New Semi-Fragile Image Authentication Watermarking Techniques Using Random Bias and Nonuniform Quantization

Kurato Maeno, Qibin Sun, Shih-Fu Chang, *Fellow, IEEE*, and Masayuki Suto

***Abstract*—Semi-fragile watermarking techniques aim at detecting malicious manipulations on an image, while allowing acceptable manipulations such as lossy compression. Although both of these manipulations are considered to be pixel value changes, semi-fragile watermarks should be sensitive to malicious manipulations but robust to the degradation introduced by lossy compression and other defined acceptable manipulations. In this paper, after studying the characteristics of both natural images and malicious manipulations, we propose two new semi-fragile authentication techniques robust against lossy compression, using random bias and nonuniform quantization, to improve the performance of the methods proposed by Lin and Chang.**

***Index Terms*—JPEG2000, nonuniform quantization, random bias, semi-fragile watermark, wavelet transform.**

I. Introduction

MANY fragile watermarking techniques for digital content authentication have been studied in the past few years. Fragile watermarks are used to determine if a watermarked image has been altered, and distinguish altered areas from nonaltered areas without referring to the original image. Fragile watermarking can be roughly classified into two types of approaches. The first one embeds certain key-dependent patterns imperceptibly into the images and then detects the alterations when the patterns are tampered with [2], [3]. The other embeds the features extracted from the image and detects the alterations by comparing these embedded features with the actual features re-extracted from the image [4], [5].

Most fragile watermarks are designed to verify exact image data integrity. It is therefore not feasible for the imaging related applications such as lossy compression in the image transmission or storage. Though it only changes the entire image slightly, the whole image data integrity is always lost. That is, fragile watermarks will be easily destroyed if lossy compression is performed because the patterns embedded imperceptibly in the least significant bit (LSB) are destroyed, or that the hash values are changed into entirely different values due to the slight changes of the image.

Manuscript received March 20, 2002; revised November 29, 2004. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Radu Serban Jasinschi.

K. Maeno and M. Suto are with Oki Electric Industry Co., Ltd., Warabi, Saitama 335-8510, Japan (e-mail: maeno284@oki.com; sutou627@oki.com).

Q. Sun is with Institute for Infocomm Research, Singapore 119613 (e-mail: qibin@i2r.a-star.edu.sg).

S.-F. Chang is with the Department of Electrical Engineering, Columbia University, New York, NY 10027 USA (e-mail: sfchang@ee.columbia.edu).

Digital Object Identifier 10.1109/TMM.2005.861293

Recent studies proposed some semi-fragile watermarking techniques which allow acceptable manipulations such as lossy compression while still detect other malicious manipulations. For example, the method proposed by Lin and Delp [6] embeds the block-based patterns as the watermarks and detects the alterations by verifying the correlations on these patterns. Nonetheless, this method still has some problems such as failure to detect alterations to dc coefficients only or substitutions of blocks with same address generated from the same key. It also presumes that most natural images have smooth features; that is, false alarms near edges can occur due to low correlations. Therefore, further studies are required to adjust the tradeoff between the alteration detection sensitivity and the false alarm for practical applications. Another technique is proposed by Eggers and Girod [8], in which binary sequence is embedded using Scalar Costa Scheme (SCS) Watermarking [7], and the alterations are detected by conducting likelihood test of the sequence. This method has the same problems as Lin and Delp's approach, because image features are not used.

Differing from the techniques described above, Lin and Chang [1] proposed a novel solution in which image features are used. It generates the invariant features at lossy compression, and embeds them into middle frequency coefficients of discrete cosine transform (DCT) blocks. As this method separates the process of feature generating from feature embedding, it could scramble the relationships between the coefficients for feature generating and embedding, thereby making it robust against a substitution of blocks. This approach has an advantage over Lin and Delp's technique in that false alarms near edges in images hardly occur as image features have been incorporated for alteration detection.

To address the noise caused by practical implementations (such as the noise caused by finite word lengths), it introduced an error tolerance margin to reduce the false alarm rate. But the use of such error margins may also cause the algorithm to miss some malicious alterations of images. One example of such a content altering operation is the smoothing manipulation (e.g., objects deletion by filling with background colors/textures), in which the changes to the DCT coefficient difference may be within the tolerance margin, thus it is unable to detect this type of manipulations. The above issue is attributed to two sources of limitation in the original technique. First, due to the requirements in controlling the signature length, the relationship of two DCT coefficients in the same pair is encoded by one single bit only. Second, relationships among the DCT coefficients in a local proximity area are not explored.

In this paper, we address these two problems and propose two techniques to improve the performance of the semi-fragile authentication watermarking. In addition, we extend the JPEG DCT-based watermarking technique to the wavelet domain and extend the acceptable compression to JPEG2000. Specifically, our objective is to improve the performance tradeoff between the alteration detection sensitivity and the false alarm rate and apply them to authenticating JPEG2000 images.

In our first method, we explore the correlation among coefficients in a local window. An interesting phenomenon shown in experiments indicated that a given manipulation tends to cause similar change patterns to coefficients in a local window. Such similar patterns result in a clustered distribution in the (original difference—new difference) plane. The fixed encoding boundary used in the original technique has a potential issue of missing all the pairs of coefficients for such a malicious manipulation. In this new method, we introduce a novel component which adds a random bias factor to the decision boundary. Such a randomization factor spreads out to each signature bit for catching the malicious manipulations. Specifically, random biases will randomly change the authentication thresholds on each individual result of the coefficient-pair comparison. In the original method, the thresholds are fixed at zero. In the new method, the threshold values have a zero-mean random distribution (e.g., Gaussian). The tolerance margin for handling errors depending on the implementation is still kept to control the false alarm rate.

In our second method, we propose a nonuniform quantization scheme which uses a multibit nonuniform quantizer to encode the transform coefficient difference in each pair, and uses the different quantizers at the signature verification site. We use multiple bits to improve the accuracy in encoding the relationships between paired transform coefficients. We use nonuniform quantizers to explore the nonlinear mapping between the coefficient differences in the original image and the compressed image. The coefficient pair is formed by selecting two coefficients from the same subband but at different locations.

After analyzing the properties of different distortions caused by the acceptable (e.g., lossy compression) and the unacceptable (e.g., copy-paste) manipulations and the problems in the original method in Section II, the two new approaches are detailed in Section III. Experiments in Section IV further demonstrate that the proposed solutions improve the performance significantly in distinguishing acceptable manipulations from nonacceptable ones. Finally, the paper is concluded in Section V.

II. Previous Work on the DCT-Based Semi-Fragile Watermarking

In this section, we review the semi-fragile watermarking approach proposed by Lin and Chang [1], together with analyzing the properties of different distortions caused by the acceptable (e.g., lossy compression) and the unacceptable (e.g., copy-paste) manipulations. [1] is well recognized for its capability of providing a deterministic guarantee of a zero false alarm rate and a statistical guarantee of a miss rate in distinguishing malicious manipulations from JPEG lossy compression. The authors have deployed popular software that is freely downloadable and available for testing from an online web site [7].

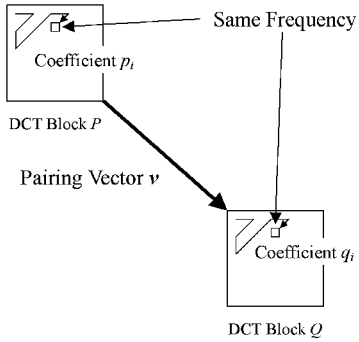

Fig. 1. Coefficients' selection: A signature bit is generated for two coefficients p_i and q_i. p_i and q_i belong to the same frequency and are selected by pairing vector v_i.

When an image is compressed with JPEG, its image pixels are transformed to DCT coefficients, and then quantized. Lin and Chang found that the magnitude relationship between two coefficients remains invariable through repetitive JPEG compression. They demonstrated that semi-fragile image authentication for JPEG is feasible using this property [1]. The authenticity of the image could be verified by a 1-bit signature which represents the magnitude relationship between the two DCT coefficients.

At the signature generation site (shown in Fig. 2), a signature bit is generated from the two coefficients corresponding to the same frequency in two different DCT blocks, which are selected using a "pairing vector" determined by a pseudo-random sequence. Given a pair of coefficients (q_i and q_i) from these two blocks, (1) is applied (see Fig. 1)

$$\mathrm{Sig}_i = \begin{cases} 0, & (p_i - q_i \geq 0) \\ 1, & (p_i - q_i < 0) \end{cases} \tag{1}$$

where p_i *and* q_i are DCT transformed coefficients in the same frequency location from two different blocks, and the location of q_i is determined by the location of p_i and vector $\boldsymbol{v}_i$, $\boldsymbol{q}_i = \boldsymbol{p}_i + \boldsymbol{v}_i$. Sig_i is the signature bit for the relationship between p_i and q_i.

The signature bits are then embedded into other DCT coefficients, which are selected using another pseudo-random sequence, from upper-left ac coefficients of other DCT blocks. Dc coefficients are not used to avoid visible block artifacts, and lower-right ac coefficients are also not embedded. Relationships between signature generation pairs and embedding locations are scrambled for security purpose. For the details of watermark embedding, readers are referred to [1].

