Multipurpose Watermarking for Image Authentication and Protection

Chun-Shien Lu, *Member, IEEE,* and Hong-Yuan Mark Liao, *Member, IEEE*

***Abstract*—We propose a novel multipurpose watermarking scheme, in which robust and fragile watermarks are simultaneously embedded, for copyright protection and content authentication. By quantizing a host image's wavelet coefficients as masking threshold units (MTUs), two complementary watermarks are embedded using cocktail watermarking and they can be blindly extracted without access to the host image. For the purpose of image protection, the new scheme guarantees that, no matter what kind of attack is encountered, at least one watermark can survive well. On the other hand, for the purpose of image authentication, our approach can locate the part of the image that has been tampered with and tolerate some incidental processes that have been executed. Experimental results show that the performance of our multipurpose watermarking scheme is indeed superb in terms of robustness and fragility.**

***Index Terms*—Authentication, copyright protection, fragile watermarking, fragility, robust watermarking, robustness, wavelet transform.**

I. Introduction

COPYRIGHT marking [24], [28] is a relatively new technique used for hiding multimedia information. Its application is broad, including ownership protection [3], [19], [29], [32], [33], content authentication [7], [13], [17], [37], [39], side information conveyance [25] and so on. For ownership protection, robustness [19] is one of the major points of concern. Watermarks embedded for this purpose are called robust watermarks. For content authentication, the embedded watermark should be fragile so that changes or modifications of a media will be reflected in the hidden watermark. This type of watermark is called a fragile watermark. In side information conveyance, a watermark is required to convey more information than a robust watermark does. As a consequence, less redundancy can be employed in this type of watermark [24]. Usually, people call this kind of watermark a captioning watermark. Most of the existing watermarking schemes are designed for either ownership protection or content authentication. If there are multiple purposes, then multiple watermarks must be embedded. Because watermarks of different sorts play different roles, as Mintzer and Braudaway [24] noted, the order for hidden watermarks is important. They suggested that ownership watermarks should be embedded first, captioning watermarks should be embedded next and fragile watermarks should be embedded last. In other words, if multiple watermarks having different missions are to be embedded, then one has to worry about the order of hiding.

In this paper, our purpose is to develop an oblivious yet highly robust watermarking scheme which can achieve the goal of image authentication and protection simultaneously. As to the content protection, we have proposed the concept of cocktail watermarking [19], which can resist different kinds of attacks (except for geometric attacks [15], [26], [30]). However, the first version of the cocktail watermarking algorithm was not oblivious. Here, we propose an oblivious detection technique to achieve the goals of robust watermarking and fragile watermarking simultaneously. In the literature, some previous works [1], [10], [12], [14], [33] have achieved the oblivious detection requirement but at the expense of robustness especially under stronger attacks or repeated (combined) attacks. Basically, the methodology they adopted for detecting watermarks was based on prediction and was independent of the hiding techniques. In [34], Voloshynovskiy *et al.* proposed a general method based on a stochastic model to address the watermark prediction problem.

As to content authentication, the previous techniques [7], [37] focused on detecting whether an image was tampered with or not. However, they did not clearly specify how and where the image was changed. A representative method called "telltale tamper-proofing" was proposed by Kundur and Hatzinakos [13] to determine the extent of tampering using a statistics-based tamper assessment function. However, their approach violates the nature of the human visual system [36]; thus, their system is confused when an image is compressed first and then maliciously tampered. Another disadvantage associated with Kundur and Hatzinakos's approach [13] is that their tampering detection results are very unstable. Perturbation of a wavelet coefficient to the left or to the right by a certain quantity will make the extracted mark different from the embedded one. Besides, if the perturbation exceeds one quantization interval, then the extracted watermark value can be either the same as or different from the embedded one (depending on the quantity of deviation). Hence, the watermark value may be determined accidentally and by the same token, not every modified pixel is guaranteed to be correctly detected. Another alternative approach for media authentication is the "digital signature." The digital signature-based methods for image authentication can be roughly classified to be hash function-based [7], feature points-based [2], [6], relation-based [17] and structure-based [22]. Unfortunately, the digital signature-based methods can only be used for image authentication but not for copyright protection since the original image is not watermarked. More

Manuscript received March 13, 2000; revised June 4, 2001. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Naohisa Ohta.

The authors are with the Institute of Information Science, Academia Sinica, Taipei 115, Taiwan, R.O.C (e-mail: lcs@iis.sinica.edu.tw; liao@iis.sinica.edu.tw).

Publisher Item Identifier S 1057-7149(01)08210-0.

complete reviews of image protection and image authentication can be found in [28], [32] and [13], [18], respectively. Besides, a theoretical analysis about copyright protection has been conducted in [11].

In this paper, we propose a multipurpose watermarking scheme which can simultaneously achieve copyright protection and content authentication by hiding multipurpose watermarks at the same time. The validity of our method is based on simultaneous detection of the robust watermark and the fragile watermark. As a consequence, the order of hiding [24] is no longer an important issue. We propose to quantize the selected wavelet coefficients into masking threshold units. Then, the watermarks can be encoded by modulating the quantization result into either a right or a left masking threshold unit using cocktail watermarking [19]. In the meantime, the original quantization result can be recorded as the hidden watermark because it is the closest neighbor to the modulated quantization. Hence, the hidden watermark carries the information of the host image, which can be used to recover the host image with indistinguishable perceptual degradation. This information is very useful in calculating the detector responses about robust watermarking and fragile watermarking.

The major contribution of this work is twofold. First, a new oblivious watermark detection technique which is associated with our previously developed cocktail watermarking scheme is proposed. Since the good characteristics of cocktail watermarking are still maintained, the new oblivious scheme preserves high robustness for copyright protection. Second, the extent of modification can be estimated by comparing the hidden watermark with the extracted one. Under these circumstances, malicious tampering can be detected while some incidental manipulations can be tolerated.

The remainder of this paper is organized as follows. In Section II, the nonoblivious cocktail watermarking scheme is briefly reviewed. Then, multipurpose watermarking for image protection and authentication is described in detail in Section III. Analysis of our method with respect to fragile watermarking is conducted in Section IV. Finally, simulation results and conclusions are given in Section V and Section VI, respectively.

II. Review of Cocktail Watermarking

In this section, the previously proposed image protection scheme called "cocktail watermarking" [19] is briefly reviewed because its concept will be adopted in this paper. In [19], we analyzed and pointed out the inadequacy of the available modulation techniques commonly used in ordinary spread spectrum watermarking methods and visual model-based ones. To resolve this inadequacy, two watermarks which play complementary roles are simultaneously embedded into a host image using a complementary modulation strategy. This complementary modulation strategy, including positive modulation (PM) and negative modulation (NM), was derived from the viewpoint of detection in order to obtain higher detector responses. In cocktail watermarking, the first watermark is inserted based on a positive modulation rule employed to increasingly modulate the transformed coefficients of a host image and the second watermark is embedded based on a negative modulation rule used to decreasingly modulate the transformed coefficients of a host image. Based on analysis on the behaviors of attacks, we have confirmed that the new watermarking scheme guarantees that, no matter what kind of attack is encountered, at least one watermark can survive well. We also conduct a statistical analysis to derive the lower bound of the worst likelihood that the better watermark (out of the two) can be extracted. With this "high" lower bound, it is ensured that a "better" extracted watermark will always be obtained for noise-like watermark hiding as well as bipolar watermark hiding under the constraint that the original image is required in the detection process.

In the cocktail watermarking scheme [19], three conditions were derived to achieve robustness. They were

1) bipolar watermarking (the designated watermark);
2) complementary modulation (the hiding rule);
3) use of a wavelet-based human visual system [36] to control the hiding strength.

Owing to two complementary watermarks are embedded, the hiding places, selected as those wavelet coefficients larger than their corresponding masking thresholds, are randomly divided into groups. The first group with coordinates denoted as (x_p, y_p) will be used to hide the first watermark by positive modulation and the second group with coordinates denoted as (x_n, y_n) will be used to embed the second watermark by negative modulation. The relation between the hiding coordinate in the wavelet domain (x, y) and the index i in a sorted watermark sequence is a mapping function p, which can be defined as follows:

$$p(x,y) = \begin{cases} i, & \text{for positive modulation} \\ -i, & \text{for negative modulation.} \end{cases} \tag{1}$$

From the sign of the mapping function p, we can know where the first/second watermark is embedded. In addition, from the value of the mapping function p, we can also know the order of embedded watermark values, which is important for calculating the detector response. Basically, the mapping results must be stored for watermark detection and should be kept secret such that the pirates cannot easily remove the hidden watermarks. In cocktail watermarking detector side, two correlation values will be obtained. The larger one indicates the presence/absence of a watermark.

III. Proposed Multipurpose Watermarking Algorithm

This section will elaborate on the proposed approach in detail. In order to satisfy copyright protection and content authentication requirements simultaneously, a hidden watermark should be designed in a form that can carry the approximate information of a host image. Because wavelet transformation is used as the watermarking domain, we shall provide a brief introduction on wavelet transformation in Section III-A. In Section III-B, a visual model-based quantization is proposed to encode two complementary watermarks in the wavelet domain. Section III-C discusses the means used to recover a host image. In Section III-D, we describe four different ways which can be applied to detect robust watermarks and fragile watermarks under different situations. In Section III-E, we shall discuss how

to normalize the values of a hidden watermark. Note that this multipurpose watermarking scheme is performed by embedding watermarks only *once* without considering their hiding order. For a specific application, a suitable watermark detection process should be determined by the user.

