AUTHENTICATION OF DIGITAL IMAGES VIA TREE-STRUCTURED DIGITAL SIGNATURE

Chun-Shien Lu and Hong-Yuan Mark Liao

Institute of Information Science, Academia Sinica,
Taipei, Taiwan, R.O.C.
E-mail: {lcs, liao}@iis.sinica.edu.tw

Abstract

The existing digital data verification methods are able to detect tampered regions, but are too fragile to resist incidental manipulations. This paper proposes a new digital signature scheme which makes use of an image's contents to construct a tree-structured *digital signature (TSDS) for image authentication. The characteristic of TSDS is that it can tolerate content-preserving modifications while detecting content-changing modifications. Many incidental manipulations, which were detected as malicious modifications in the previous digital signature or fragile watermarking schemes, can be bypassed in the proposed scheme. Performance analysis and experimental results have shown the superiority of the proposed scheme.*

1. INTRODUCTION

Owing to the popularity of data digitization, it is easy to tamper with digitized data without leaving any clue. However, this will raise an emergent need of data integrity verification in order to judge which is authentic or fake. Conventionally, content verification can be classified into two categories: digital signature-based [2, 3, 5, 7, 8, 10] and watermark-based [4, 6, 9, 12, 13, 14, 15, 16]. A digital signature represents a specific characteristic of a media data and is stored as a file, which is used later for authentication. Watermarking, on the other hand, is used to embed hidden information into a media data and the hidden information is later extracted to verify data. Both types are expected to be sensitive to modification so that changes of data can be reflected on the digital signature or the watermark.

According to the underlying technology used, some of the above methods can be roughly classified as hash function-based [5], quantization-based [6, 9], feature-based [2, 3], and relation-based [7, 8]. For quantization-based methods, Kundur and Hatzinakos [6] designed a quantization technique to encode a watermark such that the hidden watermark will be more/less sensitive to modifications at high/low frequency in the wavelet domain. However, the main disadvantage of [6] is that the tampering detection results are very unstable. Perturbation of a wavelet coefficient may make the extracted mark different from or the same as the embedded one. That is, the extracted result is totally unpredictable. Once the perturbation exceeds one quantization interval, the extracted watermark value will be either the same as or different from the embedded one. Another drawback is that their method cannot resist incidental modifications.

For feature-based authentication systems, Bhattacharjee and Kutter [2] proposed to generate a digital signature by encrypting the feature points' positions of an image. Authentication is then accomplished by comparing the positions of the feature points extracted from a questionable image with those decrypted from the previously encrypted digital signature. Again, it is wondered that whether this approach can resist $JPEG$ compression with middle-to-high ratios because the feature points are liable to be shifted. Recently, Dittmann *et al.* [3] presented a content-based digital signature approach for image/video authentication using edge characteristics. Their content features are similar to [2], but different extraction techniques are used.

On the other hand, in order to make the designed image authentication system survive $JPEG$ compression, Lin and Chang [7, 8] were dedicated to exploring the operation in the $JPEG$ system. They proposed to preserve the invariant relationships between any two DCT coefficients, which are at the same positions of different 8×8 blocks, to form a digital signature. This is because they found that these invariance properties can be always preserved before and after $JPEG$ quantization. However, it was not clear how their method could survive other incidental manipulations. Although the

authors [7, 8] used the invariance property to authenticate images, this relationship is random because the invariance property of any two *random DCT* blocks are stored as the digital signature. The merit of image structure is actually ignored.

In this paper, we shall develop a new image authentication scheme, which is totally different from the existing methods in that we don't care the positions of feature points or the relationship of any two random coefficients. On the contrary, we consider the "*tree-structure*" of an image's content as the digital signature. The tree-structure of an image's contents is composed of the parent-child pairs in a wavelet domain. We investigate how this tree-structured digital signature can be robust under image content-preserving manipulations and can be fragile under image content-changing manipulations. Performance analysis of this structured digital signature-based image authentication scheme has been conducted to prove its powerfulness, and as does our experimental results. This paper is an extension of its preliminary version [10].

The remainder of this paper is organized as follows. In Sec. 2, we will present the proposed content-based digital signature image authentication scheme. This will include the construction and verification of a tree-structured digital signature. In addition, the operations of non-oblivious and oblivious watermark detection techniques are, respectively, discussed. An analysis on the performance of our proposed scheme will be conducted in Sec. 3. We will discuss the false positive and false negative problems when incidental distortions and/or malicious tampering are encountered. In addition, we will analyze the effect caused when the size of a tree-structured digital signature is changing. Based on the analysis a systematic way can be derived to determine the best size for use. In Sec. 4, a series of experiments will be conducted and their results will be reported. Concluding remarks will be given in Sec. 5.

