Hindawi Publishing Corporation
Advances in Multimedia
Volume 2012, Article ID 875759, 17 pages
doi:10.1155/2012/875759

Research Article

Robust Signature-Based Copyright Protection Scheme Using the Most Significant Gray-Scale Bits of the Image

Mohammad Awrangjeb

Cooperative Research Centre for Spatial Information, Department of Infrastructure Engineering, University of Melbourne, VIC 3010, Australia

Correspondence should be addressed to Mohammad Awrangjeb, mawr@unimelb.edu.au

Received 15 November 2011; Revised 2 March 2012; Accepted 27 March 2012

Academic Editor: Xian-Sheng Hua

The *most significant bit-* (MSB-) plane of an image is least likely to change by the most signal processing operations. This paper presents a novel multibit logo-based signature, using the most significant gray-scale bits, which is then used to develop an extremely simple but robust copyright protection scheme, where images along with their signatures are sent to a trusted third party when a dispute arises. Different ways of processing the MSB-plane before calculating the robust signature have been developed. This paper then presents an innovative classifier-based technique to test the robustness and uniqueness of any signature-based scheme. A new MSB-based attack, which would defeat our scheme most, has also been proposed. Experimental results have clearly demonstrated the superiority of the proposed scheme showing the high robustness of different MSB-based signatures over the existing signature-based schemes.

1. Introduction

For last few years, we have been using electronic commerce that includes online and offline distribution of multimedia data like images, audios, and videos. However, digital multimedia files can be easily manipulated using commercial graphics tools. Duplicating digital files has become as simple as clicking a button. Since maintaining an exact or manipulated duplicate of any digital data is easier than before, the enforcement of copyright protection has become more imperative than ever. Although copyright laws are being applied against abusers in order to ensure secure electronic commerce, the current problems with copyright protection obstruct the rapid evolution of computer and communication networks. As a result, the enhancement and further development of digital copyright protection is in central to the development of future communication networks [1]. There may be three types of solutions to the copyright protection problem: cryptographic tools, digital watermarking techniques, and digital signature-based techniques.

Cryptographic tools [2] can be used to encrypt a multimedia file using some secret key. The encrypted file is no more perceptually understandable and can be distributed to the users. Only the appropriate user that holds the secret key can decrypt and use this file. Such a technique while suitable for text documents is not suitable for multimedia data for the following two reasons. First, multimedia file size is much larger than that of text. Therefore, encrypting or decrypting a multimedia file is highly time consuming. Second, the encrypted media file is not useful in the public domain, for example, in the Internet. Because the encrypted file is not perceptually understandable and if the encrypted information is decrypted once, the information is no longer protected. However, the multimedia file provides an opportunity that the text document does not. That is, while no distortion is allowed in the signed text, some distortions are allowed in the signed multimedia file as long as it is perceptually similar to the original file.

Digital watermarking techniques take the opportunity of the abovementioned property of the media file. They embed a watermark such as logos, seals, or sequence numbers, into the original image. The embedded watermark should survive against both malicious and nonmalicious attacks depending on the applications. Latter, the embedded information is extracted from or detected in the watermarked image in order to verify the ownership [3–11].

Any watermarking technique should satisfy a number of essential properties [1, 5, 6]. However, many of the existing techniques do not satisfy some of the properties and, therefore, may not be applicable to build a proper copyright protection system [1, 8, 9]. They always distort the original image that might not be acceptable in some applications like medical imagery, law enforcement, and astrophysics research [7]. The amount of distortions increases with the increase of the embedding strength which though increases the chance of the survival of the watermark under different signal processing attacks. Some attacks like geometric distortions, collusion, and copy (averaging) attacks still challenge the robustness property. The watermark can also be removed using denoising [9]. Multiple watermarking (buyer's and seller's watermarks) in a single media is also problematic, since previous embedded watermark cannot be guaranteed to survive after the embedding of next watermark. Publicly verification of watermarking is another unsolved problem.

Digital signature-based copyright protection schemes [1, 12–15] combine the advantages of both digital watermarking and cryptographic solutions. This technique, in general, calculates a digital signature using a logo and the extracted features from the original image (see Figure 1). The signature may then be protected using cryptography and certified by a *trusted third party* (TTP). Later, the signature is used to retrieve the logo from the test image. The retrieved logo is compared with the original logo using some similarity measurement function and a decision is made based on a threshold.

The reason of using a logo as a watermark [16] or to calculate signature [1, 12–15] is because it is a true representative of a company, an owner, or a customer. In the verification phase, in addition to "yes" or "no" answer based on the threshold, logo-based copyright protection schemes also allow perceptual recognition of the logo. Watermarking techniques embedding logos [16] mainly embed small binary logos and are unable to use large multibit (e.g., gray-scale) logos due to limited embedding capacity. However, large multibit logos are more practical and offer greater security than small binary logos. In contrast, signature-based schemes may calculate signature using any type (e.g., binary, gray-scale) and size of logos. There are also other signature-based schemes [17, 18], which do not use logos.

There are many advantages of signature-based schemes over watermarking techniques. They cause no visual quality degradation to images as they do not embed any information. They offer cryptographic security and can sign any sizes of logos. They resolve multiple ownership claims by adding timestamp with the signature. They can use both buyer and seller logos while calculating the signature, thus providing practical usefulness of the copyright protection system in the network world. They can use any multibit logos that offer greater opportunity to survive than binary logos. In addition, they allow public verification when the signature is generated using public key cryptographic infrastructure.

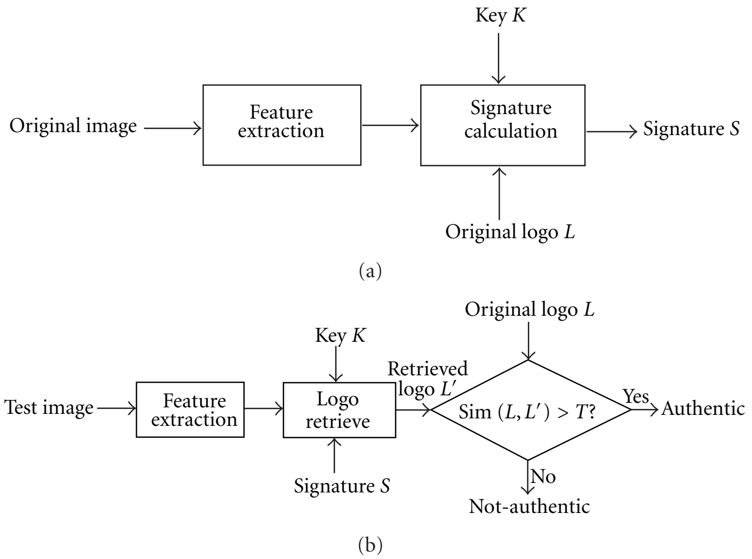
Katzenbeisser [19] argued that watermarking alone is not sufficient to resolve rightful ownership of digital data; therefore, a protocol relying on the existing cryptographic tools is necessary. Macq et al. [20] mentioned that watermarking along with registration authorities and transaction certifications are essential for digital right management of Internet distributed images. The signature-based schemes along with cryptographic tools can be considered as the complementary to the watermarking techniques to design a proper digital right management system.

In this paper, we propose a computationally inexpensive signature-based gray-scale image copyright protection scheme intuitively using the *most significant bit-* (MSB-) plane (MSB-based scheme), which is least likely to change by any image processing operation. The MSB-plane of an image can be chosen in different ways before calculating the signature using the bit-planes of the logo: (i) directly choosing the MSB-plane at a *region-of-interest* (ROI), (ii) choosing the MSB-planes of textured blocks, (iii) choosing the MSBs of DC coefficients of the MSB-plane, and (iv) choosing the MSB-plane after t-scale wavelet decomposition. Besides being image size invariant, the proposed scheme can be used with any n-bit logo. In order to prove the robustness and the uniqueness of this scheme, we also present a novel idea of finding a classifier to separate logo retrieval instances of attacked images with the original signature against all other possible alternatives. To avoid any bias, we further propose a new MSB-based attack, which would defeat our scheme most. We then present a comprehensive TTP management policy that uses classifier-based thresholds in order to minimize false alarms. Experimental results not only reveal very high logo retrieval rate and visual quality of the retrieved logos by the proposed scheme against those by the existing schemes [12, 13] that also use multibit logos but also show the weakness of the latter as they fail to produce any classifier as discussed above. Note that the proposed signature-based scheme along with some preliminary results was published in [21].

The rest of the paper is organized as follows: Section 2 presents the previous signature-based schemes using logos; Section 3 describes why we have chosen MSB bit-plane for the proposed scheme; Section 4 presents the proposed scheme; Section 5 presents the experimental results and then compares the proposed scheme with the existing schemes; finally Section 6 concludes the paper with future research directions.

2. Previous Works

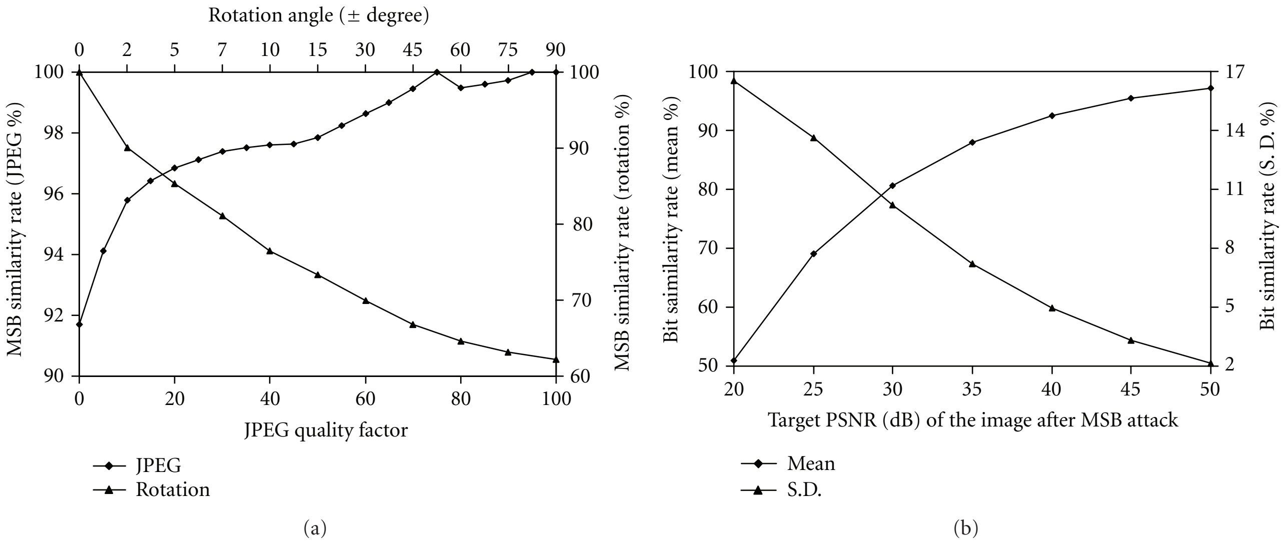
Lee and Chen [13] calculated the signature of an image with a gray-scale logo using *vector quantization* (VQ) on the coarse scale of the image obtained by a t-scale wavelet transform. The scheme is publicly verifiable and robust to a wide variety of attacks. However, it is weak to high lossy compression and geometric distortions. It cannot calculate signature if the type of the logo and the image is different, for example, binary logo and gray-scale image. The size of the coarse image reduces exponentially as t increases. Compounded with the approximation due to VQ, this can potentially lead to a very poor quality of the retrieved logo, especially when



(a)

(b)

Figure 1: Signature-based scheme using logo: (a) signature calculation and (b) logo retrieval operation and verification.