A. Some Basic Concepts about Wavelet Transform

Conventionally, the Fourier transform (FT) has been extensively used in characterizing spectral behaviors of signals by transforming from the spatial (or time) domain to the frequency domain globally. However, owing to the global property of FT, it is quite inadequate to be used in representing the signals with nonstationary properties. Gabor [9] had observed the deficiency and introduced a "window function" which could slide in the whole spatial domain such that information could be extracted locally. This type of transform is called windowed Fourier transform or short-time Fourier transform (STFT). However, the drawback of STFT is that its window size is fixed once it is chosen. Recently, a dilation parameter has been introduced to dynamically change the window size such that one can detect information locally in distinct spaces and scales. If the aforementioned window function added with the, ψ (with a dilation parameter s), satisfies the "admissibility" condition

$$C_\psi = \int_{-\infty}^{\infty} \frac{|\hat{\psi}(\mathbf{w})|}{|\mathbf{w}|} d\mathbf{w} < \infty \tag{2}$$

then we can call ψ can be called a "basic wavelet" or "mother wavelet." The finiteness of (2) implies $\hat{\psi}(0) = 0$ and is equivalent to

$$\int_{-\infty}^{\infty} \psi(\mathbf{x}) dx = 0. \tag{3}$$

A sequence of local functions, $\psi(\mathbf{x}-\mathbf{b}/s)$, can be produced by translation and dilation of the mother wavelet, $\psi(\mathbf{x})$, where $\mathbf{b} \in \mathcal{R}^2$ and $s \in \mathcal{R}$ with $s \neq 0$. The wavelet transform of an image f can be defined as

$$\begin{aligned}(\mathcal{W}f)(\mathbf{b}, s) &= \frac{1}{s^2} \int_{R^2} f(\mathbf{x}) \overline{\psi(\frac{\mathbf{x}-\mathbf{b}}{s})} d\mathbf{x} \\ &= \int_{R^2} \hat{f}(\mathbf{w}) \overline{\hat{\psi}(s\mathbf{w})} e^{-j(\mathbf{w}^T\mathbf{b})} d\mathbf{w}\end{aligned} \tag{4}$$

where $\overline{\psi(\mathbf{x})}$ denotes the complex conjugate of $\psi(\mathbf{x})$.

If the scale parameter s is set to be a power of two, this wavelet is called dyadic wavelet transform. The wavelet decomposition of a signal $f(x)$ is performed by the convolution of the signal with a family of basis functions, $\psi(\mathbf{x}-\mathbf{b}/s)$. In fact, a wavelet decomposition can be efficiently performed by a pyramidal algorithm [23], in which a pair of wavelet filters including a low-pass filter and a high-pass filter are utilized to calculate wavelet coefficients. With the pyramid-structured wavelet transform, the original image will encounter different combinations of a low-pass filter and a high-pass filter and then based on the convolution with these filters to generate the low-low (LL), low-high (LH), high-low (HL) and high-high (HH) subimages. The decomposition can be repeatedly performed on the low-low subimage to obtain the next four subimages. Fig. 1 shows the one-scale and two-scale wavelet decompositions, respectively. The second scale decomposition on the LL part of Fig. 1(a) is shown at the top left of Fig. 1(b). With the pyramid-structured wavelet transform, the size of the original image is equivalent to summing all the decomposed channels up. Using this decomposition structure, there will be no information lost when the decomposed pieces are reconstructed. This property is extremely useful when it is applied to the watermarking problem. Readers who are interested in wavelets should refer [5], [23] for more details.

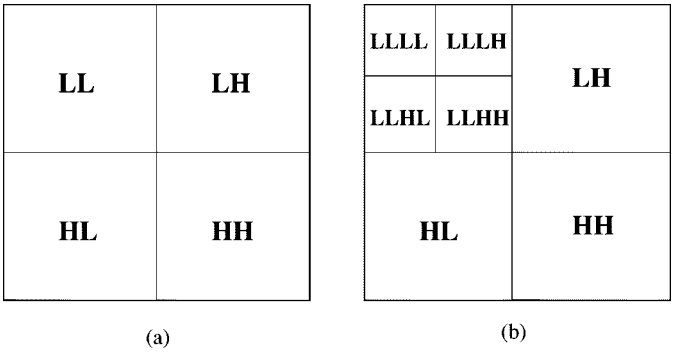


Fig. 1. Wavelet decomposition into (a) one layer and (b) two layers where LL, LH, HL, and HH denote low-low, low-high, high-low, and high-high filtering, respectively.

B. Watermark Hiding: Quantization of Wavelet Coefficients as Masking Threshold Units

In this section, we will describe how to embed watermarks and record the host image's information. Conventionally, watermarks are embedded in transformed coefficients which are larger in magnitude. Let $w_{s,o}(x,y)$ be a selected wavelet coefficient with scale s, orientation o and position (x,y) and let $J_{s,o}(x,y)$ be the masking threshold [36] corresponding to $w_{s,o}(x,y)$. Based on the JND values, the real-axis about the magnitudes of wavelet coefficients is divided into masking threshold units (MTUs). Each MTU is represented by a quantization value, q, which is calculated as

$$q(|p(x,y)|) = \left\lfloor \frac{w_{s,o}(x,y)}{J_{s,o}(x,y)} \right\rfloor \tag{5}$$

where $\lfloor \cdot \rfloor$ denotes the *floor* operation; as a result, $q(|p(x,y)|) \in \mathcal{Z}$ and $|q(|p(x,y)|)| \geq 1$ because wavelet coefficients are selected to satisfy $|w_{s,o}(x,y)| > |J_{s,o}(x,y)|$. This means that $w_{s,o}(x,y)$ is located at the $q(|p(x,y)|)$th MTU. In the hiding process, the goal of quantization-based modulation is to move the selected wavelet coefficient $w_{s,o}(x,y)$ into another masking threshold unit. In order to obtain a transparent watermarked image, the modulated quantity should not be moved away from its current location exceeding 1 MTU. So, a wavelet coefficient $w_{s,o}(x,y)$, located at the $q(|p(x,y)|)$th MTU, must be confined to move into its neighboring unit. Using cocktail watermarking, we can embed two watermarks, respectively, based on the concept of a negative modulation (NM) rule and a positive modulation (PM) rule by quantization as follows.

Negative modulation:

$$w^m_{s,o}(x,y)=\begin{cases} q(-p(x,y))\cdot J_{s,o}(x,y)-1, \\ \quad \text{if } w_{s,o}(x,y)>J_{s,o}(x,y) \\ q(-p(x,y))\cdot J_{s,o}(x,y)+1, \\ \quad \text{if } w_{s,o}(x,y)<-J_{s,o}(x,y). \end{cases} \tag{6}$$

According to (1), $p(x,y)$ is negative for negative modulation.

Positive modulation:

$$w^m_{s,o}(x,y)=Q(p(x,y))\cdot J_{s,o}(x,y) \tag{7}$$

where

$$Q(p(x,y))=\left\lceil \frac{w_{s,o}(x,y)}{J_{s,o}(x,y)} \right\rceil \tag{8}$$

and

$$|Q(p(x,y))|=|q(p(x,y))|+1$$

where $\lceil\cdot\rceil$ denotes the *ceiling* operation and $p(x,y)$ is positive for positive modulation.

The modulated wavelet coefficient, $w^m_{s,o}(x,y)$, either falls into the $(q(-p(x,y))-1)$th MTU after negative modulation is applied or falls into the $Q(p(x,y))$th MTU after positive modulation is applied. In other words, the original and the modulated wavelet coefficients are located at different but contiguous MTUs, no matter what type of modulation rule is applied. From the modulated wavelet coefficients shown in (6) and (7), one can calculate the modulated quantization index, q^m, as

$$|q^m(|p(x,y)|)|=\begin{cases} |q(-p(x,y))|-1, & \text{for NM} \\ |q(p(x,y))|+1, & \text{for PM.} \end{cases} \tag{9}$$

The integer value $q^m(|p(x,y)|)$ is regarded as the embedded watermark values, $k(|p(x,y)|)$, based on the sign of $p(x,y)$. That is, two watermarks with the different orders but with the same statistical property are embedded. If we want to take $k(|p(x,y)|)$ into consideration, the watermark hiding rules in (6) and (7) should be rewritten as follows.

Negative modulation: See equation (10) at the bottom of the page.

Positive Modulation:

$$w^m_{s,o}(x,y)=k(p(x,y))\cdot J_{s,o}(x,y). \tag{11}$$

The hidden watermark K, composed of $k|p(x,y)|$, can be used to evaluate the robustness and the fragility of the extracted watermark without accessing the original image. More specifically, we use the characteristics of wavelet transforms to approximate the original image and only part (watermark's size) of the approximate version is used to design a hidden watermark. As a result, the original image will never be used again; thus, we can call the proposed multipurpose watermarking scheme an oblivious one. On the other hand, since each image is associated with a hidden watermark, it means the hidden watermark is image-dependent. As Craver *et al.* have mentioned in [4], the image-dependent watermark is able to solve the "watermark invertibility" problem. Because our hidden watermark is generated from the image itself, one advantageous point is that we can prove how the original hidden watermark is generated. But we have to admit that the security level of our scheme is lower than that of a scheme which adopts the well-known one-way hash function [4].