2. TREE-STRUCTURED DIGITAL SIGNATURE ($TSDS$)

Our digital signature scheme is based on the wavelet transform due to its excellent multiscale and precise localization properties. Basically, the multiscale representation of an image is by nature highly suitable for designing a tree-structured digital signature.

2.1. Defining $TSDS$ based on Interscale Relationship of Wavelet Coefficients

Let $w_{s,o}(x,y)$ represent a wavelet coefficient (at scale s, orientation o, and position (x,y)) in the orthogonally downsampled wavelet transform of an image $\mathbf{I}$. Suppose a J-scale wavelet transform is performed, then $0 \le s < J$. The interscale relationships of wavelet coefficients can then be converted into the relationships between the parent node $w_{s+1,o}(x,y)$ and its four child nodes $w_{s,o}(2x+i,2y+j)$ with

$$||w_{s+1,o}(x,y)| - |w_{s,o}(2x+i,2y+j)|| \ge 0. \quad (1)$$

The new signature, tree-structured digital signature ($TSDS$), can be constructed from the interscale relationships of wavelet coefficients of an image. The basic concept relies on (i) the interscale relationship should be difficult to be destroyed after content-preserving manipulations; and (ii) this interscale relationship should be difficult to be preserved after content-changing manipulations. Because these interscale relationships are resulted from the tree-structure of an image (say $\mathbf{I}$) in the wavelet domain, we define them as the tree-structured digital signature of $\mathbf{I}$ —— $TSDS(\mathbf{I})$.

The tree-structured digital signature of an image consists of a set of parent-child pairs, which satisfy

$$||w_{s+1,o}(x,y)| - |w_{s,o}(2x+i,2y+j)|| \ge \sigma \ (\sigma > 0). \quad (2)$$

The above constraint is stricter than the original interscale relationship of wavelet coefficients shown in Eq. (1). The size of σ will determine the number of parent-child pairs recorded in a $TSDS(\mathbf{I})$. The smaller the σ is, the larger the amount of elements in a $TSDS$ is. We do not intend to keep all the parent-child pairs as the elements of a $TSDS$ because some of the elements may not be significant enough. The significance of a parent-child pair is completely dependent on their magnitude difference. The larger the difference, the more significant the parent-child pair is. From a parent-child pair whose magnitude difference is small is equivalent to having a "small" quantization interval in the quantization-based approach [6, 9]. Therefore, it will be very sensitive to modifications including some minor incidental ones. In order to design a robust image authentication scheme, we only keep those parent-child pairs whose magnitude differences are large as the elements of a tree-structured digital signature. In order to appropriately detect a malicious tampering while tolerating an incidental modification, we use the size of a tree-structured digital signature to control the tradeoff between fragility and robustness. In general, the construction of a tree-structured digital signature is very easy because there is no feature selection involved [2, 3] is not required.

Once the parent-child pairs are selected by the constraint defined in Eq. (2), each pair is assigned a symbol, which represents what kind of relationship this pair carries. These symbols will be formally defined in Sec.

2.2. The above mentioned symbols and their locations in the wavelet domain will be encrypted by a public key algorithm, RSA [11]. Finally, the encrypted information will be stored and used for image authentication later.

2.2. Labeling a $TSDS$

According to the interscale relationship among wavelet coefficients, there are four possible relationship types of a $TSDS$. Assume the magnitude of a parent node p is larger than that of its child node c (i.e., $|p| > |c|$), then the four possible relationships of the pair, $< p, c >$, are: (i) $p \geq 0, c \geq 0$; (ii) $p \geq 0, c \leq 0$; (iii) $p \leq 0, c \geq 0$; (iv) $p \leq 0, c \leq 0$. Considering the case when $|p| > |c|$ and c is small. In order to make $< p, c >$ still credible when incidental modifications are encountered, the value of c is not important. Therefore, the relations (i) and (ii) can be merged to form a signature symbol I, under the condition that $p \geq 0$ and c don't care. On the other hand, the relations (iii) and (iv) can be merged to form another signature symbol II, under the condition that $p \leq 0$ and c don't care. In other words, we intend to keep the sign of the larger element unchanged while disregarding the smaller one under the constraint that their original interscale relationship is still preserved. Similarly, the signature symbol III (under the condition that $c \geq 0$ and p don't care) and IV (under the condition that $c \leq 0$ and p don't care) can be defined under the constraint $|p| < |c|$. For those pairs that are not recorded in a $TSDS$ are all labeled by the fifth signature symbol V. Hence, we represent the signature symbol of a parent-child pair as $sym(< p, c >)$, which can be one of the above defined symbol types.