(a)

(b)

Figure 2: (a) Most significant bit (MSB) similarity rates of gray-scale image at different JPEG and rotation attacks; (b) mean and standard deviation of gray-scale MSB similarity under the newly proposed MSB attack. Note that the rotation angle axis in (a) is nonlinear.

the original image size is small as demanded by the WWW. Chen et al. [1] later extended this idea for binary logos by replacing VQ with a polarity table. However, uniqueness of the signature, where it should verify the corresponding image only, may not be guaranteed with binary logos.

Chang et al. [14] calculated signature with a gray-scale logo using torus automorphism functions. To survive in cropping attacks, the idea of using a rectangular *region-of-interest* (ROI) in the image was introduced in [12]. This technique can be used for cartoon graphics and survives on repainting. Nevertheless, it still cannot survive in high lossy compression and geometric distortions. It also cannot calculate signature if the type of the logo and the image is different, for example, binary logo and gray-scale image.

The scheme in [15] used visual secret sharing technique to calculate signature using binary logos. It offers cryptographic security and allows generating meaningful share. It also allows multiple owners to share the same image. However, robustness depends on the sorting algorithm; that is, if the image is modified moderately, the sorting algorithm may result different share. Consequently, it cannot survive in high JPEG compression and small geometric distortions.

All the above existing schemes offer very high time complexity. The time complexity increases, due to use of VQ encoding [13], torus automorphism [12, 14], permutation [1], or visual cryptography [15], with the increase of image size. Some of the above schemes [1, 13] incorporate digital signature including timestamp with the published image

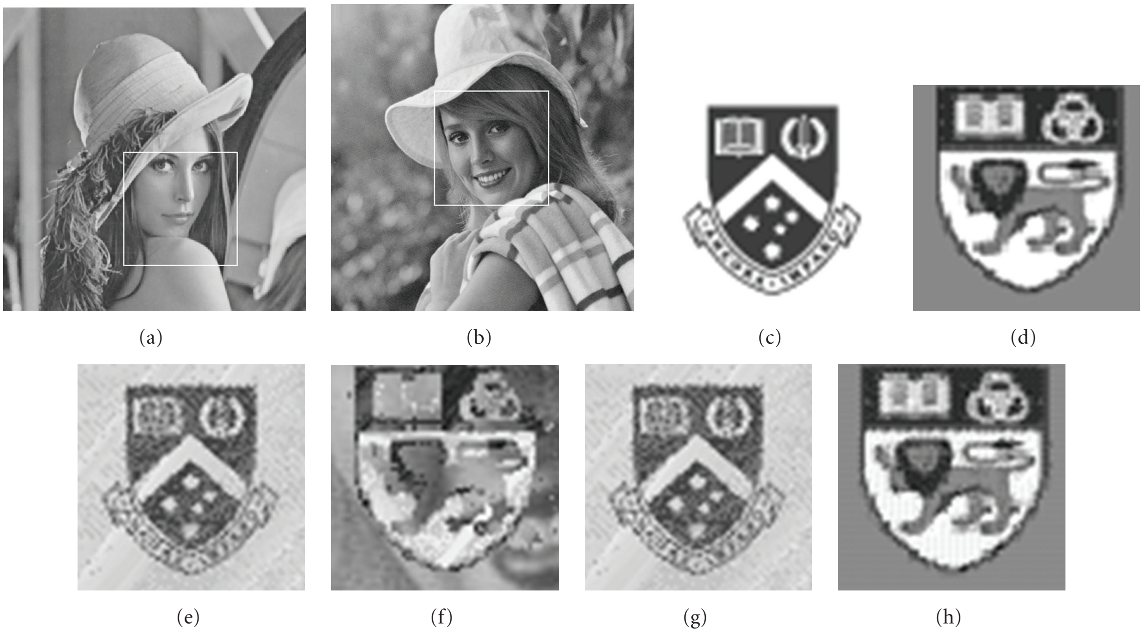


Figure 3: Original images (a) Lena and (b) Elaine with their ROIs used; original logos (c) Monash and (d) NUS; mapped logos by TROI-based scheme [12] (e) Monash (15.19 dB, 53%) and (f) NUS (17.47 dB, 55%); and coded logos by VQ-based scheme [13] (g) Monash (23.40 dB, 64%) and (h) NUS (25.35 dB, 66%). Note that all images (512 × 512) and logos (64 × 64) are 8-bit gray-scale. Request granted to use logos for research purposes only.

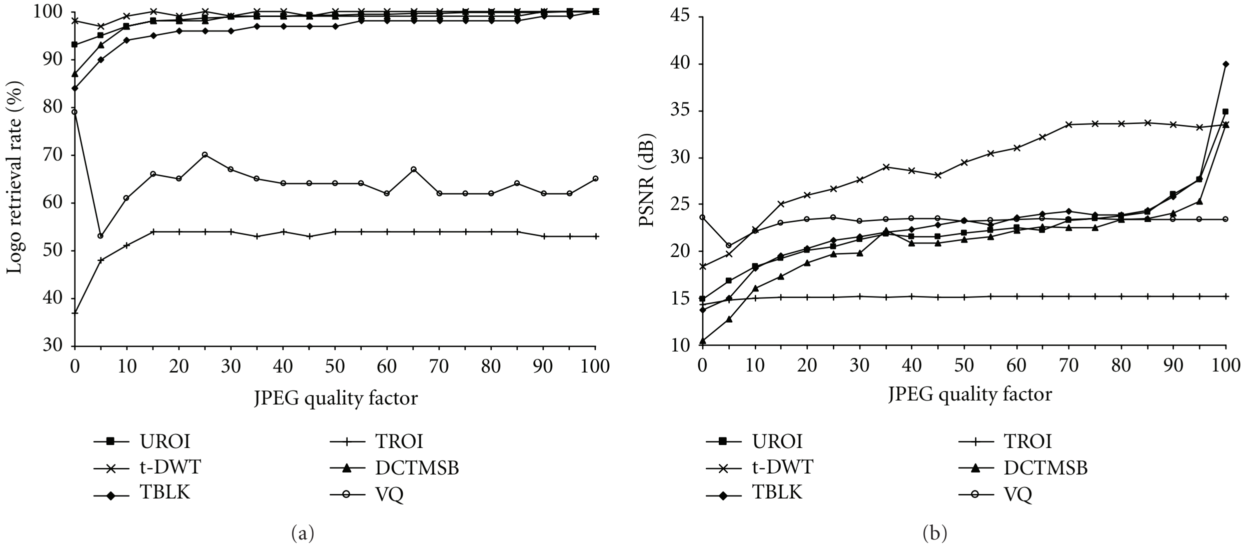


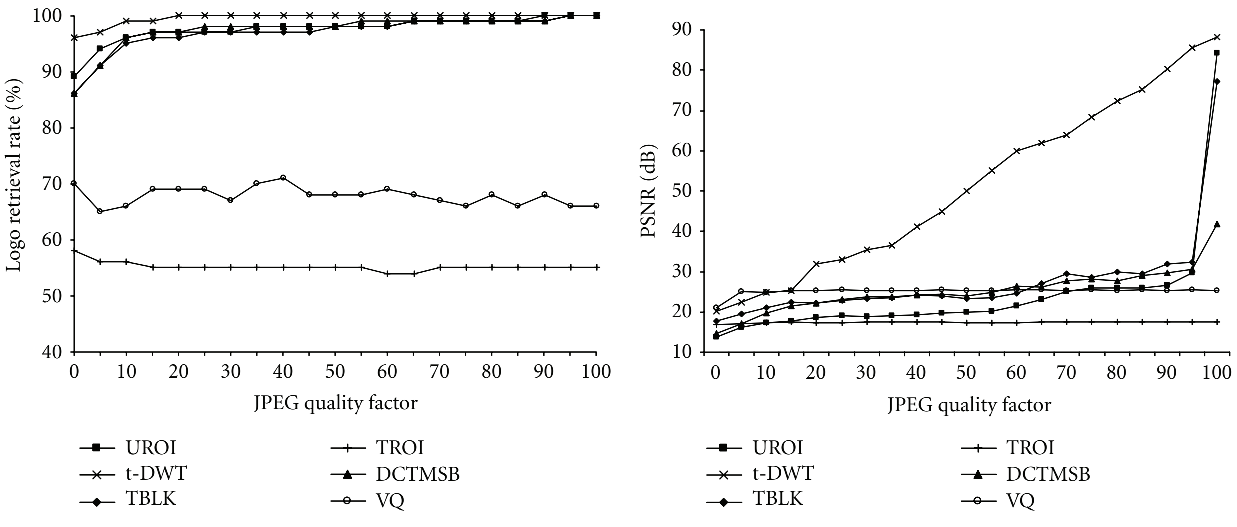
Figure 4: (a) Logo retrieval rate and (b) PSNR using Lena image and Monash logo by different approaches of the proposed MSB-based scheme and existing TROI-based [12] and VQ-based [13] schemes under different JPEG quality factors.

allowing public verification. Nonetheless, they increase the file size and the risk of losing copyright if the signature is removed from the header accidentally or intentionally.

3. Why the Most Significant Bit?

The MSBs are least likely to change by any image processing operation, for example, JPEG compression, filtering, and so forth. However, watermarking techniques cannot embed the watermark in the MSB-plane of an image. Because changes to MSBs introduce higher noticeable distortions. In the following experiments, we observed that the robustness of the MSB-based digital signature would be very high.

We conducted experiments on a large database of 1032 images [22], including the benchmark ones [23]. In each case, we measured the MSB similarity rate, which means the percentage of MSBs that remain unchanged under the attack. Figure 2(a) shows that on average more than 91%



(a)

(b)

Figure 5: (a) Logo retrieval rate and (b) PSNR using Elaine image and NUS logo by different approaches of the proposed MSB-based scheme and existing TROI-based [12] and VQ-based [13] schemes under different JPEG quality factors.

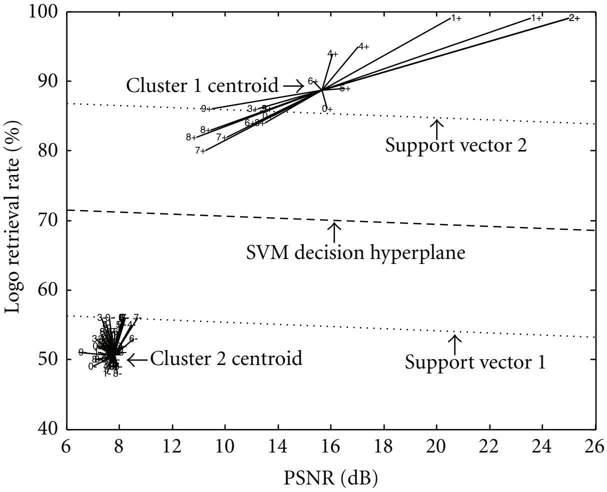


Figure 6: SVM classification and K-means clustering results by the UROI approach of the proposed MSB-based scheme. Note that the distance between support vectors by SVM [27] is $d = 30.2$ and cluster 1 and cluster 2 are positive and negative clusters, respectively, by K-means clustering algorithm [28]. Attack numbers 0–9 are referred using Table 3.

