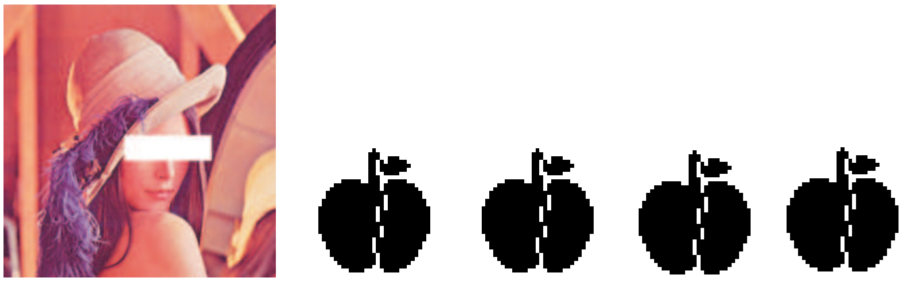
  Figure 3 shows the watermarking image and the extracted watermark without any destruction. The PSNR is 42 dB and NC value is 1.0.

Figure 2: (a)The host image “Lena” of size 255 × 255 (b)The watermark “Apple” of size 32 × 32

Figure 3: (a)The watermarked image (b)The extracted watermark without attacks

- Experiment 2 — Image Cropping:

  Figure 4 shows the results under image cropped attack. Extracting three watermarks from R, G and B channels and utilizing the majority methods to obtain the real watermark. The PSNR is reduced to 20.3 dB. The NC value is 0.97.

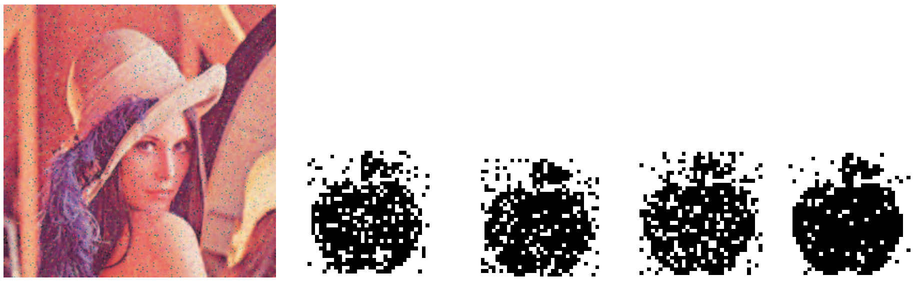


(a) PSNR = 20.3 (b) NC=0.97 R channel (c) NC=0.97 G channel (d) NC=0.97 B channel (e) NC=0.97 Majority Vote

Figure 4: The Image Cropping Attack

- Experiment 3 — The Salt and Pepper Attack:

  We added "salt and pepper" noise to the watermarked image "Lena" as shown in Figure 5, in which the PSNR is reduced to 18.2 dB. The NC value is 0.93. The results demonstrate our algorithm is robust to "salt and pepper" noise by utilizing the majority voting.



(a) PSNR = 18.2 dB (b) NC=0.84 R channel (c) NC=0.84 G channel (d) NC=0.82 B channel (e) NC=0.93 Majority Vote

Figure 5: The "salt and pepper" Noise Attack

- Experiment 4 — The Edge Sharpening Attack:

  We sharpened the watermarked image "Lena" as shown in Figure 6, the PSNR is reduced to 14.9 dB. The NC value is 0.99. From the results, we can clearly see that the proposed scheme is very robust to “Edge Sharpening Attack”.

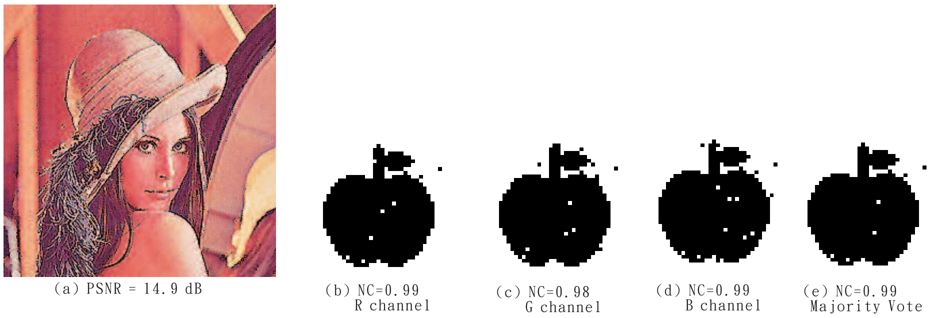


Figure 6: The Edge Sharpening Attack

- Experiment 5 — The Image Blurring Attack:

  We blurred the watermarked image “Lena” as shown in Figure 7. The PSNR is reduced to 36.8 dB. The NC value is 0.90.