At the verification site (shown in Fig. 3), DCT coefficients are verified by these signature bits, which is similar to the signature generation site. The verification procedure consists of three steps: 1) extracting signatures that have been embedded by the embedding site; 2) generating difference values from the DCT coefficients; and 3) verifying the extracted signatures and the generated difference values according to three conditions 1, 2, and 3 listed below. Condition 2 is used to have a certain margin to tolerate the noise introduced by some acceptable manipulations, such as color transforms, different codec implementations, and integer rounding. A relationship that satisfies any one

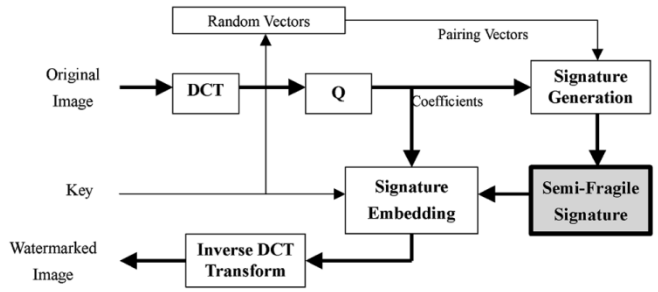

Fig. 2. Semi-fragile watermark generation steps.

of these 1–3 conditions shall be considered unmanipulated; otherwise, the coefficient pairs are considered manipulated.

$$\begin{cases} p'_i - q'_i > M & \text{and } \mathrm{Sig}_i = 0 \quad \text{(condition 1)} \\ |p'_i - q'_i| \le M & \text{(don't care for } \mathrm{Sig}_i\text{)} \quad \text{(condition 2)} \\ p'_i - q'_i < -M & \text{and } \mathrm{Sig}_i = 1 \quad \text{(condition 3)} \end{cases}$$

where p'_i and q'_i are DCT transformed coefficients which are used to generate the signature bits "Sig_i" at the verification site (typically, after lossy compression), and the location of q'_i is determined by the location of p'_i and vector $\boldsymbol{v}_i$ (the same as generator), $\boldsymbol{p}'_i = \boldsymbol{q}'_i + \boldsymbol{v}_i$. M is the margin value to avoid false alarms caused by lossy compression by different quantizers, or noises introduced by different implementations.

As a result, a pair of coefficients falling into $p_i - q_i \ge 0$ at the signature generation site shall be considered manipulated if it falls into $p'_i - q'_i < M$ (the size relationship is reversed) at the verification site. Similarly, one falling into $p_i - q_i < 0$ at the signature generation site shall be considered manipulated if it falls into $p'_i - q'_i > -M$ (the size relationship is reversed) at the verification site.

Here, a big security hole may arise from the relationships which fall into $|p'_i - q'_i| \le M$ (condition 2) that is placed here to allow for some noises at the verification site, because they are not considered manipulated regardless of the size relationships at the signature generation site. Thus, if the image is manipulated to make the absolute value of the difference between p'_i and q'_i below the margin value M, this type of manipulation will never be detected no matter what the coefficient values p_i and q_i (and v_i) at signature generation are (meshed area in Fig. 4).

Note the original method by Lin and Chang takes advantage of the relationship invariance property under JPEG-type quantization. Under such operations, the (original difference-new difference) points will be located at the diagonal line $(\mathrm{slope} = 1)$ if there is no implementation noise, or near the diagonal line when the noise exists. However, due to the use of only one bit in representation, the acceptable regions (the entire upper right quadrant and the entire lower left quadrant) include areas that may lead to undetected manipulations.

If this type of manipulation is practically meaningless, impossible and/or very difficult to achieve, this problem may be negligible. In reality, however, it is very easy to achieve and can even be very harmful to certain content. For example, we have the following.

Deletion of objects:

Objects can be deleted very easily especially for the images with a very homogeneous background such as a document image. Objects can also be deleted by pasting a smooth textural background over them.

Addition of light-colored objects:

It can be done by drawing very light-colored objects on backgrounds.

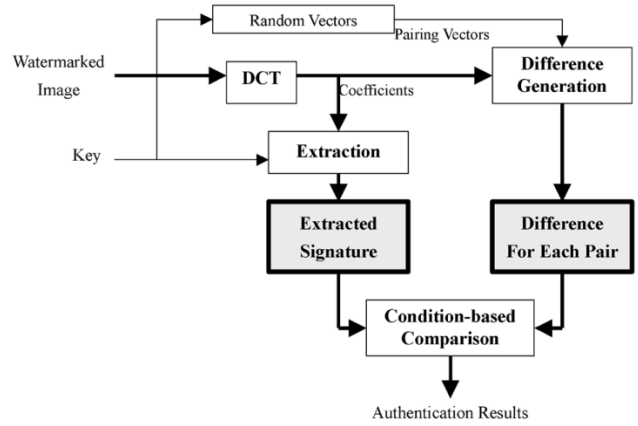

Fig. 3. Semi-fragile watermark verification steps.

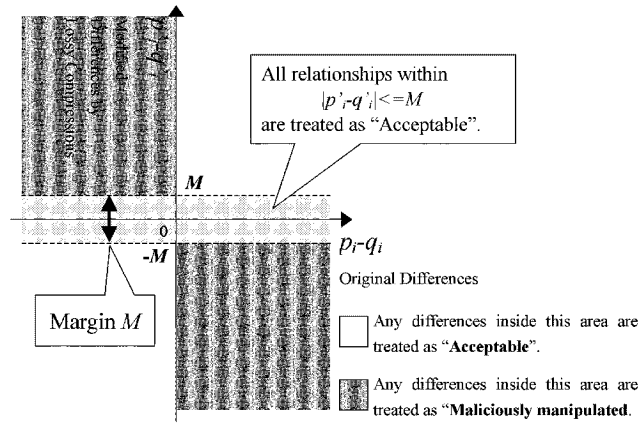

Fig. 4. Differences for manipulation detection.

Neglecting these manipulations may cause extremely harmful defects especially in case of digital watermarking, which should prevent evidential images and document images from being manipulated.

In Section III, we propose two solutions to overcome these defects and further improve the alteration detection rate: 1) the Random Bias method and 2) the Nonuniform Quantization method. We compare them with Lin and Chang's method in the wavelet domain. Note that although Lin and Chang's method was originally applied in DCT domain for JPEG image authentication, their basic concept is actually transform-domain independent because what they derived is an invariant relationship between a pair of coefficients under different quantization step size. In the rest of this paper, therefore, we only discuss our techniques in the context of the wavelet transform of JPEG2000, though the techniques can be applied to block-based transforms like DCT of JPEG as well.

III. Watermarking Algorithm

In this section, we propose: 1) the Random Bias method and 2) the Nonuniform Quantization method. Details are described

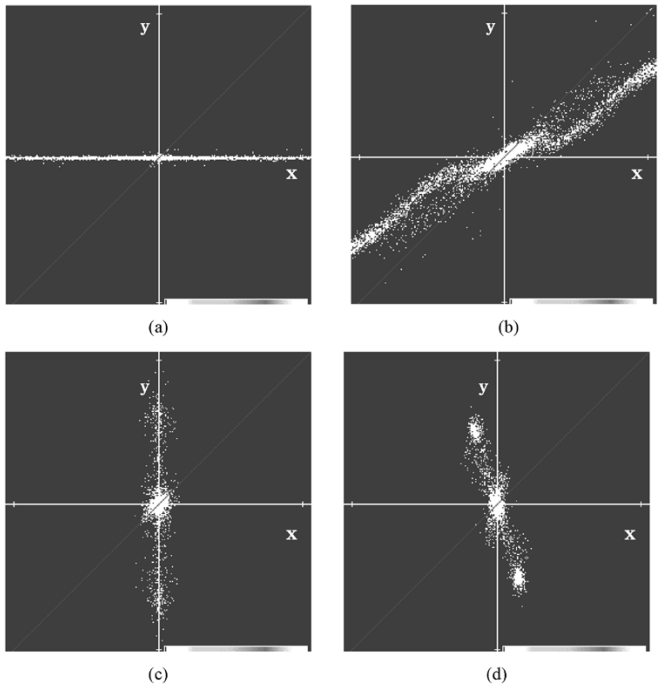

Fig. 5. Distribution of coefficient difference before and after manipulation. x axis indicates original difference values, and y axis indicates new difference values after manipulated. (a) Delete Image Objects. (b) Change luminance (from 255 to 99). (c) Delete image objects. (d) Change hue (results of a color component). Coefficients belong to 1LL subband transformed by 5×3 integer wavelet filter (JPEG2000 Compatible).

in Section IV. The Random Bias method makes it difficult for attackers to keep the difference below the margin value M by adding a random bias to the difference between two coefficients p_i and q_i. The Nonuniform Quantization method firstly removes "don't care" parts (introduced by the margin value) by using multibit representation for signature generation. It then reduces the degradation of image visual quality caused by long signature embedding by shortening signature bits with the codeword assignment table, while still keeping the high detection rate.

A. Random Bias Method

First, we study how the pairs of coefficients were affected by manipulations in the wavelet domain (see Fig. 5). We found that although different manipulations involve many different effects, sometimes they still share some common features as listed below.

- The relationships between two coefficients which have been manipulated result in a certain clustered distribution on the (original difference-new difference) plane.
- These relationships gather around zero if the manipulation such as an object deletion occurs. This can be illustrated by the graph shown in Fig. 5(a).

If the relationships between two manipulated coefficients do not lead to a clustered distribution, shifting the thresholds in Lin and Chang's method from zero might decrease the alteration detection performance, because many relationships change around zero when manipulated (see Fig. 6). In this case, in order to prevent the drop of the detection rate, the signature length should be increased and multiple thresholds must be used to verify the relationships between two coefficients. However, manipulating

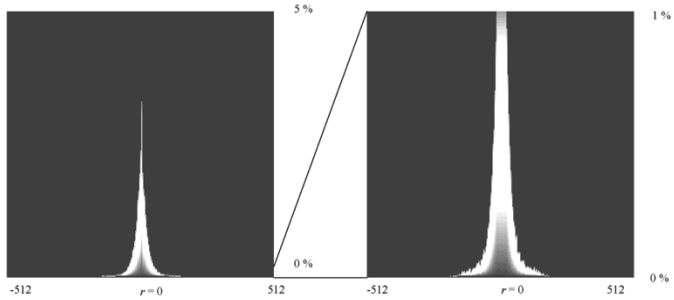

Fig. 6. Histogram of differences distributions for natural image. r indicates relationships (difference values) between two coefficients p_i and q_i.

the relationships in many cases results in a cluster. Therefore, verifying more than one relationship within the cluster with different thresholds (i.e., Fig. 7) will catch manipulations which are so far not detectable using a fixed zero-value threshold and decrease the possibility of misses.

The Random Bias method adds random values to the difference between two coefficients before the difference is encoded to the signature bit. The detailed algorithm of the Random Bias method is as follows.

At the signature generation site, the signature bit is given by

$$\mathrm{Sig}_i = \begin{cases} 0, & (p_i - q_i + B_i \geq 0) \\ 1, & (p_i - q_i + B_i < 0) \end{cases} \tag{2}$$

where p_i and q_i are wavelet transformed coefficients in the same subband, and the location of q_i is determined by the location of p_i and vector $\boldsymbol{v}_i$, $\boldsymbol{p}_i = \boldsymbol{q}_i + \boldsymbol{v}_i$. B_i is the $\boldsymbol{i}$th element of pseudo-random number sequence $\boldsymbol{B}$ as the random bias. Sig_i is the signature bit for the relationship between p_i and q_i.

At the signature verification site, a pair of coefficients satisfying any of conditions 4 –6 below shall be considered unmanipulated. Otherwise, it is considered manipulated

$$\begin{cases} p'_i - q'_i + B_i > M & \text{and } \mathrm{Sig}_i = 0 \quad \text{(condition 4)} \\ |p'_i - q'_i + B_i| \leq M & \text{(don't care for } \mathrm{Sig}_i\text{)} \quad \text{(condition 5)} \\ p'_i - q'_i + B_i < -M & \text{and } \mathrm{Sig}_i = 1 \quad \text{(condition 6)} \end{cases}$$

where p'_i and q'_i are wavelet transformed coefficients which are used to generate the signature bits "Sig_i" at the verification site (typically, after lossy compression), and the location of q'_i is determined by the location of p'_i and vector $\boldsymbol{v}_i$ (same as generator), $\boldsymbol{p}'_i = \boldsymbol{q}'_i + \boldsymbol{v}_i$. B_i is the $\boldsymbol{i}$th element of pseudorandom number sequence $\mathbf{B}$ as the random bias (same sequence of generator). M is the margin value to avoid false alarms caused by noises introduced by acceptable manipulations.

Note: It is obvious that the random sequence should be available to someone who knows the key, while it is difficult to guess for someone who does not know.

Some other issues, such as sequence generation and management, which should be taken into account for security purpose, are beyond the scope of this paper. Interested readers can find their corresponding solutions from cryptography.

Here, we describe a theoretical corroboration of margin value selection. Lin and Chang prove the following theorem in [1].

Assume p_i and q_i are transformed coefficients and Q_i is a quantization step size. Define $\Delta D_{pqi} \equiv p_i - q_i$ and, $\Delta \widetilde{D}_{pqi} \equiv \widetilde{p}_i - \widetilde{q}_i$ where $\widetilde{p}_i$ is defined as $\widetilde{p}_i \equiv Integer\ Round\,(p_i/Q_i) \cdot Q_i$.

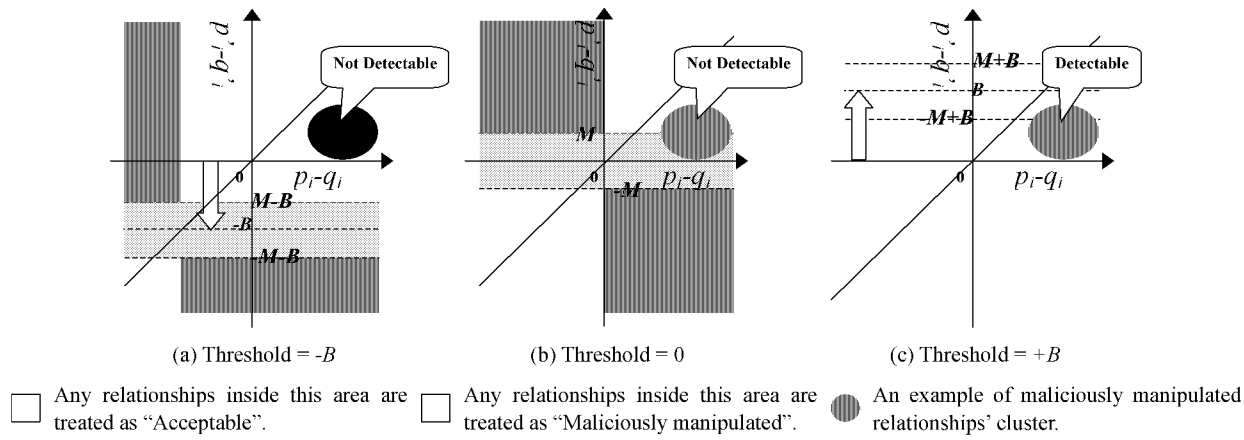

Fig. 7. Examples of various thresholds. The relationships caused by the manipulation become detectable after the threshold value is changed from zero to B.

Assume a fixed threshold $k \in \Re$ as the set of real number, define Z is the set of integer, and define $\widetilde{k}_i \equiv Integer\ Round\,(k/Q_i)$. Then

- if $\Delta D_{pqi} > k$

$$\Delta\widetilde{D}_{pqi} \geq \begin{cases} \widetilde{k}_i \cdot Q_i, & \frac{k}{Q_i} \in Z \\ \left(\widetilde{k}_i - 1\right) \cdot Q_i, & \text{elsewhere} \end{cases} \tag{3}$$

- if $\Delta D_{pqi} < k$

$$\Delta\widetilde{D}_{pqi} \leq \begin{cases} \widetilde{k}_i \cdot Q_i, & \frac{k}{Q_i} \in Z \\ \left(\widetilde{k}_i + 1\right) \cdot Q_i, & \text{elsewhere} \end{cases} \tag{4}$$

- if $\Delta D_{pqi} = k$,

$$\Delta\widetilde{D}_{pqi} = \begin{cases} \widetilde{k}_i \cdot Q_i, & \frac{k}{Q_i} \in Z \\ \left(\widetilde{k}_i \; or \; \widetilde{k}_i \pm 1\right) \cdot Q_i, & \text{elsewhere.} \end{cases} \tag{5}$$

In the case of $k = 0$, this theorem describes the invariant property of the sign of ΔD_{pqi} except for $\Delta D_{pqi} = 0$, as follows:

$$\text{if } \Delta D_{pqi} \geq 0, \quad \Delta\widetilde{D}_{pqi} \geq 0 \tag{6}$$

$$\text{if } \Delta D_{pqi} \leq 0, \quad \Delta\widetilde{D}_{pqi} \leq 0. \tag{7}$$

Next, we apply this original theorem to the Random Bias method. Assume a bias value $B_i \in Z$, which is simply generated by the fixed key, and define $\widetilde{B}_i \equiv Integer Round\,(B_i/Q_i)$. Then

- if $\Delta D_{pqi} + B_i \geq 0_i$

$$\Delta\widetilde{D}_{pqi} + B_i \geq \begin{cases} B_i - \widetilde{B}_i \cdot Q_i, & \frac{B_i}{Q_i} \in Z \\ B_i - (\widetilde{B}_i - 1) \cdot Q_i, & \text{elsewhere} \end{cases} \tag{8}$$

- if $\Delta D_{pqi} + B_i \leq 0_i$

$$\Delta\widetilde{D}_{pqi} + B_i \leq \begin{cases} B_i - \widetilde{B}_i \cdot Q_i, & \frac{B_i}{Q_i} \in Z \\ B_i - (\widetilde{B}_i + 1) \cdot Q_i, & \text{elsewhere.} \end{cases} \tag{9}$$

A difference between a bias value B_i and a quantized bias value $\widetilde{B}_i \cdot Q_i$ should be in the following range:

$$-\frac{1}{2}Q_i \leq B_i - \widetilde{B}_i \cdot Q_i \leq \frac{1}{2}Q_i. \tag{10}$$

Therefore

- if $\Delta D_{pqi} + B_i \geq 0$

$$\Delta\widetilde{D}_{pqi} + B_i \geq \begin{cases} -\frac{1}{2}Q_i, & \frac{B_i}{Q_i} \in Z \\ \frac{1}{2}Q_i, & \text{elsewhere} \end{cases} \tag{11}$$

- if $\Delta D_{pqi} + B_i \leq 0$

$$\Delta\widetilde{D}_{pqi} + B_i \leq \begin{cases} \frac{1}{2}Q_i, & \frac{B_i}{Q_i} \in Z \\ -\frac{1}{2}Q_i, & \text{elsewhere} \end{cases} \tag{12}$$

which indicates the margin value M of conditions 4–6 can be selected from $Q_i/2$ and above, which is robust to distortions caused by lossy compression with Q_i-step quantization. Accepting other manipulations such as other transform-domain compressions and some lossy operations may subject to increasing the margin value.

Again, with the original method, a manipulation is detected by comparing two coefficients in terms of their difference values. Adding a bias here shifts the basis for comparing difference value, from zero to the selected bias value. We expect that shifting biases randomly will enable detection of the alterations that have been undetectable so far, leading to an increased detection rate. For example, as shown in Fig. 7, differences (before and after the manipulation) of coefficient pairs are concentrated in a cluster. If we use a fixed threshold (0), none of the coefficient pairs will be detected. By randomly changing the threshold for each coefficient pair, we can reasonably expect some coefficient pairs to be detected when the threshold is shifted to a positive bias.

Now we can see that the malicious manipulation which makes changes to the relationship of $|p'_i - q'_i| \leq M$ is easily achievable but one which attempts to make changes to the relationship of $|p'_i - q'_i + B_i| \leq M$ will be extremely difficult to achieve because it has to know the random sequence which generates the random bias B_i. Furthermore, it is worth noting that the manipulation intending to change the current $|p'_i - q'_i| \leq M$ relationship can still render the manipulated area very smooth with background colors, etc. This results in very natural visual effects even though the image has been manipulated widely. On the other hand, with the Random Bias method, a random bias will cause the manipulated area to be an inhomogeneous noisy image if someone who knows the random sequence manipulates

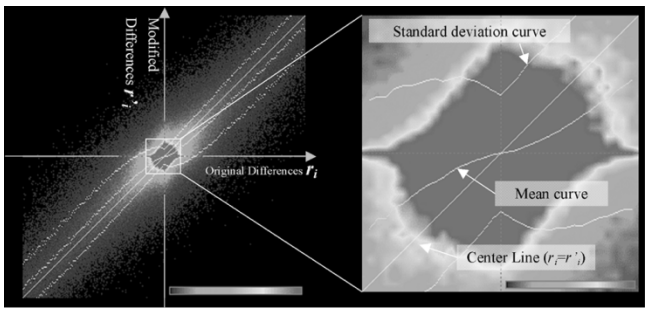

Fig. 8. Difference changes by JPEG2000 lossy compression. Original differences $r_i = p_i - q_i$. Modified differences $r'_i = p'_i - q'_i$. p_i, q_i, p'_i and q'_i are wavelet coefficients of 1LL using 5×3 wavelet filter and reversible color transform. p'_i and q'_i are modified by JPEG2000 lossy compression using 9×7 wavelet filter and irreversible color transform with 5 decomposition level and 0.25 bpp. The coefficients p_i and p'_i are at same location. q_i and q'_i are also the same.

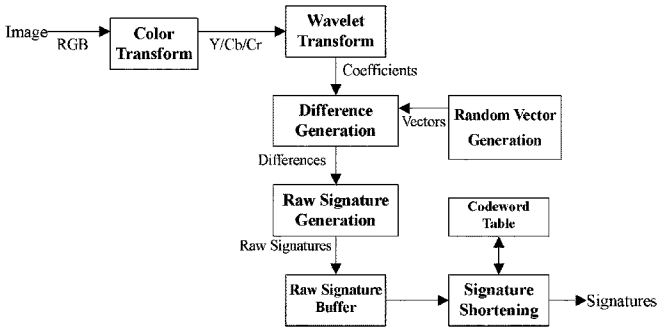

Fig. 9. Signature generator block diagram.

and deliberately controls the changes within the nondetectable range. This is the merit obtained in terms of system security.

B. Nonuniform Quantization Method

The Nonuniform Quantization method consists of two steps. The first step generates the raw signatures from the difference between a pair of coefficients p_i and q_i, by quantization. Unlike the previous approach, here each raw signature is represented by multiple bits. The second step concatenates a certain number of pairs of these raw signatures to produce one new signature, and then shortens it by hashing, thereby making the average representation of the whole signature 1 bit per one pair, the same as our previous approaches.

We call this method "Nonuniform Quantization" for two reasons: the first reason is that changing the quantization step sizes depends on the magnitude of the difference value; the second one is that the quantization step sizes used at the signature verification site may differ from those used at the signature generation site.

1) Analysis of Difference Changes by Lossy Compression: We describe our observation of how a pair of coefficients is affected by lossy compression in the wavelet domain. Fig. 8 shows how the difference value of a pair of coefficients changes when a natural image is lossy-compressed by JPEG2000. It plots on a $r_i - r'_i$ plane with two difference values (r_i, r'_i) obtained respectively from the identical points of two images (the original and the lossy-compressed). The x-axis indicates the difference values (r_i) obtained from the original image, and the y-axis indicates the difference values (r'_i) modified by JPEG2000 lossy compression. The mean curve and the standard deviation curve indicate the overall distribution of the mean value and standard deviation, respectively, calculated based on the difference value from the original image.

As a result of observation, we have the following findings in most cases.

- After lossy compression, the difference value decreases when it is positive, while it increases when negative. (It gets closer to zero in both cases)
- The difference value changes considerably around the value zero (although the absolute variance value is small)

Images compressed by other lossy compression such as JPEG supports the above observations as well. In addition, these observations also hold for a wide range of image types, such as document image, natural image and computer graphics image.

We analyze the possible reasons for these phenomena. We may say that lossy compression is a kind of low-pass filtering since it intends to diminish the energy of the image data as it contains much higher frequency elements. The image will be smoothed more and the difference between wavelet coefficients will be smaller when the low-pass filtering is applied to the image. This is the most likely reason that absolute values of differences of many coefficients become smaller than the originals. Additionally, a noise called ringing effect in JPEG2000, or mosquito noise in JPEG, may appear near the border of the image. These noises cause coefficient values near the border to fluctuate and therefore cause the difference values to fluctuate too. This seems to be another reason for causing some variations in distribution.

From the observations described above, it seems that the possibility of a false alarm may decrease while the detection efficiency increases if we generalize the above observations and assume that: 1) the magnitudes of the difference values around zero change more dramatically than others and 2) the magnitudes of the difference values at the signature verification site are smaller on average than that at the signature generation site.

2) Nonuniform Quantization: The Nonuniform Quantization method is developed in response to the above observations and hypothesis.

Figs. 9 and 12 are the block diagrams of the Nonuniform Quantization method. The modules before the "Differences Generation" block are the same as Lin and Chang's method and the Random Bias method described earlier. The unique functions of this method are realized in the subsequent modules.

Here, we describe the signature generation procedure. The input image is represented in wavelet coefficients after color transform and wavelet transform as in the Random Bias method. The vector obtained from the "Random Vector generation" block generates pairs of wavelet coefficients and calculates the differences from each pair (the process so far is the same as the Random Bias method and the original Lin and Chang method). The Nonuniform Quantization method generates the raw signatures that use several bits for each coefficient pair while Lin and Chang's method generates one-bit signature for each. The example of generating a raw signature with multiple

TABLE I
RAW SIGNATURES GENERATION p_i AND q_i ARE WAVELET TRANSFORMED COEFFICIENTS IN THE SAME SUBBAND, AND THE LOCATION OF q_i IS DETERMINED BY THE LOCATION OF p_i AND VECTOR $\boldsymbol{v}_i(\boldsymbol{q}_i = \boldsymbol{p}_i + \boldsymbol{v}_i)$, $\boldsymbol{Q}_1$ IS THE QUANTIZATION STEP SIZE AS THRESHOLD

Difference Range	Raw Signature
$Q_1 < p_i - q_i$	0
$\lvert p_i - q_i \rvert \le Q_1$	1
$p_i - q_i < -Q_1$	2

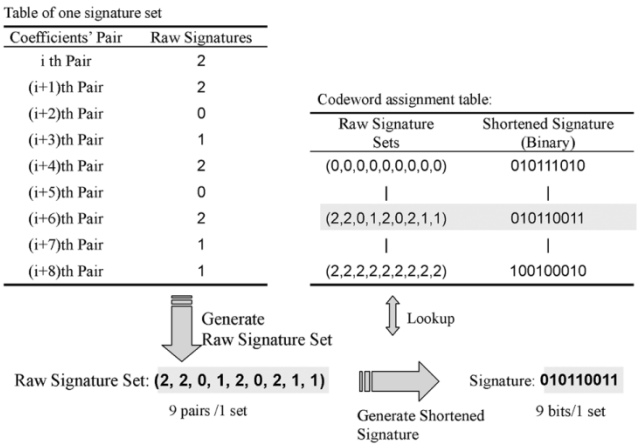

Fig. 10. Examples of signature generation.

TABLE II
ACCEPTABLE RAW SIGNATURES GENERATION p'_i AND q'_i ARE WAVELET TRANSFORMED COEFFICIENTS IN THE SAME SUBBAND, AND THE LOCATION OF q'_i IS DETERMINED BY THE LOCATION OF p'_i AND VECTOR $\boldsymbol{v}_i(\boldsymbol{q}'_i = \boldsymbol{p}'_i + \boldsymbol{v}_i)$, Q'_1 AND Q'_2 ARE THE QUANTIZATION STEP SIZES AS THRESHOLDS

Difference range	Acceptable Raw Signatures
$Q'_2 < p'_i - q'_i$	0
$Q'_1 < p'_i - q'_i \le Q'_2$	0 / 1
$\lvert p'_i - q'_i \rvert \le Q'_1$	1
$-Q'_2 \le p'_i - q'_i < -Q'_1$	1 / 2
$p'_i - q'_i < -Q'_2$	2

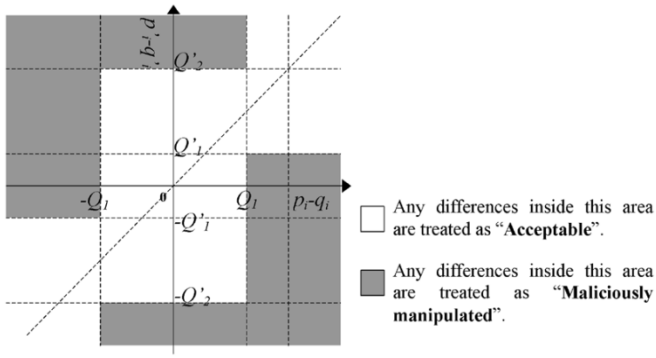

Fig. 11. Manipulation detection area for the Nonuniform Quantization method.

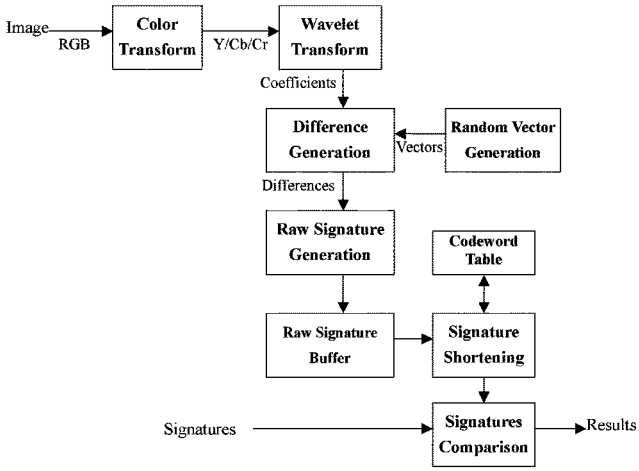

Fig. 12. Signature verifier block diagram.

bits is shown in Table I (in this example, a signature which takes three values (2 bits) is generated for each pair).

In the subsequent steps, the concatenation of a certain number of pairs (e.g., nine pairs in Fig. 10) of generated raw signatures is grouped into one set, which is called "raw signature set". "Shorten Signature" block generates a new signature, which consists of multiple bits, for each raw signature set based on looking up the codeword assignment table described in the latter section. Eventually, we generate the signature consisting of 9 bits for the set of nine pairs that makes the average of 1 bit per one pair (Apparently, the detection unit is 9 bits for nine pairs). $-Q'_2 < p'_i - q'_i \le Q'_2$.

The signature verification procedure is a little more complicated than the generation procedure. The procedure until acquisition of the difference from a pair of coefficients is the same as at the generation site. The "Nonuniform quantize" block generates all acceptable raw signatures, depending on the difference value according to the rules described in Table II. An acceptable raw signature is the signature value obtained at the signature verification site, which should be generated at the signature generation site for the difference value. For example, if "1" is generated at the signature generation site, it is considered to be unmanipulated at the signature verification site if the difference value computed at the verification site is within the range of

It is important to understand the acceptance rules listed in Table II. As shown in Fig. 11, the acceptable region in the "new difference-old difference" plane is more complicated than the one for the original method (shown in Fig. 4). Here, multiple parameters, Q_1, Q'_1, and Q'_2 can be used to control the acceptable regions and match them to the distributions observed in typical acceptable manipulations (see Fig. 8).

"Signature Shortening" block is also the same as in the signature generation site in that it generates one signature by concatenating a certain number of raw signatures, except for the fact that there is more than one raw signature acceptable while the signature generation site has only one raw signature for one pair. Consequently, the verification site generates an acceptable raw signature set from the combination of all acceptable raw signatures. Then, it generates binary signatures for each raw signature vector in the set by the same procedure as the signature generation site (see Fig. 13). The "Signature Comparison" block

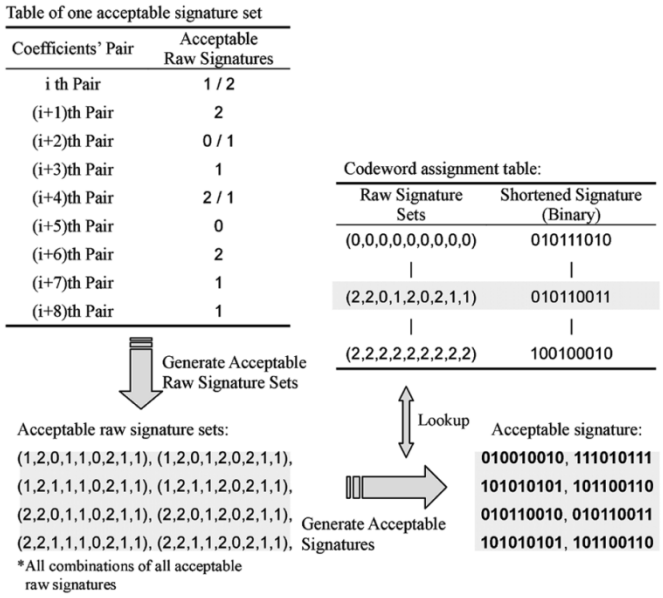

Fig. 13. Example of acceptable signatures generation.

compares the generated acceptable signature with the one generated at the signature generation site. If the signatures of the verification site do not include the signature of the generation site, it is considered manipulated; otherwise, it is considered unmanipulated.

Consequently, we can expect the high detection accuracy and obtain the semi-fragile signature of average of 1 bit per one pair, as with the case of the original method.

In association with the verification procedure, we describe a theoretical corroboration of parameters selection. Similar to the Random Bias method, multiple parameters Q_1' and Q_2' for the verification site can be given as the following steps.

Assume coefficients p_i and q_i are quantized with Q_i, define $\Delta D_{pqi} = p_i - q_i$ and $\Delta \widetilde{D}_{pqi} \equiv \widetilde{p}_i - \widetilde{q}_i$, where $\widetilde{p}_i$ is defined as $\widetilde{p}_i \equiv IntegerRound\,(p_i/Q_i) \cdot Q_i$, and define a quantized parameter $\widetilde{Q}_i \equiv IntegerRound\,(Q_1/Q_i)$, the quantized difference shown in Table II will be

- if $\Delta D_{pqi} > Q_1$

$$\Delta \widetilde{D}_{pqi} \geq \begin{cases} \widetilde{Q}_1 \cdot Q_i, & \frac{Q_1}{Q_i} \in Z \\ (\widetilde{Q}_1 - 1) \cdot Q_i, & \text{elsewhere} \end{cases} \tag{13}$$

- if $|\Delta D_{pqi}| \leq Q_{1i}$

$$\left|\Delta \widetilde{D}_{pqi}\right| \leq \begin{cases} \widetilde{Q}_1 \cdot Q_i, & \frac{Q_1}{Q_i} \in Z \\ (\widetilde{Q}_1 \; or \; \widetilde{Q}_1 \pm 1) \cdot Q_i, & \text{elsewhere} \end{cases} \tag{14}$$

- if $\Delta D_{pqi} < -Q_{1i}$

$$\Delta \widetilde{D}_{pqi} \leq \begin{cases} -\widetilde{Q}_1 \cdot Q_i, & \frac{Q_1}{Q_i} \in Z \\ (-\widetilde{Q}_1 + 1) \cdot Q_i, & \text{elsewhere.} \end{cases} \tag{15}$$

A quantized parameter $\widetilde{Q}_1$ is quantized with Q_i. Thus, $\widetilde{Q}_1 \cdot Q_i$ is in the following range:

$$Q_1 - \frac{1}{2}Q_i \leq \widetilde{Q}_1 \cdot Q_i \leq Q_1 + \frac{1}{2}Q_i \tag{16}$$

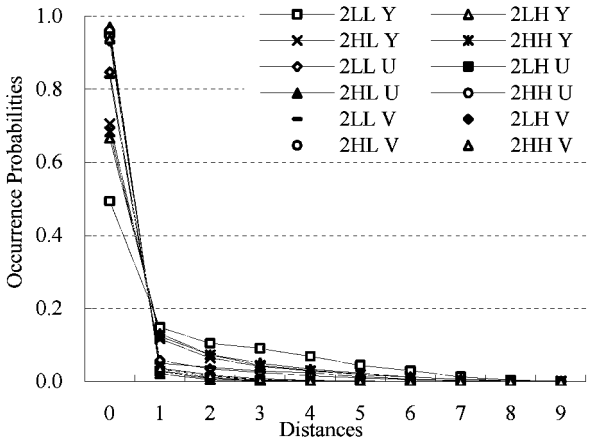

Fig. 14. Relationships between the distances and the probabilities of occurrence.

TABLE III
DISTANCE GROUPS AND COLLISIONS

Group	1st	2nd	3rd
Distance D	D=0	0<D<4	D≥4
The number of Raw Signature Sets	1	834	18 848
The number of Shortened Signatures	1	280	231
Collisions	0%	66.4%	98.8%

and then

- if $\Delta D_{pqi} > Q_1$

$$\Delta \widetilde{D}_{pqi} \geq \begin{cases} Q_1 - \frac{1}{2}Q_i, & \frac{Q_1}{Q_i} \in Z \\ Q_1 - \frac{3}{2}Q_i, & \text{elsewhere} \end{cases} \tag{17}$$

- if $|\Delta D_{pqi}| \leq Q_{1i}$

$$\left|\Delta \widetilde{D}_{pqi}\right| \leq \begin{cases} Q_1 - \frac{1}{2}Q_i, & \frac{Q_1}{Q_i} \in Z \\ Q_1 + \frac{3}{2}Q_i, & \text{elsewhere} \end{cases} \tag{18}$$

- if $\Delta D_{pqi} < -Q_{1i}$

$$\Delta \widetilde{D}_{pqi} \leq \begin{cases} -Q_1 + \frac{1}{2}Q_i, & \frac{Q_1}{Q_i} \in Z \\ -Q_1 + \frac{3}{2}Q_{ii}, & \text{elsewhere.} \end{cases} \tag{19}$$

Raw signature values shown in Table I can be mapped into ranges of $\Delta \widetilde{D}_{pqi}$. For example, either 0 or 1 can be true in a range of $Q_1 - (3/2)Q_i \leq \Delta \widetilde{D}_{pqi} \leq Q_1 + (3/2)Q_i$, and either 1 or 2 can be true in a range of $-Q_1 - (3/2)Q_i \leq \Delta \widetilde{D}_{pqi} \leq -Q_1 + (3/2)Q_i$. Thus, Q_1' and Q_2' can be defined as $Q_1' \leq Q_1 - (3/2)Q_i$ and $Q_2' \geq Q_1 + (3/2)Q_i$ to avoid false alarms caused by lossy compression with Q_i-step quantization.

3) Codeword Assignment Table Generation: When shortening signatures, a raw signature set is used as an index to refer to the codeword assignment table, and the entry (one binary vector for each raw signature set) outputs as the shortened signature. Since the number of possible raw signature sets far exceeds that of shortened binary signatures, collisions occur when different raw signatures refer to the same shortened binary signature. This may cause misses in detecting alterations. However, since we know the likelihood distributions of the raw

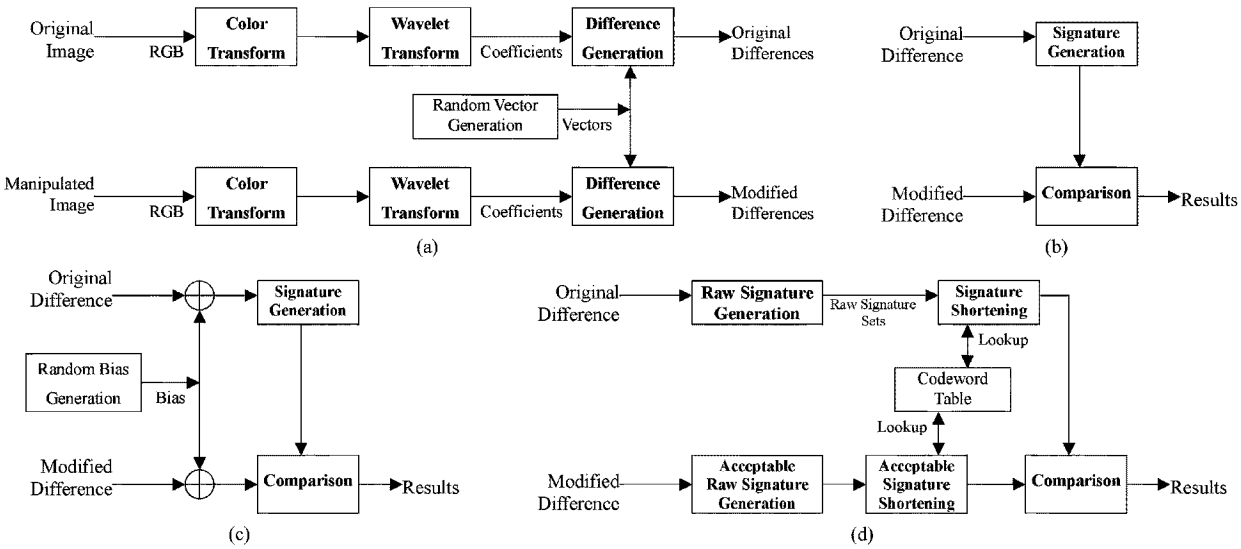

Fig. 15. Block diagrams. (a) Difference generation steps. (b) Lin and Chang's method. (c) Random Bias method. (d) Nonuniform Quantization method.

signatures, we can optimize the codeword assignment table to minimize the codeword collision probability mentioned above.

Raw signatures around the center ($|p_i - q_i| \leq Q_1$) have the highest probability of appearance. Therefore, raw signature sets consisting of the raw signatures at the center (in Table I, Table II). (1, 1, 1, 1, 1, 1, 1, 1, 1) has the highest probability. Farther away from the center, the raw signature sets have a lower probability of occurrence. Fig. 14 shows the relationships between the probability of occurrence and the raw signature's distances from the center. Note that the distance D from the center to the raw signature set $A(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9)$ is calculated as (20). The probability is obtained by empirical simulations using real images (similar to the distributions shown in Fig. 6) and is based on the assumption of independence among coefficient pairs

$$D = \sum_{i=1}^{9} |a_i - 1|. \tag{20}$$

From these results, we can see that it takes the overwhelmingly high probability (50%–99%) when $D = 0$. And the probability of $D = 0$ for LL subbands and low-frequency elements are lower than others. Thus, we can expect that optimizing the probability of collisions based on the probability of appearances will improve the detection accuracy. For example, if we set the $D = 0$ table entries for no collisions, 50% of all signatures will be collision free for coefficients in the 2LL subband. If we adapt it to 1LH of U component, 99% of all will be collision free.

Given the occurrence probabilities, the total number of input symbols, and the codeword length (e.g., 9 bits), one could obtain the optimal codeword assignment following a procedure similar to the one used in the Huffman Code. Here, to simplify the testing, we categorize the raw signature sets to three groups depending on the distance D. The first group consists of raw signature sets of $D = 0$, the second group contains raw signature sets of $0 < D < 4$, and the third group contains others ($D \leq 4$) (see Table III).

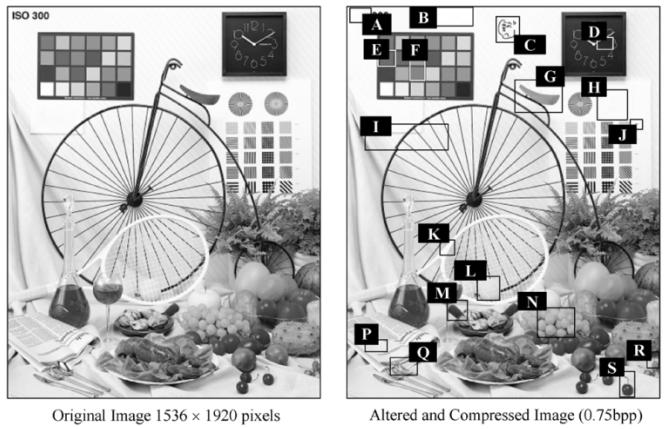

Fig. 16. Testing patterns for "Natural Image".

In the first group, there exists only (1,1,1,1,1,1,1,1,1). Therefore, assigning only one shortened signature to this group will eliminate collisions. However, if we assign 1 bit per one pair, we can only use a 9-bit (512 patterns) shortened signature per raw signature set. There are 19 683 patterns for all raw signature sets and the codeword assignment table has 19 683 entries. In each entry, one pattern out of 512 signatures is recorded. Consequently, it is obvious there exists collision because the identical signature value is used for more than one entry.

Here, we assign the minimum number of binary signatures to the third group, which has the lowest probability of occurrence, while we assign 280 binary signatures to the second group to which 834 raw signature sets belong. On the average, two to three raw signature sets have the identical signature in the second group. Similarly, 231 binary signatures are assigned to 18 848 raw signatures sets in the third group with the lowest probability of occurrence. In this case, approximately 80 raw signature sets take the identical signature.

When forming the codeword assignment table in practice, the pseudorandom sequence can be performed to randomize index values, shortened signatures, and overlapping patterns in each

Fig. 17. Testing patterns for Document, Color Chart, Portrait, Compound Document, and Circuit Diagram.

group. It can also divide the image into blocks using a random assignment in each group for each block in order to enhance the system security.

The method described above will minimize the miss probability resulting from shortening signatures and achieve the goal of shortening the signature length to 1 bit per one pair.

IV. Experimental Results

We have tested the above-mentioned methods with various images. Manipulations of different types were simulated, including the following.

A. Delete (fill background textures).
B. Delete Background textures.
C. Add a line drawing.
D. Delete (fill background textures).
E. Paste another contents.
F. Desaturate.
G. Change Hue.
H. Delete.
I. Move.
J. Replace by computer generated texts
K. Delete light colored contents
L. Delete racket strings
M. Add Grip.
N. Skew.
P. Delete papers contents.
Q. Copy.
R. Desaturate.
S. Copy.

Fig. 15 shows the block diagram for tests of Lin and Chang's method, the proposed Random Bias method, and the Nonuniform Quantization method. In each diagram, the upper row illustrates the signature generation site, and the lower row illustrates the signature verification site. Both generate the same random vectors, the same random biases and the same codeword assignment table by the same pseudo-random sequence. Figs. 16 and 17 show the test images, which are altered by some unacceptable manipulations, and are lossy-compressed by JPEG2000 VM8.6 as acceptable manipulations. All methods are tested on the wavelet domain, and all wavelet coefficients for differences generation are transformed using parameters listed in Table V. To evaluate the robustness to the other transform-domain compression, the acceptable JPEG2000 compressions are applied using the different wavelet filter, the different tile size and the different color transform listed in Table IV. To compare the detection performances, the same detection block size, which consists of 3×3 coefficients in the 2LL subband, is used for each method. To generate the differences, each coefficient is given another pairing coefficient, which is selected using a pairing vector determined by a pseudorandom sequence. A block, which consists of more than one alteration-detected coefficient, is treated as a detected block for Lin and Chang's method and the Random Bias method. For the Nonuniform Quantization method, the alteration detection is performed in the units of a block because nine raw signatures, which are generated from all of nine differences in a block, are shortened into one 9-bit signature using the codeword assignment table. Regarding detection parameters, we selected M and Q_1, which are the lowest of values, with which false alarms caused by compression distortion do not occur. As described earlier, there is a tradeoff between detection rates and false alarm rates. For both parameters, lower values can achieve a higher detection rate with a lot of false alarms and higher values can achieve no false alarm with a lot of missing detections. Therefore, the lowest of values that do not cause false alarms are used in this testing, to indicate the detection capabilities after removing the necessity of considering false alarm existences in the detected results. Further discussions could be needed for measuring performances of a semi-fragile watermarking.

Fig. 19 shows the alteration detection rates for each compression ratio. At all compression ratios, from 1.0 to 0.25 bpp, detection rates improve approximately 10% to 300% when using

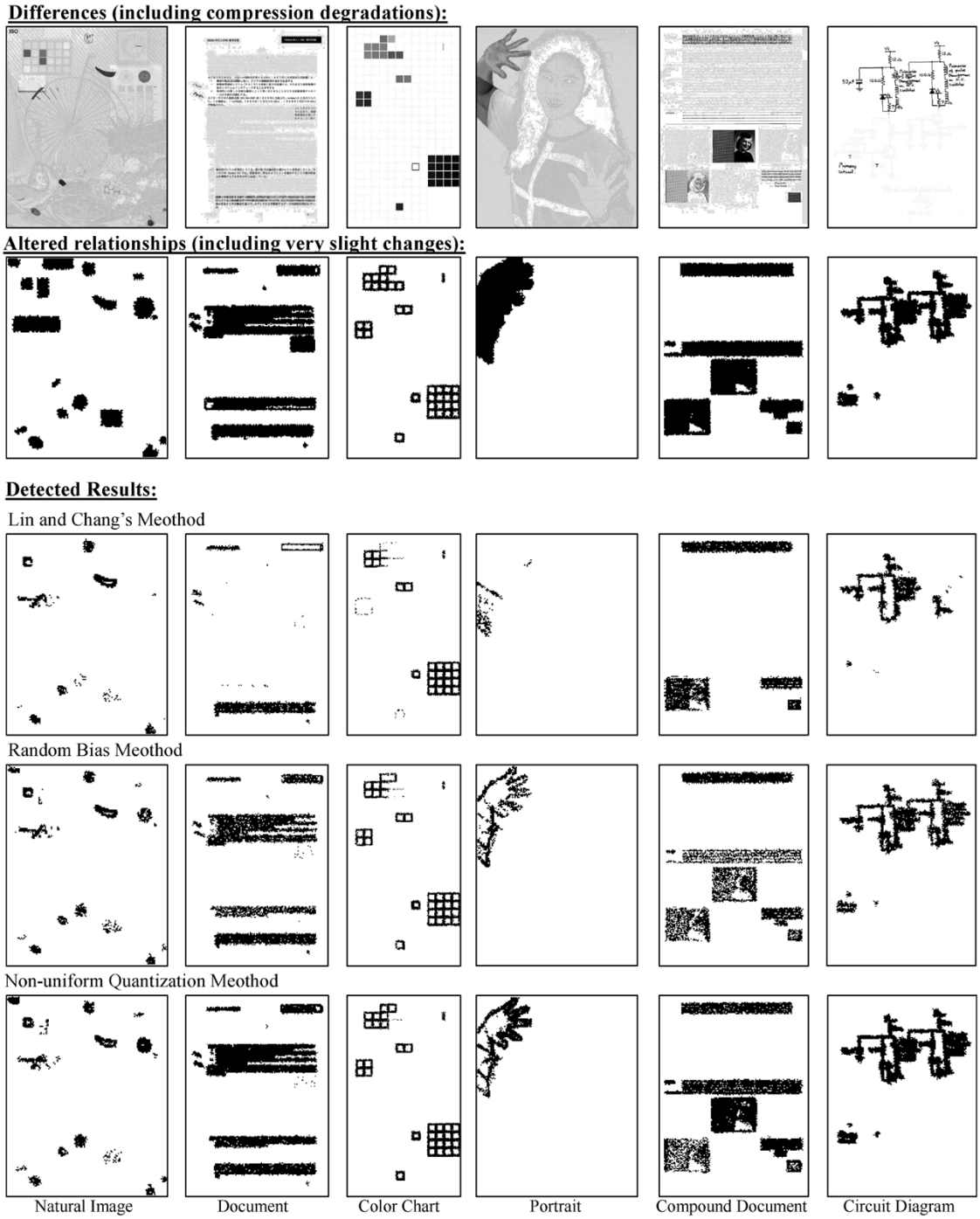

Fig. 18. Experimental Results. The difference images indicate differences between altered images and original images. All altered images are compressed by JPEG2000 with 0.75 bpp. Most light gray pixels in the difference images are JPEG2000 compression distortion, and dark gray pixels are caused by the alterations. The altered relationship images indicate the changed relationships caused only by the alterations.

TABLE IV
CONDITIONS FOR LOSSY COMPRESSIONS AS ACCEPTABLE MANIPULATIONS

Compress options	Values
Lossy Compressor	JPEG2000 VM8.6
Wavelet Transform	9 × 7 Floating Point
Color Transform	Irreversible YCbCr
Tile size	128 × 128 (pixels)
Decomposition Level	5
Bitrate	1.0 / 0.75 / 0.5 / 0.25 (bpp)

TABLE V
CONDITIONS FOR TESTING COEFFICIENTS GENERATION

Testing Options	Values
Wavelet Transform	5 × 3 Integer
Color Transform	Reversible (RCT)
Tile Size	256 × 256 (pixels)
Testing Subband	2LL
Pairing vector range	± 4 (Vertical & Horizontal)
Note: Select Parameters to guarantee no false alarm	

either the Random Bias method or the Nonuniform Quantization method even as the compression domain belongs to the different wavelet domain. In the case of highly compressed at 0.25 bpp, the detection rates are low; however, it keeps better

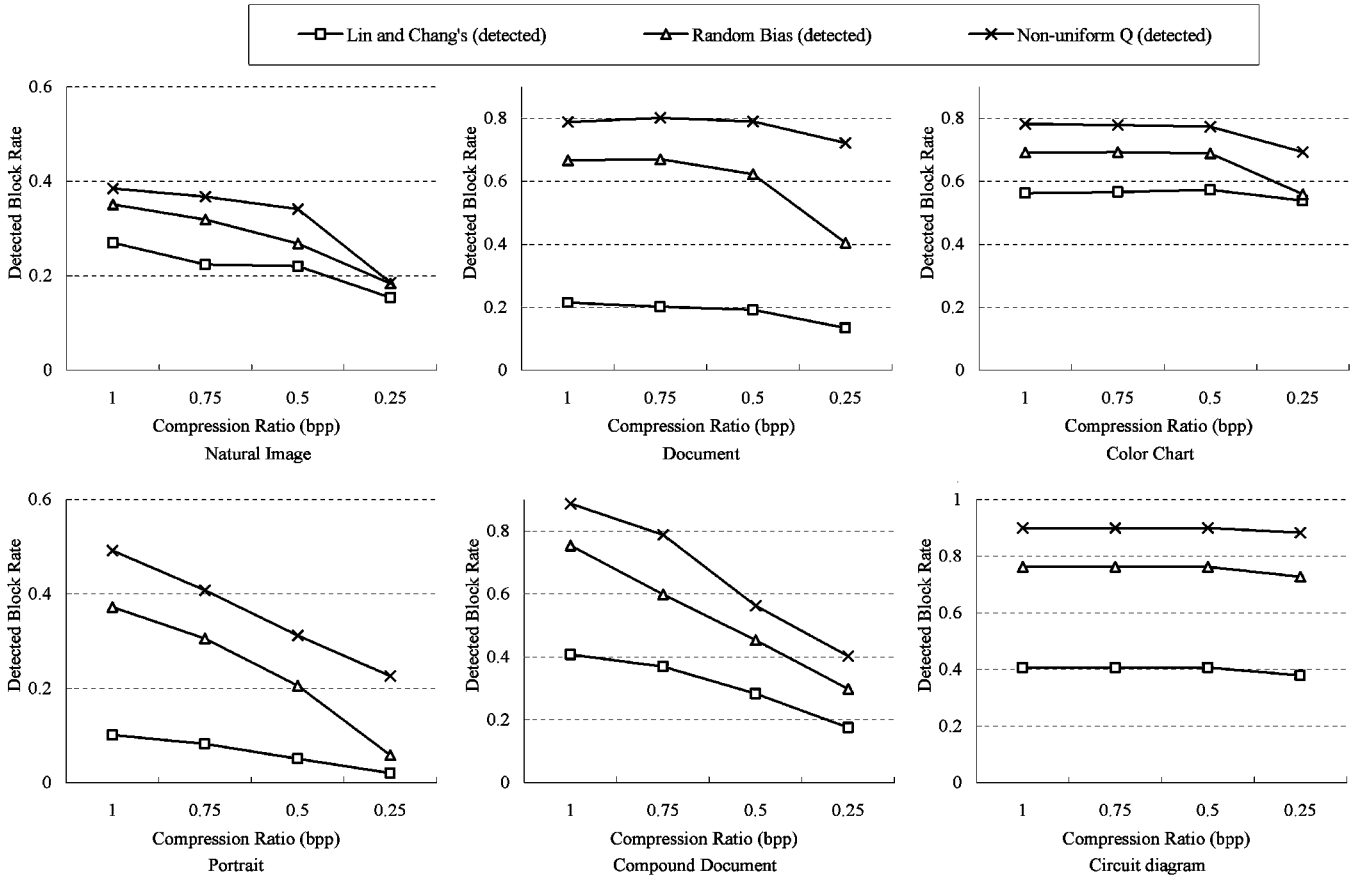

Fig. 19. Detection performance in the 2LL subband of the wavelet domain. The solid lines indicate the rates of detected 3 × 3 blocks in the altered blocks.

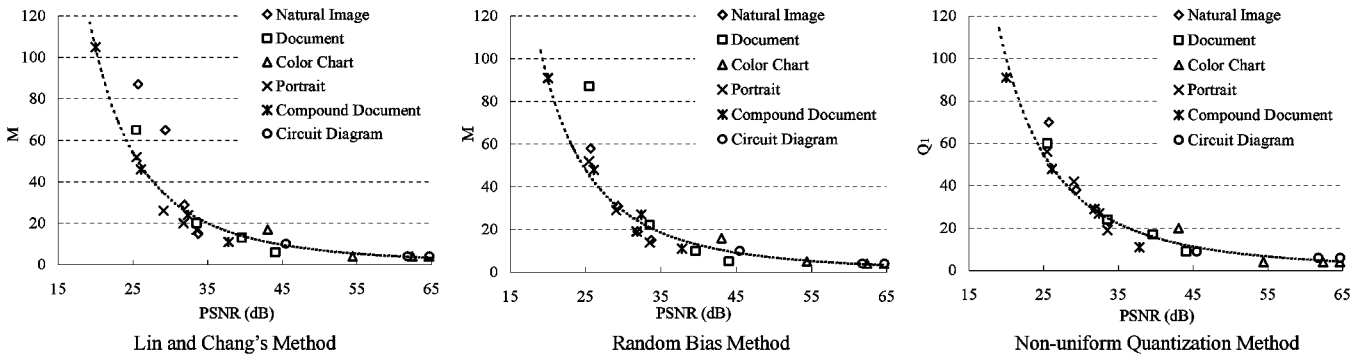

Fig. 20. Relationships between the detection parameters and PSNR (dB). PSNR indicates JPEG2000 compression distortion. The random bias ranges for the Random Bias method are set from $-M \times 1.5$ to $+M \times 1.5$. For the Nonuniform Quantization method, Q_1' values are set to $Q_1 \times 0.6$ and Q_2' values are set to $Q_1 \times 2$.

results than Lin and Chang's method. Generally speaking, as the compression ratio increases, it becomes more difficult to distinguish between alterations and compression distortion. To achieve a higher detection rate, a small amount of false alarms could be allowed in practical use. In the case of photographic images ("Natural images" and "Portrait"), the detection rates are relatively low due to many minor alterations, which are slight changes under compression distortion. These results could be reasonable if a barometer of alterations is found in the degree of image degradation.

Regarding detection performance for each type of alterations in Figs. 16 and 17, almost all altered areas including cropped parts, which cannot be detected by the original Lin and Chang's method (area A, D and H of Fig. 16), can be detected with either the Random Bias method or the Nonuniform Quantization method, as shown in Fig. 18. The detection rates for the areas where the luminance/color levels are slightly changed (area F of Fig. 16) are low in all algorithms. All methods cannot detect the very slight changes (area B of Fig. 16) whose differences are below compression distortion as shown in the top-left image of Fig. 18.

Our new methods can also detect the borders of flat-to-flat alterations, where the flat areas, which are larger than pairing vector ranges and are originally flat before alteration, are hard to be detected by the relationship-based algorithms, because a difference between two coefficients within a flat area always

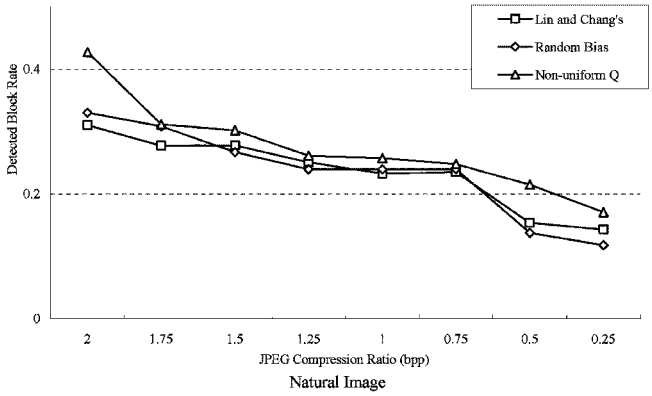

Fig. 21. Detection performance for the JPEG compressed image.

takes the same value. The width of the detected borders depends on the length of the pairing vectors.

Fig. 20 shows the relationships between the detection parameters, which are selected to avoid a false alarm as noted earlier, and the image quality (PSNR) degraded by lossy compression. For all images, they stand at the similar distributions correlated with the image quality. It seems that they could be selected in conjunction with the tolerance image quality in practical use.

The robustness of our proposed solutions to the DCT-based JPEG compression is shown in Fig. 21, in terms of block-based detection rates. We can see that the detection rates are slightly lower than those done by JPEG2000, at the same compression ratio. The possible reasons are, the compression efficiency of JPEG2000 is better than JPEG, which means at the same compression ratio, the image quality compressed by JPEG2000 is better than that by JPEG.

Further discussions could be focused on each targeted application; for instance, whether a highly compressed image is considered a malicious alteration, whether a small amount of false alarms in a highly compressed image should be allowed as a suspicion of an alteration, and whether a minor alteration should be allowed as an insignificant change, etc.

V. Conclusions

In this paper, we address the problems of a popular semi-fragile authentication watermarking technique and proposed new signature generation/verification algorithms. Our techniques improve the alteration detection sensitivity by analyzing and observing the impact of various image manipulations on the transform coefficients and their relationships. Furthermore, we apply these algorithms to the coefficients that have been wavelet-transformed; within the scope of the experiments conducted, we proved that we can detect image manipulations even after JPEG2000 lossy compression with different filters, and that no false alarm occurs while keeping the reasonable detection sensitivity even for the object cropping manipulation.

In conclusion, our new algorithms demonstrate very encouraging performances for detecting various types of unallowable manipulations (including object cropping), even for images with a very homogeneous background such as a document image. In a field where the very strict image authenticity is strongly required, such as certificates, we can combine with the fragile watermarking to satisfy such strict requirements (our methods allow the fragile watermarking which is considered to be acceptable operation). In this case, the fragile watermarking can be used to ensure the whole image authenticity while the semi-fragile watermarking can be used to locate the altered points where whole image authentication fails. For authentication, the advantages of our methods are: 1) locating the altered points even if the altered image has been lossy-compressed and 2) allowing flexible specification of the level of acceptable manipulation by setting a comparison threshold value. Our methods, like the original Lin and Chang method, can be effectively used as an externally stored image signature, rather than embedded image watermarks.

Our future work includes addressing lossy compression with different wavelet transform filters, studying the alteration detection sensibility when an image size changes, and more extensive testing using more images of various types and different parameters.

Acknowledgment

The authors appreciate the help provided by the Dr. C.-Y. Lin in providing comments and advice during their research.

References

[1] C. Y. Lin and S. F. Chang, "Semi-fragile watermarking for authenticating JPEG visual content," in *Proc. SPIE, Security and Watermarking of Multimedia Contents*, San Jose, CA, Jan. 2000, pp. 140–151.

[2] R. Wolfgang and E. J. Delp, "A watermark for digital images," in *Proc. IEEE Int. Conf. Image Processing*, vol. 3, 1996, pp. 219–222.

[3] R. B. Wolfgang and E. J. Delp, "Fragile watermarking using the VW2D watermark," in *Proc. SPIE/IS&T Int. Conf. Security and Watermarking of Multimedia Contents*, vol. 3657, San Jose, CA, Jan. 25–27, 1999, pp. 204–213.

[4] S. Walton, "Information authentication for a slippery new age," *Dr. Dobbs J.*, vol. 20, no. 4, pp. 18–26, Apr. 1995.

[5] P. Wong, "A watermark for image integrity and ownership verification," in *Final Program and Proc. IS&T PICS 99*, Savanna, GA, Apr. 1999, pp. 374–379.

[6] E. T. Lin, C. I. Podilchuk, and E. J. Delp, "Detection of image alterations using semi-fragile watermarks," in *Proc. SPIE Int. Conf. Security and Watermarking of Multimedia Contents II*, vol. 3971, San Jose, CA, Jan. 23–28, 2000.

[7] J. J. Eggers, J. K. Su, and B. Girod, "A blind watermarking scheme based on structured codeblocks," in *Proc. IEE Colloq. Secure Images and Image Authentication*, London, U.K., Apr. 2000, pp. 4/1–4/6.

[8] J. J. Eggers and B. Girod, "Blind watermarking applied to image authentication," in *Proc. ICASSP'2001 Int. Conf. Acoustics, Speech and Signal Processing*, Salt Lake City, UT, May 7–11, 2001.

[9] S. Bhattacharjee and M. Kutter, "Compression tolerant image authentication," in *Proc. IEEE Int. Conf. Image Processing*, Chicago, IL, Oct. 1998.

[10] M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," in *Proc. IEEE ICMP*, Santa Barbara, CA, Oct. 1997.

[11] M. Wu and B. Liu, "Watermarking for image authentication," in *Proc. IEEE ICIP*, Chicago, IL, Oct. 1998.

[12] J. Fridrich, "Image watermarking for tamper detection," in *Proc. IEEE Int. Conf. Image Processing*, Chicago, IL, Oct. 1998.

[13] M. P. Queluz, "Content-based integrity protection of digital images," in *SPIE Conf. Security and Watermarking of Multimedia Contents*, vol. 3657, San Jose, CA, Jan. 1999, pp. 85–93.

[14] Self Authentication and Recovery Image (SARI) Software and Testing Site. [Online]. Available: http://www.ctr.columbia.edu/sari/

[15] K. Maeno, Q. Sun, S. F. Chang, and M. Suto, "New semi-fragile watermarking techniques using random bias and nonuniform quantization," in *Proc. SPIE, Security and Watermarking of Multimedia Contents IV*, vol. 4675, San Jose, CA, Jan. 2002, pp. 659–670.

[16] M. Kaji, "Graphic Technology—Prepress Digital Data Exchange—Standard Color Image Data(SCID) ISO/JIS-SCID," JSA, Tokyo, Japan, 1995.

Kurato Maeno received the B.E. and M.S. degrees in electrical engineering, from Mie University, Mie, Japan, in 1993 and 1995, respectively.

Since 1995, he has been with Oki Electric Industry Co., Ltd., Saitama, Japan. From 2000 to 2001, he was a Visiting Scholar at Columbia University, New York. His research interests include image and video coding, image analysis, data hiding, and information security.

Qibin Sun received his Doctoral degrees in electrical engineering, from University of Science and Technology of China, Anhui, China, in 1988 and 1997, respectively.

Since 1996, he has been with the Institute for Info-Comm Research, Singapore, where he is responsible for industrial as well as academic research projects in the area of face recognition, media security, and image and video analysis. He was with Columbia University, New York, during 2000–2001 as a Research Scientist.

Shih-Fu Chang (F'04) is a Professor in the Department of Electrical Engineering, Columbia University, New York. He leads Columbia University's Digital Video/Multimedia Lab (http://www.ee.columbia.edu/dvmm) and the ADVENT research consortium, conducting research in multimedia content analysis, video indexing, multimedia authentication, and video adaptation. Systems developed by his group have been widely used, including VisualSEEk, VideoQ, WebSEEk for image/video searching, WebClip for networked video editing, and Sari for online image authentication. He has initiated major projects in several domains, including a digital video library in echocardiogram, a content-adaptive streaming system for sports, and a topic tracking system for multisource broadcast news video (http://www.ee.columbia.edu/~sfchang). His group has made significant contributions to development of MPEG-7 multimedia description schemes. He has also been a Consultant for several media technology companies.

Dr. Chang and his students have received six best paper or student paper awards from the IEEE, ACM, and SPIE. He was a Distinguished Lecturer of the IEEE Circuits and Systems Society (2001–2002), a recipient of a Navy ONR Young Investigator Award, an IBM Faculty Development Award, and a National Science Foundation CAREER Award. He served as a General Co-Chair for ACM Multimedia Conference 2000 and IEEE ICME 2004.

Masayuki Suto received the B.E. degree in electrical engineering from Sophia University, Tokyo, Japan, in 1982.

Since 2000, he has been a Senior Manager of IT Business Incubation Division at Oki Electric Industry Co., Ltd., Saitama, Japan. His current research interests include computer architecture, image processing, digital watermarking, and information security.