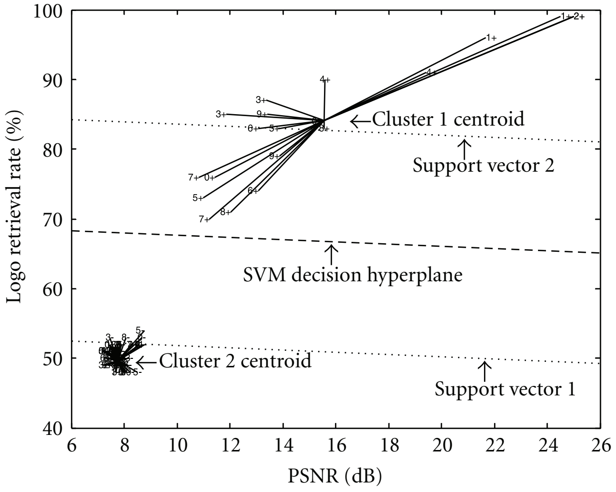


Figure 7: SVM classification and K-means clustering results by the TBLK approach of the proposed MSB-based scheme. Note that the distance between support vectors by SVM [27] is $d = 31.5$ and cluster 1 and cluster 2 are positive and negative clusters, respectively, by K-means clustering algorithm [28]. Attack numbers 0–9 are referred using Table 3.

of the gray-scale MSBs remained the same even when JPEG quality was set at the minimum; while more than 88% of the MSBs remained unchanged if the image is rotated by no more than ±5°. We further observed that under median filter, histogram equalization, salt and pepper noise, and Gaussian noise attacks on average more than 97%, 80%, 97%, and 90% of MSBs, respectively, remained unchanged, as shown in Table 1. In addition, we also tested the MSB similarity rate in the following four cases: (i) the MSB-plane at an ROI, (ii) the MSB-planes of textured blocks, (iii) the MSBs of DC coefficients of the MSB-plane, and (iv) the MSB-plane after 4-scale wavelet decomposition. Table 1 shows that histogram equalization and rotation attacks changed more MSBs than filtering and noising attacks. In StirMark attacks [24] like small random distortions, first three cases kept more than 80% MSBs unchanged and 4-level wavelet decomposition case is the most sensitive to these attacks. We will discuss how the MSBs were extracted in these four cases in Section 4.1.

In order to avoid any bias, we now propose a new attack, namely, the MSB attack, where for a given target image-quality, in *peak-signal-to-noise ratio* (PSNR), the maximum number of gray-scale MSBs are changed. We sort the pixels in

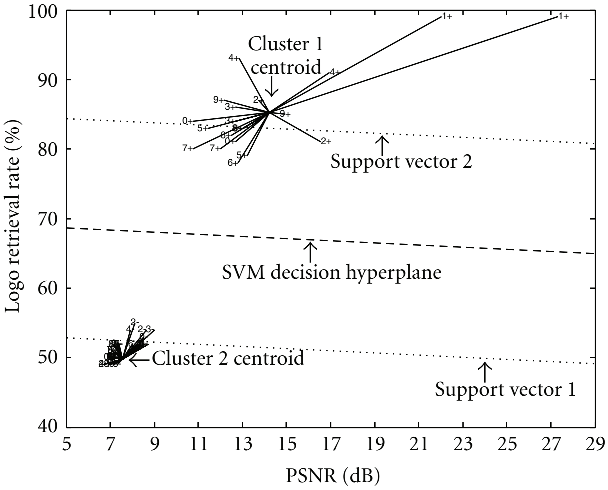


FIGURE 8: SVM classification and K-means clustering results by the DCTMSB approach of the proposed MSB-based scheme. Note that the distance between support vectors by SVM [27] is $d = 31.3$ and cluster 1 and cluster 2 are positive and negative clusters, respectively, by K-means clustering algorithm [28]. Attack numbers 0–9 are referred using Table 3.

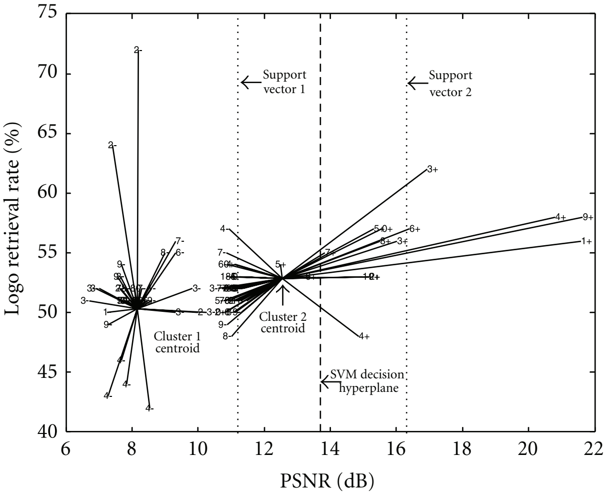


FIGURE 10: SVM classification and K-means clustering results by the existing TROI-based scheme [12]. Note that the distance between support vectors by SVM [27] is $d = 5.1$ and cluster 1 and cluster 2 are positive and negative clusters, respectively, by K-means clustering algorithm [28]. Attack numbers 0–9 are referred using Table 3.

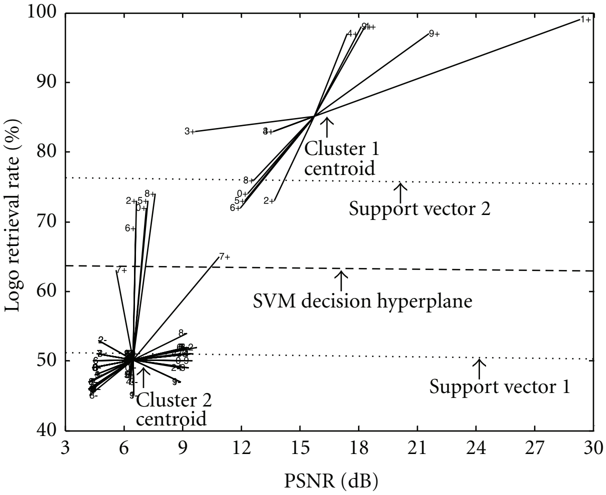


FIGURE 9: SVM classification and K-means clustering results by the t-DWT ($t = 4$) approach of the proposed MSB-based scheme. Note that the distance between support vectors by SVM [27] is $d = 25.1$ and cluster 1 and cluster 2 are positive and negative clusters, respectively, by K-means clustering algorithm [28]. Attack numbers 0–9 are referred using Table 3.

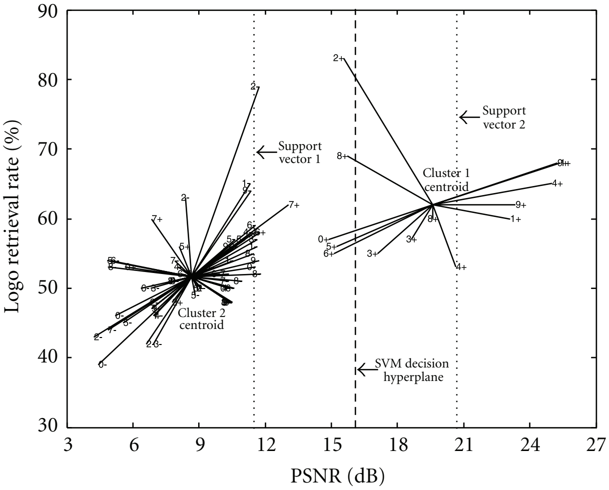


FIGURE 11: SVM classification and K-means clustering results by the existing VQ-based scheme [13]. Note that the distance between support vectors by SVM [27] is $D = 9.2$ and cluster 1 and cluster 2 are positive and negative clusters, respectively, by K-means clustering algorithm [28]. Attack numbers 0–9 are referred using Table 3.

an array in the ascending order according to their differences with the mid-gray value. Then, the MSB of the pixel with the lowest difference is flipped first and the entry for that pixel in the sorted list is taken out. This operation is continued until a certain PSNR is obtained. Figure 2(b) shows that on average more than 80% of the MSBs, with no more than 10% standard deviation, remained unchanged at 30 dB target PSNR, below which the visual quality of the image is unacceptable to the human eyes [13]. Table 1 also shows that in above four cases, on the average 85% MSB remained the same at 35 dB target PSNR, and among these cases 4-level DWT decomposition left most of the MSBs unchanged.

From Figure 2 and Table 1, it is observed that even when the images are distorted to a limit where the PSNR becomes as low as 15 dB to 30 dB, the majority of the MSBs still remain the same. This is because in signal processing attacks (JPEG, filtering, etc.), image pixels do not change their locations and thus majority of the MSBs do not change. On the other hand, in geometric attacks (rotation, scaling, etc.) image pixels change their locations and thus the MSB similarity rate drops even in small rotation angle change. In the case of high geometric distortions, it is possible to estimate the transformation parameters first [25] and then to reverse the transformation before using the MSBs for signature calculation.

4. Proposed Scheme

The proposed MSB-based scheme first selects a set of MSBs from the image and then calculates digital signature of an image for a logo. The signature is certified by the TTP. When a dispute arises between two images of two parties, both parties send their certified signatures and images along with their corresponding parameters to the TTP to judge.

4.1. Selecting the MSBs. The MSBs can be selected in different ways. In this section, we discuss four of them.

Consider an n-bit gray-scale image $I = \{i_b(x,y)\}$ of size $w_I \times h_I$ pixels where $1 \leq x \leq w_I$, $1 \leq y \leq h_I$, and $1 \leq b \leq n$. Similarly, consider an n-bit gray-scale logo $L = \{l_b(x,y)\}$ of size $w_L \times h_L$. Depending on the different ways of pre-processing the MSB-plane of the image, the MSB-based scheme may be named as different approaches.

(i) UROI. The MSB-plane at an ROI of the image is chosen directly. Notice that an ROI can be user defined and can be located using reference points, for example, corners [26].

(ii) TBLK. The MSB-planes of textured blocks at the ROI are chosen. We select 8 × 8 textured blocks from the image using the technique represented in [7]. The MSB-planes of the selected textured blocks are accumulated as a single MSB-plane, where textured blocks are first taken in row-wise and then in column-wise.

(iii) DCTMSB. We can choose the MSBs of DC coefficients of MSB-plane. We divide the MSB-plane into 8 × 8 blocks before taking DCT. Then we take the MSB of DCT coefficients in original space order (without sorting them).

(iv) t-DWT. The MSB-plane of LL_t after t-scale wavelet decomposition of the original image is chosen.

