

A Blind Image Watermarking Based on Dual Detector^{*}

CHIN-PAN HUANG¹, CHI-JEN LIAO² AND CHAUR-HEH HSIEH¹

¹*Department of Computer and Communication Engineering*

Ming Chuan University

Taoyuan, 333 Taiwan

²*Department of Information Engineering*

I-Shou University

Kaohsiung, 840 Taiwan

This paper presents a blind image watermarking technique based on a novel detection scheme which contains two detectors aiming at the positive attack and negative attack, respectively. The analysis on signal processing attack indicates that there exist unreliable transformed coefficients in the attacked image which result in errors of the extraction of watermark data. The novel detection scheme removes the unreliable transformed coefficients and employs the remaining reliable coefficients for the extraction of embedded watermark. The experimental results indicate the proposed technique improves robustness significantly, as compared to the existing single detector scheme.

Keywords: image watermarking, attacks, discrete cosine transform, robustness, dual detector

1. INTRODUCTION

Digital watermarking can prove to be useful to avoid the illegal use of digital media. Generally, it can be classified into two types: robust watermarking and fragile watermarking. The requirements for robust watermarking are transparency, robustness, security, capacity, universality, and unambiguousness [1]. Among them, transparency and robustness are most important. Transparency refers to the perceptual quality of the image being protected. In other words, the watermark should be invisible over the original image. Robustness refers to the ability to detect the watermark after unintentional attack, *i.e.*, common signal processing operations [2]. The technique presented in this paper belongs to the robust type. Depending upon a work domain that watermark is embedded in, watermarking techniques can be classified into two categories: spatial domain and transform domain [3-15]. Recent efforts are mostly based on transform-domain because it offers better robustness.

According to whether the host signal is needed or not during the detection, watermarking technique can be roughly categorized into two types: non-blind and blind [16]. Non-blind method requires the original host in the detection end, whereas blind one does not. The blind methods are more useful than non-blind because the host image may be not available in real-world scenarios. Generally, blind methods are often less robust and also harder to implement than non-blind ones. Many blind image watermarking schemes [16-22] have been presented recently.

Received February 26, 2008; revised June 9 & August 4, 2008; accepted August 22, 2008.

Communicated by H. Y. Mark Liao.

^{*} This paper was partially supported by the National Science Council of Taiwan, R.O.C., No. NSC 92-2213-E-214-009.

The existing blind schemes can be roughly classified into three types [16]: (a) correlation-based; (b) based on absolute modulation of individual primary or secondary elements of an image; (c) based on relative modulation of pair elements. Most of these schemes focus on embedding strategy. In addition, they do not exploit the characteristics of the attacks. In this work, we aim at the design of an efficient detection scheme that takes signal processing attacks into account.

Detection is an inverse process of embedding. Most detection schemes of transform-domain watermarking in the literature use all transformed coefficients of the test attacked image to extract watermark. In this paper, the analysis on the attacked images indicates that there are unreliable transformed coefficients which would yield the extraction error of watermark data. To attack the problem, we develop a new detection scheme that removes the unreliable transformed coefficients. The new detection contains two detectors that are based on positive attack (PA) and negative attack (NA), which are obtained through analyses and experiments. The proposed dual-detector scheme is different from the cocktail watermarking [15] which also employs two detectors. The cocktail watermarking is a non-blind scheme which embeds two complementary watermarks, called positive hiding (PH) and negative hiding (NH), into the host image simultaneously. In detection, two corresponding detectors are used to extract PH and NH watermarks. In such case, at least one watermark survives when any attacks occurs. Therefore, the missed detection rate will be reduced and thus improving robustness significantly. However, if no watermark is embedded into the host image and the image suffers from positive attack or negative attack, our previous study [23-25] indicate that cocktail method will introduce high false alarm rate. Unlike the cocktail method, in this work we embed only one watermark, and design two detectors to raise the detection rate of watermark. These two detectors are mainly based on characteristics of attacks, which are not directly related to the embedding scheme like cocktail approach. The other difference between the cocktail method and this work is the cocktail scheme [15] is a non-blind one.

The remaining sections are organized as follows. The proposed watermarking system is described in section 2. A single detector algorithm is first presented. Then a novel dual detector scheme based on attack characteristics is developed. In section 3, experimental results with a single detector and our dual detector methods are provided. The conclusions are drawn in section 4.

2. PROPOSED BLIND WATERMARKING

The proposed watermarking system is shown in Fig. 1. The host image is transformed by a full-domain DCT. The DC coefficient is discarded, and the remaining two-dimensional AC coefficients are converted into one-dimensional coefficient sequence $F(k)$ via zig-zag scanning. The binary watermark is embedded into the coefficient sequence. In the detection end, the received watermarked image is transformed with DCT as in the embedding end, and the resulting AC coefficients are fed into positive-attack detector and negative-attack detector simultaneously. The larger response of the two detectors is input to a thresholding device. If it is greater than the detection threshold ρ , we claim that the watermark exists; otherwise, the watermark does not exist. The designs of embedding and detection are performed on the above AC coefficient sequence, and the design details are described in the following.

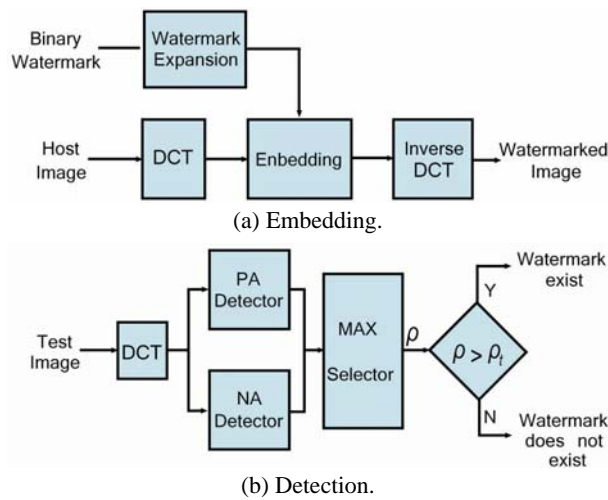


Fig. 1. Proposed blind watermarking system.

2.1 Embedding

We calculate a reference (estimate) sequence from the AC coefficient sequence $F(k)$ by a slide window of $(2m + 1)$; *i.e.*

$$\bar{F}(k) = \text{sign}(F(k)) \cdot \frac{1}{(2m+1)} \sum_{j=-m}^m |F(k+j)|. \quad (1)$$

In this work, the slide window length is 5 ($m = 2$). The binary watermark W_i is embedded by the following rule:

$$F_m(k) = \bar{F}(k) + \text{sign}(W_i) \cdot \alpha |\bar{F}(k)| \quad (2)$$

where α is a hiding factor with the value between 0 and 1 (in this work, $\alpha = 0.5$), $\text{sign}(x)$ is a sign function, and $F_m(k)$ is the resulting signal with watermark embedded. In Eq. (2), if the watermark bit to be embedded is 1, $F_m(k)$ is the sum of the reference $\bar{F}(k)$ and a positive embedded energy $\alpha |\bar{F}(k)|$; otherwise, if the watermark bit is -1 , $F_m(k)$ is the difference of the reference and $\alpha |\bar{F}(k)|$.

In detection, the watermark can be easily extracted by

$$W^e(i) = \text{sign}(F_m^a(k) - \bar{F}_m^a(k)). \quad (3)$$

More specifically, if $F_m^a(k) > \bar{F}_m^a(k)$, the extracted watermark bit is 1; otherwise it is -1 . In the above equation, $F_m^a(k)$ is the DCT coefficient sequence of the test image which suffered from attack; $\bar{F}_m^a(k)$ is its corresponding reference coefficient sequence, which is calculated using the estimation scheme in Eq. (1). The above detection scheme has been widely used in most blinding watermarking techniques, which doesn't consider the

attack characteristics. It employs one detector only, so we refer to it as *single detector* for comparison purpose.

In general, the length of a watermark sequence, B_L , is much smaller than that of the media to be embedded (the AC coefficient sequence), M_L . To increase the security and prevent interaction between the successive embedded data, we expand randomly the original binary watermark stream, a sequence of $\{+1, -1\}$, into a ternary stream, a sequence of $\{+1, -1, 0\}$. The coefficients corresponding to the symbol 0 are not embedded with watermark message. The length of the ternary stream, T_L , is obtained according to the range of the AC coefficient to be hidden. T_L is larger than B_L but smaller than M_L . Fig. 2 illustrates the pseudo-random expansion using a simple example, in which a watermark sequence with length of 3 bits is mapped into a ternary stream with length of 10 symbols. It is seen that the original watermark bits are permuted in the ternary stream. Through this manner, a short watermark sequence can be embedded in a long AC coefficient sequence in a pseudo-random way, which is controlled by a key.

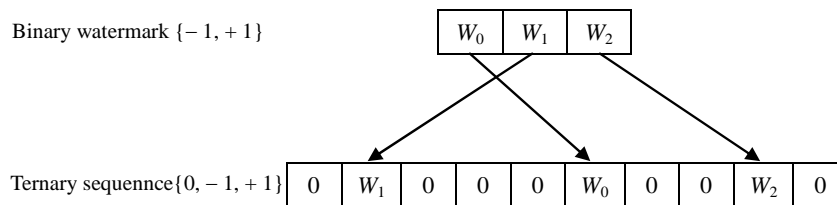


Fig. 2. Watermark expansion from binary symbol to ternary symbol.

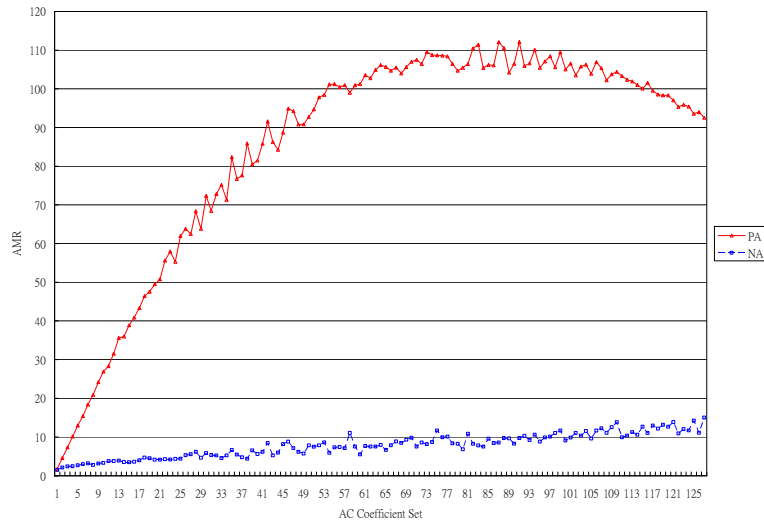
2.2 Detection

As mentioned earlier, detection is an inverse process of embedding. Thus it does not consider the characteristics of the attacks. This paper aims to develop a new detection scheme which takes attacks into account. The attacks can be classified into three categories: positive attack (PA), negative attack (NA) and hybrid attack (HA) and they are not image dependent. Note that the hybrid (random) attack can be regarded as a combination of positive and negative attack. The details of characteristics of these attacks can be found in our previous works [23-25]. The new scheme categorizes the attacks into positive attack (PA) and negative attack (NA) and then design two detectors accordingly. We call the detection scheme as *dual detector* for convenience. The scheme is designed mainly based on the analysis of the typical image processing attacks in Table 1. The attacks correspond to the signal processing category (noise and convo filter) of StirMark benchmark [21]. Here we summarize the characteristics of the attacks in the following, which are related directly to this work. The details can be found in [24, 25].

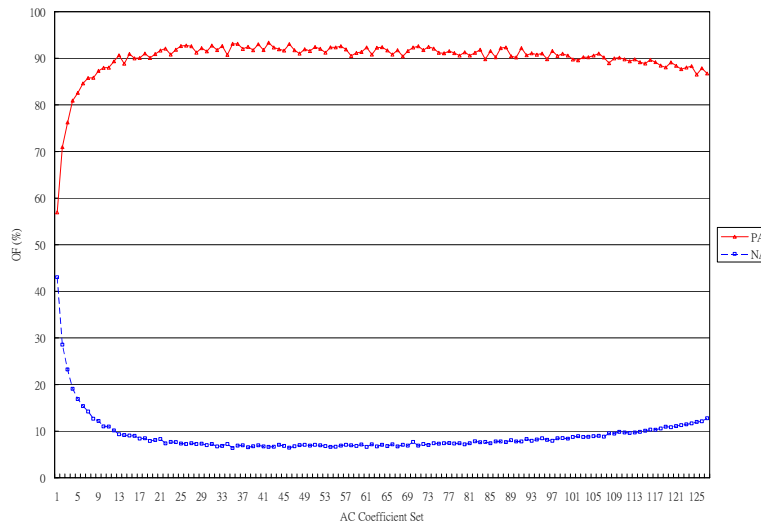
Each signal processing attack yields in both positive modulation (PM) and negative modulation (NM) to the host image [15, 23-25]. PM (NM) denotes that the magnitude of an AC coefficient of the attacked image is greater (less) than that of the unattacked image. To characterize the attacks, we employed two measures to investigate the characteristics of the AC coefficient sequence $F(k)$. One is the average coefficient magnitude change ratio (AMR) before and after attack, and the other is occurrence frequency (OF) before and after attack. The former measures the average attack energy for a whole image, and

Table 1. Image processing attacks.

Image Processing Functions and classifications			
01- Average (7 × 7)	NA	08- Enhance Edges (75)	PA
02- Blur (75)	NA	09- Enhance Focus	PA
03- Gaussian Blur (7 × 7)	NA	10- Focus Restoration	PA
04- Soften (75)	NA	11- Sharpen (50)	PA
05- JPEG compression (75)	NA	12- Random Noise (±16)	HA
06- JPEG compression (25)	NA	13- Random Noise (±8)	HA
07- Enhance Detail	PA		



(a) AMR.



(b) OF.

Fig. 3. Results of sharpening operation.

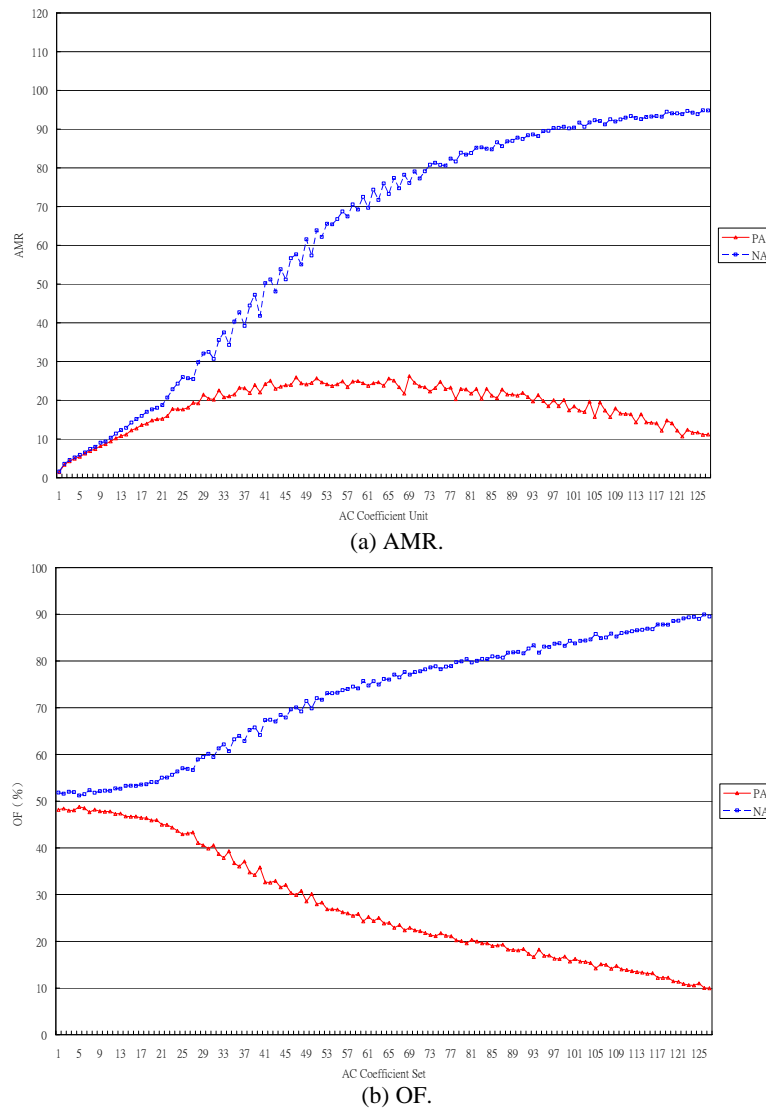


Fig. 4. Results of JPEG compression.

the later evaluates the number of coefficients attacked (called attack frequency). Fig. 3 shows the two measures when images are suffered from *sharpening* attack. The figure compares the two measures for PM and NM, respectively. It is obvious that for the *sharpening* operation, PM dominates both in attack energy and attack frequency. Therefore, it is classified as a positive attack. On the contrary, as seen in Fig. 4, for *JPEG compression*, NM dominates, thus it is regarded as a negative attack. Using the two measures, all signal processing attacks can be classified.

Positive attack will move the embedded coefficients away from the reference value. Thus the attacked signal is more robust to noise than the unattacked one. So positive at-

tack is helpful for extraction of watermark. On the contrary, negative attack will pull embedded coefficients such that they are close to the reference value. In this case, even a small noise may cause the signal jumping from above (or below) reference to below (above) reference, which yield the error of extraction of watermark. The dynamic range (the difference between positive reference and negative reference) becomes larger after positive attack and smaller after negative attack.

Furthermore, for negative attack, when attack energy is high, all the coefficients may be reduced to approximate zero value. In such case, the detection of watermark would fail. So, it is reasonable to say that if the value of a coefficient is very small, the coefficient is probably suffered from a large negative attack. Therefore, it is not reliable and should not be used for the detection.

As mentioned before, some of the coefficients of the attacked image are not reliable. The unreliable coefficients should not be included for watermark extraction; otherwise, it will yield errors of extraction. In this work, we present a novel detection scheme that removes the unreliable coefficients and uses the remaining reliable coefficients for extraction of watermark. It contains two detectors that exploit the characteristics of positive attack and negative attacks, respectively.

2.3 Dual Detector

For convenience, we define an attack magnitude deviation ratio as $R(k) = |(F_m^a(k) - \overline{F_m^a(k)}) / \overline{F_m^a(k)}|$. If no attack exists, it is easy to obtain $R(k) = \alpha$ from Eq. (2). Therefore, if $R(k) > \alpha$ we can say that positive attack occurs; otherwise, negative attack occurs when $R(k) < \alpha$. The decision rule is suited for the ideal case in which the reference $\overline{F_m^a(k)}$ is a fixed value. However, our investigation indicates that $\overline{F_m^a(k)}$ may fluctuate slightly with different k and different attacks. To avoid the classification error of attack types, we narrow down the PA range by introducing the parameter β which is larger than α . Specifically, if $R(k) > \beta$ ($\beta > \alpha$), the attack is regarded as positive. Based on the concept, we design a detector for extracting the coefficients suffered from positive attack as follows. Unlike most techniques in the literature, the detectors of our technique are designed according to the types of amplitude attacks mentioned above, rather than the corresponding embedding scheme.

- Positive Attack Detector:

The watermark is extracted by

$$W_p^e(i) = \begin{cases} 1, & \text{if } R(k) > \beta \text{ and } \text{sign}(F_m^a(k) - \overline{F_m^a(k)}) = \text{sign}(F_m^a(k)) > 0 \\ -1, & \text{if } R(k) > \beta \text{ and } \text{sign}(F_m^a(k) - \overline{F_m^a(k)}) = \text{sign}(F_m^a(k)) < 0 \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

The rule in the top line of Eq. (4) is for positive coefficients (the sign of the coefficient is positive) of the received signal, whereas the rule in the middle line is for negative coefficients. The extracted watermark bits for unreliable coefficients are set to zero (bottom line of Eq. (4)) such that they are useless in the calculation of detection response. The

action is equivalent to removing the unreliable coefficients for detection of watermark. The extracted watermark bits for the reliable coefficients are + 1 or - 1. It is obvious that the detector output contains three symbols: + 1, - 1, and 0. This is unlike the conventional detection scheme in which two symbols (+ 1 and - 1) are employed. The detector response (normalized correlation) between the original watermark stream and extracted watermark stream under positive attack is defined as

$$\rho_{mm,p}(W, W_p^e) = \frac{\sum W(i) \cdot W_p^e(i)}{\sum |W(i) \cdot W_p^e(i)|}. \quad (5)$$

The denominator is the total number symbols of + 1 and - 1 extracted.

As mentioned before, negative attack may make the R very small, or the reference value close to zero. In either case, the extraction of watermark is unreliable because it is sensitive to noise. In order to raise the reliability of watermark extraction, we remove the unreliable coefficients that satisfy $R(k) < \varepsilon$ or $\overline{F}_m^a(k) < \sigma$, and thus obtain the negative attack detector in the following.

- Negative Attack Detector:

The watermark is extracted by

$$W_n^e(i) = \begin{cases} \text{sign}(F_m^a(k) - \overline{F}_m^a(k)), & \text{if } \varepsilon < R(k) < \beta \text{ and } \overline{F}_m^a(k) > \sigma. \\ 0, & \text{otherwise} \end{cases}. \quad (6)$$

Like the positive attack detector, the bottom line in Eq. (6) is used to remove the unreliable coefficients. The detector output also contains three symbols: + 1, - 1, and 0. The normalized correlation between the original watermark stream and extracted watermark stream under negative attack is defined as $\rho_{mn,n}$, using the same equation as in Eq. (5) but replacing the positive extraction parameter $W_p^e(i)$ with $W_n^e(i)$.

The larger of the above two detection responses, $\max\{\rho_{mm,p}, \rho_{mn,n}\}$, is used to judge whether the watermark is present or absent by comparing it with a predefined detection threshold (ρ , in Fig. 1). If it is greater than the threshold, the watermark exists; otherwise, it doesn't exist.

It is seen from Eq. (4) that if β is set higher, more coefficients would be regarded as unreliable; consequently, it may reduce false alarm rate, whereas increase missed detection rate. On the other hand, if β is set lower, fewer coefficients would be regarded as unreliable, which may increase false alarm rate while reduce missed detection rate. Thus, the value of β is determined by taking the compromise of false alarm and missed detection. Similar conclusion is applied for the determination of the values of ε and σ in Eq. (6). In addition, the values of parameters ε and β depend on the value of α . The relationship is hard to achieve theoretically. Our experience indicates that $\beta \geq 1.25\alpha$ and $\varepsilon \leq 0.75\alpha$ are good choices. In addition, the threshold σ is determined experimentally and $\sigma = 20$ is also a good choice.

3. SIMULATIONS

The experiments are conducted on 50 test images with size of 128×128 from IM-AGEMORE Cooperation [22]. A binary watermark length with length of 1024 is obtained by generating a zero-mean pseudo-random sequence with length of 1024, and then taking the sign of each data point of the sequence. The binary watermark is expanded into a ternary stream with length 1024×15 , and then modulated into the host images. Thirteen types of image processing attacks (listed in Table 1) including positive (*e.g.*, sharpening), negative (*e.g.*, blurring) and hybrid attacks, are applied to the test images, and thus totally 650 attacked images are obtained. The hiding factor is chosen as $\alpha = 0.5$, which yields good embedded picture quality. Fig. 5 demonstrates some typical images embedded with watermarks. The detection parameters ε and β are chosen experimentally as $\varepsilon = 0.2$ and $\beta = 0.7$. Note that the magnitude of an AC coefficient is generally related to its frequency band. The small coefficient corresponds to higher frequency band and its effect is at the detail of an image. Although the small coefficient in lower band may change a relative large value, it is very rare from experiences of our experiments. It is clear that the small coefficient causes very limited effect on quality of the watermarked image so that the image quality can be guaranteed.



Fig. 5. Typical images embedded with watermark.

The test images are used to evaluate the *single detector* and our proposed *dual detector* scheme. The comparison of the two detection schemes is in terms of false negative rate (missed detection rate) and false positive rate (false alarm rate). The former corresponds to robustness, and the later to false alarm. The two performances conflict each other. More specifically, in detection, when the detection threshold (ρ_t in Fig. 1) is set higher, the false alarm rate can be reduced, but the false negative rate will become higher. In real applications, a compromise needs to be taken by choosing an appropriate detec-

tion threshold value. Because the two measures conflict, we use the total error rate (the sum of the two error rates) as the performance metric. The smaller the total error rate, the better the system performance. Table 2 lists the total error rates of the two schemes for various values of detection threshold. It indicates the total error rate of our *dual detector* scheme is less than one half of the *single detector* scheme. The result can be confirmed from ROC (receiver operating curve) performance comparison in Fig. 6.

Table 2. Performance comparison of single detector and dual detector under various threshold values.

Methods	Criteria	Threshold values					
		0.025	0.05	0.1	0.2	0.3	0.4
Single Detector	Missed detection rate	0.068	0.114667	0.224	0.3733	0.42933	0.48133
	False alarm rate	0.21733	0.048	0	0	0	0
	Total error rate	0.28533	0.162667	0.224	0.3733	0.42933	0.48133
Dual Detector	Missed detection rate	0.00667	0.00667	0.012	0.05067	0.07067	0.12666
	False alarm rate	0.62533	0.45333	0.164	0.02533	0.00933	0.00266
	Total error rate	0.63200	0.46	0.176	0.07600	0.08000	0.12932

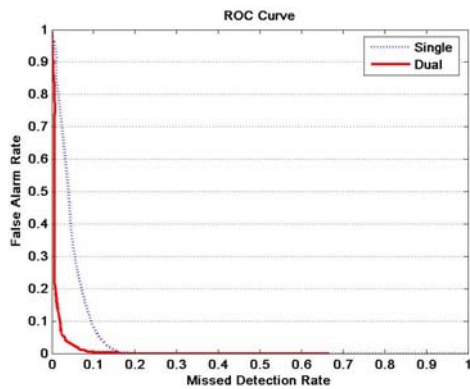


Fig. 6. The ROC performances of single detector and dual detector.

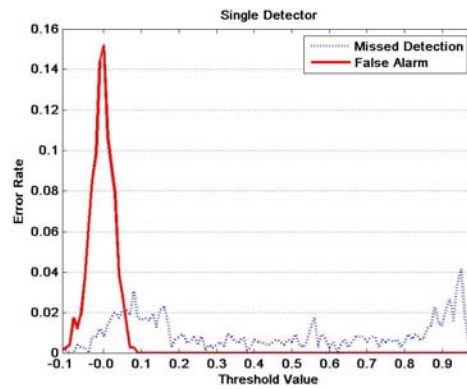


Fig. 7. The error rates vs. detection threshold values for single detector.

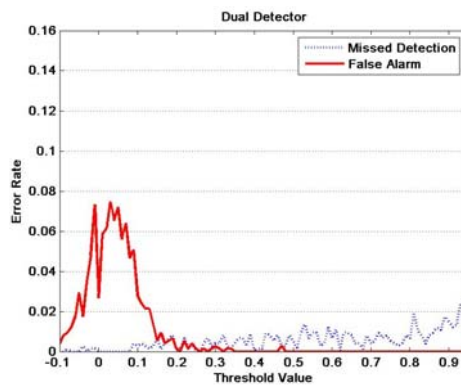


Fig. 8. The error rates vs. detection threshold values for dual detector.

Figs. 7 and 8 show the curves of the two error rates under various detection threshold values. The figures provide the cue for the selection of appropriate threshold values to meet the requirements of users. It is seen from Fig. 8 that if threshold is set in the range of 0.2 to 0.3, the *dual detector* gives approximate zero missed detection and false alarm rates. However, Fig. 8 indicates that the *single detector* definitely yields errors (either missed detection or false alarm or both) whatever the threshold values are chosen. Obviously, the *dual detector* is better than *single detector* even from the viewpoint of threshold selection.

4. CONCLUSIONS

A blind image watermarking technique based on the characteristics of amplitude attacks has been proposed. In the novel method, two detectors are designed which aim at extracting reliable transformed coefficients under positive attack and negative attack, respectively. The removal of unreliable coefficients is very useful to reduce the error of watermark extraction. The results indicate that our scheme performs much better than the single detector that uses all the transformed coefficients and does not consider the attack characteristics.

The system presented here is just for demonstrating the benefit of the novel detection scheme. It could be applied to other transformations such as discrete wavelet transform [26, 27]. Furthermore, the proposed detection scheme can be applied to any existing watermarking systems to further improve their performances. The major limitation of our scheme is that the determination of parameters values is performed experimentally. An automatic calculation mechanism for the parameters may be worth further investigating in the future.

REFERENCES

1. F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of IEEE*, Vol. 87, 1999, pp. 1079-1107.
2. I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers, Los Altos, CA, 2002.
3. S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, Boston, London, 2000.
4. M. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM System Journal*, Vol. 35, 1996, pp. 313-336.
5. N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures," in *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing*, 1996, pp. 2168-2171.
6. R. B. Wolfgang and E. J. Delp, "A watermark for digital images," in *Proceedings of International Conference on Image Processing*, Vol. 3, 1996, pp. 219-222.
7. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoan, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, Vol. 6, 1997, pp. 1673-1687.
8. C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models,"

- IEEE Journal on Selected Areas in Communications*, Vol. 16, 1998, pp. 529-539.
9. A. Piva, M. Barni, E. Bartoloni, and V. Cappellini, "DCT-based watermarking recovering without resorting to the uncorrupted original image," in *Proceedings of IEEE International Conference on Image Processing*, Vol. 1, 1997, pp. 520-523.
 10. C. T. Hsu and J. L. Wu, "Multiresolution watermarking for digital images," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, Vol. 45, 1998, pp. 1097-1101.
 11. S. H. Wang and Y. P. Lin, "Wavelet tree quantization for copyright protection," *IEEE Transactions on Image Processing*, Vol. 13, 2004, pp. 154-165.
 12. C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Transactions on Image Processing*, Vol. 10, 2001, pp. 1579-1592.
 13. C. W. Tang and H. M. Hang, "A feature-based robust digital image watermarking scheme," *IEEE Transactions on Signal Processing*, Vol. 51, 2003, pp. 950-959.
 14. A. M. Ahmed and D. D. Day, "Applications of the naturalness preserving transform to image watermarking and data hiding," *Digital Signal Processing*, Vol. 14, 2004, pp. 513-549.
 15. C. S. Lu, C. J. Sze, and H. Y. M. Liao, "Cocktail watermarking for digital image protection," *IEEE Transactions on Multimedia*, Vol. 2, 2000, pp. 209-224.
 16. Y. Wang and A. Pearlman, "Blind image data hiding based on self reference," *Pattern Recognition Letters*, Vol. 25, 2004, pp. 1681-1689.
 17. C. Jiang, M. Yu, S. Shi, X. Liu, and Y. D. Kim, "New blind image watermarking in DCT domain," in *Proceedings of International Conference on Signal Processing*, Vol. 2, 2002, pp. 1580-1583.
 18. M. K. Mihcak and R. Venkatesan, "Blind image watermarking via derivation and quantization of robust semi-global statistics," in *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing*, Vol. 4, 2002, pp. 3453-3456.
 19. J. J. Eggers, J. K. Su, and B. Girod, "Robustness of a blind image watermarking scheme," in *Proceedings of IEEE International Conference on Image Processing*, Vol. 3, 2000, pp. 17-20.
 20. Y. Hu, W. Q. Lid, Y. Deng, W. He, and J. Dai, "Readable watermarking algorithm based on wavelet tree quantization," in *Proceedings of International Conference on Communications, Circuits and Systems*, Vol. 1, 2004, pp. 579-583.
 21. <http://www.petitcolas.net/fabien/watermarking/stirmark/>.
 22. <http://www.imagemore.com.tw/>.
 23. C. J. Liao and C. H. Hsieh, "A new digital image watermarking method based on complementary detectors," in *Proceedings of the 17th Conference of Computer Vision, Graphics, and Image Processing*, Vol. E3-4, 2004.
 24. C. H. Hsieh, C. J. Liao, and J. C. Tsai, "Analysis of amplitude attack in image watermarking system," in *Proceedings of International Symposium on Communication*, 2005.
 25. C. H. Hsieh and C. J. Liao, "A novel image watermarking scheme based on amplitude attack," *Pattern Recognition*, Vol. 40, 2007, pp. 1342-1354.
 26. N. Kaewkamnerd and K. R. Rao, "Wavelet based image adaptive watermarking scheme," *Electronics Letters*, Vol. 36, 2000, pp. 312-313.

27. J. J. K. O. Ruanaidh, W. J. Dowling, and F. M. Boland, "Phase watermarking of digital images," in *Proceedings of IEEE International Conference on Image Processing*, Vol. 3, 1996, pp. 239-242.



Chin-Pan Huang (黃金本) was born in 1959 in Taiwan, R.O.C. He received the B.S. and M.S. degrees in Electrical Engineering from Chung Cheng Institute of Technology, Taiwan, in 1981, in 1985, respectively. In 1996, he received the Ph.D. degree in Electrical Engineering from University of Pittsburgh, Pittsburgh, PA, U.S.A. In 1996-2002, he was an associate scientist of Electronic System Division in Chung Shan Institute of Science and Technology. He then joined the department of Computer and Communication Engineering at Ming Chuan University in August 2002, and is currently an assistant professor there. His recent research interests include data compression, computer vision, digital image/signal processing, and pattern recognition.



Chi-Jen Liao (廖吉仁) was born in Keelung, Taiwan. He received the master degree in Department of Information Engineering in 2004 from I-Shou University (ISU), Taiwan, R.O.C., where he is currently working toward the Ph.D. degree. His major research interests include image processing, watermarking, color management and image quality evaluation.



Chaur-Heh Hsieh (謝朝和) received Ph.D. degree in Electrical Engineering in 1990 from Chung Cheng Institute of Technology (CCIT), Taiwan, R.O.C. In 1981, He joined the faculty of the Department of Electrical Engineering at CCIT, and became a professor in 1993. From 1996 he joined I-Shou University (ISU) as a full professor of Information Engineering Department. In 1997, He developed a research group for video and image processing at ISU. From 1999 to 2002, he served as the chairman of the department. He was a Visiting Scholar in the Department of Electrical Engineering at University of Washington from February to July in 2006. From 2007 he joined Ming Chuan University as a full professor of Computer and Communication Engineering Department. His research interests include content-based image/video retrieval, sport video analysis, video understanding, advanced video coding, image watermarking, statistical pattern recognition and visual inspection. He has published more than 150 papers in these subjects. Dr. Hsieh received Grade-A

Research Awards from National Science Council eleven times (from 1991 to 2001). In 2002, he received Outstanding Electrical Engineer Award, Kaohsiung Chapter of The Chinese Institute of Electrical Engineering Society. He is a reviewer of IEEE journals and conferences as well as other leading international journals. He has served on the program committee of several conferences and workshops. He is an IEEE senior member. He is a fellow of IET.