A certificate-based watermarking scheme for coloured images

N.-I. Wu*[a], C.-M. Wang[a], C.-S. Tsai[b] and M.-S. Hwang[b]
[a]Institute of Computer Science and Engineering, National Chung Hsing University, 250 Kuo Kuang Road, Taichung 402, Taiwan

[b]Department of Management Information Systems, National Chung Hsing University, 250 Kuo Kuang Road, Taichung 402, Taiwan

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, to enhance the digital image copyright protection. However, 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, the authors propose a novel watermarking method to solve this problem. Also depending on the Image Certification Authority for copyright protection, the authors' new method makes a difference by providing the user with the power to process masses of digital image watermarking tasks using just one private key. The results of the authors' 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 Joint Photographic Experts Group compression, low pass filtering and high pass filtering as well as noise contamination.

Keywords: copyright protection, watermarking, PRivate key, robustness

1 INTRODUCTION

Owing 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.[1] 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

The MS was accepted for publication on 5 February 2008.
* *Corresponding author: Nan-I, Department of Management Information Systems, National Chung Hsing University, 250 Kuo Kuang Road, Taichung 402, Taiwan; email rocjfk2000@yahoo.com.tw*

 IMAG mp116 © RPS 2008 DOI: 10.1179/174313108X299516

major challenge a watermarking scheme has to face is the establishment of the robustness against various image processing attacks.[2]

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[3] proposed a robust transparent watermarking system that can resist various image attacks by hiding watermark bits in the edge areas. Besides, Liu and Chen[4] presented a two layer watermarking scheme that can resist both high and low frequency destruction. In addition, in Ref. 5, there is a spatial watermarking technique focused on buyer authentication. Also, Wong *et al.*[6] 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[7] 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.*[8] 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[9] to recover watermarks without the original images. However, Cox *et al.*'s and Chu's schemes are, according to Das *et al.*,[10,11] insecure under the single watermarked copy attack. To improve the robustness of Cox's scheme, Lu *et al.*[12] proposed a cocktail watermark to fix this flaw. In their scheme, the human visual system is used to obtain better image quality after watermark embedding. Wong *et al.*[13] presented three blind multiple watermarking techniques for different purposes that embed watermark bits in the DCT coefficients. In addition, based on mean quantisation watermarking, the method proposed by Chen and Lin[14] functions by altering the DWT coefficients. When dealing with high resolution pictures such as medical images, Giakoumaki *et al.*[15] utilise their watermarking technique 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.[16,17]

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.[18–22] Lee and Chen[22] proposed a publicly verifiable copyright protection technique where everyone can verify the existence of the watermark using a PUblic key (PUK) but cannot remove the watermark without using the PRivate key (PRK) even if he/she has the PUK. 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 Ref. 21, where three secret keys must be kept by the image owner after one watermark gets embedded into one digital image.

In this paper, the authors shall propose an efficient watermarking technique to hide binary watermarks into colour images. In the design of the authors' 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 the 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 the 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.

The remainder of this paper is organised as follows. In the section on 'Proposed method', present the proposed watermarking algorithms will be presented. Then, in the section on 'Experimental results and comparison', the experimental results will be offered to demonstrate the robustness of the new scheme. Finally, a brief conclusion will be given in the section on 'Conclusions'.

2 PROPOSED METHOD

In the new scheme, for each image to hold a watermark (or watermarks), an application has to be made at the 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. 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 PRK and the encrypted data are 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 the sections on 'Embedding algorithm' and 'Extracting algorithm' respectively.

2.1 Embedding algorithm

It is assumed that I is a colour image with $M \times N$ pixels which consists of channels R, G and B. The three channels are divided into a set of $n \times n$ (n is odd) non-overlapping subblocks. In general, the size of the subblock has an influence on the robustness of the watermark. Each watermark bit can be embedded into one subblock by modifying the values of the subblock's middle pixel and the other pixels. Let us define m as the middle pixel value and u as the mean value of the other pixels. For example, it is supposed that the authors have a 3×3 subblock as shown in Fig. 1. In this case, P_5 is the middle pixel value m and the mean value of the other pixels can be computed by $\mu=(P_1+P_2+P_3+P_4+P_6+P_7+P_8+P_9)/8$. To control the balance between the robustness and image quality, the robustness coefficient value T must be used. In this paper, different robustness coefficient values for channels R, G and B are used:

P_1	P_2	P_3
P_4	P_5	P_6
P_7	P_8	P_9

1 Subblock of sized 3×3

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 channels 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 the 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 subblocks respectively
2. random select the subblock 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. 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 following the algorithm below

If ($W_k=1$) and ($m-u \geq T$)
  No modify
Else

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

If ($W_k=0$) and ($u-m \geq T$)
  No modify
Else

$$(u,m)=(u+\lceil|(u-m)-\frac{T}{2}|\rceil,m-\lfloor|(u-m)-\frac{T}{2}|\rfloor) \quad (2)$$

In equations (1) and (2), the u value can be adjusted 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

2 (a) host image 'Lena' of size 255×255 and (b) watermark 'Apple' of size 32×32

3 (a) watermarked image, PSNR=42 dB and (b) extracted watermark without attacks, NC=1

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

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 subblocks 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 subblock
4. recover the watermark bit by comparing m with μ according to the following algorithm

If $m \geqslant \mu$
  The watermark bit '1' is extracted
Else
  The watermark bit '0' is extracted

5. read the next watermarked subblock and repeat Steps (3) and (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 using the proposed extracting algorithm. Further more, the authors can confirm the watermark bits are extracted by utilising the majority voting mechanism.

3 EXPERIMENTAL RESULTS AND COMPARISON

In this section, some experimental results are presented to test the robustness of the scheme. In the authors' experiments, the colour image 'Lena' as shown in Fig. 2*a* with the size of 255×255. The watermark 'Apple' is a binary image with the size of 32×32 as shown in Fig. 2*b*. Each channel of the colour image was divided into 85×85 non-overlapping blocks with the size of 3×3 respectively and set the robustness coefficient values $T_R=9$, $T_G=7$ and $T_B=11$ respectively. The authors use the peak signal to noise ratio (PSNR) to evaluate the image quality after embedding watermark, and use the normalised correlation (NC) to evaluate the quality of the extracted watermark. The PSNR and NC are individually defined as follows

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

where

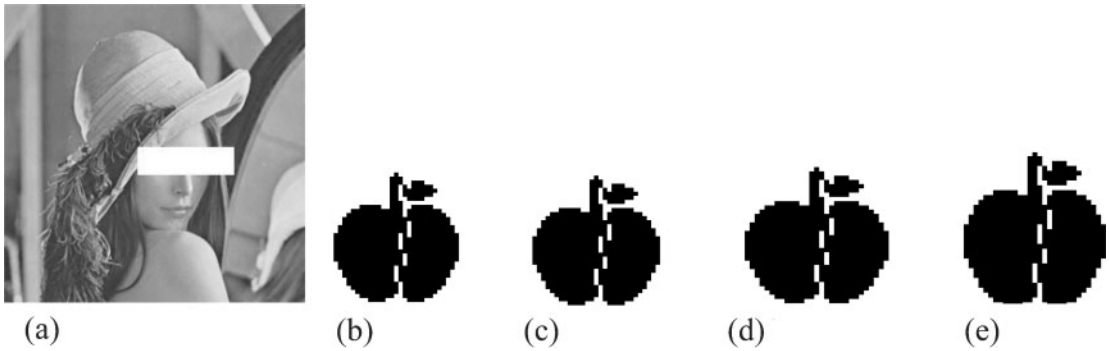
$$MSE = \left(\frac{1}{M \times N} \right) \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (\alpha_{i,j} - \beta_{i,j})^2$$

$$NC = \frac{\sum_{i=0}^{M_w-1} \sum_{j=0}^{N_w-1} W(i,j) W'(i,j)}{\sum_{i=0}^{M_w-1} \sum_{j=0}^{N_w-1} W(i,j)^2}$$

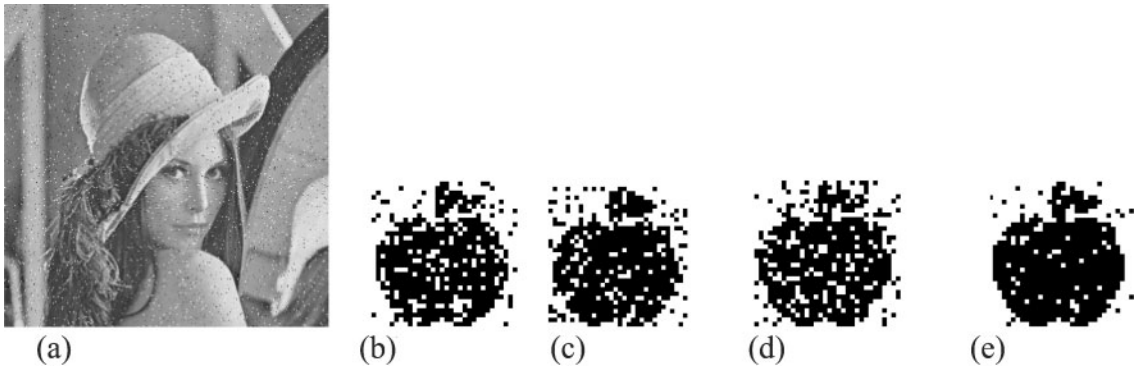
where $\alpha_{i,j}$ is the original image pixel which the coordinate is (i, j) and $\beta_{i,j}$ is the watermarked image pixel which the coordinate is (i, j). The M and N represented the size of the colour image. The $W(i, j)$ is the original watermark without any destruction and $W'(i, j)$ is the 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.

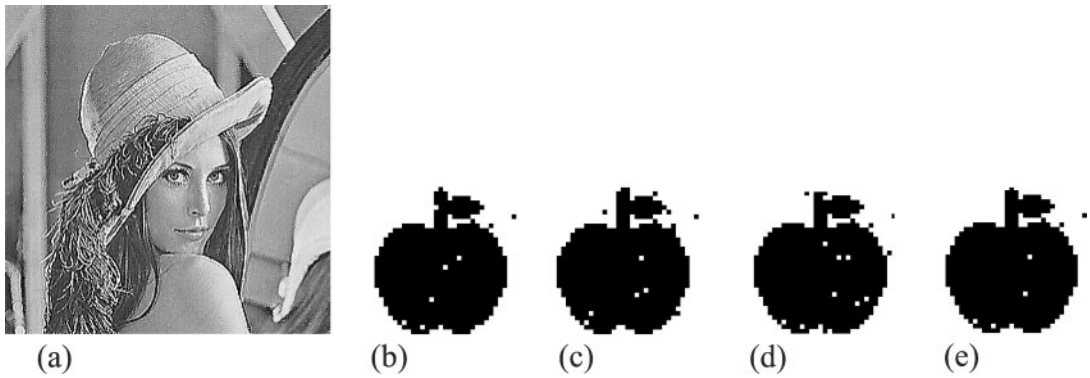
Experiment 2: image cropping. Figure 4 shows the results under image cropped attack. Three



4 Image cropping attack: (a) PSNR=20.3 dB; (b) R channel, NC=0.97; (c) G channel, NC=0.97; (d) B channel, NC=0.97; (e) majority voting, NC=0.97



5 'Salt and pepper' noise attack: (a) PSNR=18.2 dB; (b) R channel, NC=0.84; (c) G channel, NC=0.84; (d) B channel, NC=0.82; (e) majority voting, NC=0.93



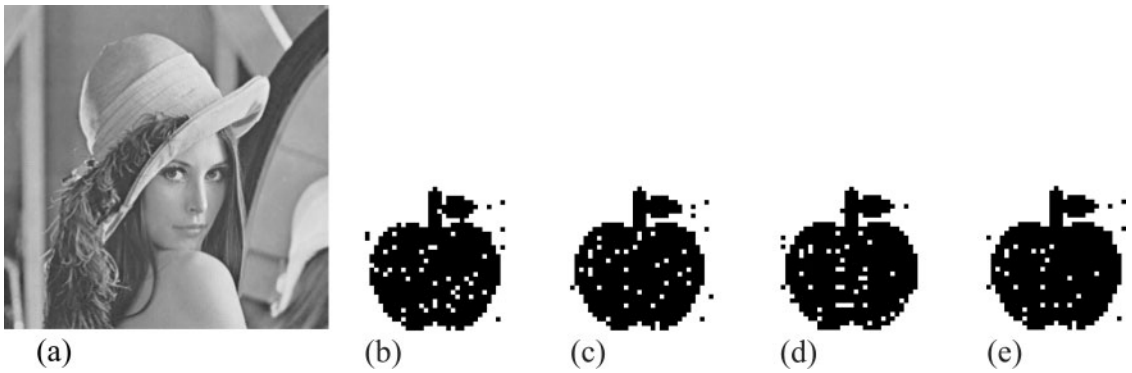
6 Edge sharpening attack: (a) PSNR=14.9 dB; (b) R channel, NC=0.99; (c) G channel, NC=0.984; (d) B channel, NC=0.99; (e) majority voting, NC=0.99

watermarks are extracted from the R, G and B channels respectively and the majority voting scheme is utilized to obtain the real watermark. The PSNR is reduced to 20.3 dB. The NC value is 0.97.

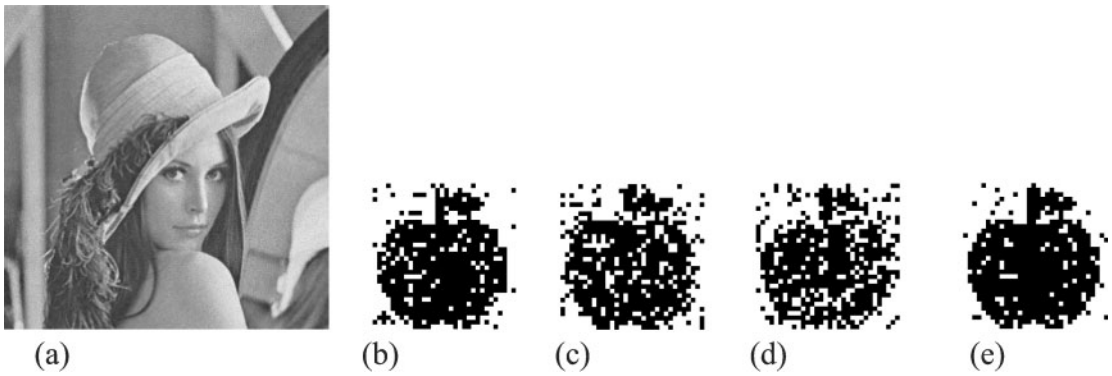
Experiment 3: the salt and pepper attack. The authors added 'salt and pepper' noise to the watermarked image 'Lena' as shown in Fig. 5, in which the PSNR is reduced to 18.2 dB. The NC value is 0.93. The results demonstrate that the authors' algorithm is robust to 'salt and pepper' noise utilizing the majority voting.

Experiment 4: the edge sharpening attack. The authors sharpened the watermarked image 'Lena' as shown in Fig. 6, the PSNR is reduced to 14.9 dB. The NC value is 0.99. It can clearly be seen from the results that the proposed scheme is very robust to 'edge sharpening attack'.

7 Image blurring attack: (a) PSNR=36.8 dB; (b) R channel, NC=0.90; (c) G channel, NC=0.90; (d) B channel, NC=0.88; (e) majority voting, NC=0.90



8 Image JPEG compression attack: (a) PSNR=38.9 dB; (b) R channel, NC=0.97; (c) G channel, NC=0.97; (d) B channel, NC=0.96; (e) majority voting, NC=0.97



9 Gaussian noise attack: (a) add Gaussian noise 3%, PSNR=30.4 dB; (b) R channel, NC=0.92; (c) G channel, NC=0.92; (d) B channel, NC=0.78; (e) majority voting, NC=0.92

Experiment 5: the image blurring attack. The authors blurred the watermarked image 'Lena' as shown in Fig. 7. The PSNR is reduced to 36.8 dB. The NC value is 0.90.

Experiment 6: the image Joint Photographic Experts Group (JPEG) compression attack.

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

Experiment 7: the Gaussian noise attack. The authors added Gaussian noise to the watermarked image as shown in Fig. 9, the PSNR is reduced to 30.4 dB. The NC value is 0.92. It can be seen from the results that the B channel was seriously damaged. But it can still extract better watermarks depending on the majority of votes.

The above experimental results prove that the authors' scheme is robust. In addition, compared with Huang *et al.*'s[21] and Lee and Chen's methods,[22] the authors' 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 means a heavy load on the image owner.

4 CONCLUSIONS

The authors have proposed a new certificate based watermarking scheme for coloured 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 Karthik, K. and Hatzinakos, D. Decryption key design for joint fingerprinting and decryption in the sign bit plane for multicast content protection. *Int. J. Network Security*, 2007, 254–265.

2 Feng, J. B, Lin, I. C, Tsai, C. S. and Chu, Y. P. Reversible watermarking: current status and key issues. *Int. J. Network Security*, 2006, 161–170.

3 Lin, P. L. Robust transparent image watermarking system with spatial mechanisms. *J. Syst. Softwarer*. 2000, **50**, 107–116.

4 Liu, J. C. and Chen, S. Y. Fast two-layer image watermarking without referring to the original image and watermark. *Image and Vision Comput.,* 2001, **19**, 1083–1097.

5 Mukherjee, D. P, Maitra, S. and Acton, S. T. Spatial domain digtal watermarking of multimedia objects for buyer authentication. *IEEE Trans. Multimedia*, 2004, **6**, 1–15.

6 Wong, P. W. and Memon, N. Secret and public key image watermarking schemes for image authentication and ownership verification, *IEEE Trans. Image Process*, 2001, **10**, 1539–1601.

7 Pei, S. C. and Guo, J. M. High-capacity data hiding in halftone images using minimal-error bit searching and least-mean square filter. *IEEE Trans. Image Process*, 2006, **15**, 1665–1679.

8 Cox, I. J, Kilian, J., Leighton, F. T. and Shamoon, T. Secure spread spectrum watermarking for multimedia. *IEEE Trans. Image Process*, 1997, **6**, 1673–1687.

9 Chu, W. C. DCT - based image watermarking using subsampling. *IEEE Trans. Multimedia.*, 2003, **5**, 34–38.

10 Das, T. K. and Maitra , S. Cryptanalysis of correlation-based watermarking schemes using single watermarked copy. *IEEE Signal Processing Lett*, 2004, **11**, 446–449.

11 Das, T. K. and Maitra, S. and Zhou, J. Y. Cryptanalysis of chu's dct based watermarking scheme. *IEEE Trans. Multimedia*, 2006, **8**, 629–632.

12 Lu, C. S., Huang, S. K., Sze, C. J. and Liao, H. Y. M. Cocktail watermarking for digital image protection. *IEEE Trans. Multimedia*, 2000, **2**, 209–224.

13 Wong, H. W., Au, O. C. and Yeung, Y. M. A novel blind multiple watermarking technique for images. *IEEE Trans. Circuits Syst. Video Technol.* 2003, **13**, 813–830.

14 Chen, L. H. and Lin, J. J. Mean quantization based image watermarking. *Image Vision Comput.*, 2003, **21**, 717–727.

15 Giakoumaki, A., Pavlopoulos, S. and Koutsouris, D. Multiple image watermarking applied to health information management. *IEEE Trans. Inf. Technol. Biomed.,* 2006, **10**, 722–732.

16 Hsia, S. C., Jou, I. C. and Hwang, S. M. A gray level watermarking algorithm using double layer hidden approach. *IEICE Trans Funda.,*2002, **E85-A**, 463–471.

17 Shih, F. Y. and Wu, S. Y. T. Combinational image watermarking in the spatial and frequency domains. *Pattern Recognit.*, 2003, **36**, 969–975.

18 Chang, C. C, Hwang, K. F and Hwang, M. S. A feature-oriented copyright owner proving technique for still images. *Int. J. Software Eng. Knowl. Eng.*, 2002, **12**, 317–330.

19 Chang, C. C., Hwang, K. F. and Hwang, M. S. A robust authentication scheme for protecting copyrights of images and graphics. *IEE Proc. Vis., Image Signal Process*, 2002, **149**, 43–50.

20 Chen, T. H., Horng, G. G. and Lee, W. B. A publicly verifiable copyrightproving scheme resistant to malicious attacks. *IEEE Trans. Ind. Electron.*, 2005, **52**, 327–334.

21 Huang, H. C., Wang, F. H. and Pan, J. S. A VQ - based robust multiwatermarking algorithm. *IEICE Trans. Fundm*, 2002, **E85-A**, 1719–1726.

22 Lee, W. B. and Chen, T. H. A public verifiable copy protection technique for still images. *J of Syst. Software*, 2002, **87**, 195–204.