4.2. Signature Calculation. Let $M_I = \{m_j\}$, where $1 \leq j \leq z$, be the collective set of MSBs selected from I using one of the above approaches. Without any loss of generality, it is assumed that

$$z \geq n w_L h_L. \tag{1}$$

The signature S_I of I for L with M_I is thus calculated as

$$S_I(j = (b-1)w_L h_L + (y-1)h_L + x) = m_j \oplus l_b(x,y). \tag{2}$$

If the generality assumption in (1) cannot be met, m_j's could be reused iteratively once exhausted. Moreover, any color image can be signed using its gray-scale equivalent with even a colored logo after stripping it into three gray-scale channels. Once the signature is calculated, the owner sends the following message, in the form of a triplet, to the TTP using public key cryptography:

$$M_{OT} = E_{T,\text{ PUB}}(E_{O,\text{ PRV}}([I, S_I, A_I])), \tag{3}$$

where $E_{T,\text{PUB}}$ and $E_{O,\text{PRV}}$ are the public and private key encryptions of the TTP and the owner respectively and A_I contains information about the MSB selection approach. On receiving the above message from the owner O at time TS, the message is first decrypted to receive the signature triplet as follows:

$$[I, S_I, A_I] = D_{O,\text{PUB}}(D_{T,\text{PRV}}(\text{Msg})), \tag{4}$$

where $D_{O,\text{PUB}}$ and $D_{T,\text{PRV}}$ are the public and private key decryptions of the owner and the TTP, respectively. The TTP verifies S_I for I using A_I, appends timestamp TS, and sends back the following message to the owner:

$$M_{TO} = E_{O,\text{PUB}}(E_{T,\text{PRV}}(S_I || TS)), \tag{5}$$

where $E_{O,\text{PUB}}$ and $E_{T,\text{PRV}}$ are the public and private key encryptions of the owner and the TTP, respectively. The owner decrypts the above message with his private key as

$$S_I^c = E_{T,\text{PRV}}(S_I || \text{TS}) = D_{O,\text{PRV}}(M_2), \tag{6}$$

where $D_{O,\text{PRV}}$ is the private key decryptions of the owner. We name S_I^c as the certified signature for the image I.

4.3. Signature Verification. When a dispute arises for two images I_i and I_j between two persons P_1 and P_2, they send the following messages claiming the ownership to the TTP:

$$\begin{aligned} M_{P_1T} &= E_{T,\text{PUB}}\left(E_{P_1,\text{PRV}}\left(I_i, L_1, S^c_{I_i}, A_{I_i}\right)\right), \\ M_{P_2T} &= E_{T,\text{PUB}}\left(E_{P_2,\text{PRV}}\left(I_j, L_2, S^c_{I_j}, A_{I_j}\right)\right), \end{aligned} \tag{7}$$

where $E_{P_1,\text{PRV}}$ and $E_{P_2,\text{PRV}}$ are the private key encryptions of P_1 and P_2, respectively. The TTP decrypts the above messages as

$$\begin{aligned} \left[I_i, L_1, S^c_{I_i}, A_{I_i}\right] &= D_{P_1,\text{PUB}}(D_{T,\text{PRV}}(M_{P_1T})), \\ \left[I_j, L_2, S^c_{I_j}, A_{I_j}\right] &= D_{P_2,\text{PUB}}(D_{T,\text{PRV}}(M_{P_2T})), \end{aligned} \tag{8}$$

where $D_{P_1,\text{PUB}}$ and $D_{P_2,\text{PUB}}$ are the public key decryptions of P_1 and P_2, respectively. The TTP then decrypted the certified signatures $S^c_{I_i}$ and $S^c_{I_j}$ with its public key; this ensures the certificates have been issued by the TTP and the timestamps have not been changed afterwards their generation:

$$S_{I_i}\middle\|\text{TS}_i = D_{T,\text{PUB}}\left(S^c_{I_i}\right), \qquad S_{I_j}\middle\|\text{TS}_j = D_{T,\text{PUB}}\left(S^c_{I_j}\right). \tag{9}$$

The TTP recalculates the signatures S_{I_i} and S_{I_j} and compares with the existing ones. This check ensures that encrypted signatures $S^c_{I_j}$ and $S^c_{I_j}$ have been generated for images I_i and I_j, respectively.

Table 1: *Most significant bit* (MSB) similarity rate under different attacks.

Attacks	PSNR (dB)	MSB similarity rate (%)				
		MSB-plane	ROI[1]	Text blocks[2]	DC of MSB[3]	DWT ($t = 4$)[4]
Average filter[5]	28.23	96.4	95.6	96.0	96.3	99.6
BPM (25 dB)	22.94	89.0	91.0	85.0	89.4	97.0
Gauss. (G) filter[5]	36.99	98.8	98.6	99.0	98.8	100
G filter[5] & noise	20.19	90.2	89.4	85.0	89.5	98.2
G noise	20.40	90.8	89.8	85.0	89.3	98.2
Histogram equal.	16.51	80.0	79.0	92.4	84.3	80.8
JPEG (quality 0)	22.87	90.8	90.0	87.0	87.3	94.2
JPEG (quality 5)	25.13	93.8	92.6	91.0	93.3	96.0
JPEG (quality 10)	27.49	95.4	94.6	94.0	96.5	98.6
LSRD[6]	20.16	85.0	88.0	75.0	88.7	92.0
Median filter[5]	29.65	97.4	96.6	98.0	97.3	99.4
Motion filter[5]	26.02	95.2	94.2	92.0	95.5	98.8
MSB (30 dB)	30.00	81.0	75.0	75.0	79.6	93.0
MSB (35 dB)	35.00	85.0	86.0	82.0	89.2	98.0
Rot.-crop (2°)	17.15	88.0	88.6	81.0	93.5	89.6
Rot.-scale (2°)	14.18	84.4	86.0	75.0	89.8	85.6
Salt and pepper	17.95	97.8	97.4	98.0	96.8	98.0
Self similarities	26.04	90.0	95.0	90.0	90.2	99.0
Small rand. dist.	16.27	83.0	83.0	80.0	87.0	75.0
unZign	29.08	97.0	97.0	96.0	99.7	100
Wiener filter[5]	34.61	97.8	97.6	98.0	97.8	100

[1] Region-of-interest.

[2] 512 textured blocks 8 × 8 were chosen from each image.

[3] MSB-plane was divided into 8 × 8 blocks before taking DCT.

[4] 4-level wavelet decomposition.

[5] 3 × 3 window.

[6] Latest small random distortion.

4.3.1. Finding Disputable Images. Let $L = S^{-1}(I, S_I, A_I)$ denote the logo retrieval operation using the inverse process in (2) (see Figure 1(b)). The TTP has to confirm whether images I_i and I_j are disputable before taking a final decision based on the timestamps TS_i and TS_j. Two images are disputable if they are the same image or one is an attacked version of another. To do that the TTP executes the following two test cases:

$$\begin{aligned} \text{TC}_1 &= S^{-1}\left(I_i, S_{I_j}, A_{I_j}\right) \mid S^{-1}\left(I_j, S_{I_j}, A_{I_j}\right), \\ \text{TC}_2 &= S^{-1}\left(I_j, S_{I_i}, A_{I_i}\right) \mid S^{-1}(I_i, S_{I_i}, A_{I_i}), \end{aligned} \tag{10}$$

where the logo retrieved from I_i using signature and feature of I_j is compared against the logo of P_2, and vice versa. If the *logo retrieval rate* (LRR), which is the percentage of unchanged bits, and the PSNR (with respect to original logos L_1 and L_2) of above two test cases TC_1 and TC_2 are above certain *identification thresholds* (Th_{LRR}, Th_{PSNR}), then the images are considered as disputable.

4.3.2. Verification. If I_i and I_j are proved to be disputable, then the TTP compares timestamps TS_i and TS_j. The image is authenticated for P_1 if $\text{TS}_i < \text{TS}_j$ or for P_2 if $\text{TS}_i < \text{TS}_j$.

4.4. Estimating Identification Thresholds. To avoid the risk of error due to arbitrary selection of identification thresholds (Th_{LRR}, Th_{PSNR}), we propose the following innovative classifier-based threshold estimation technique, which can also be used to test the robustness and uniqueness of any signature-based scheme. The lower the value of (Th_{LRR}, Th_{PSNR}), the lower the scheme is robust.

Let $\text{TD} = \{[I_i, S_{I_i}, A_{I_i}]\}$ be a large image *training database* and let $B_i = \{I_i(j)\}$ be a set of *attacked* images from I_i for all i. Let

$$\text{TC}(a, b, c, d, j) = S^{-1}\left(I_a(j), S_{I_b}, A_{I_c}\right) \mid S^{-1}\left(I_d, S_{I_d}, A_{I_d}\right) \tag{11}$$

be a *test case* where the logo retrieved from the jth attacked image of I_a using the signature of I_b and the feature of I_c is compared against the logo used to sign I_d, $1 \leq a, b, c, d \leq |\text{TD}|$, and $1 \leq j \leq |B_a|$. Let the positive (C_+) and negative (C_-) classes be defined as

$$\begin{aligned} C_+ &= \{\forall a, \forall j : \text{TC}(a, a, a, a, j)\}, \\ C_- &= \{\forall a, \forall b, \forall c, \forall d, \forall j : \text{TC}(a, b, c, d, j)\} - C_+. \end{aligned} \tag{12}$$

Note that the LRR and PSNR of all the test cases in (C_+) should ideally be significantly higher than those in (C_-). Any

Table 2: Experimental results (PSNR in dB and LRR in %) by different approaches of the proposed MSB-based scheme and existing TROI-based [12] and VQ-based [13] schemes against various attacks using Lena image and Monash logo.

		Proposed MSB-based scheme								Existing schemes			
Attacks	PSNR	UROI		TBLK		DCTMSB		t-DWT[1]		TROI [12]		VQ [13]	
		PSNR	LRR	PSNR	LRR	PSNR	LRR	PSNR	LRR	PSNR	LRR	PSNR	LRR
Affine (XY)[5]	20.66	19.30	96	14.44	88	14.09	94	10.52	88	14.73	54	14.79	58
Avg. filter[2]	36.85	20.58	99	21.41	96	22.04	99	30.20	100	14.97	53	23.08	60
BPM (25 dB)	22.94	14.36	91	12.97	85	11.19	89	15.18	96	13.85	56	23.67	73
Cropping	10.67	∞	100	13.16	94	13.75	87	6.69	71	15.19	53	15.57	83
Gauss. (G) filter[2]	36.89	20.58	99	21.43	96	22.04	99	30.20	100	14.97	53	23.12	60
G filter[2] & noise	26.56	16.37	94	16.24	91	16.23	96	24.67	100	14.69	55	23.07	61
G noise	23.03	14.59	90	14.54	89	14.49	95	22.09	99	14.52	57	23.45	66
Histogram equal.	19.36	13.08	86	14.16	89	12.00	86	18.79	98	16.94	62	17.10	55
JPEG (quality 0)	24.88	14.96	93	13.73	84	10.51	87	18.42	98	14.30	37	23.64	79
JPEG (quality 5)	28.23	16.89	95	15.06	90	12.81	93	16.75	97	14.86	48	20.65	53
LSRD[3]	20.16	12.66	88	11.92	72	10.87	86	14.19	95	13.81	55	21.76	70
Median filter[2]	37.20	20.57	99	20.95	96	21.47	99	21.01	99	15.27	53	23.27	61
Motion filter[2]	22.27	12.85	90	12.54	78	13.73	89	14.01	94	11.58	53	17.62	63
Print-copy-scan	11.63	10.98	72	10.64	71	10.00	72	10.07	78	13.20	61	20.72	71
Print-scan	12.52	11.36	74	10.83	72	10.08	73	10.37	87	14.10	63	22.17	69
MSB (30 dB)	30.00	10.82	75	10.28	77	8.15	76	13.91	94	15.13	53	23.14	62
MSB (35 dB)	35.00	13.36	86	12.57	85	11.65	87	18.68	98	15.16	53	23.35	62
MSB (40 dB)	40.00	15.75	92	15.28	91	15.87	94	24.16	100	15.18	53	23.39	64
Rot.-crop (2°)	19.48	16.12	89	10.26	73	11.84	86	11.61	91	13.37	53	19.74	64
Rot.-scale (2°)	19.33	16.22	89	10.21	73	11.70	85	11.36	90	13.34	53	19.65	64
Rot.-scale (5°)	11.66	11.41	82	10.38	70	10.27	70	5.68	62	11.03	52	6.86	60
RCR[4] (1 in 10)[5]	34.06	23.82	99	23.42	97	22.39	99	25.40	100	15.11	53	23.43	61
Salt and pepper	18.55	20.56	97	20.43	98	30.60	100	17.38	98	12.99	53	23.04	65
Scaling (×0.5)[5]	33.98	19.07	98	19.63	94	21.13	98	30.81	100	15.02	53	23.41	62
Scaling (×2)[5]	39.34	24.73	99	23.70	98	24.13	99	23.64	100	15.16	53	23.49	66
Self similarities	26.04	16.47	95	15.21	90	11.37	90	25.61	100	16.71	57	23.47	66
Small rand. dist.	16.27	10.98	83	11.45	72	12.92	84	6.75	71	11.55	53	16.31	69
unZign	29.08	18.18	97	18.48	94	21.69	98	∞	100	14.68	54	23.38	65
Wiener filter[2]	41.32	23.81	99	22.11	98	23.27	99	30.66	100	15.25	53	24.00	66

[1] Decomposition level $t = 4$.
[2] 3×3 window.
[3] Latest small rand. dist.
[4] Row-col-removal.
[5] Resized to original.

efficient classifier can now be used to separate the positive and negative classes based on the LRR and PSNR of all the test cases and the values of ($\mathrm{Th}_{\mathrm{LRR}}$, $\mathrm{Th}_{\mathrm{PSNR}}$) can then be estimated synergistically from this classifier.