2.3. Verification

If one would like to verify an unknown image ($\tilde{\mathbf{I}}$), it is first wavelet transformed and then its tree-structured digital signature $TSDS(\tilde{\mathbf{I}})$ should be constructed. On the other hand, the encrypted tree-structured digital signature of the original image $\mathbf{I}$ is retrieved and then decrypted to obtain its corresponding $TSDS(\mathbf{I})$. One can say the interscale relationship of a pair $< p, c >$ in $\mathbf{I}$ is still unchanged in $\tilde{\mathbf{I}}$ if their signature symbols are the same. That is, the relation

$$sym(< p, c >) = sym(< \tilde{p}, \tilde{c} >) \tag{3}$$

holds, where the pair $< \tilde{p}, \tilde{c} >$ in $\tilde{\mathbf{I}}$ is the corresponding pair of $< p, c >$ in $\mathbf{I}$. Finally, we calculate the completeness of the $TSDS$ ($CoTSDS$) in $\tilde{\mathbf{I}}$, which is defined as the similarity degree, Sim, between $TSDS(\mathbf{I})$ and $TSDS(\tilde{\mathbf{I}})$:

$$CoTSDS(\tilde{\mathbf{I}}) = Sim(TSDS(\mathbf{I}), TSDS(\tilde{\mathbf{I}})) = \frac{N^+ - N^-}{|TSDS(\mathbf{I})|}, \tag{4}$$

where N^+ represents the number of pairs satisfying Eq. (3) and N^- represents the number of pairs violating Eq. (3). $|TSDS(\mathbf{I})|$ is used to denote the number of parent-child pairs in $TSDS(\mathbf{I})$. A larger $CoTSDS$ means the suspect image $\tilde{\mathbf{I}}$ is reliable; otherwise it means $\tilde{\mathbf{I}}$ has been maliciously tampered. In addition, the locations of tampering can be easily detected from those parent-child pairs whose signature symbols have been updated.

Let the magnitudes of the difference of parent-child pairs in a tree-structured digital signature be arranged in a decreasing order. It is known that the elements with larger magnitudes (preceding elements) are not vulnerable to attacks while those with smaller magnitudes (posterior elements) tend to be easily attacked. Therefore, one can use the preceding elements to indicate the robustness and use the posterior elements to reflect the fragility. Under these circumstances, when the size of a tree-structured digital signature becomes large, the preceding elements become to be easily changed such that the robustness property is more or less affected. On the other hand, the modification of the posterior elements will reflect accurately the degree of fragility. When $|TSDS|$ becomes large, the robustness property will be more or less affected since the posterior elements tend to be changed. On the other hand, due to the posterior elements are easily changed, they are used to reflect fragility. So, if $|TSDS|$ is small enough, then the fragility property may disappear because all elements are selected to be larger enough. Therefore, a suitable $TSDS$'s size needs to be determined in order to achieve a compromise between robustness and fragility. In Sec. 3, we will give a systematic way to determine σ (which also determines the $|TSDS|$) by statistical analysis of the distributions of a $TSDS$ and an attack's behaviors.

2.4. Length of A Tree-Structured Digital Signature

Let the number of parent-child pairs in a $TSDS$ be n. The first part of a $TSDS$ we should store is the child locations of the n parent-child pairs. The reason why the child locations instead of the parent locations are examined is that they are easy to be backtracked. For example, if a child node's location is (x, y), then it's parent's location is $(x/2, y/2)$. On the contrary, if a parent node's location is (x, y), there are four possible locations for a child. They are $(2x + i, 2y + j)$ where

$0 \leq i, j \leq 1$. For n parent-child pairs, $2 \times n$ bytes are required to store their locations because each location needs two bytes. In addition, each parent-child pair has four possible interscale relationships. Since each interscale relationship needs two bits to express it, there are in total $\frac{n}{4}$ bytes required to store all the interscale relationships.

In fact, the storage can be further saved if the locations of child nodes are stored based on their predefined ordering. Under the circumstances, the number of occurrence of every signature symbol is counted. For the first four types of symbols, we store the number of parent-child pairs and then the locations of these pairs. In this way, the memory used for storing the signature symbols will be reduced from $\frac{n}{4}$ bytes to 4 bytes. That is, there are in total $(2n + 4)$ bytes required to store a tree-structured digital signature before encryption.

3. PERFORMANCE ANALYSIS

Usually, a watermarking or digital signature-based method must be justified through the false positive (probability of false alarm) and false negative (probability of miss detection) probability analyses such as those have been done in [6, 7]. For image authentication purpose, a false positive probability is defined as that an image is detected to be maliciously tampered but in fact the image has not been tampered with. On the other hand, a false negative probability means that an image is actually modified by a malicious tampering but some tampered areas are not detected. A practical signature system should ensure that both the false positive and false negative probabilities are reasonably small. Due to space limit, please refer to the preliminary version [10] for these analyses. In this paper, we shall consider another two problems, as discussed in the following.

3.1. The Relation between σ and the Strength of Attacks

Attacks can be roughly classified into two categories: incidental manipulations and malicious distortions. To simplify the analysis, we assume the strength of an attack, a, is a Gaussian distribution, $\mathcal{G}^A$, with zero mean. According to Gaussian modeling of attacks [6, 9], we can have the following analysis. Usually, an incidental manipulation tends to have a small standard deviation ρ_I while a malicious tampering tend to have a large standard deviation ρ_M, i.e., $\rho_I < \rho_M$. Based on our scheme, a tree-structured digital signature is constructed by selecting those parent-child pairs whose differences in magnitudes (sign does not matter) are larger than σ. The difference in magnitude, d, may have two forms: positive difference ($d \geq 0$) and negative difference ($d < 0$). The positive difference portion and the negative difference portion both form a Gaussian distribution, $\mathcal{G}^S$, without zero mean. Their standard deviations are denoted as ρ_S, which is usually very large (scale of hundreds) because the variance of d is large in the wavelet domain and is in magnitude larger than ρ_I. The possible relations between $\mathcal{G}^A$ and $\mathcal{G}^S$ are depicted in Fig. 1. In Fig. 1, the Gaussian distributions shown in the middle part are $\mathcal{G}^A$, whereas the right/left one is $\mathcal{G}^S$ corresponding to positive/negative d. τ is defined as the intersection point of $\mathcal{G}^A$ and $\mathcal{G}^S$. The shaded areas, which represent the parent-child pairs with smaller difference $|d|$ in the tails of $\mathcal{G}^S$, will be updated based on the value of $\|a\|$ in the tails of $\mathcal{G}^A$. Next, we will analyze the effect of ρ_I and ρ_M on σ, respectively.

First, let an incoming attack be an incidental one such as $JPEG/SPIHT$ compression, rescaling, and so on. The probability that the relation of parent-child pairs may be destroyed (i.e., d's sign is changed) is denoted as p^I (the shaded areas in Fig. 1) and can be calculated by

$$\begin{aligned} p^I &= 2 \times (P\{0 < d < \tau - \sigma\} + P\{\tau < a < \infty\}) \\ &= 2 \times (P\{0 < d < \tau - \sigma\} + (1 - P\{0 < a \leq \tau\})) \\ &= 2 \times (erf(\frac{\tau - \sigma}{2\rho_S}) + [1 - erf(\frac{\tau}{2\rho_I})]), \end{aligned} \quad (5)$$

where $erf(\cdot)$ represents the error function [1] which is defined as:

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

In Eq. (5), the constant 2 appears due to the two symmetric $\mathcal{G}^S$'s belonging, respectively, to the positive and negative d. Because the attack under consideration is incidental, $\tau - \sigma$ is usually small. Since the standard deviation ρ_S of $\mathcal{G}_S$ is of the scale of hundreds, $\frac{\tau - \sigma}{2\rho_S}$ is thus very small. Under the circumstances, the first term in Eq. (5), $erf(\frac{\tau - \sigma}{2\rho_S})$, approximates zero. On the other hand, τ satisfies $\tau > \sigma$ and σ is chosen to be large (Eq. (2)), so τ is also large enough. For an incidental attack, we know the value of ρ_I is usually small. Therefore, $\frac{\tau}{2\rho_I}$ is large. As a consequence the second term, $[1 - erf(\frac{\tau}{2\rho_I}))]$, should be a very small one. In sum, the above discussion explains why the probability P^I can be sufficiently small if the incoming attack is incidental with small ρ_I. That is,

$$p^I \approx 2 \times [1 - erf(\frac{\tau}{2\rho_I})] \approx 0. \quad (6)$$

The near-optimal σ can be derived based on the condition that the incoming attack is incidental and the

value of p^I is smaller than a pre-determined threshold ϵ (e.g., $\epsilon = 0.1$). Under the circumstances, the near-optimal σ can be derived by

$$p^I \approx 2 \times [1 - erf(\frac{\tau}{2\rho_I})] < \epsilon.$$

Thus, we have

$$1 - \frac{\epsilon}{2} < erf(\frac{\tau}{2\rho_I}). \quad (7)$$

Using a predetermined ϵ together with ρ_I and checking the tables of error function [1], we should be able to obtain the lower bound of τ. From this τ, the lower bound of the near-optimal σ can be approximately determined because σ is close to τ based on the Gaussian models shown in Fig. 1.