C. Host Image Recovery

Using the hidden watermark K, we can approximately reconstruct a host image with negligible degradation. Let the ith watermark value be $k(i)$; it is equal to the quantization index, $q^m(|p(x,y)|)$, as indicated in (9). The recovered quantization value, $q^r(|p(x,y)|)$, can be derived from (9) as shown in the equation at the bottom of the page. The difference, Δ, between a recovered wavelet coefficient and its corresponding original wavelet coefficient is bounded by $J_{s,o}(x,y)$. That is

$$\Delta=|q^r(|p(x,y)|)\cdot J_{s,o}(x,y)-w_{s,o}(x,y)|<J_{s,o}(x,y) \tag{12}$$

where $w_{s,o}(x,y)$ is a selected wavelet coefficient for hiding. Since our scheme has been designed based on the characteristics of the human visual system, the recovered host image should be perceptually indistinguishable from the original image.

D. Watermark Detection

Let $w^a_{s,o}(x,y)$ be a modulated wavelet coefficient which has experienced attacks; the positively/negatively modulated watermark value can be extracted without accessing the original image using a quantization process

$$k^e(|p(x,y)|)=\left\lfloor \frac{w^a_{s,o}(x,y)}{J_{s,o}(x,y)} \right\rfloor \tag{13}$$

which depends on the sign of $p(x,y)$ [defined in (1)]. By comparing the hidden watermark (K) and the extracted one (K^e),

$$w^m_{s,o}(x,y)=\begin{cases} (k(-p(x,y))+1)\cdot J_{s,o}(x,y)-1, & \text{if } w_{s,o}(x,y)>J_{s,o}(x,y) \\ (k(-p(x,y))-1)\cdot J_{s,o}(x,y)+1, & \text{if } w_{s,o}(x,y)<-J_{s,o}(x,y) \end{cases} \tag{10}$$

$$|q^r(|p(x,y)|)|=\begin{cases} |q^m(-p(x,y))|+1=|k(-p(x,y))|+1, & \text{for NM} \\ |q^m(p(x,y))|-1=|k(p(x,y))|-1, & \text{for PM} \end{cases}$$

the purpose of fragile watermarking can be achieved. On the other hand, by comparing the hidden watermark, the extracted watermark and the host image's information (q^r), the goal of robust watermarking can be achieved. Note that the detector response regarding robustness or fragility can be separately calculated in our scheme. In what follows, we shall describe in detail how this can be done.

1) Detection of Robust Watermarks: If the signs of $(k(i) - q^r(i))$ and $(k^e(i) - q^r(i))$ are the same, i.e., the majority of the transformed coefficients in the modulation and attacking processes are updated toward the same polarity, then they contribute positively to the detector response [19]. A higher detector response provides stronger evidence that K^e is a genuine watermark. The detector response of robust watermarking (called "robust detector response") is defined as shown in (14) at the bottom of the page, where N_w is the watermark length and

$$\text{sign}(u) = \begin{cases} 1, & u \geq 0 \\ -1, & u < 0. \end{cases} \tag{15}$$

For robust watermarking, two detector responses are obtained with respect to the two complementary watermarks. The larger one is chosen as the final detector response.

2) Detection of Fragile Watermarks Based on the Characteristics of the Human Visual System: Fragile watermarks are different from robust watermarks and are supposed to be sensitive to tampering. Based on the standard of the human visual system, an image pixel is considered to have been tampered with if the difference between a hidden watermark value and its corresponding extracted watermark value is larger than t $(t \geq 1)$ masking units. When t is set to be one, this means that if the amount of modification exceeds the tolerance of the human visual system, then this modification will be considered to be malicious. However, images may be unavoidably manipulated by some incidental processes, such as compression. Under these circumstances, we cannot think of these incidental processes as malicious ones. In other words, a fragile watermarking scheme should be robust to incidental distortions. As we have noted with respect to cocktail watermarking [19], incidental modification like compression tends to decrease the magnitudes of the transformed coefficients. On the other hand, incidental modification like sharpening tends to increase the magnitudes of the transformed coefficients. In what follows, we shall discuss the safe range into which a fragile watermark should fall when incidental distortions are encountered.

Suppose a wavelet coefficient x was originally located at the $(j+1)$th masking unit, is moved to the jth masking unit and, thus, becomes x^M after NM. x^M is considered to not have been tampered with as long as the tampered coefficient, x^T, falls in the range between the $(j-t)$th and the $(j+1)$th masking units. Under these circumstances, the number of masking units (corresponding to NM) in the left interval and the right interval of x^M is t and 1, respectively. In other words, the untampered range

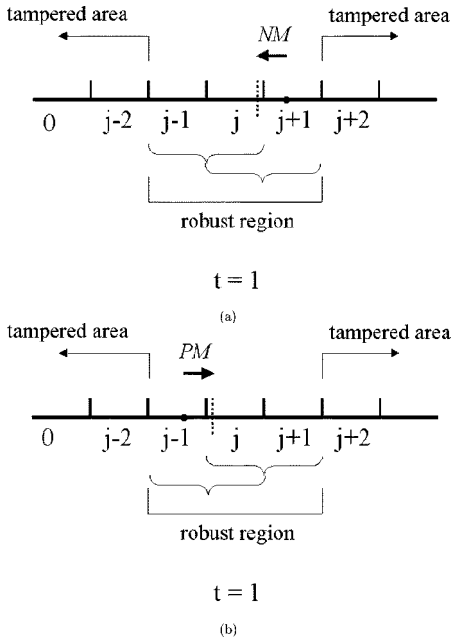


Fig. 2. Illustration of the tampered region and the robust region for (a) negative modulation (NM) and (b) positive modulation (PM) when $t = 1$. The arrow with the label NM or PM indicates the direction of alternation in the hiding process. Note that the robust region (indicated with {) is asymmentric with respect to j for $t > 1$.

is *asymmetric* with respect to x^M. This situation also applies similarly to PM. The tampered region and the robust region corresponding to negative modulation and positive modulation are illustrated in Fig. 2. Basically, our watermarking strategy makes the authentication process more robust (less fragile) to incidental distortions. If x^T is obtained by applying a compression/enhancing process, then x^M still has a good chance of being credible because the left/right interval of x^M is longer. On the other hand, fragility is determined from the other shorter interval (only *one* masking unit). Hence, tampering detection in a negatively modulated watermark is defined as

$$T^{\text{neg}}(i) = \begin{cases} 1, & |k(i)| > |k^e(i)| \wedge |k(i) - k^e(i)| > t \\ 1, & |k(i)| \leq |k^e(i)| \wedge |k(i) - k^e(i)| > 1 \\ 0, & \text{otherwise} \end{cases}$$

where $\wedge$ is an "*and*" operation. On the other hand, tampering detection about a positively modulated watermark is similarly defined as

$$T^{\text{pos}}(i) = \begin{cases} 1, & |k(i)| \geq |k^e(i)| \wedge |k(i) - k^e(i)| > 1 \\ 1, & |k(i)| < |k^e(i)| \wedge |k(i) - k^e(i)| > t \\ 0, & \text{otherwise.} \end{cases}$$

In sum, the global detector response of fragile watermarking (called "fragile detector response") is defined as

$$\rho^{\text{neg}}_{\text{fragile}}(K, K^e) = \frac{\sum_{i=1}^{N_w} T^{\text{neg}}(i)}{N_w}$$

$$\rho_{\text{robust}}(K, K^e) = \frac{\sum_{i=1}^{N_w} \text{sign}(k(i) - q^r(i)) \cdot \text{sign}(k^e(i) - q^r(i))}{N_w} \tag{14}$$

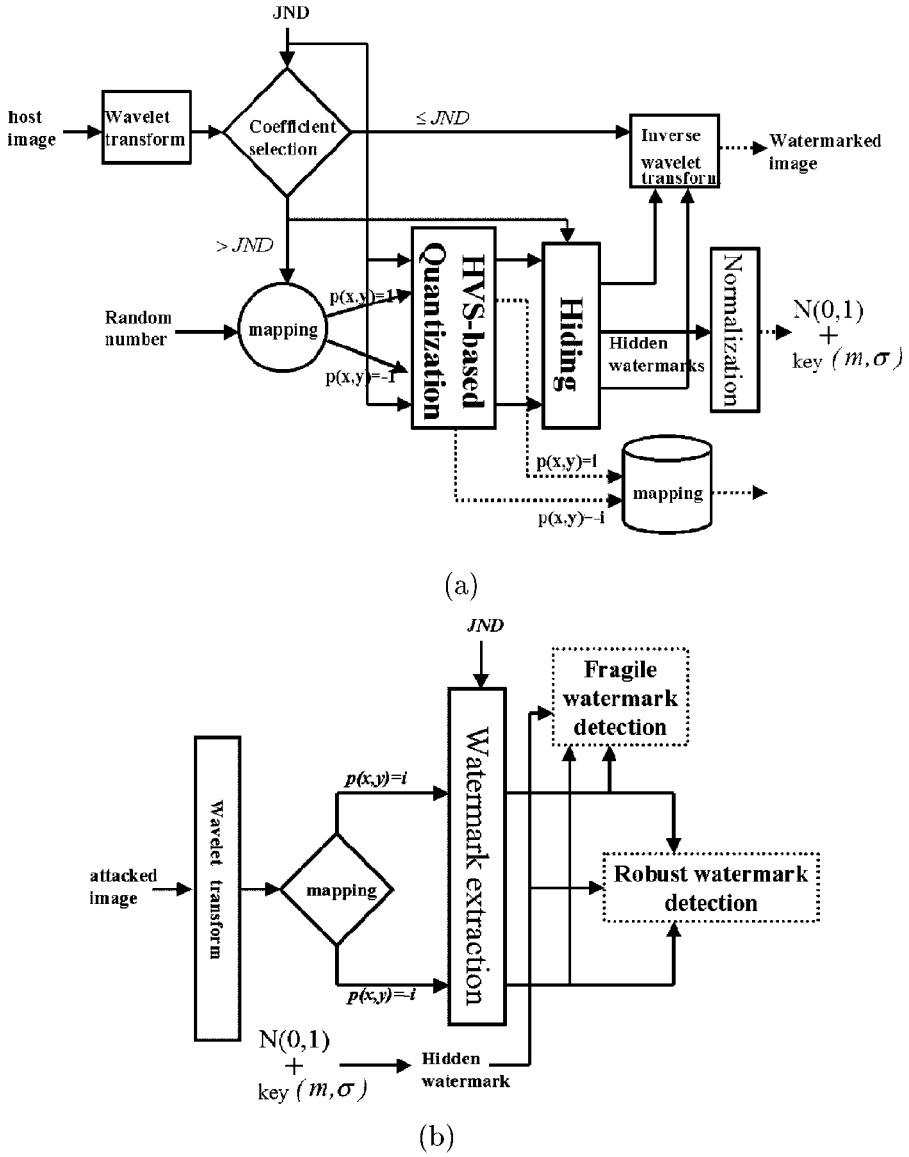


Fig. 3. Flowchart of our multipurpose watermaking scheme (a) watermark hiding and (b) watermark detection.

and

$$\rho^{\text{pos}}_{\text{fragile}}(K,K^e)=\frac{\sum_{i=1}^{N_w}T^{\text{pos}}(i)}{N_w}$$

respectively, for a negatively modulated watermark and a positively modulated watermark. Note that different t values enable our authentication scheme to adapt to various distortions. The fragility of an incidental process can be determined by

$$MIN(\rho^{\text{neg}}_{\text{fragile}}(K,K^e),\rho^{\text{pos}}_{\text{fragile}}(K,K^e)). \tag{16}$$

3) Detection of Fragile Watermarks Based on Tendency of Attacks: As we have described in Section III-D2, incidental tampering is said to have occurred if the detector response of a fragile watermark (16) is smaller than a preset threshold. However, the threshold is sometimes difficult to determine. In this section, another criterion is provided to judge the fragility based on the assumption that incidental manipulation tends to behave consistently while malicious one dose not. The consistency of attacking behavior can be defined as BR_{fragile}, which is expressed as

$$BR_{\text{fragile}}=\frac{MAX(\rho^{\text{pos}}_{\text{fragile}}(\cdot,\cdot),\rho^{\text{neg}}_{\text{fragile}}(\cdot,\cdot))}{MIN(\rho^{\text{pos}}_{\text{fragile}}(\cdot,\cdot),\rho^{\text{neg}}_{\text{fragile}}(\cdot,\cdot))} \tag{17}$$

where $MAX(\cdot,\cdot)$ and $MIN(\cdot,\cdot)$ are the maximum and the minimum operations, respectively. Incidental processing will have the tendency to have a large BR_{fragile} value. The threshold used for deciding the existence of nonmalicious tampering is easier to derive than the one chosen in (16).

4) Detection of Fragile Watermarks Based on Invariance Property: Tampering can also be detected by checking some invariance properties. It has been found that perception-based fragility (Section III-D2) can resist compression (*JPEG* or *SPIHT*) up to the middle compression ratio. Previous feature point-based image authentication methods [2], [6] suffered from the problem of shifting feature points when the compression ratios ranged from middle to high. Lin and Chang

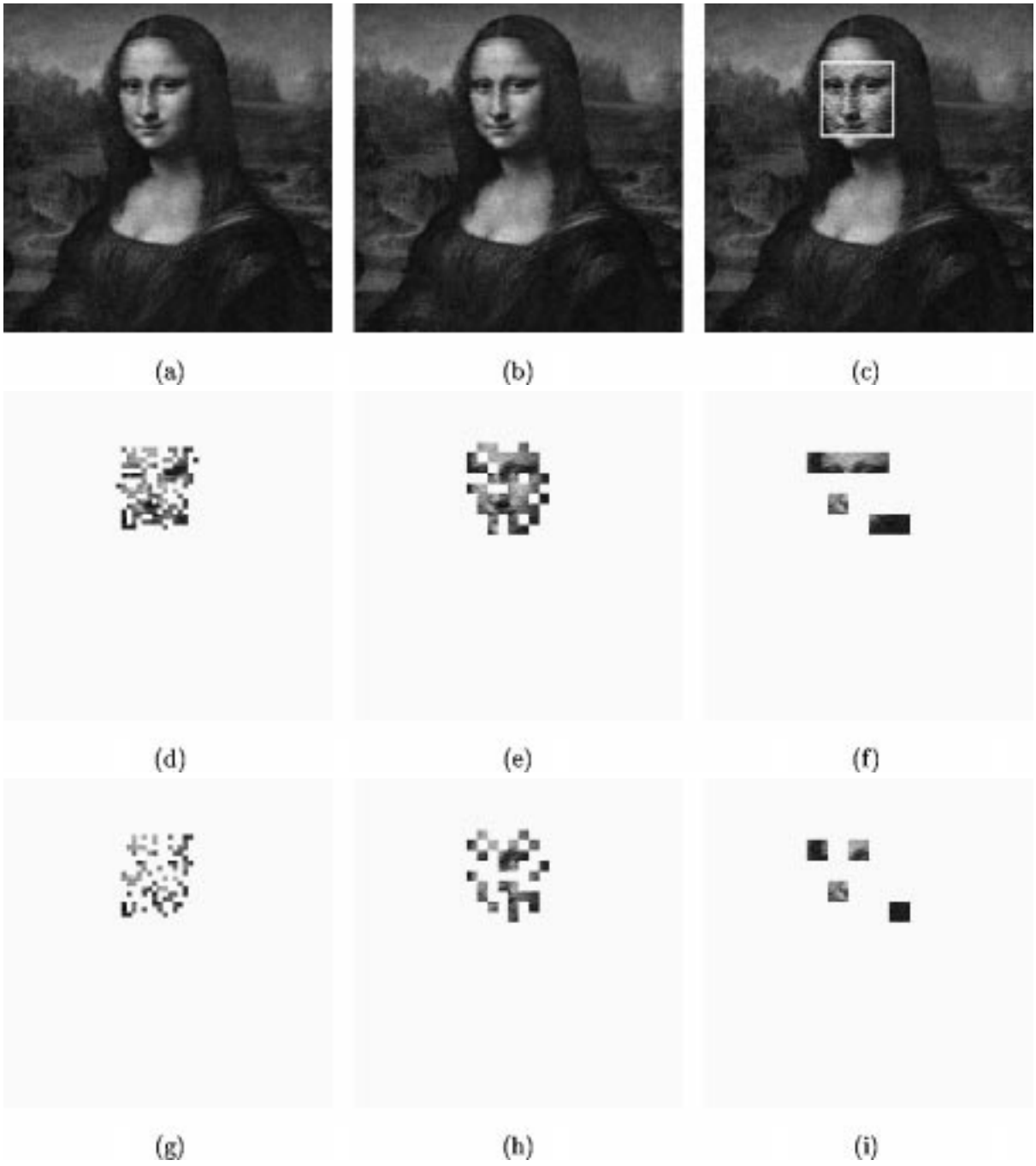


Fig. 4. Malicious tampering detection: (a) host image; (b) watermark image; (c) image after malicious tampering; (d)–(f) the tampering detection results at the $2^2 \sim 2^4$ scales with respect to $t = 1$; and (g)–(i) the tampering detection results at the $2^2 \sim 2^4$ scales with respect to $t = 10$.

[17] proposed to preserve the invariance between DCT coefficients at two different blocks as a solution of tolerating *JPEG* compression with any ratios. In this work, we shall adopt a similar invariance property to check the degree of similarity between watermarks. Because two complementary watermarks are embedded in our multipurpose watermarking scheme, the invariance property is checked based on the two watermarks. It is expected that the relationship between the two hidden watermarks will be maintained after incidental manipulations. Let K_{neg} and K_{pos} be the two watermarks hidden by means of negative modulation and positive modulation, respectively and let K^e_{neg} and K^e_{pos} be the two extracted watermarks. We define the invariance property between a pair of watermark values located in the same position as follows:

- if $k_{\text{neg}}(i) - k_{\text{pos}}(i) > 0$ then $k^e_{\text{neg}}(i) - k^e_{\text{pos}}(i) \geq 0$;
- if $k_{\text{neg}}(i) - k_{\text{pos}}(i) < 0$ then $k^e_{\text{neg}}(i) - k^e_{\text{pos}}(i) \leq 0$;
- if $k_{\text{neg}}(i) - k_{\text{pos}}(i) = 0$ then $k^e_{\text{neg}}(i) - k^e_{\text{pos}}(i) = 0$.

If any one of the above three conditions is satisfied, then we can say that there no tampering has occurred.

E. Normalization of the Hidden Watermark K

The hidden watermark K is designed to carry the information of a host image and is, therefore, dependent on the host image.

Fig. 5. Tampering detection of object placement: (a) host image; (b) watermarked image; (c) image after object placing; (d)–(f) the tampering detection results at the $2^2 \sim 2^4$ scales with respect to $t = 1$; and (g)–(i) the tampering detection results at the $2^2 \sim 2^4$ scales with respect to $t = 10$.

Any randomly selected watermark K_r may be highly correlated with the hidden watermark K and this will cause a severe false positive problem. Hence, K should be normalized to $N(0,1)$ as Cox *et al.* did in [3]. This procedure will make K and K_r statistically independent. Let (m, σ) be the mean and the standard deviation of the hidden watermark K. The normalized K is denoted as K_G, where

$$k_G(i) = \frac{k(i) - m}{\sigma}. \tag{18}$$

To compute the false positive and false negative probability, the Gaussian distributed watermark K_G is used. The pair (m, σ) is regarded as an image-dependent watermark (IDW) key and is jointly used with K_G to generate K [using (18)] for watermark hiding (Section III-B), host image recovery (Section III-C) and watermark detection (Section III-D).

IV. Performance Analysis

In this section, we will analyze the robustness and the fragility of the proposed multipurpose watermarking scheme used for fragile watermarking. As to robust watermarking, false negative and false positive analysis had been conducted in [19]. Suppose a wavelet coefficient $w_{s,o}(x,y)$ was originally located at the $(j+1)$th masking unit, is moved to the jth masking unit after NM and becomes $w^m_{s,o}(x,y)$. The tampering effect can be modeled as follows:

$$w^a_{s,o}(x,y) = w^m_{s,o}(x,y) + n_{s,o}(x,y) \tag{19}$$

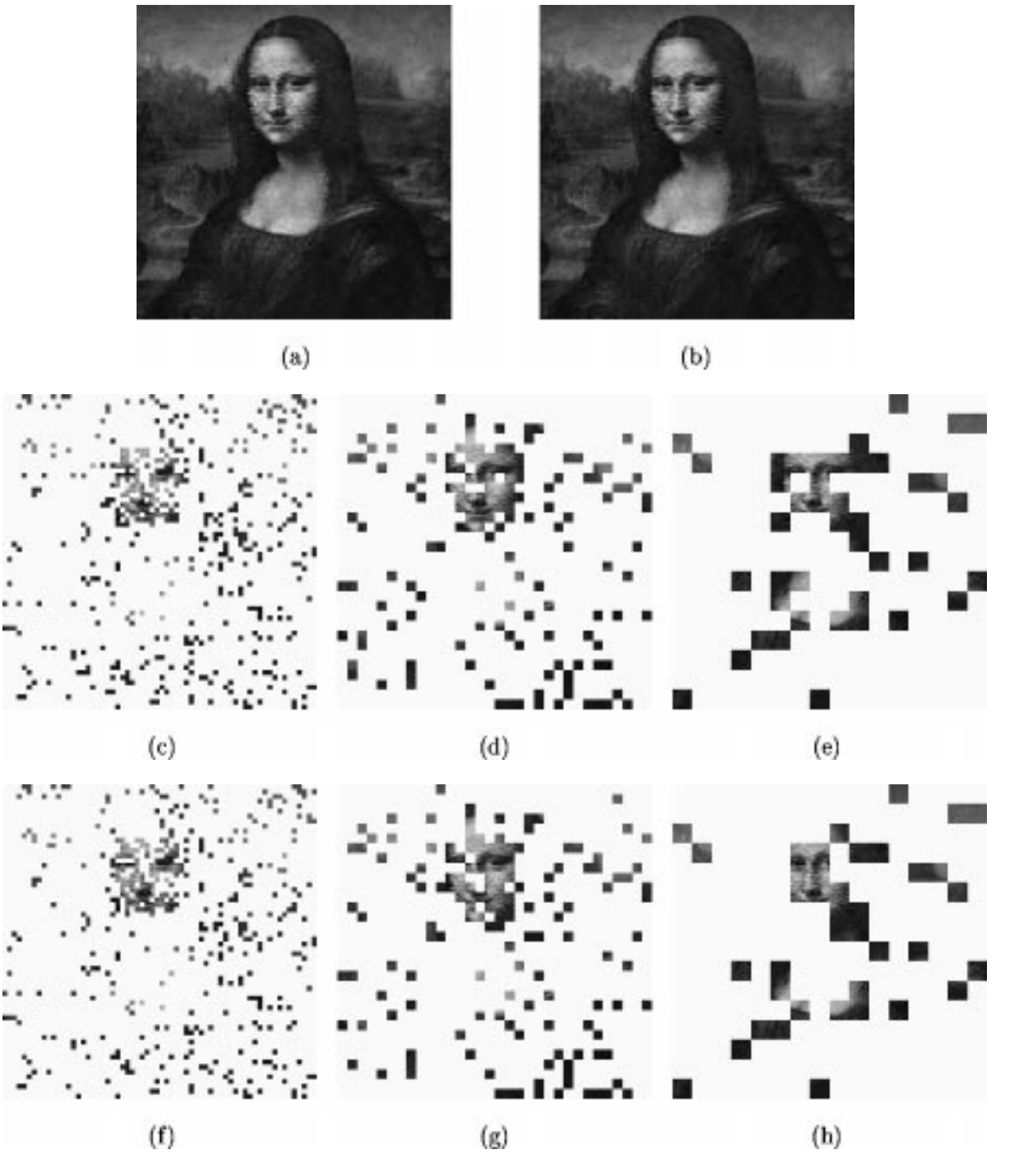


Fig. 6. Fragile watermarking on the watermarked MonaLisa image Fig. 4(b) which were both incidently and maliciously modified: (a) Fig. 4(b) first texture modified at the face position and then SPIHT compresssed with a ratio 8 : 1; (b) Fig. 4(b) first SPIHT compresssed with a ratio 8 : 1 and then texture modified at the face position; (c)–(e) show the tampering detection results of (a) at the $2^2 \sim 2^4$ scales with $t = 1$; and (f)–(h) show the tampering detection results of (b) at the $2^2 \sim 2^4$ scales with $t = 1$.

where $w^a_{s,o}(x,y)$ is the tampered coefficient and the amount of modification $n_{s,o}(x,y)$ is assumed to be Gaussian distributed with zero mean and variance σ^2. Under negative modulation, $w^a_{s,o}(x,y)$ is thought of as untampered if $w^a_{s,o}(x,y)$ falls into the robust range, which is t masking units to the left of $w^m_{s,o}(x,y)$ and 1 masking unit to the right of $w^m_{s,o}(x,y)$. Therefore, the probability that a coefficient will still be credible after attacks is defined as

$$p^{\text{neg}}_{rr} = P\{-t \cdot J_{s,o}(x,y) < n_{s,o}(x,y) < 1 \cdot J_{s,o}(x,y)\}. \quad (20)$$

p^{neg}_{rr} can be rewritten as

$$\begin{aligned} p^{\text{neg}}_{rr} =& P\{-t \cdot J_{s,o}(x,y) < n_{s,o}(x,y) < 0\} \\ &+ P\{0 < n_{s,o}(x,y) < 1 \cdot J_{s,o}(x,y)\} \\ =& erf\left(\frac{t \cdot J_{s,o}(x,y)}{2\sigma}\right) + erf\left(\frac{J_{s,o}(x,y)}{2\sigma}\right) \\ =& P^{\text{neg}}_{l} + P^{\text{neg}}_{r} \end{aligned} \quad (21)$$

where $erf(\cdot)$ is the error function, defined as

$$erf(\epsilon) = \frac{2}{\sqrt{\pi}} \int_0^{\epsilon} e^{-u^2} du.$$

For positive modulation, a similar result can be derived, where

$$\begin{aligned} p_{rr}^{\text{pos}} =& P\{-J_{s,o}(x,y) < n_{s,o}(x,y) < t \cdot J_{s,o}(x,y)\} \\ =& P\{-J_{s,o}(x,y) < n_{s,o}(x,y) < 0\} \\ &+ P\{0 < n_{s,o}(x,y) < t \cdot J_{s,o}(x,y)\} \\ =& erf\left(\frac{J_{s,o}(x,y)}{2\sigma}\right) + erf\left(\frac{t \cdot J_{s,o}(x,y)}{2\sigma}\right) \\ =& P_l^{\text{pos}} + P_r^{\text{pos}}. \end{aligned} \tag{22}$$

According to (21) and (22), we know that

$$P_l^{\text{neg}} = P_r^{\text{pos}} \geq P_r^{\text{neg}} = P_l^{\text{pos}}$$

where P_l^{neg} and P_r^{pos} reflect the degree of robustness against incidental distortions, such as compression and sharpening. On the other hand, the degree of sensitivity in response to malicious tampering is determined by P_r^{neg} and P_l^{pos}.

The three parameters, J, t and σ, are closely related to p_{rr}^{neg} and p_{rr}^{pos}. First, the larger $J_{s,o}(x,y)$ is, the more robust (less fragile) the watermark is. This is because either p_{rr}^{neg} or p_{rr}^{pos} is large. If t and σ are fixed at all wavelet-transformed scales, then our scheme is more sensitive to distortions at lower frequencies in terms of fragility. Secondly, t controls the tradeoff between robustness and fragility in our fragile watermarking scheme, as described in Section III-D2. In other words, the larger t is, the larger P_l^{neg} and P_r^{pos} are. This means that under NM/PM, tampering on the left/right interval of $x_{s,o}^m(x,y)$ is more robust than tampering on the right/left interval of $x_{s,o}^m(x,y)$. This again confirms our assertion with regard to perception-based fragile watermark detection given in Section III-D2. Thirdly, it should be noted that the smaller σ is, the larger P_l^{neg} and P_r^{pos} are. This implies that like distortions with smaller σ are easy to tolerate because they are similar to modifications like compression with small-to-middle ratios. For manipulation like content replacement, σ is often larger and the manipulation is expected to be detected whenever t is not very large.

V. Experimental Results

A series of experiments was conducted to demonstrate the robustness and the fragility of the proposed multipurpose watermarking scheme. In addition to gray-scale images, color images were also considered. Among the existing color systems, $YCbCr$ was chosen for two reasons: 1) it has been adopted in many compression standards and 2) masking thresholds are available [36]. For color image watermarking, the watermarks were embedded and detected in the Y channel because humans are more sensitive to this channel. The lowest wavelet subband used in this work is constrained to be 16×16. The flowchart of our method is illustrated in Fig. 3. In addition to results of one-bit watermark detection shown in the following experiments, we also considered a payload of 64-bits as a watermark in our working system. This is because a 64-bits payload corresponding to the length of standard copyright identifiers has been widely used.

TABLE I
Tamering Degree Evaluation Under JPEG Compression

Compression Ratio (Quality Factor %)	*Degree of tampering*						
	t=1		*t=2*		*t=3*		*INV*
	NM	*PM*	*NM*	*PM*	*NM*	*PM*	
6.07(70%)	0.036	0.131	0.035	0.129	0.035	0.128	0.038
7.54(60%)	0.023	0.200	0.057	0.199	0.057	0.199	0.043
8.93(50%)	0.075	0.261	0.067	0.259	0.067	0.260	0.049
10.84(40%)	0.105	0.338	0.090	0.331	0.089	0.332	0.050
13.70(30%)	0.143	0.418	0.114	0.410	0.111	0.408	0.051
19.57(20%)	0.191	0.558	0.143	0.546	0.134	0.535	0.054
32.09(10%)	0.275	0.719	0.216	0.686	0.185	0.670	0.074

TABLE II
Tamering Degree Evaluation Under SPIHT Compression

Compression Ratio	*Degree of tampering*						
	t=1		*t=2*		*t=3*		*INV*
	NM	*PM*	*NM*	*PM*	*NM*	*PM*	
4	0.001	0.023	0.000	0.023	0.000	0.023	0.016
8	0.013	0.086	0.010	0.086	0.009	0.086	0.022
16	0.078	0.380	0.049	0.375	0.046	0.374	0.024
32	0.133	0.670	0.066	0.666	0.047	0.665	0.023
64	0.241	0.846	0.147	0.834	0.093	0.827	0.031

A. Results of Fragile Watermarking

The degree of fragility was verified using the gray-scale "MonaLisa" image, size 256×256, as shown in Fig. 4(a). The length of a watermark depends on both the host image and the wavelet-based visual model. Here, its length was dynamically determined to 6593. Using cocktail watermarking [19], 13 186 wavelet coefficients were modulated. The PSNR of the watermarked image shown in Fig. 4(b) was 39.7 dB. Next, the watermarked MonaLisa image was maliciously modified at the position of her face by means of texturing, as shown in Fig. 4(c). We wanted to see whether our fragile watermarks were sensitive to texture changes. Figs. 4(d)–(f) show when $t = 1$, the tampering detection results at different scales. Figs. 4(g)–(i) show another set of results when $t = 10$. It is found that in Fig. 4 that the altered regions were almost located. It is worth noticing that for different t values, the difference between K and K^e only slightly reduced even when t has been changed from one to ten. This implies that our multipurpose watermarking scheme is indeed fragile enough because the change of t would not affect fragility significantly.

As for color images, the beach image with size 512×512 (shown in Fig. 5) was also used to demonstrate the fragility of our approach. The watermarks were embedded in the illumination channel and the PSNR was 41.2 dB [Fig. 5(b)]. An umbrella was placed on the watermarked image to change the image, as shown in Fig. 5(c). Fig. 5 (d)–(i) show the tampering detection results at different scales with respect to $t = 1$ and $t = 10$, respectively. Again, we can see that all the altered regions were successfully detected. Currently, our method cannot detect color changes if color is modified but leaving the intensity unchanged.

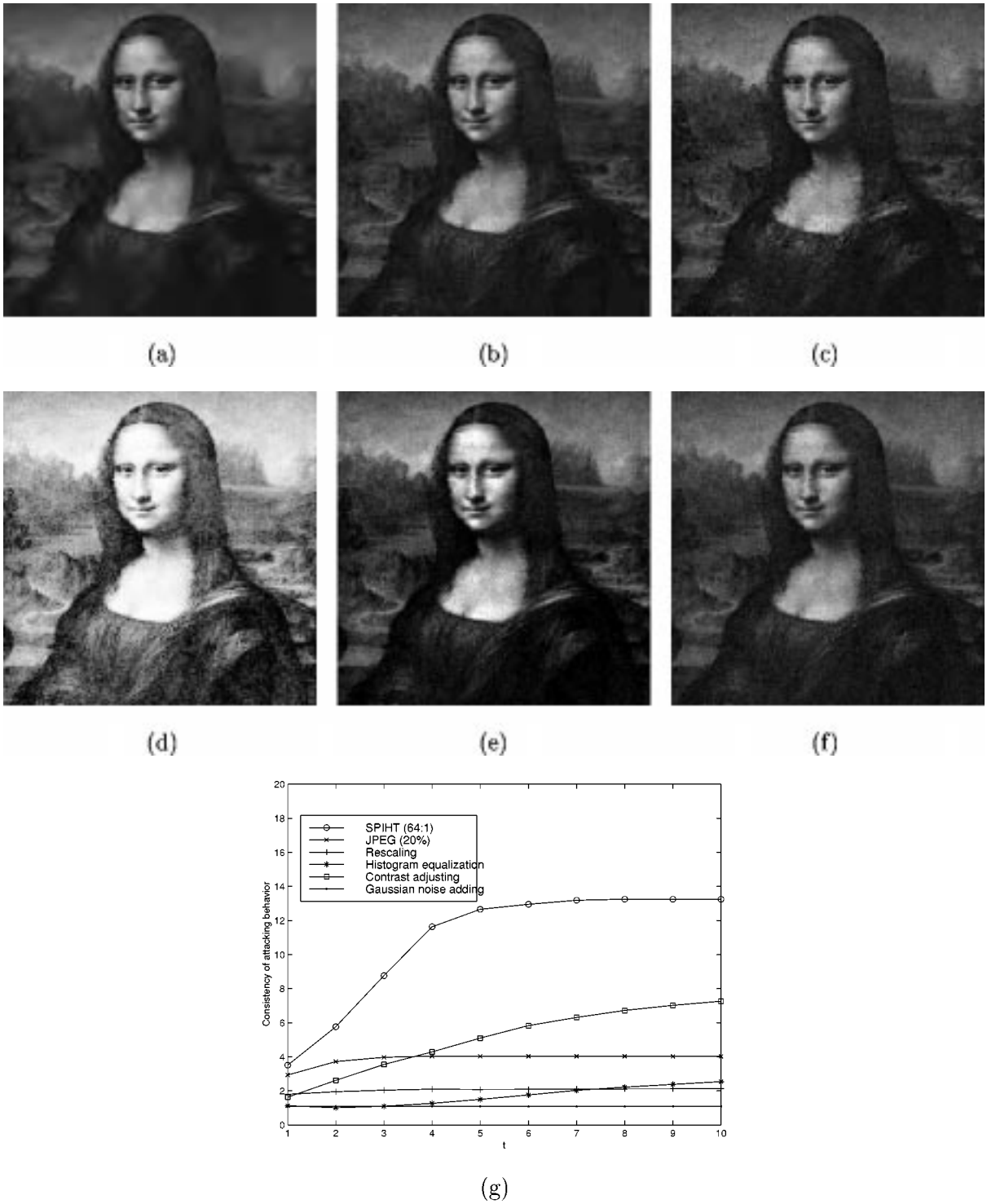


Fig. 7. Fragile watermarks facing incidental tampering: (a) *SPIHT* with compression ratio 64 : 1; (b) JPEG with quality factor 20% (compression ratio ≈ 20 : 1); (c) rescaled; (d) histogram equalized; (e) contrast adjusted; (f) Gaussian noise added; and (g) the BR_{fragile} values obtained at different $t(1 \leq t \leq 10)$ with respect to six distinct incidental manipulations.

One possible solution to this problem is to randomly select the hiding places from one of the Y, Cb, and Cr channels for watermarking. That is, the same position is only selected from one of the three channels such that the transparency requirement can be satisfied.

On the other hand, we also conducted an experiment about images [Fig. 6(a) and (b)], which encountered a combination of incidental manipulation and malicious tampering. Fig. 6(a) was obtained by introducing a malicious texture change on the face [Fig. 4(c)] followed by *SPIHT* compression at a ratio 8 : 1. Fig. 6(b) was obtained similarly but with an inverse order of attacks. The detection results of Figs. 6(a) and (b) obtained at different scales (with $t = 1$) were shown in Fig. 6 (c)–(e) and (f)–(h), respectively. We can see that the regions corresponding to where the face was modified were mostly located. However, some distorted regions which corresponded to the compression

effect were detected but they were sparsely spreaded. In this paper, we only show the tampering detection results at multiple scales. In [38], we have presented an information fusion technique which can integrate all the results at multiple scales to emphasize the maliciously modified regions and suppress the incidentally modified regions.

In addition to malicious tampering, compression, the most popular manipulation, was used to check the robustness of our fragile watermarking scheme. The perception-based fragility and the invariance-based fragility were compared with respect to *JPEG* and *SPIHT* compression, respectively. The results of these comparisons are summarized in Tables I and II. From the two tables, it is obvious that the watermark embedded using negative modulation (NM) was more robust to compression than was that embedded using positive modulation (PM) by comparing their fragile detector response. Besides, a threshold (e.g., 0.15) can be used [13] to judge the robustness of a fragile watermarking scheme. This threshold may be application-dependent and is sometimes hard to determine. However, if the fragile detector response with respect to incidental modification could be controlled to be as small as possible, then it will be helpful to the selection of a threshold. As we can see in Tables I and II, the fragile detector responses with respect to NM are much smaller than those of [13] and are almost comparable with those of *INV* (invariance). This means that the robustness of incidental manipulation could be achieved to some extent while preserving fragility of malicious tampering. On the other hand, if the *INV* between watermark values is utilized, our approach can be extremely robust to compression.

In addition to compression, there are also some incidental manipulations [6] needed to be handled for fragile watermarking. The criterion mentioned in Section III-D3 was used to measure the robustness of our fragile watermarking scheme. The cocktail watermarked MonaLisa image [Fig. 4(b)] was modified by SPIHT with compression ratio (64:1), JPEG compression with quality factor (20%), rescaling, histogram equalization, contrast enhancement and Gaussian noise addition, respectively, as shown in Fig. 7(a)–(f). The behavior ratio of fragility (BR_{fragile}) with respect to t $(1 \leq t \leq 10)$ is depicted in Fig. 7(g). As we have described previously, there was no significant fragility loss even t was increased from one to ten. It can be observed from Fig. 7(g) that all curves turned flat when t was increased. The above mentioned experimental results indicate that a larger t will be beneficial to robustness but will not seriously affect fragility. On the other hand, a larger behavior ratio of fragility (BR_{fragile}) resulted from a larger t reflects that the behaviors of an attack can be captured by NM or PM. These phenomena confirmed what we have discussed in Section III-D3. The experimental results shown in Fig. 7(g) can be summarized as follows. The value of BR_{fragile} is always larger than or equal to four as t increases under the *SPIHT* compression, contrast adjusting and *JPEG* compression. All of these manipulations can thus be considered as incidental. On the other hand, our approach fails to tolerate Gaussian noise adding because BR_{fragile} is too small. For the cases of histogram equalization[1] and rescaling, our approach sometimes works but sometimes doesn't. Once again, if the *INV* between watermark values is utilized, our approach tolerates these incidental modifications well. So, even some operations are regarded as incidental, but their effects should also taken into account in the application of fragile watermarking. That is, some improved histogram equalization techniques such as the one proposed in [31] should be considered as really incidental instead of the original one used in this paper.

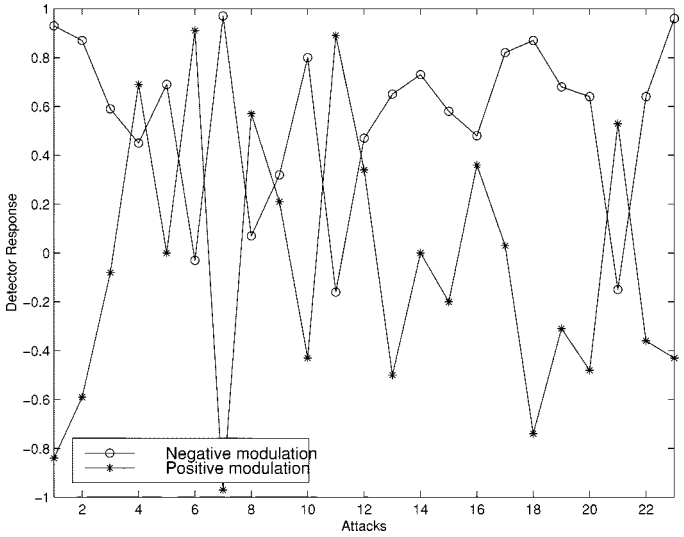


Fig. 8. Detector response for robust watermarks.

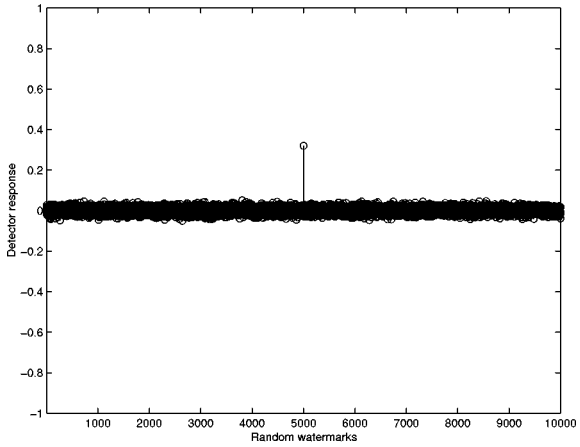
B. Results of Robust Watermarking

In this section, we shall discuss the experimental results with regard to robust watermarking. The same watermarked "MonaLisa" image [Fig. 4(b)], used for fragile test in the previous section, had also been used for robustness test in [20] under several attacks. Here, we used a different image for robust watermarking to demonstrate that our scheme adapts to different images. The "sailboat" image with size 256×256 was used to evaluate the robustness of our scheme. After watermarking, 23 different attacks including blurring, median filtering, rescaling, histogram equalization, jitter attack, changing the brightness/contrast, the negative film effect, segmentation, Gaussian noise adding, mosaicing, sharpening, texturizing, shading, the ripple effect, netdotting, uniform noise adding, the twirl effect, *SPIHT* compression, *JPEG* compression, StirMark[2] [27], dithering, pixel spreading, and cropping were selected to test the robustness of our watermarking scheme. Fig. 8 shows the robust watermark detection results. For each pair of detected watermarks, one watermark could be destroyed (with lower response) while the other survived well (with higher detector response). The lowest detector response as shown in Fig. 8 was 0.32 (the ninth attack), which corresponds to the Gaussian noise attack. We used the worst result to verify the uniqueness requirement, i.e., to show the false positive probability. Fig. 9 shows the detector responses with respect to 10 000 random marks (including the hidden one, i.e., the 500th mark). It is

[1]Please note that although histogram equalization is useful in enhancing image contrast, its effect is sometimes too severe in many purposes [31].

[2]In the following experiments, StirMark of version 2.3 with all default parameters is used.

(a)



(b)

Fig. 9. Uniqueness verification of robust watermarking under a Gaussian noise adding attack (a) attacked image after the Gaussian noise was added and (b) the detector responses of the extracted watermark with respect to 10 000 random marks (including the hidden the hidden one, the 5000th mark).

obvious that the response with respect to the hidden one is a recognizable spike.

VI. Conclusion

A multipurpose watermarking scheme which can be applied to achieve both authentication and protection of multimedia data has been presented in this paper. Watermarks are embedded once in the hiding process and can be blindly extracted for different applications in the detection process. The proposed scheme has three special features:

1) The approximation information of a host image is kept in the hiding process by utilizing masking thresholds [36].
2) Oblivious and robust watermarking is achieved for copyright protection.
3) Fragile watermarking is achieved for detection of malicious modifications and tolerance of incidental manipulations.

In addition to images (gray-scale and color), this method has been extended to audio watermarking [21]. To the best of our knowledge, this is the first method that combines both robust watermarking and fragile watermarking into a single one for image/audio authentication and protection.

There are still some issues that deserve further exploration. First, we shall focus on the issue of how to eliminate the need of storing and retrieving the mapping file and the hidden watermarks (considered as secret keys) for watermark detection. It is believed that secret key detection will encumber the automation and portability of watermarking. We shall spend more time on the issue of public-key detection [8]. Second, trying to devise a general enough mechanism which can resist a great variety of attacks is a very difficult problem because attackers can always design smarter attacks [16], [35]. Therefore, we shall spend some time on this issue in our future research. Third, we shall seriously deal with the multiple watermarking problem in the future. To the best of our knowledge, if multiple watermarking is used by other people for malicious purpose, then it is equivalent to the "ownership deadlock" problem [4]. On the other hand, if multiple watermarking is used by the owner himself for commercial purpose, then this scenario is similar to the fingerprinting problem. Our future work will consider combining fragile watermarking and fingerprinting together. By and large, the aforementioned mechanism is still an open problem and requires to be further explored.

Acknowledgment

The authors would like to thank the anonymous reviewers for their comments and suggestions which have improved the readability and technical content of this paper. The authors also thank Dr. M. Kutter for providing the color images shown in Fig. 5.

References

[1] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "Copyright protection of digital images by embedded unperceivable marks," *Image Vis. Comput.*, vol. 16, pp. 897–906, 1998.
[2] S. Bhattacharjee and M. Kutter, "Compression tolerant image authentication," in *Proc. IEEE Int. Conf. on Image Processing*, 1998.
[3] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, vol. 6, pp. 1673–1687, Dec. 1997.
[4] S. Craver, N. Memon, B.-L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks and implications," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 573–586, 1998.
[5] I. Daubechies, "Ten lectures on wavelets," in *CBMS-NSF Regional Conference Series in Applied Mathematics*. Philadelphia, PA: SIAM, 1992.
[6] J. Dittmann, A. Steinmetz, and R. Steinmetz, "Content-based digital signature for motion pictures authentication and content-fragile watermarking," in *IEEE Int. Conf. Multimedia Computing Systems*, 1999.
[7] G. L. Friedman, "The trustworthy digital camera: restoring credibility to the photographic image," *IEEE Trans. Consum. Electron.*, vol. 39, pp. 905–910, 1993.
[8] T. Furon and F. P. Duhamel, "Robustness of an asymmetric watermarking method," in *Proc. IEEE Int. Conf. on Image Processing*, Vancouver, BC, Canada, 2000, pp. 21–24.
[9] D. Gabor, "Theory of communication," *J. Inst. Elect. Eng.*, vol. 93, pp. 429–457, 1946.
[10] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Process.*, vol. 66, pp. 283–302, 1998.
[11] J. R. Hernandez and F. Perez-Gonzalez, "Statistical analysis of watermarking schemes for copyright protection of images," *Proc. IEEE*, vol. 87, pp. 1142–1166, July 1999.

[12] D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," in *Proc. IEEE Conf. Acoust., Speech, Signal Processing*, vol. 5, 1998, pp. 2969–2972.
[13] ——, "Digital watermarking for telltale tamper proofing and authentication," *Proc. IEEE*, vol. 87, pp. 1167–1180, 1999.
[14] M. Kutter, F. Jordan, and F. Bossen, "Digital signature of color images using amplitude modulation," *J. Electron. Imag.*, vol. 7, pp. 326–332, 1998.
[15] M. Kutter, "Watermarking resisting to translation, rotation and scaling," in *Proc. SPIE Multimedia Systems Applications*, vol. 3528, Boston, MA, Nov. 1998, pp. 423–431.
[16] M. Kutter, S. Voloshynovskiy, and A. Herrigel, "The watermark copy attack," in *Proc. SPIE Security Watermarking Multimedia Contents II*, San Jose, CA, 2000.
[17] C.-Y. Lin and S.-F. Chang, "A robust image authentication method surviving JPEG lossy compression," *Proc. SPIE*, vol. 3312, 1998.
[18] ——, "Issues and solutions for authenticating MPEG video," *Proc. SPIE*, 1999.
[19] C. S. Lu, S. K. Huang, C. J. Sze, and H. Y. M. Liao, "Cocktail watermarking for digital image protection," *IEEE Trans. Multimedia*, vol. 2, pp. 209–224, Dec. 2000.
[20] C. S. Lu, H. Y. M. Liao, and C. J. Sze, "Combined watermarking for image authentication and protection," in *Proc. IEEE Conf. Multimedia Expo*, vol. III, USA, 2000, pp. 1415–1418.
[21] C. S. Lu, H. Y. M. Liao, and L. H. Chen, "Multipurpose audio watermarking," in *Proc. 15th Int. Conf. Pattern Recognition*, Barcelona, Spain, 2000, pp. 286–289.
[22] C. S. Lu and H. Y. M. Liao, "Structural digital signature for image authentication: An incidental distortion resistant scheme," in *Proc. Multimedia Security Workshop, 8th ACM Int. Conf. Multimedia*, Los Angeles, CA, 2000, pp. 115–118.
[23] S. G. Mallat, "A theory for multiresolution signal decomposition: The wavelet representation," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 11, pp. 674–693, July 1989.
[24] F. Mintzer and G. W. Braudaway, "If one watermark is good, are more better?," in *Int. Conf. Acoustics, Speech, Signal Processing*, 1999, pp. 2067–2070.
[25] D. Mukherjee, J. J. Chae, S. K. Mitra, and B. S. Manjunath, "A source and channel-coding framework for video-based data hiding in video," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 10, pp. 630–645, 2000.
[26] S. Pereira and T. Pun, "Fast robust template matching for affine resistant image watermarks," in *Proc. 3rd Int. Workshop Information Hiding , LNCS 1768*, 1999, pp. 199–210.
[27] F. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *Proc. 2nd Workshop Information Hiding*, 1998, pp. 218–238.
[28] ——, "Information hiding: A survey," *Proc. IEEE*, vol. 87, pp. 1062–1078, July 1999.
[29] C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 525–539, 1998.
[30] J. J. K. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Process.*, vol. 66, pp. 303–318, 1998.
[31] J. A. Stark, "Adaptive image contrast enhancement using generalizations of histogram equalization," *IEEE Trans. Image Processing*, vol. 9, pp. 889–896, May 2000.
[32] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proc. IEEE*, vol. 86, pp. 1064–1087, 1998.
[33] P. C. Su, C.-C. J. Kuo, and H. J. Wang, "Blind digital watermarking for cartoon and map images," *Proc. SPIE*, 1999.
[34] S. Voloshynovskiy, A. Herrigel, N. Baumgartner, and T. Pun, "A stochastic approach to content adaptive digital image watermarking," in *Proc. 3rd Int. Workshop Information Hiding*, Dresden, Germany , Sept. 1999, pp. 211–236.
[35] S. Voloshynvskiy, S. Pereira, A. Herrigel, N. Baumgartner, and T. Pun, "A generalized watermark attack based on stochastic watermark estimation and perceptual remodulation," *Proc. SPIE*, 2000.
[36] A. B. Watson, G. Y. Yang, J. A. Solomon, and J. Villasenor, "Visibility of wavelet quantization noise," *IEEE Trans. Image Processing*, vol. 6, pp. 1164–1175, Aug. 1997.
[37] M. M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," in *Proc. IEEE Conf. Image Processing*, vol. 2, 1997, pp. 680–683.
[38] G. J. Yu, C. S. Lu, and H. Y. M. Liao, "Mean quantization-based fragile watermarking for image authentication," *Opt. Eng. J.*, 2001, to be published.
[39] B. Zhu, M. D. Swanson, and A. H. Tewfik, "Transparent robust authentication and distortion measurement technique for images," in *Proc. IEEE Digital Signal Processing Workshop*, 1996, pp. 45–48.

Chun-Shien Lu (M'99) was born in Tainan, Taiwan, R.O.C., in 1967. He received the Ph.D. degree in electrical engineering from National Cheng-Kung University, Tainan, in 1998.

From September 1994 to June 1998, he was a Research Assistant with the Institute of Information Science, Academia Sinica, Taipei, Taiwan. Since October 1998, he has been a Postdoctoral Fellow. His current research interests include digital watermarking/data hiding, multimedia information processing, image/signal processing, and visual communications.

Dr. Lu was the recipient of the Excellent Paper Award of the Image Processing and Pattern Recognition Society of Taiwan in 2000 for his work on digital watermarking and the Paper Award from the same society in 1997, 1999, and 2001. He organized a special session on data hiding and multimedia security for the Second IEEE Pacific-Rim Conference on Multimedia (PCM'2001), Beijing, China, in 2001.

Hong-Yuan Mark Liao (S'87–M'88) received the B.S. degree in physics from the National Tsing-Hua University, Hsinchu, Taiwan, R.O.C., in 1981 and the M.S. and Ph.D. degrees in electrical engineering from Northwestern University, Evanston, IL, in 1985 and 1990, respectively.

He was a Research Associate with the Computer Vision and Image Processing Laboratory at Northwestern University during 1990–1991. In July 1991, he joined the Institute of Information Science, Academia Sinica, Taipei, Taiwan, as an Assistant Research Fellow. He was promoted to Associate Research Fellow and then Research Fellow in 1995 and 1998, respectively. From August 1997 to July 2000, he served as the Deputy Director of the institute. Currently, he is the Acting Director of Institute of Applied Science and Engineering Research, Academia Sinica. His current research interests include multimedia signal processing, wavelet-based image analysis, content-based multimedia retrieval, and multimedia protection. He is is on the editorial boards of the *International Journal of Visual Communication and Image Representation*; the *Acta Automatica Sinica*; the *Tamkang Journal of Science and Engineering*; and the *Journal of Information Science and Engineering*.

Dr. Liao was the recipient of the Young Investigators Award of Academia Sinica in 1998; the Excellent Paper Award of the Image Processing and Pattern Recognition Society of Taiwan in 1998 and 2000 and the Paper Award from the same society in 1996 and 1999. Dr. Liao served as the program chair of the International Symposium on Multimedia Information Processing (ISMIP'1997) and will serve as the Program Co-chair of the second IEEE Pacific-Rim Conference on Multimedia (2001). He also served on the program committees of several international and local conferences. He is on the editorial board of the IEEE TRANSACTIONS ON MULTIMEDIA. He is a member of the IEEE Computer Society.