4.5. Robustness and Uniqueness Tests. The identification thresholds ($\mathrm{Th}_{\mathrm{LRR}}$, $\mathrm{Th}_{\mathrm{PSNR}}$) defined in the previous section is useful for determination of robustness and uniqueness properties of a scheme. A scheme is not robust to a particular attack if the logo retrieved from the corresponding attacked image offers low PSNR and LRR with respect to ($\mathrm{Th}_{\mathrm{LRR}}$, $\mathrm{Th}_{\mathrm{PSNR}}$). In that case, the corresponding (PSNR, LRR) entry in C_+ causes a false negative alarm by the classifier. We need to consider all the tests cases of C_+, as defined by (12), in robustness tests. On the other hand, a scheme fails uniqueness test to a particular attack if the signature calculated from image I_d verifies the corresponding attacked version of a different image I_a. In that case, the corresponding (PSNR, LRR) entry in C_-, as defined by (12), is high with respect to ($\mathrm{Th}_{\mathrm{LRR}}$, $\mathrm{Th}_{\mathrm{PSNR}}$) and causes a false-positive alarm by the classifier. Therefore, we need to consider only the following test cases of the class C_- in uniqueness tests:

$$C'_- = \{\forall a, \forall d \neq a, \forall j : \mathrm{TC}(a, b, c, d, j)\}. \qquad (13)$$

Table 3: Attacks considered while designing the classifier.

Attacks		PSNR (dB)	
Number	Name	Lena	Elaine
0	Affine[1]	20.66	18.69
1	Blurring[2]	36.89	42.74
2	Cropping[3]	10.67	9.64
3	Histogram equal.	19.36	18.23
4	JPEG (quality 5)	28.23	28.02
5	Rot.-crop 2°	19.48	17.68
6	Rot.-scale 2°	19.33	17.58
7	Rot.-scale 5°	11.66	11.53
8	Small rand. dist.	16.27	18.55
9	MSB attack	35.00	35.00

[1] Resized to original after XY-shearing.
[2] Gaussian filter.
[3] Cropping excluding ROI.

5. Performance Study

We implemented the proposed MSB-based scheme and existing TROI-based [12] and VQ-based [13] schemes with MATLAB 7 and tested their robustness using all the watermarking benchmark images in [23] with different logos against many attacks including those in stirMark 4.0 [24]. However, as we decided almost the same performance for each pair of a benchmark image and a logo, only results obtained using “Lena” and “Elaine” images signed by Monash and NUS logos, respectively (shown in Figure 3), are presented. Where necessary, the attacked images were resized to original. In fact, a corner matching technique can be used to undo the geometric transformations before verifying the copyright information [26].

We used the following two metrics to evaluate the performance: (i) PSNR determines the visual quality of the attacked media or retrieved logo with respect to its original copy; (ii) LRR determines the percentage of bits that are correctly retrieved from the given image using the given signature.

In Section 5.1, we present different types of attacks we considered in our experiments. Section 5.2 presents the detail classifier setup by different signature-based schemes. Section 5.3 presents the experimental results and discussions. Finally, Section 5.4 provides detail discussions on the overall performance of different signature-based schemes.

5.1. Attacks. All the attacks we tested to prove the efficacy of the proposed schemes are in Table 2. Below, we represent some attacks that require detail discussions. If not mentioned, the attack was done using MATLAB 7.

5.1.1. BPM Attack. In *blind pattern matching* (BPM) attack, we divided Lena image into 4 × 4 nonoverlapping blocks. For each block, the most similar 4 × 4 block was found out from Elaine image at 25 dB. The block with PSNR greater than or equal to 25 dB was considered as a similar one. Total 15736 blocks were replaced when the attacked image PSNR became 22.94 dB. In the same way, when we attacked Elaine image using Lena image, we replaced total 16371 blocks and attacked image PSNR was 21.99 dB.

5.1.2. Print-Copy-Scan. We printed each image using a 1200 dpi laser printer. The printed image was then photocopied and scanned using a 300 dpi and 8-bit gray-scale scanner. Finally, it was resized to 512 × 512. The PSNR of Lena image after print-copy-scan attack was 11.63 dB and that of Elaine image was 19.56 dB.

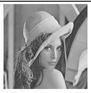
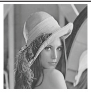
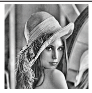
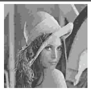
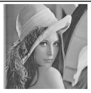
5.1.3. MSB Attack. We attacked each image by flipping its MSB-plane. Maximum MSBs were changed at a particular PSNR. First, we found absolute difference of each pixel to flip its MSB. Second, we sorted the absolute differences in the ascending order. Finally, we flipped the MSB of the pixel with lowest absolute difference first. We continued flipping until the PSNR is decreased beyond a particular value. Since this attack changes the maximum number of MSBs for a given target PSNR, the proposed MSB-based scheme should suffer the most. However, we observed that most images cannot be degraded to less than 20 dB even if all of its MSBs were flipped. After the MSB attack at 30 dB the MSB similarity rate for Lena image was 73% and for Elaine image was 70%.

5.1.4. unZign Attack. The image was divided into 8 × 8 blocks. A pixel was selected randomly from each block and was either deleted or repeated randomly. All blocks were then put back in their original positions. The PSNR of Lena image after unZign attack was 29.08 dB and that of Elaine image was 29.79 dB.

5.1.5. Self-Similarities. This attack was done by stirMark 4.0 in RGB space of the image. The image was then converted to its gray-scale equivalent. The PSNR of Lena image after this attack was 26.04 dB and that of Elaine image was 25.48 dB.

5.2. Classifiers. In order to design classifiers for the different approaches, that is, UROI, TBLK, DCTMSB, and t-DWT, of the proposed MSB-based and existing TROI-based [12] and VQ-based [13] schemes, we used 10 different types of attacked images as shown in Table 3. We assigned numbers to the attacks for later references. The image Lena was signed using Monash logo and the image Elaine was signed with NUS logo. Then, different attacked images of Lena and Elaine were sent after signing with different logos with different or same A_I for verification. For UROI approach and TROI-based scheme, A_I indicates the same or different ROIs; while for t-DWT approach and VQ-based scheme, A_I indicates the same or different decomposition levels; and for TBLK approach, A_I indicates same or different set of textured blocks. We had total 8 different types of data points with two pairs of images and logos (Lena-Monash and Elaine-NUS). Therefore, maximum 160 logo retrieval instances (20 in C_+ and 140 in C_-) were used while designing each classifier. However, in the case of DCTMSB approach, there were total 80 instances (20 in C_+ and 60 in C_-); since for the same type and size (8-bit, 64 × 64) of logo, the image was

Table 4: Attacked images along with their corresponding retrieved logos using Lena image and Monash logo by different approaches of the proposed MSB-based scheme and existing TROI-based [12] and VQ-based [13] schemes.

	Affine[2]	BPM[3]	Blurring[4]	Crop.[5]	Hist. Eq.	JPEG (5)	PCS[6]	Rot.-crop 2°	unZign
Attacks[1] →									
Schemes[7] ↓	20.66	22.94	36.89	10.67	19.36	28.23	11.63	19.48	29.08
UROI	 19.30, 96	 14.36, 91	 20.58, 99	 ∞,100	 13.08, 86	 16.89, 95	 10.98, 72	 16.12, 89	 18.18, 97
TBLK	 14.44, 88	 12.97, 85	 21.43, 96	 13.16, 94	 14.16, 89	 15.06, 90	 10.64, 71	 10.26, 73	 18.48, 94
DCTMSB	 14.09, 94	 11.19, 89	 22.04, 99	 13.75, 87	 12.00, 86	 12.81, 93	 10.00, 72	 11.84, 86	 21.69, 98
t-DWT ($t = 4$)	 10.52, 88	 15.18, 96	 30.20, 100	 6.69, 71	 18.79, 98	 16.75, 97	 10.07, 78	 11.61, 91	 ∞, 100
TROI [12]	 14.73, 54	 13.85, 56	 14.97, 53	 15.19, 53	 16.94, 62	 14.86, 48	 13.20, 61	 13.37, 53	 14.68, 54
VQ [13]	 14.79, 58	 23.67, 73	 23.12, 60	 15.57, 83	 17.10, 55	 20.65, 53	 20.72, 71	 19.74, 64	 23.38, 65

[1] Attacked images with PSNR (dB).

[2] Resized to original after XY-shearing.

[3] PSNR of similar blocks (4×4) ≥25 dB.

[4] Gaussian filter.

[5] Cropping excluding ROI.

[6] Print-copy-scan.

[7] Retrieved logos with PSNR (dB) and LRR (%).

divided into blocks of the same size (4×2) before taking DCT, assuming the image size (512×512) also remained the same. On the other hand, for VQ-based scheme, there were total 120 instances (20 in C_+ and 100 in C_-); since with different decomposition levels t, logo retrieval operation was not possible from a smaller codebook (due to larger t) using the indices set containing higher indices values, while it was possible from a bigger codebook (due to smaller t) using the indices set containing lower indices values.

We used *support vector machines* (SVMs) with linear kernel [27] and K-means clustering [28] separately for classification. Results by both SVM classification and K-means clustering are useful for the determination of the robustness and the uniqueness properties of the proposed and existing schemes. SVM results, especially, enabled to find out the values for identification thresholds (Th_{LRR}, Th_{PSNR}), defined in Section 4.3. The more the accuracy of the classification and the distance d between the support vectors of the SVM for a scheme, the more the scheme is robust (i.e., the two classes are well separated).

