Improved autocorrelation function based watermarking with side information

Choong-Hoon Lee
Heung-Kyu Lee
Korea Advanced Institute of Science and Technology (KAIST)
Department of Computer Science and Advanced Information Technology Research Center (AITrc)
Guseong-Dong, Yuseong-Gu, Daejon, 305-701, Korea
E-mail: {chlee,hklee}@casaturn.kaist.ac.kr

Abstract. *We propose an improved autocorrelation function (ACF)-based image watermarking that is robust to combined geometric and removal attacks. ACF-based watermarking is thought of as one of the most effective watermarking schemes that resist geometric attacks. In this watermarking scheme, the autocorrelation peaks of the watermark play an important role for geometric attack estimation. The peaks, however, are vulnerable to attacks. The proposed scheme enhances the performance of ACF-based watermarking by improving the strength of the peaks. The information of an original image is used at the embedding time, so that the detector can extract strong autocorrelation peaks. Experimental results show that the proposed scheme yields better robustness than conventional ACF based watermarking against combined geometric-removal attacks.* © *2005 SPIE and IS&T.* [DOI: 10.1117/1.1868000]

1 Introduction

Recently, digital watermarking has attracted attention as a possible solution for the multimedia copyright protection.[1,2] Digital watermarking is a process of hiding copyright information in multimedia data. To be effectively used for the copyright protection, digital watermarking should satisfy the following requirements: unobtrusiveness and robustness. Unobtrusiveness means that watermark embedding should not affect the quality of data. Robustness refers to the requirement that embedded watermarks should be detected reliably even after some attacks.

In the digital watermarking world, geometric attacks are regarded as very strong and harmful attacks. In most watermarking schemes, including the spread spectrum watermarking,[3,4] the synchronization of an embedded watermark with the reference watermark is crucial for the watermark detection. Geometric attacks prevent watermark detection by desynchronizing the embedded watermark. Even slight rotation or scaling of the marked image can cause watermark detection failure if the watermark detector does not have a synchronization mechanism.

One watermarking method that handles geometric attacks is to embed a watermark into a geometric-invariant domain. The Fourier-Mellin-transform-based method[5,6] belongs to this approach. This method seems to provide a nice solution theoretically. The implementation, however, is quite difficult because the perfect inversion of the Fourier-Mellin transform is impossible. Due to the same reason, the quality of the marked image is poor.

Feature-based watermarking is another watermarking scheme that resists geometric attacks.[7,8] This method extracts geometric-invariant features, such as edges or corners, from an image and embeds a watermark according to the features. This method requires a stable feature extractor that always finds the same features even after the image has been processed. Such a feature extractor is not easy to design.

Template-based watermarking is also one of the watermarking schemes to address geometric attacks.[9,10] In this scheme, a template is embedded into a host image in addition to an actual watermark. The template does not contain copyright information, but is used to estimate the applied geometric transforms. The watermark is detected after inverting the geometric transforms. This method has two failure modes. Any detection failure of the template or watermark leads to watermark detection failure. Moreover, attackers can easily remove templates since the template has no security.[11]

Autocorrelation function (ACF)-based watermarking is yet another approach.[12–14] In this scheme, a periodic watermark pattern is embedded into an image. The periodic watermark makes periodic peaks in the ACF of the watermark. The geometric transforms that have been applied to the marked image are estimated by inspecting the pattern of the extracted peak. This scheme also has the two detection failure modes. For reliable watermark detection, both the autocorrelation AC peaks and the embedded watermark should survive attacks.

Watermarking systems are often required to resist combined geometric and removal attacks. The removal attacks refer to some processing that can remove or attenuate an embedded watermark signal. The printing-scanning process, which is one of the most popular geometric attacks, is also a kind of combined attack. During the printing-scanning process, slight rotation or scaling of the image is inevitable. At the same time, analog-to-digital (A/D) and digital-to-analog (D/A) conversions, which are a kind of removal attack, are also applied. Thus, an image is affected by both the geometric attacks and removal attacks during

Paper 03066 received May 20, 2003; revised manuscript received Feb. 23, 2004; accepted for publication May 10, 2004; published online Mar. 4, 2005.
1017-9909/2005/$22.00 © 2005 SPIE and IS&T.

the printing-scanning process. Another example is lossy compression. Since multimedia data have high capacity, they are generally compressed by a lossy algorithm to be stored or transmitted. Geometrically distorted images are also often stored after lossy compression. Lossy compression is also a kind of removal attack.

The watermarking schemes already introduced resist geometric attacks well. Nevertheless, most of them show poor robustness against combined geometric-removal attacks. Although ACF-based watermarking is known as the most effective method against such attacks,[15] it does not yet show satisfactory performance.

In this paper, we propose an improved ACF-based watermarking that is robust to combined geometric-removal attacks. A problem of ACF-based watermarking is that the AC peaks are not strong enough. Since the AC peaks are more vulnerable than an embedded watermark to attacks, the overall performance of an ACF-based watermarking is more dependent on the AC peaks. In this paper, we improve the robustness of ACF-based watermarking by enhancing the strength of the AC peaks. To achieve this goal, the proposed scheme uses the watermarking with a side information mechanism.[16] Contrary to conventional ACF watermarking, which simply adds a periodic watermark to a host image, the proposed scheme uses information of the host image more actively at the embedding time, so that the detector can achieve stronger AC peaks.

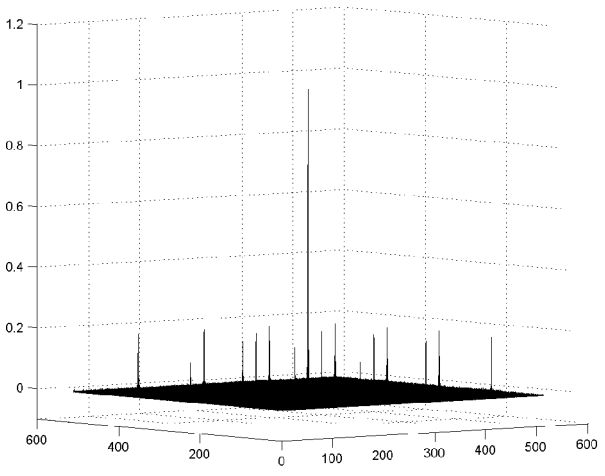
This paper is organized as follows. Section 2 briefly describes the problem of ACF-based watermarking and the basic idea of the proposed scheme to overcome it. Section 3 describes the detailed algorithm of the proposed method. Section 4 presents the experimental results showing that the proposed scheme provides stronger AC peaks and yields better detection results than previous ACF-based watermarking schemes. Finally, Sec. 5 provides concluding remarks.

2 Problem Statement and Basic Idea

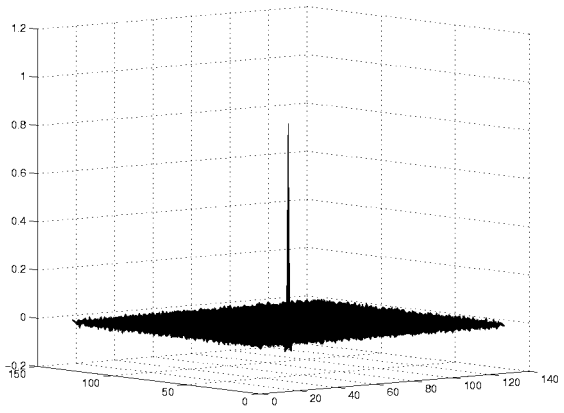
The weak point of ACF-based watermarking is the vulnerable AC peaks. Figure 1 shows a comparison of AC peaks and watermark detector response. For this test, a basic watermark pattern is generated using spread spectrum coding[3] and is periodically embedded into an image. The embedded watermark is extracted using a Wiener filter[17], and the AC peaks and detector response are examined. The figure shows that the AC peaks have much lower strength than the detector response. [The central peak in Fig. 1(a) is always 1 because it is the zero-offset AC.]