On the other hand, let the incoming attack be malicious such as object placement, cloning, and so on. The probability that the relations of parent-child pairs in a tree-structured digital signature may be destroyed is defined as

$$\begin{aligned} p^M &= 2 \times (P\{0 < d < \tau - \sigma\} + P\{\tau < a < \infty\}) \\ &= 2 \times (P\{0 < d < \tau - \sigma\} + (1 - P\{0 < a \leq \tau\}) \\ &= 2 \times (erf(\frac{\tau - \sigma}{2\rho_S}) + [1 - erf(\frac{\tau}{2\rho_M})]). \end{aligned} \quad (8)$$

In Eq. (8), $\tau - \sigma$ is known to be small and, thus, $\frac{\tau-\sigma}{2\rho_S}$ is very small. As a consequence, the first term in Eq. (8), $erf(\frac{\tau-\sigma}{2\rho_S})$, has a value close to zero because it corresponds to an incidental modification. On the other hand, it is known that ρ_M is usually large which leads to a small $\frac{\tau}{2\rho_M}$. As a consequence, the second term of Eq. (8), $[1 - erf(\frac{\tau}{2\rho_M}))]$, has a value which is far away from zero. In general, the detection rate of maliciously tampered regions is determined mainly based on the second term. Once again, given P^M sufficiently large, the estimated standard deviation ρ_M of malicious manipulations, and checking the error function tables [1], we shall obtain the upper bound of τ. From this derived τ, the upper bound of near-optimal σ will also be approximately obtained as in the case of incidental modifications.

In sum, the interval which the near-optimal σ should fall into can be mathematically derived from the above analysis.

3.2. Tampering at the Locations Where $TSDS$ is not Recorded

If the locations of the elements in a $TSDS$ are correctly guessed, the attacker may try to tamper with those positions which are not recorded in the corresponding $TSDS(\mathbf{I})$ and thus disable our method. Fortunately, the attackers cannot succeed in this case because if the parent-child pairs are not recorded in a $TSDS(\mathbf{I})$ that means their interscale relationships do not satisfy the condition in Eq. (2). In other words, we can verify easily by checking the signature symbols of those parent-child pairs that are not recorded in $TSDS(\mathbf{I})$ and $TSDS(\tilde{\mathbf{I}})$. Let $< w_{s,o}(x,y), w_{s+1,o}(2x+i, 2y+j) >$ be a parent-child pair which is not in a $TSDS(\mathbf{I})$ and assume its corresponding pair $< \tilde{w}_{s,o}(x,y), \tilde{w}_{s+1,o}(2x+i, 2y+j) >$ is not in a $TSDS(\tilde{\mathbf{I}})$, where $0 \leq i, j \leq 1$. We can determine whether the $< w_{s,o}(x,y), w_{s+1,o}(2x+i, 2y+j) >$ pair is tampered or not by checking $sym < \tilde{w}_{s,o}(x,y), \tilde{w}_{s+1,o}(2x+i, 2y+j) >$. If $sym < \tilde{w}_{s,o}(x,y), \tilde{w}_{s+1,o}(2x+i, 2y+j) >$ is equal to V, then it is tampered. It is known that the condition for $sym < \tilde{w}_{s,o}(x,y), \tilde{w}_{s+1,o}(2x+i, 2y+j) >$ to belong to V is $||\tilde{w}_{s,o}(x,y)| - |\tilde{w}_{s+1,o}(2x+i, 2y+j)|| < \sigma$.

4. EXPERIMENTAL RESULTS

Our tree-structured digital signature-based image authentication scheme was first tested against a Beach image with 256×256 size. A large "umbrella" was placed on the Beach image and formed a tampered image, which is very similar to Fig. 2(a) without compression effect. The parent-child pairs whose difference d satisfying $|d| > \sigma = 256/\sigma = 128$ were, respectively, chosen to construct a $TSDS$. As we expected from the detection results, the $TSDS$ with a smaller size will lose some tampered pixels. However, the integration of multiscale results was sufficiently to reflect the tampered area. The above experiments provided a good example showing the compromise between robustness and fragility under two tree-structured digital signatures with different sizes. Other results can also be found in [10].

In the second part of our experiments, we applied several incidental distortions on the Beach image to test the robustness of our scheme. Three tree-structured digital signatures with different number of parent-child pairs were constructed. It can imagine that the $TSDS$ with a smaller/larger $|TSDS|$ (corresponding to a larger /smaller σ) would result in few/more elements. In our results, perfect completeness of $TSDS$ can be obtained under different $SPIHT$ compression ratios using three different σ. For $JPEG$ compression, perfect preservations of $TSDS$ (except for the results obtained from $\sigma = 64$) were also obtained for quality factors ranging from 60% (7 : 1) to 10% (21.7 : 1). In addition, Table 1 summarized the verification results obtained under other incidental distortions including rescaling, histogram equalization, blurring, median filtering, sharpening, and Gaussian noise adding. These

manipulations are sometimes unavoidable in image processing and thus cannot be considered as malicious modifications. From the above results, we can find that the completeness of tree-structured digital signature was consistently very high for incidental manipulations when $\sigma > 64$ except for the case of median filtering. This indicates that our method can really tolerate common incidental modifications very well for σ large enough. Practically, a reasonable σ can be determined mathematically based in the analysis described in Sec. 3.

In the third part of our experiments, we shall use our scheme to authenticate those images which were modified by an incidental manipulation and a malicious distortion simultaneously. Fig. 2(a) shows a beach image which was first $JPEG$ compressed with quality factor 10% and then an "umbrella" object was placed. The verification results obtained at $2^2 - 2^4$ scales using $\sigma = 128$ were shown in Figs. 2(b)$\sim$(d), respectively. As we can see from these results the area where the umbrella was placed could be approximately detected and the $JPEG$ compressed does not affect the verification results. Another set of experiments is shown in Fig. 3. The beach image was first scaled down to 128×128 from 256×256 and then the umbrella object was placed on it. Finally, the image was rescaled to the original size 256×256, as shown in Fig. 3(a). When σ was set to be 128, Figs. 3(b)$\sim$(d) showed the placed umbrella was detected at $2^2 - 2^4$ scales. However, some small fragments which were not the targets were mistaken detected. This is because the changes of wavelet coefficients resulted from rescaling are liable to destroy the tree-structured digital signature than the $JPEG$ does.

Finally, we conducted an experiment to demonstrate if a malicious tampering was operated on the areas which were not recorded in a $TSDS$, then they could also be detected as we have analyzed in Sec. 3.2. In Fig. 4(a), a helicopter was placed on the sky portion of the beach image. In fact, the wavelet coefficients in the sky area do not belong to the tree-structured digital signature. Using the proposed scheme, the tampered area could be detected at $2^2 - 2^4$ scales and shown, respectively, in Figs. 4(b)$\sim$ (d) when $\sigma = 128$. It can be observed that the helicopter can be approximately detected at multiple scales. The blocky effect shown in Fig. 4(b)$\sim$ (d) was the natural results inherited from the multiresolution representation of the wavelet transform.

From the above experiments, we could make a conclusion about the selection of σ. The value of σ can be mathematically determined from the analysis described in Sec. 3. However, the assumptions used in Sec. 3 may not always hold, so we can empirically choose σ to be ≥ 128 which has been confirmed by several experimental results.

5. CONCLUSION

For image authentication, it is desired that the verification method is able to resist content-preserving modifications while being sensitive to content-changing modifications. In this paper, a new tree-structured digital signature scheme has been proposed for image authentication. We make use of the structure of a wavelet-transformed image itself to construct the digital signature. The only way to destroy the structure of our digital signature is to significantly change the image's content, however, malicious modifications would be detected. In addition, some unavoidable image processing techniques will preserve a great many of $TSDS$ which would be detected to be incidental. Performance analysis and experimental results have been given to show that our scheme is really robust to content-preserving manipulations and fragile to content-changing distortions.

Our future work will consider the geometric distortions such as rotation, which cannot be tolerated in this paper because the tree-structured digital signature is variant to rotation.

6. REFERENCES

[1] M. Abramowitz and I. A. Stegun, "Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables", *Dover Publications*, Inc., New York, 1965.

[2] S. Bhattacharjee and M. Kutter, "Compression Tolerant Image Authentication", *IEEE Inter. Conf. on Image Processing*, USA, pp. 435-439, 1998.

[3] J. Dittmann, A. Steinmetz, and R. Steinmetz, "Content-based Digital Signature for Motion Pictures Authentication and Content-Fragile Watermarking", *IEEE Inter. Conf. Multimedia Computing and Systems*, Vol. II, Italy, pp. 209-213, 1999.

[4] J. Fridrich, "Methods for Detecting Changes in Digital Images", *Proc. IEEE Int. Workshop on Intell. Signal Processing and Communication Systems*, 1998.

[5] G. L. Friedman, "The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image", *IEEE Trans. Consumer Electronics*, Vol. 39, pp. 905-910, 1993.

[6] D. Kundur and D. Hatzinakos, "Digital Watermarking for TellTale Tamper Proofing and Authentication", *Procceedings of the IEEE*, Vol. 87, pp. 1167-1180, 1999.

[7] C.-Y. Lin and S.-F. Chang, "A Robust Image Authentication Method Surviving JPEG Lossy Compression", *SPIE Storage and Retrieval of Image/Video Database*, Vol. 3312, San Jose, 1998.

[8] C.-Y. Lin and S.-F. Chang, "Generating Robust Digital Signature for Image/Video Authentication", *Multimedia and Security Workshop at ACM Multimedia*, UK, 1998.

[9] C. S. Lu, H. Y. Mark Liao and C. J. Sze, "Combined Watermarking for Image Authentication and Protection", *Proc. 1st IEEE Int. Conf. on Multimedia and Expo*, USA, 2000.

[10] C. S. Lu and H. Y. Mark Liao, "Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme", *Proc. Multimedia and Security Workshop at 8-th ACM Int. Conf. on Multimedia*, LosAngeles, California, USA, Nov. 4, 2000.

[11] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography", *CRC Press*, 1997.

[12] S. Walton, "Image Authentication for A Slippery New Age", *Dr. Dobb's Journal*, Vol. 20, pp. 18-26, 1995.

[13] R. B. Wolfgang and E. J. Delp, "Fragile Watermarking Using the VW2D Watermark", *Proc. SPIE/IS&T Inter. Conf. Security and Watermarking of multimedia Contents*, Vol. 3657, pp. 40-51, 1999.

[14] M. Wu and B. Liu, "Watermarking for Image Authentication", *Proc. IEEE ICIP*, 1998.

[15] M. M. Yeung and F. Mintzer, "An Invisible Watermarking Technique for Image Verification", *IEEE Conf. Image Processing*, Vol. 2, pp. 680-683, 1997.

[16] B. Zhu, M. D. Swanson, and A. H. Tewfik, "Transparent Robust Authentication and Distortion Measurement Technique for Images", *IEEE Digital Signal Processing Workshop*, pp. 45-48, 1996.

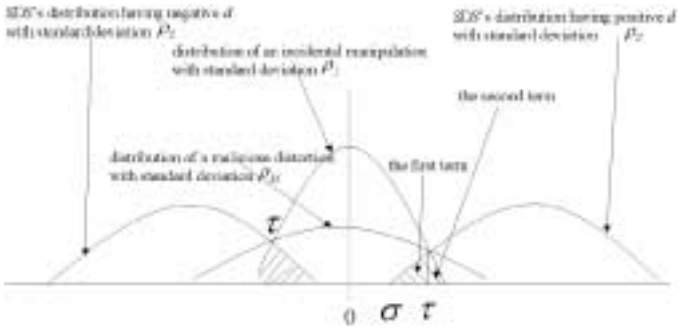
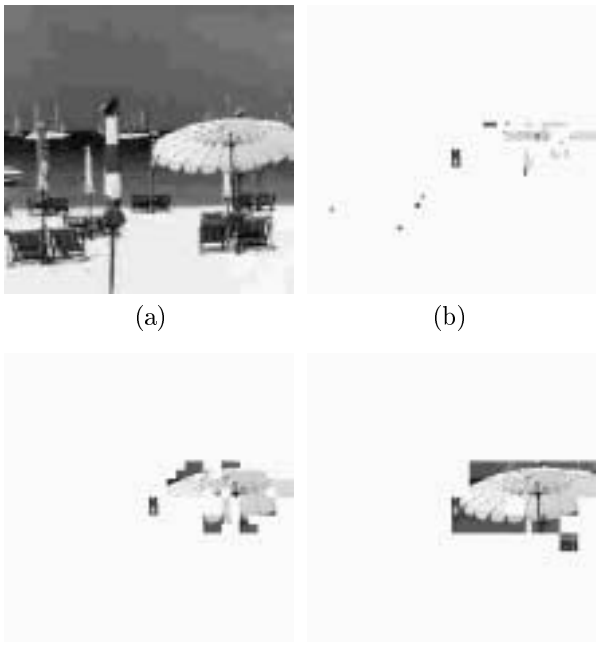


Figure 1: The possible relationship between the attack's distribution $\mathcal{G}^A$ (with standard deviation ρ_I or ρ_M) and the $TSDS$'s distribution $\mathcal{G}^S$ (with standard deviation ρ_S).

Table 1: $CoTSDS$ **of the Beach image under other incidental distortions (IDs): R (rescaling), H (histogram equalization), B (blurring,** 7×7**), M (median filtering,** 5×5**), S (sharpening), and G (Gaussian noise). Among them, sharpening and Gaussian noise adding with amount** 16 **were run using Photoshop.**

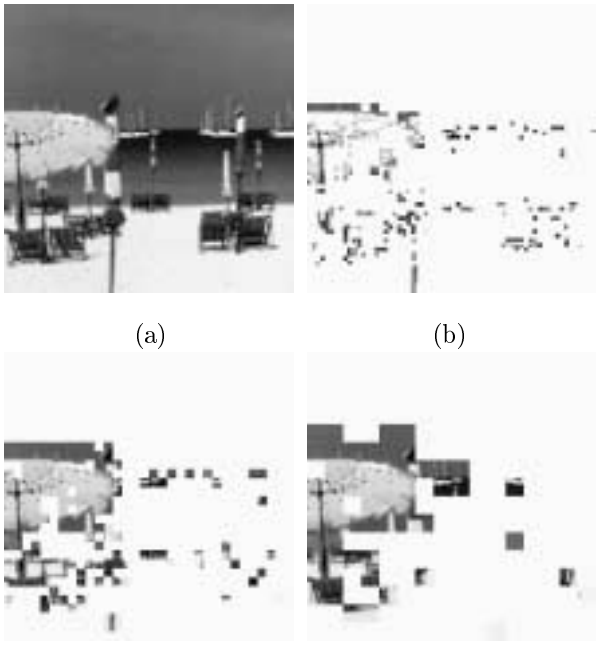
IDs	ρ_I	*Completeness of* $TSDS$		
		$\sigma = 256$	$\sigma = 128$	$\sigma = 64$
R	26.8	0.993	0.918	0.808
H	27.3	0.983	0.961	0.946
B	22.9	0.988	0.915	0.807
M	23.0	0.943	0.830	0.682
S	23.4	1.000	0.990	0.954
G	15.9	1.000	1.000	1.000



(a) (b)

(c) (d)

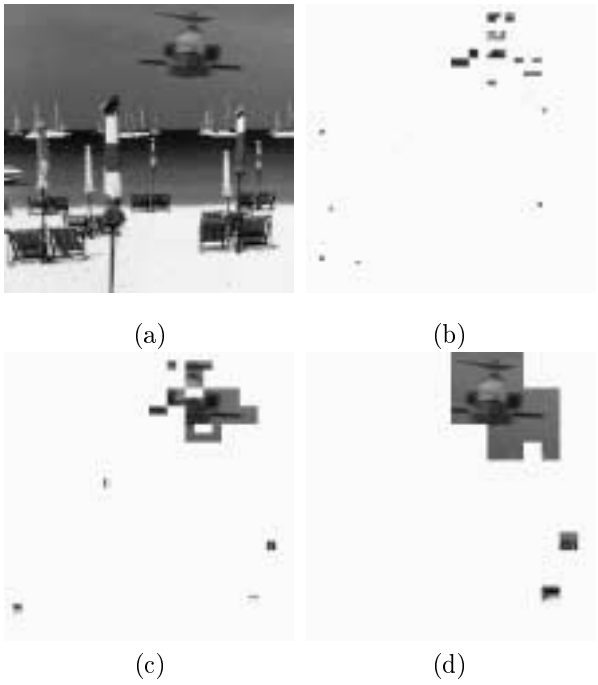
Figure 2: Combined attacks with incidental and malicious manipulations: (a) beach image after $JPEG$+"umbrella" placement; (b)∼(d) detected results of (a) at $2^2 \sim 2^4$ scales when $\sigma = 128$.



(a) (b)

(c) (d)

Figure 3: Combined attacks with incidental and malicious manipulations: (a) beach image after rescaling(scaling+"umbrella" placement); (b)∼(d) detected results of (a) at $2^2 \sim 2^4$ scales when $\sigma = 128$.



(a) (b)

(c) (d)

Figure 4: Malicious manipulations on non-$TSDS$ areas: (a) maliciously tampered image with a "helicopter" on the sky; (b)∼(d) detected results of (a) at $2^2 \sim 2^4$ scales when $\sigma = 128$.