In the robustness test, the distance from a data point in C_+ (corresponding to an attack) to the SVM decision hyperplane is used to decide different levels of robustness (high, medium, low, and no). For example, if the data point is correctly classified and resides outside the nearest support vector (i.e., far away from the decision plane), then the robustness against the corresponding attack is high. If the data point is correctly classified but stays in the space between the nearest support vector and the decision plane and then the robustness against the corresponding attack is medium (when close to the support vector) or low (when close to the decision plane). If the data point is on the other side of the hyper plane (misclassified), then the copyright scheme is not robust to the corresponding attack. In the uniqueness test, if a data point in C'_- (corresponding to an attack) is incorrectly classified then the scheme does not possess the uniqueness property under this attack.

5.3. Experimental Results. We will present the experimental results in two parts. In Section 5.3.1, we present the robustness of the proposed and existing schemes in terms of PSNR

Table 5: Experimental results (PSNR in dB and LRR in %) by different approaches of the proposed MSB-based scheme and existing TROI-based [12] and VQ-based [13] schemes against various attacks using Elaine image and NUS logo.

		Proposed MSB-based scheme								Existing schemes			
Attacks	PSNR	UROI		TBLK		DCTMSB		t-DWT[1]		TROI [12]		VQ [13]	
		PSNR	LRR	PSNR	LRR	PSNR	LRR	PSNR	LRR	PSNR	LRR	PSNR	LRR
Affine (XY)[5]	18.69	13.86	90	17.33	88	14.48	86	17.84	92	16.40	56	21.12	61
Avg. filter[2]	34.09	19.17	98	22.90	97	24.43	98	27.01	99	17.51	56	25.32	69
BPM (25 dB)	21.99	12.79	88	15.61	84	14.57	86	17.25	93	16.62	55	23.29	55
Cropping	9.64	∞	100	41.95	99	16.55	81	12.17	70	17.47	55	7.78	48
Gauss. (G) filter[2]	42.74	23.58	99	26.51	99	27.32	99	33.09	100	17.50	55	25.35	68
G filter[2] & noise	20.05	12.84	88	15.83	85	17.15	92	25.46	99	15.59	55	25.26	68
G noise	20.09	12.57	88	15.80	85	16.92	92	25.68	99	15.65	55	25.19	70
Histogram equal.	18.23	16.97	96	19.82	95	18.37	94	21.20	97	14.72	56	22.76	65
JPEG (quality 0)	25.14	13.69	89	17.74	86	14.63	86	20.26	96	16.85	58	21.13	70
JPEG (quality 5)	28.02	16.20	94	19.53	91	17.00	91	22.27	97	17.14	56	25.02	65
LSRD[3]	14.94	10.99	75	12.28	76	12.23	75	11.84	71	12.30	53	15.57	58
Median filter[2]	24.37	13.95	91	18.07	88	14.97	87	27.34	99	16.53	56	25.27	67
Motion filter[2]	25.54	14.61	93	19.00	84	18.54	94	19.41	95	17.14	55	24.35	65
Print-copy-scan	19.56	13.49	90	16.04	88	15.64	92	15.75	90	15.99	56	20.27	50
Print-scan	22.32	15.48	94	19.71	93	20.43	95	21.39	96	16.32	57	24.62	68
MSB (30 dB)	30.00	8.52	66	11.59	65	12.81	74	20.01	96	17.10	50	24.83	68
MSB (35 dB)	35.00	9.85	78	13.96	79	15.04	85	24.26	99	17.39	51	25.25	68
MSB (40 dB)	40.00	11.51	86	15.77	87	17.81	92	30.23	100	17.46	53	25.33	66
Rot.-crop (2°)	17.68	13.84	84	16.26	85	14.36	81	14.89	86	15.13	56	20.08	65
Rot.-scale (2°)	17.58	13.79	84	16.06	85	14.26	81	14.85	86	15.10	56	19.92	66
Rot.-scale (5°)	11.53	11.73	76	11.29	76	11.10	68	11.24	65	13.29	54	13.05	62
RCR[4] (1 in 10)[5]	25.20	14.48	92	18.57	89	15.72	89	29.28	99	16.68	56	25.34	69
Salt & pepper	22.60	25.61	99	25.23	99	34.72	100	22.98	99	16.24	54	25.04	72
Scaling (×0.5)[5]	25.09	14.39	92	18.29	89	15.97	90	∞	100	16.72	57	25.36	67
Scaling (×2)[5]	25.66	14.24	92	18.63	89	15.50	89	28.58	100	16.76	57	25.31	68
Self similarities	25.48	14.63	92	18.44	89	15.33	88	29.52	100	16.82	56	25.36	68
Small rand. dist.	18.55	11.99	85	16.12	84	13.62	84	17.24	91	15.10	54	20.40	67
unZign	29.79	19.02	97	23.80	97	24.03	98	33.09	100	17.26	55	25.35	68
Wiener filter[2]	36.52	20.10	98	20.96	97	25.12	99	27.90	99	15.20	52	24.45	67

[1] Decomposition level $t = 4$.
[2] 3×3 window.
[3] Latest small random distortion.
[4] Row-col-removal.
[5] Resized to original.

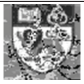
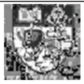
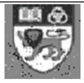
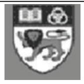
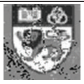
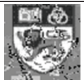
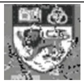
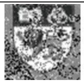
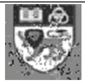
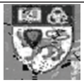
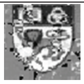
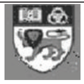
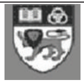
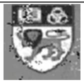
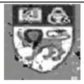
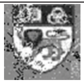
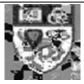
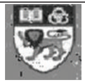
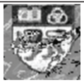
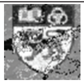
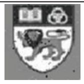
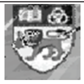
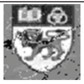
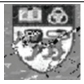
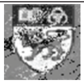
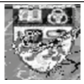
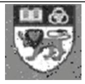
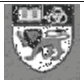
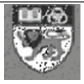
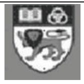
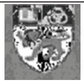
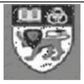
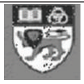
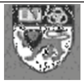
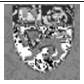
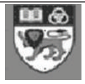
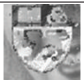
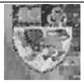
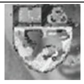
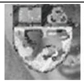
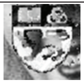
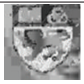
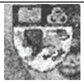
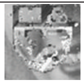
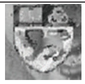
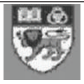
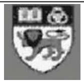
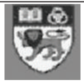
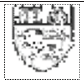
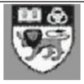
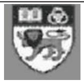
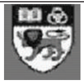
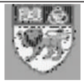
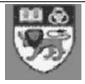
and LRR under different attacks. In Section 5.3.2, we present the classifiers from which we can evaluate overall robustness and uniqueness of the respective signature-based schemes.

5.3.1. Robustness Results. In this section, we first present and discuss robustness results of the proposed and existing schemes under different attacks. We then detail the results for two attacks—JPEG which is the most common unintentional attack and newly proposed MSB attack which would defeat our scheme the most.

Table 2 shows the logo retrieval results using Lena image and Monash logo by different approaches of the MSB-based scheme and existing TROI-based [12] and VQ-based [13] schemes. Table 4 shows the attacked images along with their corresponding retrieved logos using Lena image and Monash logo. Table 5 and Table 6 present the same, respectively, using Elaine image and NUS logo.

We observed that all the approaches of the proposed scheme performed almost the same except the t-DWT approach which was sensitive to geometric distortions. In contrast, both the TROI-based and VQ-based schemes were very much sensitive to geometric attacks and the former did not survive under high JPEG lossy compression (quality less than 10). In most of the cases, the PSNR and in all the cases the LRR of the retrieved logos by the proposed scheme were higher than those by the TROI-based scheme. In the remaining few cases, the PSNR of the retrieved logos by the proposed scheme were lower. In most of the cases,

Table 6: Attacked images along with their corresponding retrieved logos using Elaine image and NUS logo by different approaches of the proposed MSB-based scheme and existing TROI-based [12] and VQ-based [13] schemes.

	Affine[2]	BPM[3]	Blurring[4]	Crop.[5]	Hist. Eq.	JPEG (5)	PCS[6]	Rot.-crop 2°	unZign
Attacks[1] →									
Schemes[7] ↓	18.69	21.99	42.74	9.64	18.23	28.02	19.56	17.68	29.79
UROI									
	13.86, 90	12.79, 88	23.58, 99	∞, 100	16.97, 96	16.20, 94	13.49, 90	13.84, 84	19.02, 97
TBLK									
	17.33, 88	15.61, 84	26.51, 99	41.95, 99	19.82, 95	19.53, 91	16.04, 88	16.26, 85	23.80, 97
DCTMSB									
	14.48, 86	14.57, 86	27.32, 99	16.55, 81	18.37, 94	17.00, 91	15.64, 92	14.36, 81	24.03, 98
t-DWT ($t = 4$)									
	17.84, 92	17.25, 93	33.09, 100	12.17, 70	21.20, 97	22.27, 97	15.75, 90	14.89, 86	33.09, 100
TROI [12]									
	16.40, 56	16.62, 55	17.50, 55	17.47, 55	14.72, 56	17.14, 56	15.99, 56	15.13, 56	17.26, 55
VQ [13]									
	21.12, 61	23.29, 55	25.35, 68	7.78, 48	22.76, 65	25.02, 65	20.27, 50	20.08, 65	25.35, 68

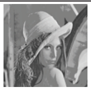
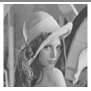
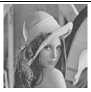
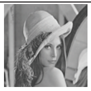
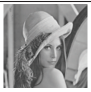
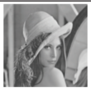
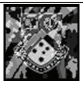
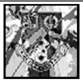
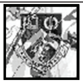
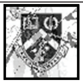
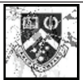
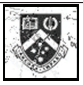
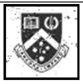
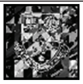
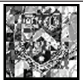
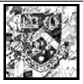
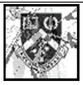
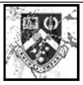
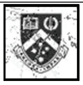
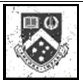
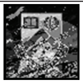
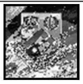
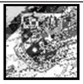
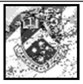
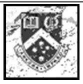
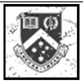
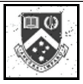
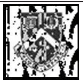
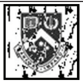
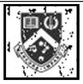
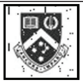
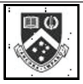
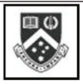
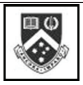
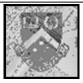
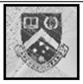
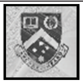
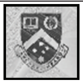
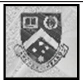
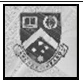
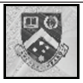
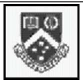
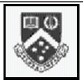
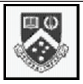
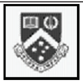
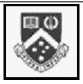
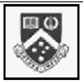
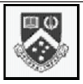
[1] Attacked images with PSNR (dB).
[2] Resized to original after XY-shearing.
[3] PSNR of similar blocks (4×4) ≥25 dB.
[4] Gaussian filter.
[5] Cropping excluding ROI.
[6] Print-copy-scan.
[7] Retrieved logos with PSNR (dB) and LRR (%).

the LRR by the MSB-based scheme was higher than the VQ-based scheme; while in many cases, the PSNR by the latter was higher due to its VQ coding. However, it is no way an indication to the superiority of the existing schemes for these kinds of attacks; because the logo quality degrades severely during the torus-mapping and VQ coding, as shown in Figures 3(e)–3(h), and as a consequence the PSNR and LRR remained almost unchanged irrespective of logos.