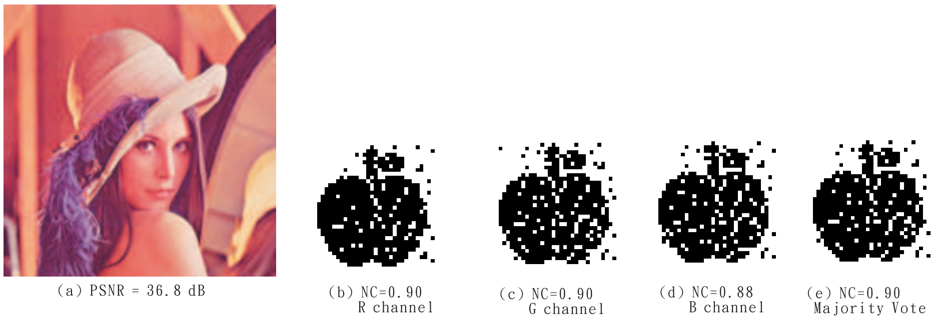


Figure 7: The Image Blurring Attack

- Experiment 6 — The Image JPEG Compression Attack:

  We used JPEG compression standard on the watermarked image as shown in Figure 8 with the compression ratio is 3.2. The PSNR reduced to 38.9 dB. The NC value is 0.97.

- Experiment 7 — The Gaussian Noise Attack:

  We added Gaussian noise to the watermarked image as shown in Figure 9, the PSNR is reduced to 30.4 dB. The NC value is 0.92. In the results, we can see the B channel was seriously damaged. But it can still extract better watermarks depending on the majority of votes.

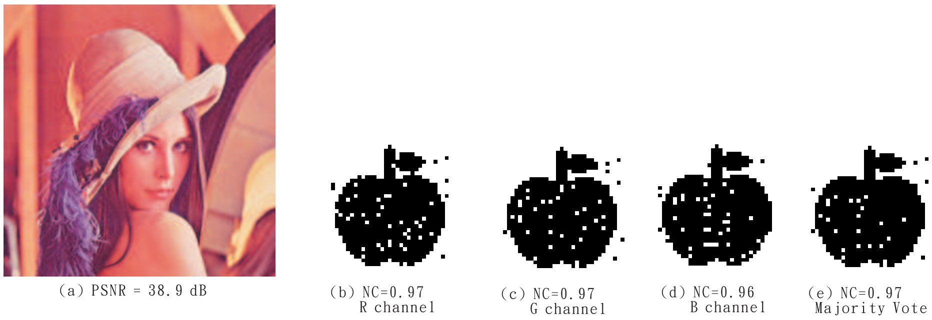


Figure 8: The Image JPEG Compression Attack

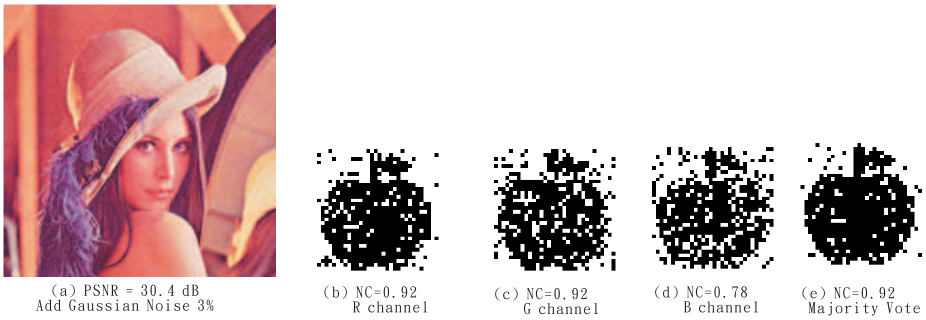


Figure 9: The Gaussian Noise Attack

As the above experimental results prove, our scheme is robust. In addition, compared with Huang et al.'s [11] and Lee and Chen's methods [12], our scheme is more efficient because the redundant secret keys are unnecessary. In Huang et al.'s scheme, three secret keys and one CT must be stored for one image watermarking task. In Lee and Chen's scheme, one secret key and one CT have to be stored for one image. Please note that each secret key, responsible for keeping track of the embedding locations, is composed of an extremely long series of bits. With Lee and Chen's and Huang et al.'s schemes, if there are many watermarked images to keep, there will be many secret keys to store, which can means a heavy load on the image owner.

4 Conclusions

We have proposed a new certificate-based watermarking scheme for color images. In the proposed scheme, each image has its unique CT assigned by the ICA. The embedding locations of the watermark bits are generated by the image owner's PRK and the image's CT. For the user, one PRK is quite enough to help manage a large number of images whose embedding locations are completely different. Compared with the existing methods, the proposed scheme is more efficient because much less secret keys are needed to offer the same level of security.

References

[1] C. C. Chang, K. F. Hwang, and M. S. Hwang, "A feature-oriented copyright owner proving technique for still images," *International Journal of Software Engineering and Knowledge Engineering*, vol. 12, no. 3, pp. 317–330, 2002.

[2] C. C. Chang, K. F. Hwang, and M. S. Hwang, "A robust authentication scheme for protecting copyrights of images and graphics," *IEE Proceedings Vision, Image and Signal Processing*, vol. 149, no. 1, pp. 43–50, 2002.

[3] L. H. Chen and J. J. Lin, "Mean quantization based image watermarking," *Image and Vision Computing*, vol. 21, pp. 717–727, Aug. 2003.

[4] T. H. Chen, G. G. Horng, and W. B. Lee, "A publicly verifiable copyright-proving scheme resistant to malicious attacks," *IEEE Trans. on Industrial Electronics*, vol. 52, pp. 327–334, Feb. 2005.

[5] W. C. Chu, "DCT - based image watermarking using subsampling," *IEEE Trans. on Multimedia.*, vol. 5, pp. 34–38, Mar. 2003.

[6] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. on Image Processing*, vol. 6, pp. 1673–1687, Dec. 1997.

[7] T. K. Das and S. Maitra, "Cryptanalysis of correlation-based watermarking schemes using single watermarked copy," *IEEE Signal Processing Letters*, vol. 11, pp. 446–449, Apr. 2004.

[8] T. K. Das, S. Maitra, and Jianying Zhou, "Cryptanalysis of chu's dct based watermarking scheme," *IEEE Trans. on Multimedia*, vol. 8, pp. 629–632, Jun. 2006.

[9] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Multiple image watermarking applied to health information management," *IEEE Trans. on Information Technology in Biomedicine*, vol. 10, pp. 722–732, Oct. 2006.

[10] S. C. Hsia, I. C. Jou, and S. M. Hwang, "A gray level watermarking algorithm using double layer hidden approach," *IEICE Trans. on Fundamental*, vol. E85-A, pp. 463–471, Feb. 2002.

[11] H. C. Huang, F. H. Wang, and J. S. Pan, "A VQ - based robust multi-watermarking algorithm," *IEICE Trans. on Fundamental*, vol. E85-A, pp. 1719–1726, Jul. 2002.

[12] W. B. Lee and T. H. Chen, "A public verifiable copy protection technique for still images," *The Journal of Systems and Software*, vol. 87, pp. 195–204, Jun. 2002.

[13] P. L. Lin, "Robust transparent image watermarking system with spatial mechanisms," *The Journal of Systems and Software*, vol. 50, pp. 107–116, 2000.

[14] J. C. Liu and S. Y. Chen, "Fast two-layer image watermarking without referring to the original image and watermark," *Image and Vision Computing*, vol. 19, pp. 1083–1097, Dec. 2001.

[15] C. S. Lu, S. K. Huang, C. J. Sze, and H. Y. M. Liao, "Cocktail watermarking for digital image protection," *IEEE Trans. on Multimedia*, vol. 2, pp. 209–224, Dec. 2000.

[16] D. P. Mukherjee, S. M., and S. T. Acton, "Spatial domain digtal watermarking of multimedia objects for buyer authentication," *IEEE Trans. on Multimedia*, vol. 6, pp. 1–15, Feb. 2004.

[17] S. C. Pei and J. M. Guo, "High-capacity data hiding in halftone images using minimal-error bit searching and least-mean square filter," *IEEE Trans. on Image Processing*, vol. 15, pp. 1665–1679, Jun. 2006.

[18] F. Y. Shih and S. Y. T. Wu, "Combinational image watermarking in the spatial and frequency domains," *Pattern Recognition*, vol. 36, pp. 969–975, Apr. 2003.

[19] H. W. Wong, O. C. Au, and Y. M. Yeung, "A novel blind multiple watermarking technique for images," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 13, pp. 813–830, Aug. 2003.

[20] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Trans. on Image Processing*, vol. 10, pp. 1539–1601, Oct. 2001.