The weak AC peaks make ACF-based watermarking scheme less robust to combined geometric-removal attacks. Suppose a removal attack that is not strong enough to remove embedded watermarks, but is strong enough to delete AC peaks. If the removal attack is applied to the marked image that has been slightly rotated, then the watermark detection will fail due to the failure in the geometric attack estimation, even though the watermark signal still remains in the image. To avoid this kind of situation, we must improve the robustness of AC peaks.

To explain the basic idea of the proposed scheme, we must look into the simple mathematical model of the ACF of an extracted watermark at the detection process. It can be modeled as



(a) Autocorrelation peaks



(b) Detector Response

Fig. 1 AC peaks versus detector response.

$$\langle w+n, w+n\rangle = \langle w,w\rangle + 2\langle w,n\rangle + \langle n,n\rangle, \tag{1}$$

where $\langle\ \rangle$ denotes correlation operator, $w+n$ is the extracted watermark signal, w is the embedded watermark signal, and n is the watermark estimation error of the watermark extractor. Since n has no periodicity, only $\langle w,w\rangle$ is a meaningful term in Eq. (1). The other terms are interferences.

The proposed method improves the robustness of AC peaks by reducing the interferences introduced by n. This can be realized by adopting watermarking with a side information mechanism. Using the watermark extractor information and an original image, the watermark embedder can approximately predict the estimation error n that will be extracted by the detector. By processing the predicted signal to have high AC, the estimation error n also becomes meaningful for achieving strong AC peaks.

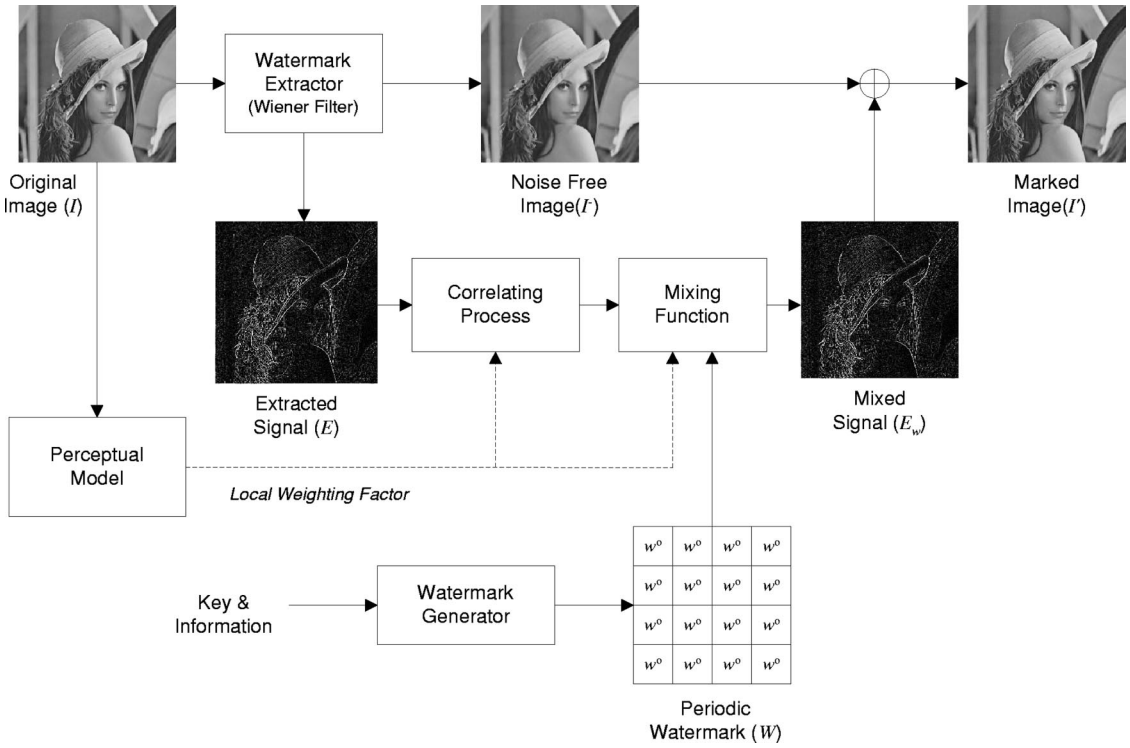


Fig. 2 Watermark embedding procedure.

3 Proposed Algorithm

3.1 *Watermark Embedding*

Figure 2 shows the proposed embedding procedure. Instead of simple addition of a periodic watermark to an original image, the proposed method uses the original image more sophisticatedly during the embedding procedure. The detailed procedure is as follows.

1. A signal E is extracted from an original image I of size $X\times Y$ using the watermark extractor. In the proposed scheme, the watermark extractor uses the Wiener filter:
$$I^-(x,y)=\mu(x,y)+\frac{\sigma^2(x,y)-s^2}{\sigma^2(x,y)}[I(x,y)-\mu(x,y)], \quad (2)$$
where $\mu(x,y)$ and $\sigma^2(x,y)$ are the local mean and local variance of the original image, respectively; and s^2 is the noise variance. Since the noise variance is not available here, we use the average of the local variances for s^2. The extracted signal E is given by
$$E=I-I^-. \quad (3)$$
2. The extracted signal E is segmented into blocks $(\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_n)$ of size $M\times M$.
3. The segmented blocks $(\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_n)$ are modified into the blocks $(\mathbf{v}_1',\mathbf{v}_2',\ldots,\mathbf{v}_N')$ that have high correlation between each other. It generates a highly autocorrelated signal E' that consists of the modified blocks. We explain this step in detail later.
4. A basic watermark pattern W° of the size $M\times M$ is generated with a user key. In this paper, we use a pseudorandom number sequence that follows $N(0,1)$ (standard normal distribution) for the basic watermark pattern.
5. The basic watermark pattern is repeated. It generates a periodic watermark W of the same size $(X\times Y)$ as the original image.
6. E' and W are mixed into E_w by
$$E_w(x,y)=\alpha_e E'(x,y)+\alpha_w\lambda(x,y)W(x,y), \quad (4)$$
where α_e and α_w are global weighting factors, and $\lambda(\cdot)$ denotes local weighting factor. We use noise visibility function (NVF)-based local weighting factor[18]:
$$\lambda=(1-\mathrm{NVF})S+\mathrm{NVF}S_1, \quad (5)$$
where S and S_1 are scaling parameters. The NVF is described by
$$\mathrm{NVF}(x,y)=\frac{1}{1+(D/\sigma^2_{\max})\sigma^2(x,y)}, \quad (6)$$
where $D\in[50,100]$, and $\sigma^2_{\max}$ is the maximum of the local variance.
7. The marked image I' is obtained by replacing the originally extracted signal E in the original image I with the mixed signal E_w:
$$I'(x,y)=I^-(x,y)+E_w(x,y). \quad (7)$$

Now, we explain the correlating process in step 3. Figure 3 describes the geometric interpretation of the process. In the figure, each vector point denotes each segmented block. A reference vector $\mathbf{R}$ is generated first, and the segmented vectors $(\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_N)$ are projected to new vectors $(\mathbf{v}_1',\mathbf{v}_2',\ldots,\mathbf{v}_N')$ that have small angles with the reference

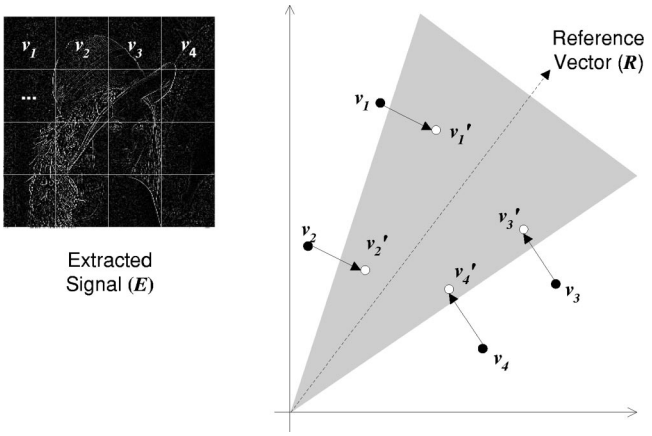


Fig. 3 Geometric interpretation of the correlating process.

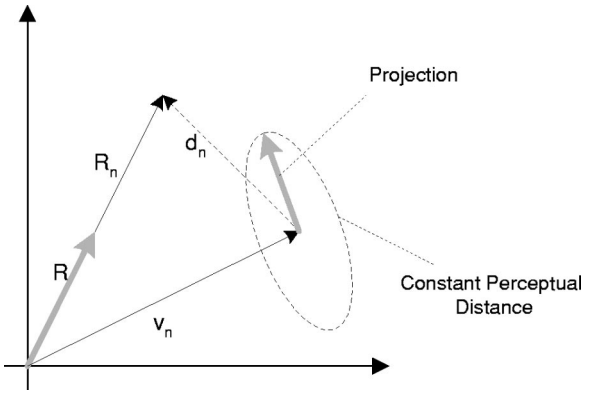


Fig. 4 Projection process for $\mathbf{v}_n$.

vector $\mathbf{R}$. This projection increases the correlation between $\mathbf{R}$ and each vector $\mathbf{v}_n'$.[19] Accordingly, the correlation between each vector also increases.

For an efficient correlating process, the reference vector should be selected carefully. If it is selected without consideration of the distribution of the segmented vectors, then the high correlation may not be achieved without excessive modification distortion.

The reference vector $\mathbf{R}$ is generated as follows. First, a bipolar vector is created for each segmented vector $\mathbf{v}_n$ by bipolar mapping:

$$b_n(i,j)=\begin{cases}1 & \text{if } \mathbf{v}_n(i,j)>0\\ 0 & \text{else if } \mathbf{v}_n(i,j)=0\\ -1 & \text{otherwise}\end{cases}. \tag{8}$$

The reference vector $\mathbf{R}$ is generated by accumulating the bipolar vectors as

$$\mathbf{R}(i,j)=\sum_{n=1}^{N} b_n(i,j). \tag{9}$$

The generated reference vector reflects the distribution of the segmented vectors. For example, if the n'th element of the reference vector has positive value, then the segmented vectors are distributed more in the positive direction along the n'th axis. Thus, the reference vector has the direction to which majority of the segmented vectors are distributed. The correlating process can be performed with minor distortion with the reference vector.

The projections are performed as follows. For each vector $\mathbf{v}_n$, the reference vector is modified to have the same length as $\mathbf{v}_n$ while keeping the original vector direction. This process is described as

$$\mathbf{R}_n=|\mathbf{v}_n|\cdot\frac{\mathbf{R}}{|\mathbf{R}|}. \tag{10}$$

Then, we have the difference vector between $\mathbf{R}_n$ and $\mathbf{v}_n$:

$$\mathbf{d}_n=\mathbf{R}_n-\mathbf{v}_n. \tag{11}$$

The segmented vector $\mathbf{v}_n$ is projected to $\mathbf{v}_n'$ by

$$\mathbf{v}_n'(i,j)=\mathbf{v}_n(i,j)+\alpha_d\lambda_n(i,j)\mathbf{d}_n(i,j), \tag{12}$$

where α_d and λ_n are global and local weighting factors, respectively. We use the NVF-based local weighting factor also here, λ is defined in the entire image as Eq. (5), and λ_n is the corresponding segment of $\mathbf{v}_n$ in λ.

Figure 4 describes how a segmented vector is projected. By the effect of the local weighting factor, the vector is projected not in the direction of the difference vector $\mathbf{d}_n$ but in the direction of the vector in the ellipse.

3.2 *Watermark Detection*

Figure 5 shows the watermark detection procedure. The detection procedure is as follows:

1. The watermark is extracted from a marked image with the Wiener filter as in embedding step 1. The extracted watermark E_w' may be a corrupted version of the mixed signal E_w.
2. The ACF of the extracted watermark is calculated. The ACF of a signal can be expressed as the convolution of the signal and its geometric inverse form. Thus, the fast Fourier transform (FFT) and the inverse FFT (IFFT) can be used to calculate the ACF to reduce the computing time. The normalized ACF is calculated by
$$\mathrm{ACF}=\frac{\mathrm{IFFT}[\mathrm{FFT}(E_w')\cdot\mathrm{FFT}(E_w')^*]}{|E_w'|^2}, \tag{13}$$
where * denotes complex conjugate operation.
3. The extracted watermark signal E_w' is restored to its original geometry using the AC peak pattern.
4. The restored signal is segmented into blocks of the size $M\times M$, and all segments are accumulated. (The accumulated block is denoted by E_f.)
5. A reference watermark pattern W_r of the size $M\times M$ is generated with user key as in the embedding procedure.
6. The watermark is detected by calculating the normalized correlation (NC) between the accumulated signal

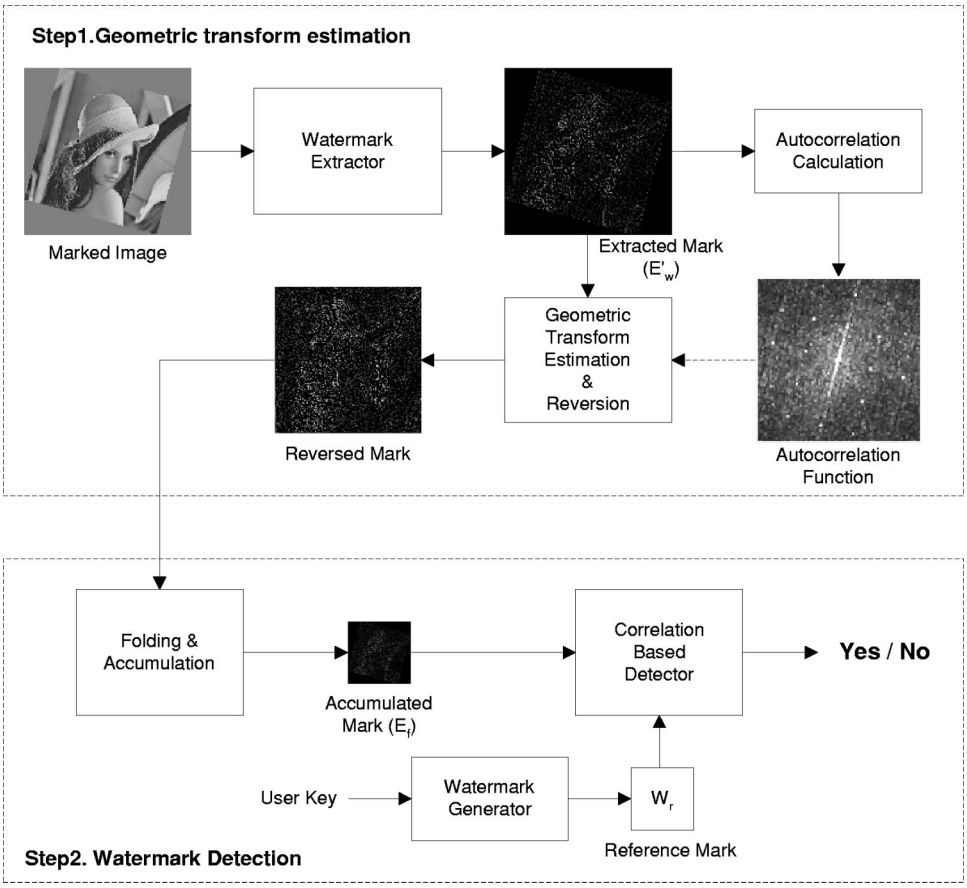


Fig. 5 Watermark detection procedure.

E_f and reference watermark W_r. To handle shift attacks, the correlation between E_f and W_r should be calculated over all possible shift. This process can be performed with reduced time complexity using the FFT as in the step 2 as

$$\mathrm{NC}=\frac{\mathrm{IFFT}(\mathrm{FFT}(E_f)\cdot\mathrm{FFT}(W_r)^*)}{|E_f||W_r|}. \tag{14}$$

Since only one shift is valid, only one correlation value is high in NC if E_f is the correct watermark. Thus, the maximum value in NC is selected for the detector response (DR) and the final decision of the detection are made by

$$\mathrm{DR}=\max_{i,j}[\mathrm{NC}(i,j)]>\tau, \tag{15}$$

where τ is the detection threshold defined by

$$\tau=\mu_{\mathrm{nc}}+\alpha_{\mathrm{nc}}\sigma_{\mathrm{nc}}, \tag{16}$$

where μ_{nc} and σ_{nc} are the average and standard deviation of NC, respectively, and α_{nc} is a constant.

The ACF of the extracted watermark often contains high correlation values that are not correct peaks. For example, if the image is rotated, the border of the image forms a high AC line. We must find the correct peak information among these high AC values.

The peaks are detected in two steps. First, we find local maximums in the ACF. A small window slides over the entire ACF, and the local maximum in each window is selected. This process removes many high correlation values that are not correct peaks. After this preprocessing, we have candidates for the peaks. In the second step, we select correct peaks among the candidates by

$$\mathrm{ACF}'(x,y)>\mu_{\mathrm{acf}}+\alpha_{\mathrm{acf}}\sigma_{\mathrm{acf}}, \tag{17}$$

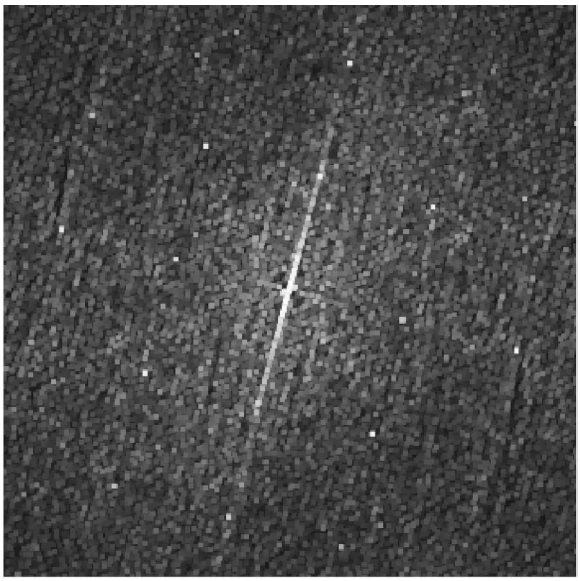
where ACF′ is the result of local maximum selection; μ_{acf} and σ_{acf} denote the average and standard deviation of the ACF, respectively; and α_{acf} is a constant.

Figure 6 shows a peak detection example. The peak was detected from the marked ''Lena'' image, which had been compressed (JPEG quality factor=50%) and rotated by 15 deg. In the figure, the calculated ACF has many high correlation values besides correct peaks. The proposed peak detector clearly detected the correct peaks from the ACF.

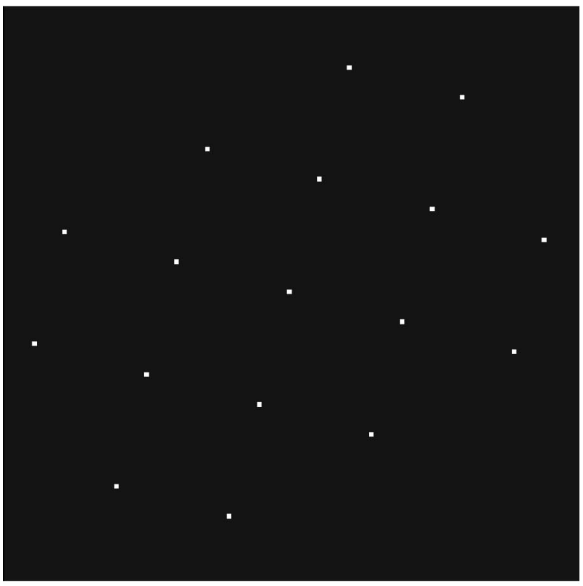
4 Experimental Results

4.1 *Test Environments*

To test the improvement by the proposed scheme, we compared the proposed scheme with an additive ACF watermarking scheme. Although previous ACF-based water-



(a) Autocorrelation function of extracted mark



(b) Detected peaks

Fig. 6 Peak detection example from the marked "Lena" image [JPEG compressed ($Q=50$) and 15 deg rotated].

marking schemes use various masking models and watermark patterns, they follow the general additive embedding model:

$$I' = I + \alpha \lambda W, \tag{18}$$

where α and λ denote the global and local weighting function, respectively. To create the same test environment, the same watermark pattern and masking function as described in Sec. 3.1 are used for both schemes.

Five images ("Lena," "F16," "Peppers," "Fishing Boats," and "Pentagon") with a size of 512×512 were used for the experiments. The size of the basic watermark block was set to 128×128.

4.2 *Threshold Selection and Analysis*

To minimize the watermark detection error, the thresholds should be selected carefully. Generally, a false positive detection error is regarded as more serious error than a false negative error. A false positive error in the final detection step in Eq. (15) results in a false positive watermark detection error. A false positive error in the AC peak detection, however, results in the false negative error since it causes error only in the geometric attack estimation. Moreover, many false peaks are removed during the local maximum finding step in the AC peak detection process, and a small number of the false peaks may not affect geometric attack estimation. Therefore, the threshold for the detector response was set to higher value than for the AC peaks. For the experiments, α_{nc} in Eq. (16) and α_{acf} in Eq. (17) were set to 6 and 3.5, respectively.

We analyze the false positive error rates of the selected threshold parameters. For the analysis, we must determine the distribution of NC in Eq. (14) and ACF in Eq. (13). Since linear correlation of two random signals can be considered to be a mean of random variables [each random variable (RV) is the product of two random variables], as in Eq. (19), by the central limit theorem, linear correlation (LC) has Gaussian distribution.[20]

$$\mathrm{LC} = \frac{1}{N}\sum_{i=1}^{N} \mathrm{RV}_1(i)\mathrm{RV}_2(i). \tag{19}$$

Although normalized correlation has the normalization term, we assume that the central limit theorem also holds here. Thus, we assume that NC and ACF of the unmarked image to follow a Gaussian distribution. Figure 7 shows the distribution of NC and ACF for the unmarked "Lena" image. The figure shows that both data follow the Gaussian distribution. With the Gaussian distribution model, the false positive error rate of the watermark detection can be approximately calculated by

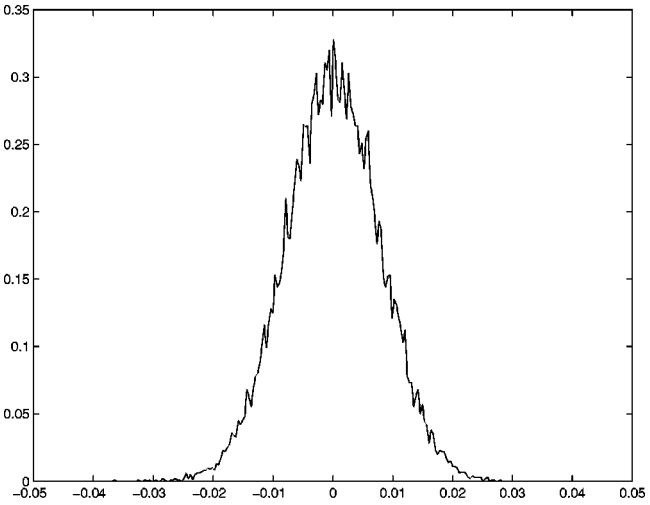
$$P_{\mathrm{fp}} = \int_{\mu_{\mathrm{nc}}+\alpha_{\mathrm{nc}}\sigma_{\mathrm{nc}}}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{nc}}} \exp\left[\frac{-(x-\mu_{\mathrm{nc}})^2}{2\sigma_{\mathrm{nc}}^2}\right] \mathrm{d}x$$

$$= \int_{\alpha_{\mathrm{nc}}}^{\infty} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-x^2}{2}\right) \mathrm{d}x. \tag{20}$$

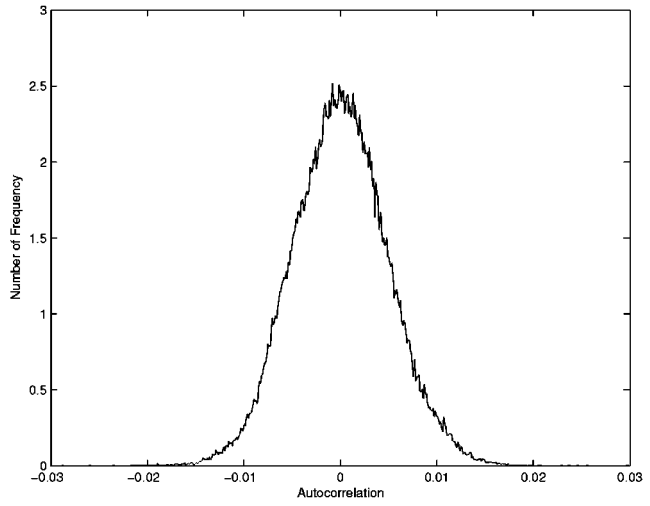
When $\alpha_{\mathrm{nc}}=6$, the false positive error probability of the watermark detection is about 9.87×10^{-10}, which is low enough for general watermarking applications. In the same way, the false positive error probability of the AC peak detection is about 2.33×10^{-4}. Figure 8 shows NC, ACF, and their thresholds for a marked "Lena" image after a JPEG 50% compression attack.

4.3 *Strength of Autocorrelation Peaks*

First, we tested the strength of the AC peaks. The test images were marked by both schemes with variant embedding

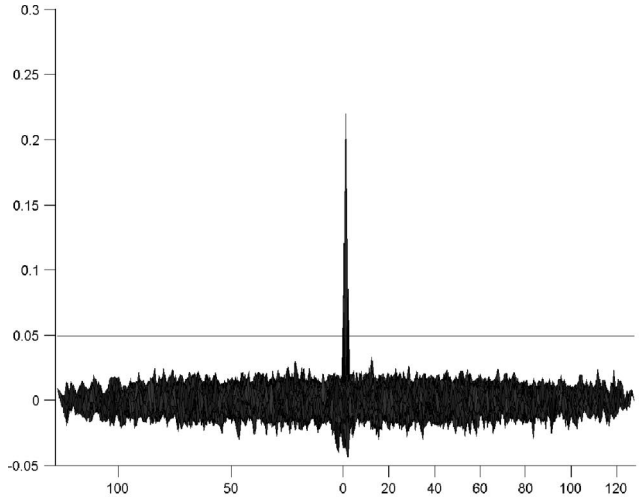


(a) NC

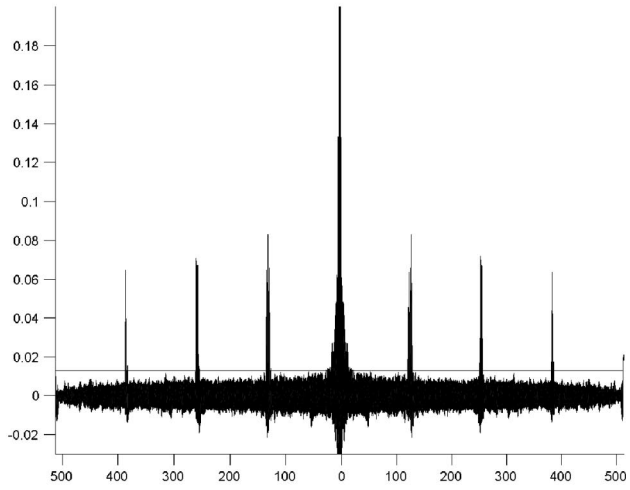


(b) AF

Fig. 7 Distribution of NC and ACF (AF) of the unmarked "Lena" image.



(a) Detector response threshold



(b) Autocorrelation peak threshold

Fig. 8 Threshold examples for watermark detection and AC peak detection for a marked "Lena" image after JPEG 50% compression.

strengths. The average ACs on correct peaks except the center peak were shown in Fig. 9. In the figures, the horizontal axis represents the marked image quality [peak SNR (PSNR)] and the vertical axis represents the average AC value of the peaks. The PSNR values of the marked images were about from 35 to 44 dB. The figure shows that the proposed scheme yields much higher AC peak values than the additive scheme when the qualities of the marked images are same.

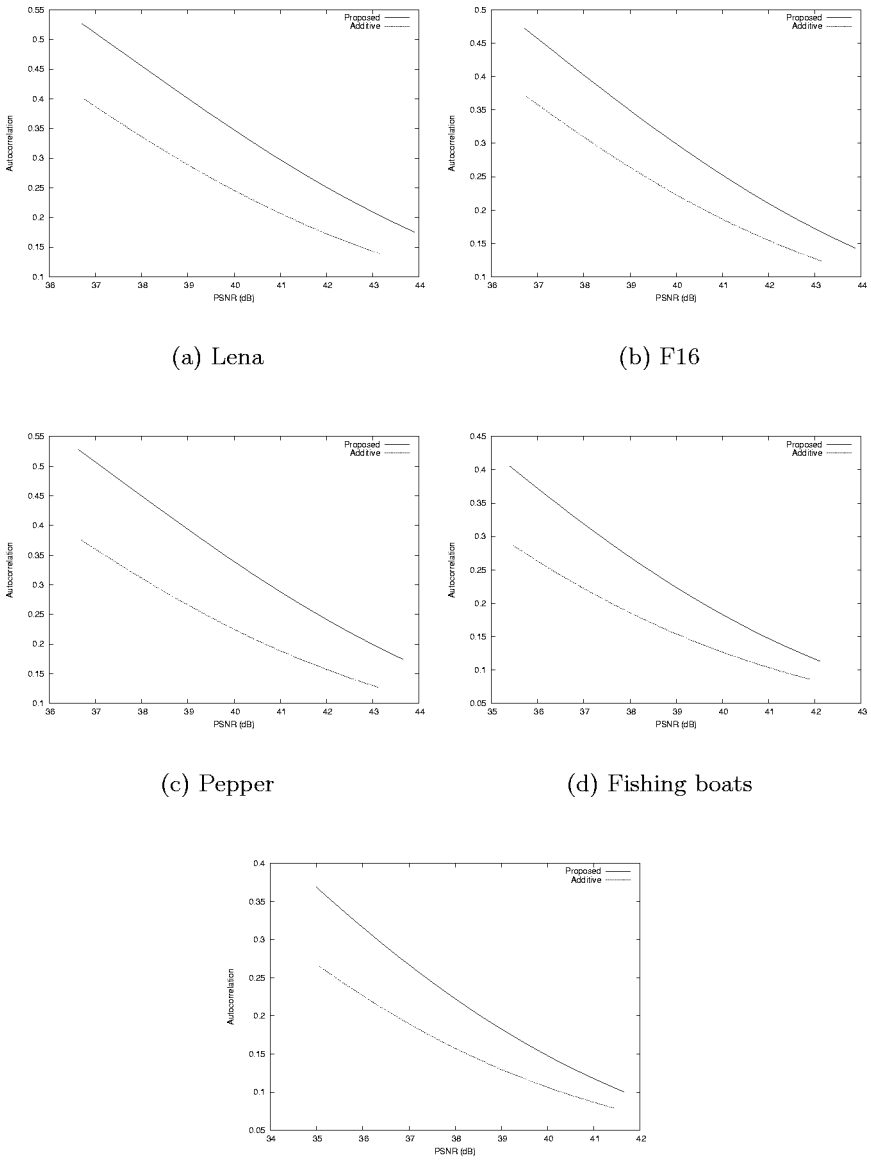
4.4 *Watermark Detection Test*

4.4.1 *Detection test after stirmark attacks*

In the previous section, we observed that the strengths of the AC peaks are much improved by the proposed scheme. Now, we must test whether this achievement results in actual detection performance improvement. For the test, each image was marked by both schemes to 38 dB in PSNR. The stirmark benchmark software[21] was used for the attacks. The stirmark is one of the most well known watermark benchmarking tools, which provides several watermark attacks as follows. (The number in each parenthesis is the number of attacks in each category.)

1. *Global geometric attacks (70)*: row column removing (5), cropping (9), flip (1), linear geometric distortion (3), aspect ratio change (8), rotation (16), rotation +scale (16), scale (6), and shearing (6).
2. *Removal attacks (19)*: median filter (3), Gaussian filter (1), sharpening (1), color reduction (1), frequency mode Laplacian removal attack (1), and JPEG compression (12).
3. *Nonlinear geometric attacks (1)*: random bending attack (1).

In this experiment, the watermark was detected after the



(a) Lena (b) F16

(c) Pepper (d) Fishing boats

(e) Pentagon

Fig. 9 Average normalized AC on correct peaks.

marked images had been attacked by the preceding attacks. The applied geometric attacks were estimated by finding the periods and angles of peaks in two different directions. For example, to estimate aspect ratio change, we should find the periods of peaks in the horizontal and vertical directions.

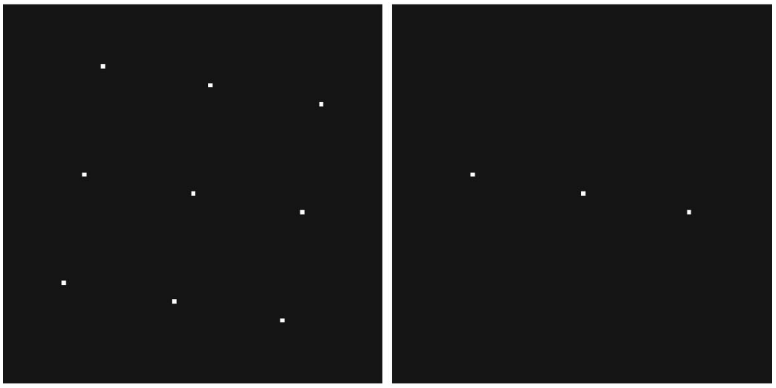
Table 1 shows the detection results after the stirmark attacks. Both schemes yielded good detection results. The proposed scheme failed in detection in only five tests among all tests, while the additive scheme failed in six tests. The proposed scheme showed better results against the geometric attacks than the additive scheme. The proposed scheme failed in three JPEG 10% compression (''Boats,'' ''F16,'' and ''Peppers'') and two random bending attacks (''Boats'' and ''Pentagon''). No detection failure occurred in global geometric attacks. On the other hand, the additive scheme failed in three rotation test (''Lena,'' ''Boats,'' and ''Pentagon'') and three random bending attacks (''Boats,'' ''Lena,'' and ''Pentagon'').

Table 1 Number of successful detection after stirmark attacks. (Total number of attacks for each image is 90.)

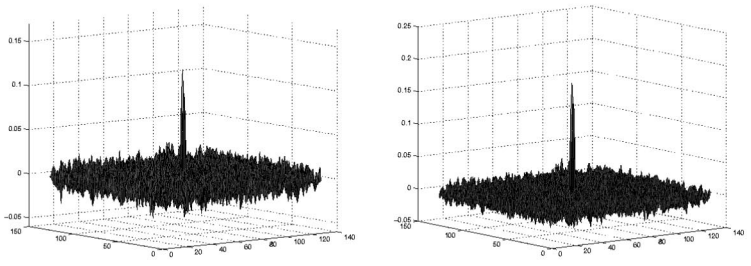
	''Lena''	''F16''	''Peppers''	''Boats''	''Pentagon''
Proposed	90	89	89	88	89
Additive	88	90	90	88	88

In the results, the proposed scheme shows slightly lower robustness to JPEG compression than the additive scheme. Because the correlating process also introduces distortion to the image, the watermark embedding strength of the proposed scheme should be little lower than that of the additive scheme to get the same marked image quality. As the

(a) Attacked Images



(b) Detected Peaks



(c) Detector Response

Fig. 10 Test examples after 100deg rotation and JPEG 50% compression of the marked ''Peppers'' image (left figures, proposed scheme; right figures, additive scheme).

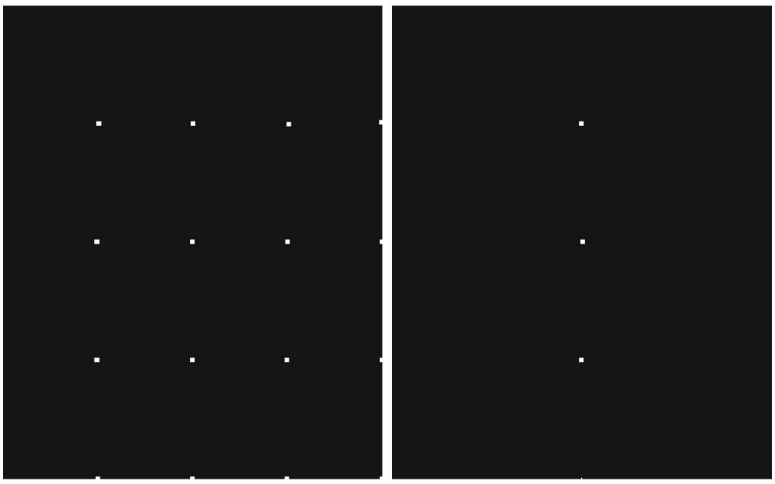
result, the detector response of the proposed scheme is slightly lower than that of the additive scheme. Nevertheless, the proposed scheme resisted JPEG compression to a 15% quality factor for all images and 10% quality for the ''Lena'' and ''Pentagon'' images. A JPEG compression quality of 15% is a high compression rate. The compressed images with this rate show poor visual quality. Thus, we think that it is sufficiently high robustness for general watermarking applications.

4.4.2 *Detection test after combined geometric-removal attacks*

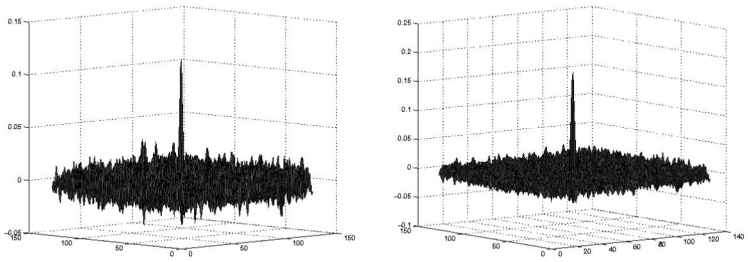
In this experiment, the marked images were first attacked by the global geometric attacks of the stirmark software and then compressed by a JPEG quality factor of 50%. The watermark detection test was performed on the attacked images.

Figures 10, 11, and 12 show detection examples after

(a) Test Image



(b) Detected Peaks



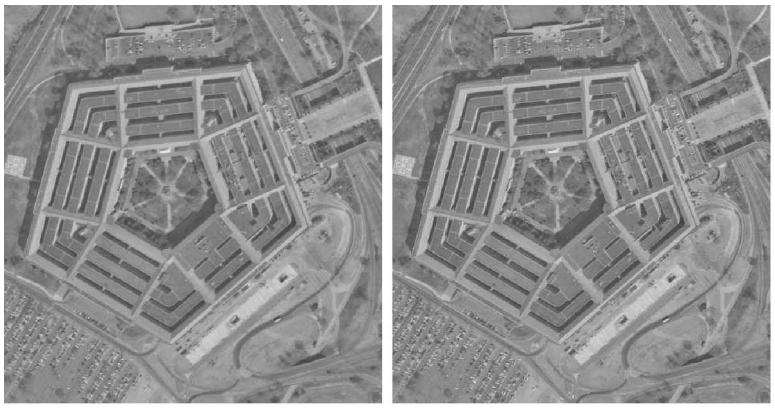
(c) Detector Response

Fig. 11 Test examples aspect ratio change (1:0.8) and JPEG 50% compression of the "F16" image (left figures, proposed scheme; right figures, additive scheme).

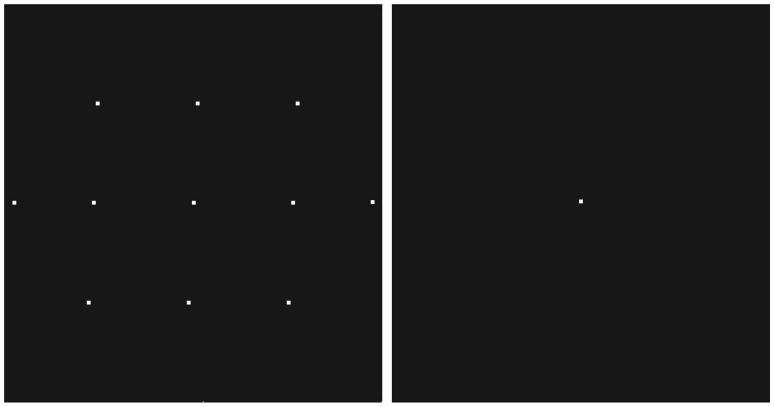
JPEG compression combined rotation, aspect ratio change, and shearing, respectively.

Figures 10(b), 11(b), and 12(b) show the peak detection result. In all tests, the proposed scheme shows clearer peak detection results. The proposed scheme can estimate the geometric transform easily with the detected peak pattern. On the other hand, the additive scheme fails to estimate the geometric transform in all tests.

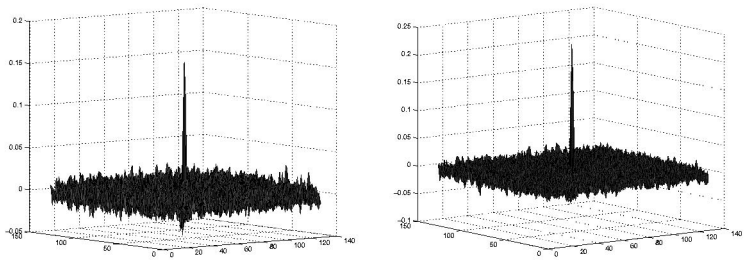
Figures 10(c), 11(c), and 12(c) show the detector responses after the inverse geometric transforms. The figures



(a) Test Image



(b) Detected Peaks



(c) Detector Response

Fig. 12 Test examples after shearing (5% in the horizontal direction) and JPEG 50% compression of the ''Pentagon'' image (left figures, proposed scheme; right figures, additive scheme).

show that the embedded watermarks still remain in the attacked images in both schemes in all tests. Although the detector responses of the proposed scheme are slightly lower than those of the additive scheme, they have sufficiently high values.

In these examples, the proposed scheme successfully detects the watermarks. The additive scheme, however, cannot detect the watermarks although the embedded watermarks still remain in the images.

The overall detection results after the combined attacks are shown in Table 2. As shown in the table, the proposed scheme showed much better detection results than the additive scheme. The additive scheme failed to detect watermark in 120 tests among 350 tests, while the proposed scheme failed in only 56 tests. In some tests, for example, the linear geometric attacks of ''Pentagon'' image, the additive scheme showed better results than proposed scheme. In these cases, the additive scheme also failed in geometric

Table 2 Watermark detection results after stirmark geometric attacks and JPEG 50% compression. (Total number of attacks for each image is 70.)

	Proposed					Additive				
Attack	"Lena"	"F16"	"Peppers"	"Boats"	"Pentagon"	"Lena"	"F16"	"Peppers"	"Boats"	"Pentagon"
Row-col. remove	5	4	5	5	5	4	5	5	3	3
Cropping	9	9	9	9	9	9	9	9	9	9
Flip	1	1	1	1	1	1	1	1	1	1
Linear	3	2	3	2	0	3	3	3	1	2
Aspect ratio	8	8	8	7	6	7	6	8	5	3
Rotation	16	11	15	10	9	12	5	14	5	3
Rotation scale	16	16	14	10	6	10	6	15	6	4
Scale	5	4	5	4	5	5	3	5	2	3
Shearing	6	5	6	5	5	6	4	6	2	3
Total	69	60	66	53	46	57	42	66	34	31
	294					230				

attack estimation. Since the linear geometric attacks modify the image geometry very slightly, the additive scheme could detect the watermark without the inverse geometric transform due to its slightly higher detector response. Except in such special cases, the proposed scheme provided much better detection results than the additive scheme.

5 Conclusion

The vulnerable AC peaks are the major problem of ACF-based watermarking. The proposed method provides more robust AC peaks by adopting watermarking with side information mechanism in the embedding process. By sophisticated use of the information of an original image and the detector structure at the embedding time, the detector can obtain strong peaks. Experimental results showed that the proposed scheme provided stronger AC peaks than the additive method. In the detection tests using the stirmark attacks, the proposed scheme yielded better detection results than the additive scheme against geometric attacks, while both scheme showed pretty good results. In the experiment with JPEG combined stirmark geometric attacks, the proposed scheme showed much better detection results (about 28% more detection successes) than the additive scheme.

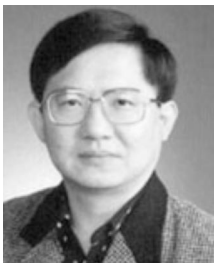
Acknowledgements

This work was supported by the Korea Science and Engineering Foundation (KOSEF) through the Advanced Information Technology Research Center (AITrc).

References

1. N. Memon and P. W. Wong, "Protecting digital media content," *Commun. ACM* **41**(7), 35–43 (1998).
2. G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data: a state-of-the-art overview," *IEEE Signal Process. Mag.* **17**(5), 20–46 (2000).
3. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.* **6**(12), 1673–1687 (1997).
4. F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *IEEE Signal Process. Mag.* **66**(3), 283–301 (1998).
5. J. J. K. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *IEEE Signal Process. Mag.* **66**(3), 303–317 (1998).
6. C.-Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and L. M. Yui, "Rotation, scale, and translation resilient watermarking for images," *IEEE Trans. Image Process.* **10**(5), 767–782 (2001).
7. M. Kutter, S. K. Bhattacharjee, and T. Ebrahimi, "Towards second generation watermarking schemes," in *Proc. IEEE Int. Conf. of Image Processing 1999*, Vol. 1, pp. 320–323, Kobe, Japan (1999).
8. P. Bas and J.-M. Chassery, "Robust watermarking based on the warping of predefined triangular patterns," in *Security and Watermarking of Multimedia Contents II*, *Proc. SPIE* **3971**, 99–109 (2000).
9. S. Pereira, J. J. K. O. Ruanaidh, F. Deguillaume, G. Csurka, and T. Pun, "Template based recovery of Fourier-based watermarks using log-polar and log-log maps," in *Proc. IEEE Intl. Conf. on Multimedia Computing and Systems*, Vol. 1, pp. 870–874 (1999).
10. S. Pereira and T. Pun, "Fast robust template matching for affine resistant image watermarking," in *Proc. Intl. Workshop on Information Hiding*, Vol. LNCS 1768 of *Lecture Notes in Computer Science*, pp. 200–210 (Oct. 1999).
11. A. Herrigel, S. Voloshynovskiy, and Y. Rytsar, "The watermark template attack," in *Security and Watermarking of Multimedia Contents III*, *Proc. SPIE* **4314**, 394–405 (2001).
12. M. Kutter, "Watermarking resisting to translation, rotation, and scaling," *Proc. SPIE* **3528**, 423–431 (1998).
13. P.-C. Su and C.-C. J. Kuo, "Synchronized detection of the block-based watermark with invisible grid embedding," in *Security and Watermarking of Multimedia Contents III*, *Proc. SPIE* **4314**, 406–417 (2001).
14. S. Voloshynovskiy, F. Deguillaume, and T. Pun, "Content adaptive watermarking based on a stochastic multiresolution image modeling," in *Proc. 10th Eur. Signal Processing Conf. (EUSIPCO'2000)*, European Association for Signal, Speech, and Image Processing (EURASIP), Tampere, Finland (2000).
15. S. Voloshynovskiy, F. Deguillaume, and T. Pun, "Multibit digital watermarking robust against local nonlinear geometric distortions," in *Proc. 2001 IEEE Int. Conf. of Image Processing (ICIP 2001)*, Vol. 3, pp. 999–1002, Thessaloniki, Greece (2001).
16. I. J. Cox, M. L. Miller, and A. L. McKellips, "Watermarking as communications with side information," *Proc. IEEE* **87**(7), 1127–1141 (1999).
17. J. S. Lim, *Two-Dimensional Signal and Image Processing*, Prentice Hall, Upper Saddle River, NJ (1990).
18. S. Voloshynovskiy, A. Herrigel, N. Baumgartner, and T. Pun, "A stochastic approach to content adaptive digital image watermarking," in *Proc. Int. Workshop on Information Hiding*, Vol. LNCS 1768 of *Lecture Notes in Computer Science*, pp. 212–236, Springer Verlag, Dresden, Germany (1999).
19. I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, Morgan Kaufman Publishers, San Francisco (2002).
20. M. L. Miller, I. J. Cox, and J. A. Bloom, "Informed embedding exploiting image and detector information during watermark insertion," in *Proc. IEEE Intl. Conf. on Image Processing*, Vol. 3, pp. 1–4 (2000).
21. http://www.petitcolas.net/fabien/watermarking/stirmark31/index.html.

Choong-Hoon Lee received his BE degree in computer engineering in 1996 from Dongguk University, Seoul, Korea, and his MS and PhD degrees in computer science from the Korea Advanced Institute of Science and Technology (KAIST), Daejon, Korea, where he is currently a post-doctoral researcher. His research interests are digital watermarking, digital right management (DRM), and image and video coding.



Heung-Kyu Lee received his BS degree in electronics engineering from the Seoul National University, Seoul, Korea, in 1978 and his MS and PhD degrees in computer science from the Korea Advanced Institute of Science and Technology (KAIST) in 1981 and 1984, respectively. From 1984 to 1985 he was a research scientist with the University of Michigan, Ann Arbor. Since 1986 he has been a professor with the Department of Computer Science, KAIST, Daejon. He received the Order of Civil Merit, SukRyu medal 5066 from the Republic of Korea in October 1992. He was a director of the Korean Society of Remote Sensing and is now a director of the digital right management (DRM) forum and a director for the international affair of Korea Institute of Information Security and Cryptology. He is also vice director of the AITRC center in the KAIST. He is an author or coauthor of more than 100 journal and conference proceedings papers in his research areas. He has been a reviewer of many international journals, including the *Journal of Electronic Imaging, Real-Time Imaging*, and the *ACM Multimedia System Journal*. He was a program chairman of IEEE real-time computing systems and applications in 1999 and 2000, respectively. His biography has been selected by Marquis Who's Who for inclusion in *Who's Who in Science and Engineering, Who's Who in America*, and *Who's Who in the World* since 1996. His major interests are digital watermarking, fingerprinting, and DRM.