Table 7 presents the MSB-attacked images along with their corresponding retrieved logos using Lena image and Monash logo by the proposed MSB-based scheme and existing TROI-based [12] and VQ-based [13] schemes. Table 8 presents the same using Elaine image and NUS logo. Among the approaches of the proposed scheme, DWT-based approach showed the highest resistance against the MSB attack. The proposed scheme survived down to PSNR 30 dB of the attacked image. Lee and Chen [13] argued that the visual quality of the image is unacceptable to the human eyes if the PSNR is less than 30 dB. Moreover, we observed that the proposed scheme performed better if the PSNR of the MSB attacked image increases, while for the existing schemes the PSNR and LRR of the retrieved logos remained almost unchanged irrespective of the PSNR of the attacked images. However, since the distortion in an image is more noticeable in the mid-gray region and sensitivity changes parabolically as the gray value fluctuates on the both sides of mid-gray level [7], as a precaution to the MSB attack, we suggest excluding mid-gray pixels during signature calculation.

Figure 4(a) plots the LRR and Figure 4(b) plots the PSNR of the retrieved logos using Lena image and Monash logo against different JPEG quality factors. Figure 5(a) and Figure 5(b) plot the same using Elaine image and NUS logo. We found that the t-DWT approach performed the best among different approaches of the MSB-based scheme and existing TROI-based and VQ-based schemes. Both the LRR and PSNR increased with the increase of JPEG quality factor for the proposed scheme, while for the existing schemes they remained almost the same. While the proposed scheme always offered higher LRR; it outperformed the existing schemes in term of the PSNR when JPEG quality factor was greater than 70. This result is consistent with the observation made in motivation.

Table 7: MSB attacked images along with their corresponding retrieved logos using Lena image and Monash logo by different approaches of the proposed MSB-based scheme and existing TROI-based [12] and VQ-based [13] schemes.

MSB Attacked[1] Images[2] → Schemes[3] ↓	 20.00, 28	 25.00, 54	 30.00, 73	 35.00, 85	 40.00, 92	 45.00, 97	 50.00, 99
UROI	 3.99, 17	 8.00, 58	 10.82, 75	 13.36, 86	 15.75, 92	 18.98, 96	 22.46, 99
TBLK	 3.84, 30	 7.59, 63	 10.28, 77	 12.57, 85	 15.28, 91	 18.33, 95	 21.93, 98
DCTMSB	 3.31, 31	 5.57, 57	 8.15, 76	 11.65, 87	 15.87, 94	 19.46, 98	 23.53, 99
t-DWT ($t = 4$)	 7.15, 73	 9.87, 86	 13.91, 94	 18.68, 98	 24.16, 100	 ∞, 100	 ∞, 100
TROI [12]	 12.36, 51	 14.92, 52	 15.13, 53	 15.16, 53	 15.18, 53	 15.19, 53	 15.19, 53
VQ [13]	 20.25, 63	 22.34, 62	 23.14, 62	 23.35, 62	 23.39, 64	 23.40, 65	 23.40, 64

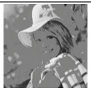
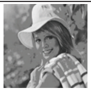
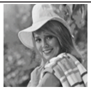
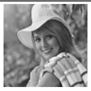
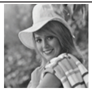
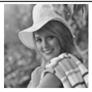
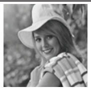
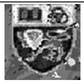
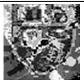
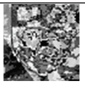
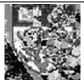
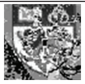
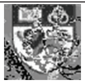
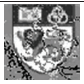
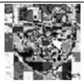
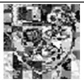
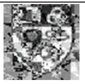
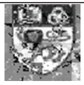
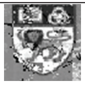
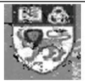
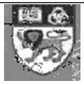
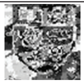
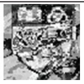
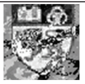
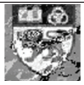
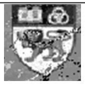
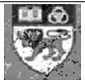
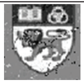
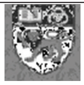
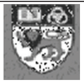
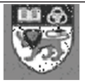
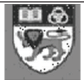
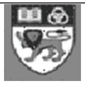
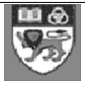
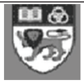
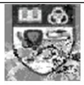
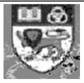
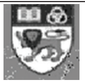
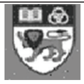
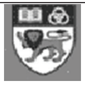
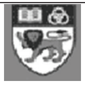
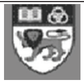
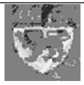
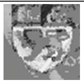
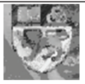
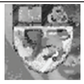
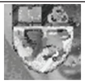
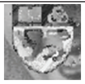
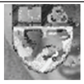
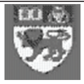
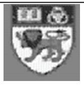
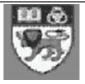
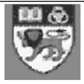
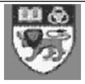
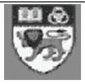
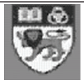
[1] Images with PSNR <30 dB are unacceptable [13].
[2] With target PSNR (dB) and MSB similarity rate (%).
[3] Retrieved logos with PSNR (dB) and LRR (%).

5.3.2. Classification Results (Robustness and Uniqueness). In this section, we present and discuss classification results of the proposed and existing schemes. We can infer the overall robustness and uniqueness of each scheme from the respective classifier.

Figures 6, 7, 8, 9, 10, and 11 present classification results using SVM with linear kernel [27] and K-means clustering [28] separating the positive and negative classes of test cases, defined in the Section 4.3, for the MSB-based scheme and existing TROI-based [12] and VQ-based [13] schemes. Though we conducted the experiments with all entries in C_{-}, for clarity we show C'_{-}, as defined in (13), instead of C_{-} in Figure 6 to Figure 11. Table 9 shows the classification results obtained by SVM and K-means. If for a scheme a data point in C_{+} corresponding to an attack is misclassified by a classifier, then the scheme is decided not to be robust under that attack. Similarly, if for a scheme a data point in C'_{-} corresponding to an attack is misclassified by a classifier, then the scheme is decided not to be unique under that attack. While the classes could be distinctively separated (no misclassification) with a large distance d between the support vectors for UROI ($d = 30.2$), TBLK ($d = 31.4$), and DCTMSB ($d = 31.4$) approaches of the proposed scheme; the SVM classifier for t-DWT approach resulted in 5% positive misclassification with a large $d = 25.0$ and the classifiers for the TROI-based ($d = 10.0$) and VQ-based ($d = 9.2$) schemes resulted in 20% and 30% positive misclassifications, respectively. We found no miss by K-means clustering for UROI, TBLK, and DCTMSB approaches, while for t-DWT approach and TROI- and VQ-based schemes, we found 35% positive, 26% negative, and 30% positive miss, respectively. Logo quality degradation due to torus-mapping and VQ coding constitute this problem for the existing schemes. Note that no misclassification and the large separation between positive and negative classes for UROI, TBLK, and DCTMSB approaches of the MSB-based scheme is so significant that simple PSNR-only (vertical) or LRR-only (horizontal) linear classifier can be used as well. Considering classification and clustering results and the distance from the SVM decision hyperplane to a corresponding entry of a particular attack, we took the decision of robustness and uniqueness tests. From Table 9, we see that UROI and DCTMSB approaches are highly robust and TBLK approach is moderately robust; while TROI-based scheme failed both robustness and uniqueness tests, and t-DWT approach and VQ-based scheme failed robustness test. We found that TBLK and t-DWT approaches are highly sensitive to geometric attacks.

5.4. Comparisons and Discussions. Table 10 presents comparisons among the different approaches of the proposed MSB-based scheme and the existing TROI-based [12] and

Table 8: MSB attacked images along with their corresponding retrieved logos using Elaine image and NUS logo by different approaches of the proposed MSB-based scheme and existing TROI-based [12] and VQ-based [13] schemes.

MSB Attacked Images[1,2] → Schemes[3] ↓	 20.00, 31	 25.00, 54	 30.00, 70	 35.00, 81	 40.00, 88	 45.00, 92	 50.00, 95
UROI	 6.41, 26	 7.04, 46	 8.52, 66	 9.85, 78	 11.51, 86	 13.21, 91	 14.93, 94
TBLK	 7.59, 23	 9.45, 44	 11.59, 65	 13.96, 79	 15.77, 87	 17.79, 91	 19.49, 94
DCTMSB	 8.04, 33	 10.41, 56	 12.81, 74	 15.04, 85	 17.81, 92	 20.00, 95	 21.51, 97
t-DWT ($t = 4$)	 13.21, 79	 16.31, 90	 20.01, 96	 24.26, 99	 30.23, 100	 37.98, 100	 ∞, 100
DCT	 15.86, 91	 20.43, 97	 26.21, 99	 34.59, 100	 44.10, 100	 69.20, 100	 ∞, 100
TROI [12]	 16.25, 45	 16.72, 49	 17.10, 50	 17.39, 51	 17.46, 53	 17.47, 53	 17.47, 54
VQ [13]	 19.20, 49	 23.28, 61	 24.83, 68	 25.25, 68	 25.33, 66	 25.34, 66	 25.34, 68

[1] Images with PSNR <30 dB are unacceptable [13].

[2] With target PSNR (dB) and MSB similarity rate (%).

[3] Retrieved logos with PSNR (dB) and LRR (%).

Table 9: Results and decisions for different approaches of the proposed MSB-based scheme and existing TROI-based [12] and VQ-based [13] schemes by the *support vector machines* (SVM) [27] and K-means clustering algorithm[28].

Schemes	Size of training set		Number of miss (%) by SVM		Number of miss (%) by K-means		Distance[1]	To individual attacks (robustness: h = high, m = moderate, l = low, and n = no robustness; and f = uniqueness fail)[2,3]										
	C_+	C_-	C_+	C_-	C_+	C_-	d	0	1	2	3	4	5	6	7	8	9	Over[4]
UROI	20	140	0 (0)	0 (0)	0 (0)	0 (0)	30.2	h	h	h	h	h	h	h	m	m	h	h
TBLK	20	140	0 (0)	0 (0)	0 (0)	0 (0)	31.5	m	h	h	h	h	l	l	l	l	m	m
DCTMSB	20	60	0 (0)	0 (0)	0 (0)	0 (0)	31.3	m	h	h	h	h	m	m	l	m	h	h
t-DWT	20	140	1 (5)	0 (0)	7 (35)	0 (0)	25.1	n	h	n	m	h	n	n	n	n	h	n
TROI [12]	20	140	6 (30)	0 (0)	0 (0)	36 (26)	5.1	n, f	l, f	n, f	m, f	l, f	n, f	n, f	n, f	n, f	m, f	n, f
VQ [13]	20	100	11 (55)	0 (0)	6 (30)	0 (0)	9.2	n	m	n	l	h	n	n	n	n	m	n

[1] Distance between support vectors.

[2] Robustness: correctly classified by both SVM and K-means with h = high PSNR and LRR, m = moderate PSNR and LRR, and l = low PSNR and LRR; no robustness: n = any false negative by SVM or K-means; and uniqueness fail: f = any false positive by SVM or K-means.

[3] Attack numbers 0-9 are referred using Table 3; and

[4] Overall decision.

Table 10: Comparisons of different approaches of the proposed scheme and existing schemes [12, 13].

Issues	Existing		Approaches of the proposed MSB-based scheme			
	TROI [12]	VQ [13]	UROI	TBLK	DCTMSB	*t*-DWT
Transparency	yes	yes	yes	yes	yes	yes
Robustness	no	no	high	moderate	high	no
Uniqueness	no	yes	yes	yes	yes	yes
Unambiguous	no	no	yes	yes	yes	no
Security	yes	yes	yes	yes	yes	yes
Blindness	semi-blind	blind	semi-blind	semi-blind	semi-blind	semi-blind
Multiple logo	yes	yes	yes	yes	yes	yes
Publicly verifiable	no	yes	no	no	no	no
StirMark resistance	no	no	moderate	low	moderate	no
MSB attack resistance	moderate	high	moderate	moderate	moderate	high
Scalability[1]	no	no	yes	yes	yes	yes
Signature addition[2]	no	yes	no	no	no	no
JPEG quality < 10	low	high	high	high	high	high
Operation domain	spatial	DWT	spatial	spatial	DCT	DWT
Time complexity	high	high	constant	low	low	low
Algorithm simplicity	no	no	yes	yes	yes	yes
Region-of-interest used	yes	no	yes	no	no	no

[1] Signature calculation using different types of image and logo.
[2] With image header.

VQ-based [13] schemes. The MSB-based scheme possesses *transparency* because it does not embed any information to the published image. UROI, TBLK, and DCTMSB approaches are robust, while *t*-DWT approach failed. In contrast, due to very low PSNR and LRR both TROI-based and VQ-based schemes are not robust and TROI-based scheme failed uniqueness test. The security of the MSB-based scheme is the same as the security of the digital signature and the digital timestamp. The classification and clustering results showed that UROI, TBLK, and DCTMSB approaches are *unambiguous* due to correctly classification by SVM with a large d between the support vectors and no miss by K-means, while *t*-DWT approach is ambiguous due to positive misclassification by both SVM and TROI. In contrast, the existing schemes are ambiguous because of high positive misclassifications. In our experiments, we also used the polynomial kernel for TROI-based and VQ-based schemes and found high misclassifications. The MSB-based scheme is not *blind* as the TTP finds whether images are disputable by comparing signatures calculated from them before taking the decision based on the timestamps. The TROI-based scheme is also not *blind* too; because as the published image does not contain any information, the original image must be used to find out the corresponding signature from the owner's database. On the other hand, the VQ-based scheme is *blind* as it adds the signature with the image header before publishing. However, this signature addition not only increases the file size but also creates severe problem of losing copyright if an attacker removes the signature from the image header. The MSB-based scheme can handle multiple logos (*multiple watermarking*) like the existing schemes. An image may be signed using the same or different types of logos by the same owner.

The scheme by Lee and Chen [13] is publicly verifiable as it adds the signature with the image header. On the other hand, the ownership dispute is handled through the TTP by the MSB-based scheme. In TROI-based scheme, the owner keeps the security parameters secret himself. The existing schemes and *t*-DWT approach is not much robust as they offer low PSNR and LRR against stirMark attacks. However, *t*-DWT approach and VQ-based schemes showed high robustness to MSB attack, while UROI, TBLK, and DCTMSB approaches and TROI-based scheme showed moderate robustness. Any type and size of logos can be signed with an 8-bit gray-scale image by the MSB-based scheme, while the TROI-based and VQ-based schemes can sign only 8-bit gray-scale logos. The existing schemes are highly time consuming due to use of torus mapping and VQ encoding. In contrast, the MSB-based scheme is simple due to use of the MSB-plane; especially, the UROI approach is the simplest as it does not involve any transform domain operation. The proposed scheme also presents a comprehensive TTP management policy in order to secure the e-commerce.

6. Conclusions

This paper has proposed an MSB-based image copyright protection scheme, which relies on a TTP to offer the following advantages over the existing schemes: (i) any type and size of images and logos can be used; (ii) extremely low computational complexity, due to use of exclusive-OR operations for signature calculation, enables real time applications; (iii) robust to almost all kinds of attacks; (iv) the comprehensive TTP management policy ensures secure e-commerce.

The existing signature-based schemes that can sign images with multibit logos are not robust against geometric attacks and neither a linear nor a polynomial kernel of the SVM can classify them correctly. Among the approaches of the proposed MSB-based scheme, *t*-DWT approach is the best against the newly proposed MSB attack and JPEG. Nevertheless, this approach fails to be correctly classified due to its weakness against geometric attacks. On the other hand, classifiers designed by the UROI, TBLK, and DCTMSB approaches are excellent in the sense that they offer no misclassification and simple PSNR-only or LRR-only classifier can be used.

References

[1] T. H. Chen, G. Horng, and W. B. Lee, "A publicly verifiable copyright-proving scheme resistant to malicious attacks," *IEEE Transactions on Industrial Electronics*, vol. 52, no. 1, pp. 327–334, 2005.

[2] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, Englewood Cliffs, NJ, USA, 2nd edition, 1999.

[3] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[4] M. Kutter, F. Jordan, and F. Bossen, "Digital watermarking of color images using amplitude modulation," *Journal of Electronic Imaging*, vol. 7, no. 2, pp. 326–332, 1998.

[5] R. K. Sharma and S. Decker, "Practical challenges for digital watermarking applications," in *Proceedings of the IEEE 4th Workshop on Multimedia Signal Processing*, pp. 237–242, October 2001.

[6] I. J. Cox, M. L. Miller, and A. L. Mckellips, "Watermarking as communications with side information," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1127–1141, 1999.

[7] M. Awrangjeb and M. S. Kankanhalli, "Reversible watermarking using a perceptual model," *Journal of Electronic Imaging*, vol. 14, no. 1, Article ID 013014, pp. 1–8, 2005.

[8] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 573–586, 1998.

[9] K. Ratakonda, R. Dugad, and N. Ahuja, "Digital image watermarking: issues in resolving rightful ownership," in *Proceedings of the International Conference on Image Processing (ICIP '98)*, vol. 2, pp. 414–418, October 1998.

[10] C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 525–539, 1998.

[11] M. Awrangjeb and G. Lu, "A robust content-based watermarking technique," in *Proceedings of the IEEE 10th Workshop on Multimedia Signal Processing (MMSP '08)*, pp. 713–718, Cairns, Australia, October 2008.

[12] C. C. Chang, K. F. Hwang, and M. S. Hwang, "Robust authentication scheme for protecting copyrights of images and graphics," *IEE Proceedings: Vision, Image and Signal Processing*, vol. 149, no. 1, pp. 43–50, 2002.

[13] W. B. Lee and T. H. Chen, "A public verifiable copy protection technique for still images," *Journal of Systems and Software*, vol. 62, no. 3, pp. 195–204, 2002.

[14] C. C. Chang, J. Y. Hsiao, and C. L. Chiang, "An image copyright protection scheme based on torus automorphism," in *Proceedings of the 1st International Symposium on Cyber Worlds*, pp. 217–224, November 2002.

[15] C. C. Chang and J. C. Chuang, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy," *Pattern Recognition Letters*, vol. 23, no. 8, pp. 931–941, 2002.

[16] H. Quan and S. Guangchuan, "A semi-blind robust watermarking for digital images," in *Proceedings of the IEEE International Conference on Accoustics, Speech, and Signal Processing*, vol. 2, pp. 541–544, April 2003.

[17] C. Y. Lin and S. F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 11, no. 2, pp. 153–168, 2001.

[18] C. S. Lu and H. Y. M. Liao, "Structural digital signature for image authentication: an incidental distortion resistant scheme," *IEEE Transactions on Multimedia*, vol. 5, no. 2, pp. 161–173, 2003.

[19] S. Katzenbeisser, "On the design of copyright protection protocols for multimedia distribution using symmetric and public-key watermarking," in *Proceedings of the 12th International Workshop on Database and Expert Systems Applications*, pp. 815–819, 2001.

[20] B. Macq, J. Dittmann, and E. J. Delp, "Benchmarking of image watermarking algorithms for digital rights management," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 971–983, 2004.

[21] M. Awrangjeb and M. Murshed, "Robust signature-based geometric invariant copyright protection," in *Proceedings of the IEEE International Conference on Image Processing (ICIP '06)*, pp. 1961–1964, Atlanta, Ga, USA, October 2006.

[22] Free Foto.com, 2005, http://www.freefoto.com.

[23] "Photo database," 2005, http://www.petitcolas.net/fabien/watermarking/image_database/.

[24] F. A. P. Petitcolas, "Watermarking schemes evaluation," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 58–64, 2000.

[25] M. Awrangjeb, G. Lu, and M. Murshed, "Global geometric distortion correction in images," in *Proceedings of the IEEE 8th Workshop on Multimedia Signal Processing (MMSP '06)*, pp. 435–440, Victoria, Canada, October 2006.

[26] M. Awrangjeb and G. Lu, "A robust corner matching technique," in *Proceedings of the IEEE International Conference onMultimedia and Expo (ICME '07)*, pp. 1483–1486, Beijing, China, July 2007.

[27] N. Cristianini and J. S. Taylor, *An Introduction to Support Vector Machines and other Kernel-Based Learning Methods*, Cambridge University Press, New York, NY, USA, 1st edition, 2000.

[28] G. A. F. Seber, *Multivariate Observations*, Wiley, New York, NY, USA, 1984.

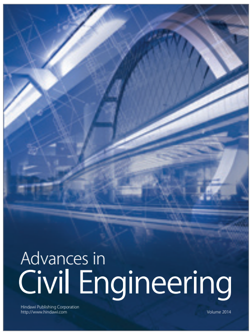
Journal of
Engineering

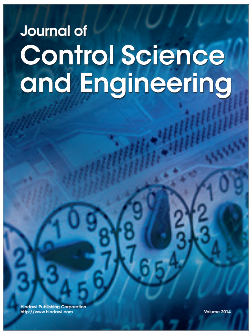
The Scientific
World Journal

International Journal of
Rotating
Machinery

Journal of
Sensors

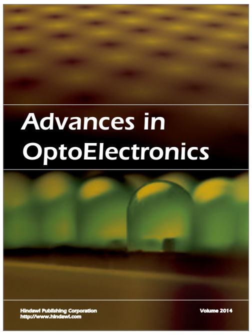
International Journal of
Distributed
Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

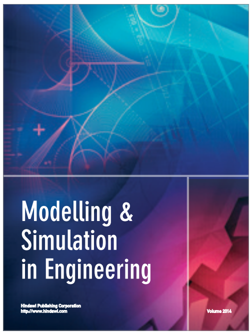
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

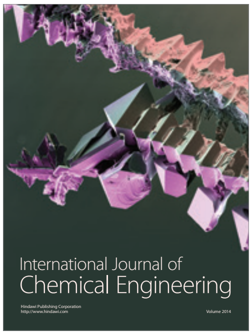

Advances in
OptoElectronics

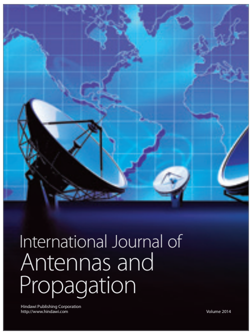
VLSI Design

International Journal of
Navigation and
Observation

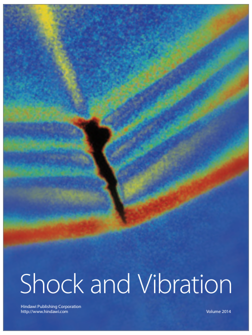

Modelling &
Simulation
in Engineering

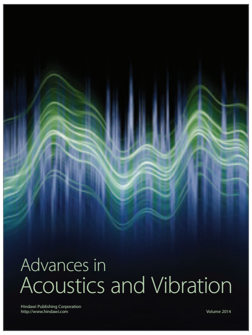
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration