J. Vis. Commun. Image R. 23 (2012) 454–466

Contents lists available at SciVerse ScienceDirect

J. Vis. Commun. Image R.

journal homepage: www.elsevier.com/locate/jvci

Novel wavelet-based QIM data hiding technique for tamper detection and correction of digital images

Amit Phadikar [a], Santi P. Maity [b], Mrinal Mandal [c,*]

[a] Department of Information Technology, MCKV Institute of Engineering, Liluah, Howrah 711 204, India
[b] Department of Information Technology, Bengal Engineering and Science University, Shibpur, Howrah 711 103, India
[c] Department of Electrical and Computer Engineering, University of Alberta, Edmonton, Canada T6G 2V4

ARTICLE INFO

Article history:
Received 12 July 2010
Accepted 10 January 2012
Available online 20 January 2012

Keywords:
Semi-fragile watermarking
Data hiding
Tamper detection
Tamper correction
Quantization index modulation
Wavelets
Integer wavelets
Image half-toning

ABSTRACT

This paper proposes a tamper detection and correction technique using semi-fragile data hiding that aims to achieve high perceptual quality of images at the user-end even after malicious modifications. A binary signature and an image digest are embedded by modulating integer wavelet coefficients using dither modulation based quantization index modulation. Half-toning technique is used to obtain image digest from the low-resolution version of the host image itself. Decoder extracts the binary signature from the watermarked image for tamper detection, while the extracted image digest is used to correct the tamper region. Unlike previously proposed techniques, this novel approach distinguishes malicious changes from various common image processing operations more efficiently and also correct tapered regions effectively. Experimental results show that the proposed technique provides a superior performance in terms of probability of miss and false alarm as well as in tamper correction, compared to several existing semi-fragile watermarking techniques.

1. Introduction

One of the major driving forces behind the emergence of the World Wide Web (WWW) is the phenomenal growth in digital techniques that allow large distribution of multimedia signals in digital form. Digital media (such as image and video) transmitted through computer networks has low level of security due to open system nature of the Internet. On the other hand, for storage and data transmission over distant places, the Internet has been found to be the fastest and cost effective way. Unfortunately, such data transmission facilities become delicate whenever security, authenticity and integrity of digital data are concerned, typically for commercial applications or protection of proprietary data. Moreover, digital content can be easily edited or modified using various image processing software and tools.

To facilitate authentication and content-integrity verification of multimedia signals, semi-fragile data hiding and digital signature have become popular over the last few years. Both techniques are used in the field of cyber frauds, court evidence, identifying forgery and even in the preservation and transmission of cultural heritages [1–6]. A digital signature is a set of features extracted from an image and are stored in a file. Later it would be compared with the extracted digital signature of an image under inspection to determine its authentication. A very important characteristic of a digital signature is that it should sufficiently represent the content of the host image. The major drawbacks of digital signature based authentication techniques [7] are: (1) inability to recover the altered regions and (2) the extracted digital signature must be transmitted together with the image file resulting in an increase of the total amount of transmitted data [7]. Data hiding, on the other hand, is an authentication/protection technique that embeds invisible information into a host data without affecting transmission rate or requiring extra channel bandwidth. For image content authentication, the watermark sequence can be extracted from the image and is then used for both verification and recovery of altered regions. The critical difference between data hiding and a digital signature is that some extra information is embedded in the former. Hence the amount of information to be embedded is limited to ensure data imperceptibility. Both techniques are expected to be sensitive to any malicious (intentional) modification applied to the image, while for an incidental (unintentional) modification, both techniques should be able to tolerate them. The so-called unintentional or common alterations typically arise from various diverse facts such as bit errors during transmission and storage, or common signal processing operations such as filtering, contrast enhancement and compression. Intentional or malicious alterations, on the other hand, may occur due to an explicit forgery attempt by a pirate with the intention of changing the contents of a

* Corresponding author. Fax: +1 780 492 1811.
E-mail addresses: amitphadikar@rediffmail.com (A. Phadikar), santipmaity@it.becs.ac.in (S.P. Maity), mmandal@ualberta.ca (M. Mandal).

1047-3203/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
doi:10.1016/j.jvcir.2012.01.005

document. In these techniques, one desires to achieve a low probability of miss (P_M) when there is a forgery attack, and at the same time, a low probability of false alarm (P_F) when one deals with allowed signal processing operations. Note that P_F indicates the probability of classifying a block/region as a tampered one when there is no-malicious operation and the P_M is the probability of classifying the same as a non-tampered one when there is a malicious operation.

Quantization index modulation (QIM) has recently become a popular technique for data hiding based on the framework of communications with side information [8]. QIM based techniques embed the information by performing quantization of the original sample values. Typical QIM is done by modulating a signal with the embedded information. Quantization is then performed with the associated quantizer. Chen et al. [9] propose a watermarking technique using dither modulation (DM), which is a special case of QIM. The QIM provides considerable performance advantages over spread-spectrum (SS) and low-bit(s) modulation in terms of the achievable performance trade-offs among distortion, rate and robustness of the embedding [10]. Images and videos are normally stored in their compressed form and quantization is the heart of any lossy compression technique. As a result, the QIM data hiding technique can easily be integrated with any compression scheme [11]. Moreover, the QIM is characterized by their ability to avoid host signal interference. In other words, the watermark detection is not influenced by the interfacing effect of the host signal.

The discrete wavelet transforms (DWT) based techniques have been shown to be efficient for tamper detection and correction. The DWT has several useful properties. First, it has multiresolution capability. Secondly, it has better space frequency localization over other transforms such as the discrete cosine transform (DCT). Thirdly, the wavelet transform decomposes an image into three spatial directions i.e., horizontal, vertical and diagonal, which reflect the anisotropic properties of human visual system (HVS) more precisely. Finally, blocking artifacts are not observed in DWT based image representations. These properties are helpful in designing a watermarking technique that is more robust against transmission and decoding errors.

This paper proposes a novel semi-fragile QIM data hiding technique for tamper detection and correction in wavelet domain [12]. The Integer wavelet transform is used in the proposed technique to achieve low computational load, low loss in image information due to DM-QIM watermarking [13], and better watermark decoding reliability.

The rest of the paper is organized as follows. Section 2 presents a review of the related works, limitations and scope of the present work. Section 3 describes the proposed data hiding technique. Section 4 presents performance evaluation of the proposed technique. Conclusions are drawn in Section 5 along with scope of future works.

2. Review of related works, limitations and scope of the present work

Data hiding was originally developed for copyright protection, ownership verification and access control of digital media [14]. Recently it has been used for some non-conventional applications, such as blind assessment of quality of services (QoS) for multimedia signals transmitted through radio mobile channel and checking of trustworthiness for digital data due to commercial and/or security reasons [15,16]. In the following subsection, we present a brief review of few selected data hiding based tamper detection and correction techniques as related works. We also discuss merits and limitations of the existing works, and scope of the present work in the subsequent subsection.

2.1. Review of related works

Wu et al. [17] proposed a lifting based semi-fragile watermarking technique for tamper detection that can tolerate lossy JPEG compression to a quality as low as 40%, and locates the tampered area accurately. Similar type of work has been proposed in [18] where adaptive quantization is used for better image authentication and tamper detection. Chamlawi et al. [19] proposed a lifting based semi-fragile watermarking technique where both tamper detection and recovery are done. The technique treats the lossy JPEG compression as a malicious alteration up to the quality factor above 70. Similar types of tamper detection and recovery mechanisms have been proposed in [20–24], although these techniques do not discuss about their performance on common image and signal processing operations. Qin et al. [25] proposed a tamper detection mechanism for remote sensing images where the edge information found by dyadic wavelet decomposition is embedded in the cover image using wavelet packet to locate the tampered area. Yung et al. [26] proposed a semi-fragile watermarking technique that allows lossy JPEG compression on the watermarked image to a pre-defined lowest quality factor and rejects crop and replacement process. Hu et al. [27] proposed a semi-fragile watermarking technique for image authentication that extracts image features from the low frequency domain to generate two watermarks: one for classifying the intentional content modification and the other one for indicating the modified location. Lu et al. [28] presented a novel multipurpose digital image watermarking method that can be applied for image authentication and copyright protection. In this algorithm, the robust watermark is embedded in the first stage using vector quantization. The semi-fragile watermark is then embedded in the second stage using a novel index constrained method. The extraction of watermark is based on the product codebook, and hence this process is very slow if one uses the full-search encoding algorithm. Moreover, the quality of the watermarked image is not very high as the scheme uses vector quantization (VQ) techniques.

Li [29] proposed a transform-domain fragile watermarking scheme for authentication and content integrity verification of JPEG images. It has been shown that high security and low computational complexity are achieved without using cryptography and hash function. Lin et al. [30] presented a novel digital watermarking method for verifying the authentication of JPEG images. The image feature is generated based on the relationships among the DCT coefficients in the low/middle frequency domain and is then embedded in the high frequency coefficients. The main drawback of the scheme is that the authenticity of the watermarked image would fail if its final JPEG compression quality is greater than the lowest authenticable JPEG quality. Similar type of work has been proposed by Lin and Chang [31], which can distinguish malicious manipulations from lossy JPEG compression regardless of the compression ratio or the number of compression iterations. Queluz [32] proposed an authentication scheme where authentication sequence is embedded via odd/even quantization of projections of column (or row) triples onto random bases. Note that the schemes reported in [28–32] are unable to recover the tampered regions. Yang and Sun [33] proposed an image adaptive semi-fragile watermarking scheme by taking full advantage of the masking characteristics of the HVS. However, the technique is unable to detect and locate the geometric attacks.

2.2. Integer wavelet transform

The integer wavelet transform has been shown to provide a superior performance compared to the traditional DWT. Simulation results obtained from experimentation over large number of images show that two levels of decomposition is good enough to

maintain acceptable rate distortion and tamper detection performance through data hiding. Therefore, we use two levels in this work. The present work employs integer Haar wavelet transform for its simplicity and ease of implementation. Other integer wavelets can also be used for better results but at the cost of larger computation [34,35]. Fig. 1(a) shows 2-level DWT of the 8-bits/pixel Lena image tile, while Fig. 1(b) shows the same corresponding to the integer wavelet decomposition. It is observed that due to lossless processing property, integer wavelet operation offers relatively better multiresolution information processing capability compared to the traditional DWT operation. This can also be visualized through close look on Fig. 1(a) and (b), respectively. Table 1 shows the average variance (over a large number of images) of selected high frequency subbands corresponding to the DWT and IWT coefficients. It is observed that the variance of the IWT coefficients is much lower than that of the DWT coefficients. This is likely to make the IWT more appropriate for reliable decoding of watermark embedding through DM-QIM which has binary modulation property.

2.3. Limitations of the existing works and scope of the present work

Majority of the semi-fragile data hiding techniques reported in the literature suffer from three shortcomings: (1) high rate of P_F when one deals with common signal processing operations; (2) low robustness to moderate JPEG compression (e.g., with quality factor 70); (3) difficulties in reconstructing regions when the alteration is malicious. To overcome these problems, a novel semi-fragile data hiding technique is proposed in this work, which serves the dual purpose of tamper detection and correction based on the IWT and QIM. The contribution and novelty of the work is briefly described as follows: (1) the use of IWT improves the processing speed of DWT and construct lossless coefficients; (2) the integration of QIM and IWT offers low value of P_M and P_F; (3) the use of DM-QIM, instead of spread-spectrum technology, is done to overcome achievable performance trade-offs among distortion, rate, and robustness of the embedding and relatively reliable binary data modulation; (4) the use of halftoning technique to generate better watermark image digest leads to effective tamper correction. Adsumilli et al. [36] proposed a SS and DWT based error concealment technique where half-toning is used to form an image digest. The image digest is used later to recover the missing part of the host image. However, use of IWT here offers better information processing/capturing capability compared to the DWT based scheme [36]. The experimental results show that the use of IWT offers low bit error rate (P_e) in binary watermark decoding compared to DWT as the former generates low variance value of the coefficients for a signal compared to the latter as shown mathematically in Eq. (1). A low P_e value leads to low value of P_M and P_F which in turn corrects the tampered regions effectively.

Note that the bit error rate (BER) P_e in binary watermark decoding is related to the standard deviation of the cover image coefficients [13,37] as follows:

$$P_e = \frac{2(M-1)}{M}\Upsilon\left(\sqrt{\frac{Nd_0^2}{4\sigma_x^2}}\right) \tag{1}$$

where d_0 is the step size (Δ) for DM, M is the number of different level of step sizes, σ_x^2 is the variance of an image block, $\Upsilon(\cdot)$ is the complimentary error function, and N is the number of host signal points over which a single watermark bit is embedded. Note that

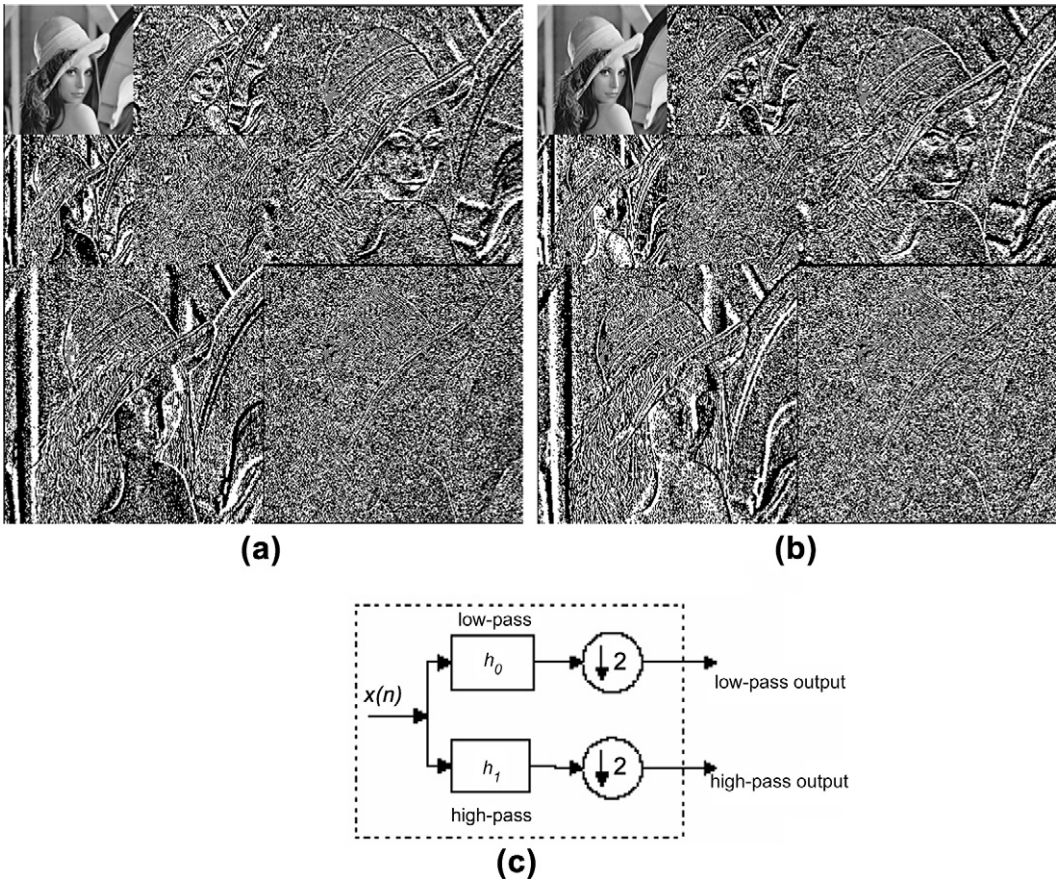

Fig. 1. (a) 2-level DWT (Haar) of the 8-bit Lena image tile; (b) 2-level integer IWT (Haar) of the 8-bit Lena image tile, (c) The DWT structure.

Table 1
The variance values for different subbands of a few selected images corresponding to integer DWT and traditional DWT decomposition.

Image	Integer DWT (Haar)				DWT (Haar)			
	HL2	LH2	HL1	LH1	HL2	LH2	HL1	LH1
Water lilies	274.51	400.16	145.12	261.16	1097.70	1599.70	145.80	261.60
Baboon	476.78	277.06	715.19	304.33	1906.00	1107.3	724.90	305.10
Lena	91.61	219.46	53.00	112.41	364.51	877.36	52.79	112.77
Cameraman	244.17	412.51	0	0	975.80	1649.60	0	0
Fishing Boat	200.90	297.71	91.03	242.15	803.00	1190.60	91.40	242.40
Opera	178.75	170.98	201.01	162.20	713.74	681.99	203.86	162.65
Pueblo bonito	588.38	155.15	555.18	118.04	2350.10	619.30	555.50	118.50
F16	264.03	243.63	166.16	158.13	1054.60	971.80	166.60	158.20
Average	243.15				664.53			

for the $\Upsilon(\cdot)$ function, a larger argument value corresponds to a smaller P_e. For DM, the value of M is set to two in this paper.

A large variety of similar functions are used to quantify the detection performance in digital data transmission through additive white Gaussian noise (AWGN) channel. It is desirable that the value of signal-to-noise power ratio (SNR) would be high to achieve low BER value. In the context of watermarking, the numerator of the argument for the function $\Upsilon(\cdot)$ contains watermark power (d_0) and the spreading factor (N); while the denominator contains the interference power from the host and/or noise signal due to attack operations. It is also seen that the objective of detection in both data transmission and data hiding is same, i.e., increase the argument value in order to decrease P_e, or in other words, to improve the robustness performance/decoding reliability. However, increase in d_0 value is limited by the imperceptibility requirement of data hiding. On the other hand, one may reduce the host power, i.e., host variance through the choice of appropriate transform for embedding space. In other words, when the value of σ_x^2 is small, the function $\Upsilon(\cdot)$ would yield low value, resulting in a low value of P_e. As shown in Table 1, the IWT coefficients have smaller variance, which would result lower value of P_e compared to DWT. Experimentally it has been observed that for the parameter values $N = 32$, $M = 2$, $d_0 = 15$, and $\sigma_x^2 = 243.15$, the value of P_e is 0.0001192 for IWT. On the other hand, for $N = 32$, $M = 2$, $d_0 = 15$, and $\sigma_x^2 = 664.53$, the value of P_e is 0.0199 for traditional DWT. The low value of P_e offers better performance in term of P_F and better extraction of image digest, which leads to better recovery of tamper region.

3. Proposed data hiding technique

In this section, we present the watermark embedding and decoding schemes for the proposed data hiding technique. The objective of the encoding scheme is to hide a binary signature and an image digest in the host image. The image digest is generated from the host image itself. On the other hand, the decoding process extracts the embedded signature and the image digest for tamper localization and recovery, respectively.

3.1. Watermark embedding

The block schematic of the proposed data embedding scheme is shown in Fig. 2(a). The IWT is first applied on the host image to decompose it into its highpass and lowpass subbands as shown in Fig. 2(a).

A binary image is chosen as a signature (watermark) in this work. The binary signature (W_{bs}) is encoded before embedding because the attacker can easily forge a watermark using the available knowledge of it. Let the original binary image signature (W_{bs}) and a 2-D random binary sequence K (which will be used as a secret key), each with size ($n \times n$), are described as follows:

$$W_{bs} = \{w_{bs}(i,j),\ 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n,\ w_{bs}(i,j) \in (0,1)\} \quad (2)$$

$$K = \{k(i,j),\ 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n, k(i,j) \in (0,1)\} \quad (3)$$

The subscript '*bs*' represents the binary signature that is used to locate the tamper region. The permuted watermark (W'_{bs}) is calculated as follows:

$$W'_{bs} = W_{bs} \oplus K \quad (4)$$

where $\oplus$ denotes the X-OR operation.

It is well known in digital watermarking that a trade-off relationship exists among imperceptibility, robustness and payload. In order to balance these characteristics properly, an image digest (a second watermark), which is a compressed version of the host image, is inserted in the host image. The image digest is generated as follows:

(1) The host image ($\boldsymbol{h}$) of size ($N \times N$) is decomposed into two levels using IWT to obtain a low-resolution image ($\boldsymbol{m}$).
(2) A halftoned image, which is used as a marker in this paper, is generated from the approximate version (LL version) of image using Floyd–Steinberg [38,39] diffusion kernel (D_{FS}) given by

$$D_{FS} = \frac{1}{16}\begin{bmatrix} 0 & 0 & 0 \\ 0 & P & 7 \\ 3 & 5 & 1 \end{bmatrix} \quad (5)$$

where P is the current pixel position. The diffusion kernel D_{FS} is typically applied on each (3×3) block of the reduced size image ($\mathbf{m}$). The resulting marker is denoted by (W_{md}) which is of size ($N/4 \times N/4$). The subscript '*md*'represents the message digest.
(3) The marker (W_{md}) is permuted to get an image digest (W'_{md}) using another secret key (K'). Ideally, the permutation of W_{md} would cause the tampered pixel of the host image to be separated as far as possible from the embedded bit of the image digest (W'_{md}). By doing so, the recovery of tampered region is made more effective. In other words, based on the extracted binary signature, the tampering is detected. Even if the image digests for a point say $P(x,y)$ is embedded far away from coordinate (x,y) at which the image is tampered, the embedded image digest for the tampered region can be extracted correctly from the image. This leads to effective recovery of the tampered region. However, if the location where the image digest for the point $P(x,y)$ stored is also corrupted, the recovery capability would be weakened. This is due to the fact that some of the bits of the extracted image digest would be wrong. Table 10 in Section 4 shows the effectiveness of this particular operation.

Both watermarks (the image digest and the binary signature) are now embedded into the host image. This is accomplished by

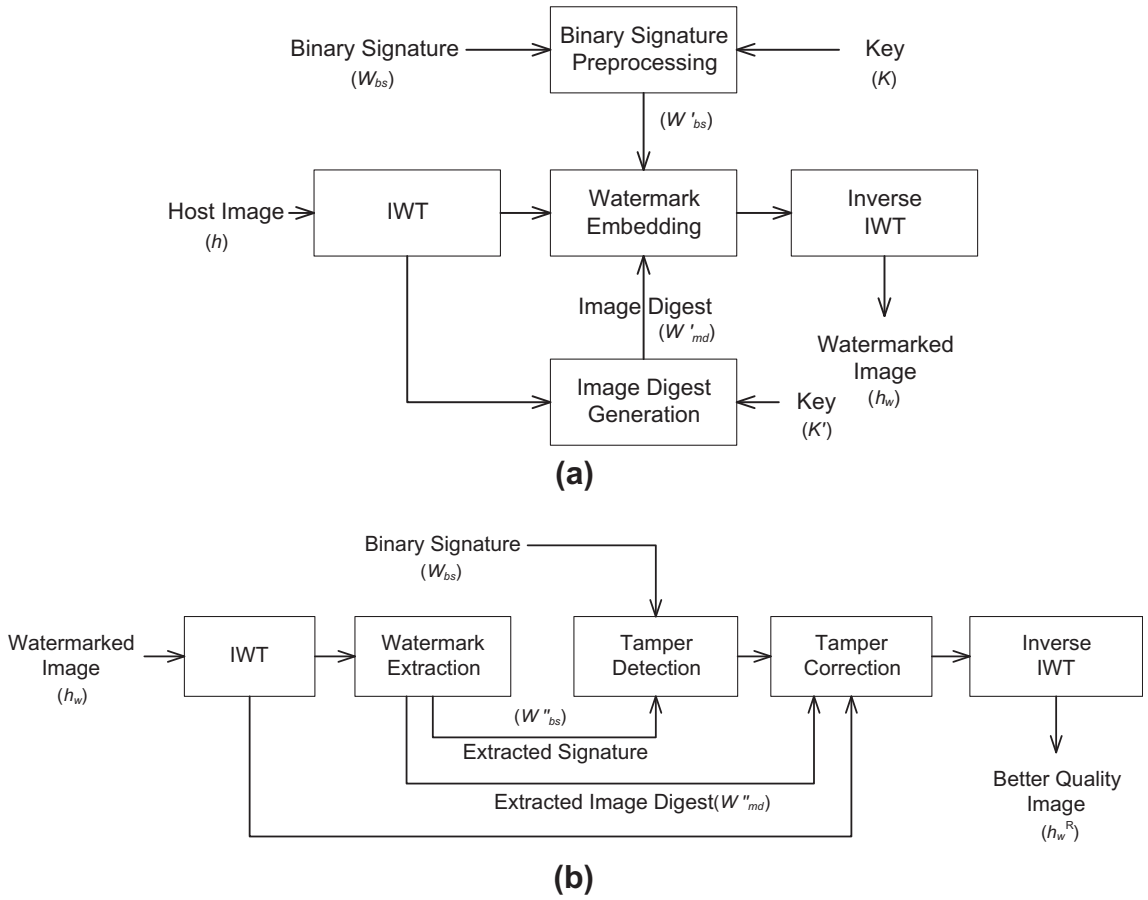

Fig. 2. Block schematic of the watermarking (a) encoding and (b) decoding process.

using two real-valued dither sequences of length L, pseudo randomly generated using a *key* with the step sizes (Δ_b). The dither sequences are generated as follows:

$$d_q(0) = \{\Re(key) \times \Delta_b\} - \Delta_b/2 \quad \text{where} \quad 0 \leqslant q \leqslant L-1 \tag{6}$$

$$d_q(1) = \begin{cases} d_q(0) + \Delta_b/2 & \text{if } d_q(0) < 0 \\ d_q(0) - \Delta_b/2 & \text{if } d_q(0) \geqslant 0 \end{cases} \tag{7}$$

where $\Re(key)$ is a random number generator. The random factor is added to increase security of the system. The distance between the corresponding elements of two dither levels ($d_q(0)$ and $d_q(1)$) is $\Delta_b/2$. The sequences $d_q(0)$ and $d_q(1)$ are used for embedding the bit 0 and bit 1, respectively. The length L depends on the number of coefficients that are selected from LH or HL subbands for embedding of each watermark bit. To make the scheme compliant to JPEG 2000 codec, the quantization step size Δ_b is calculated as follows [40]:

$$\Delta_b = 2^{R_b - \varepsilon_b}\left(1 + \frac{\mu_b}{2^{11}}\right). \tag{8}$$

where R_b is the nominal dynamic range of subband b, ε_b and μ_b denote the number of bits allocated to the exponent and the mantissa of the subband coefficients, respectively.

High frequency subbands such as low–high (LH), or high-low (HL) are chosen for data embedding. This is because the human eyes are sensitive to the low–low (LL) coefficients and the quantization step of lossy compression may discard the high-high (HH) components. Hence watermark embedding on LL subband would visually degrade the quality of the watermarked images, while faithful decoding of embedded watermark may not be possible from the HH subband after lossy compression operation. Therefore, for reasonable trade-off between imperceptibility and compression resiliency of the embedded data, the watermark information is embedded only in the HL or LH coefficients of the image. In the proposed technique, W'_{bs} is embedded in the LH2 and HL2 subbands and W'_{md} in LH1 and HL1. Note that other subbands may be used for better tamper localization and correction depending on the image characteristics. Each bit of W'_{bs} or W'_{md} is embedded by modulating a group of coefficients (G). The qth watermarked IWT coefficient S_q is calculated as follows [9]:

$$S_q = \begin{cases} Q\{X_q - d_q(0), \Delta_b\} + d_q(0) & \text{if } W(i,j) = 0 \\ Q\{X_q + d_q(1), \Delta_b\} - d_q(1) & \text{if } W(i,j) = 1 \end{cases} \tag{9}$$

where X_q is the original qth IWT coefficient, Q is a uniform quantizer (and dequantizer) with step Δ_b, odd reconstruction points represent message '1' and even reconstruction point represents message '0', and $W \in \{W'_{bs}, W'_{md}\}$. After watermark embedding, the inverse IWT is calculated and the watermarked image (h_w) is obtained.

3.2. Watermark decoding

The proposed tamper detection and correction technique through watermark decoding is blind. This means that the tamper detection and correction process does not require the host image. The block schematic for watermark decoding is shown in Fig. 2(b). First the watermarked (h_w) image (possibly distorted) is decomposed by 2D-IWT to get $h_w^{R_l}$, where the orientation $R \in \{LL, HL, LH, HH\}$ and the level $l \in \{1,2\}$. Both binary signature (W''_{bs}) and image digest (W''_{md}) are extracted from the respective subbands that are used at the time of embedding. A watermark bit $\widetilde{W}(i,j)$ is decoded by examining the group of IWT coefficients (G) using the following rule [9]:

$$\widetilde{W}(i,j) = \begin{cases} 0 & \text{if } A < B \\ 1 & \text{otherwise} \end{cases} \tag{10}$$

where the parameters A and B are calculated as follows:

$$A = \sum_{q=0}^{L-1} (|Q(Y_q - d_q(0), \Delta_b) + d_q(0) - Y_q|) \tag{11a}$$

$$B = \sum_{q=0}^{L-1} (|Q(Y_q + d_q(1), \Delta_b) - d_q(1) - Y_q|) \tag{11b}$$

where Y_q is the qth IWT coefficient (possibly distorted) of the received signal. It is important to note that the correct extraction of the watermark bits depends on the correct generation of the dither sequence governed by the appropriate 'key'. Hence, without proper knowledge of the key the attacker is unable to extract the watermark. The extracted watermark $\left(\widetilde{W}\right)$ bits are reversely permuted and are XORed with random bits to get the decoded watermark $\left(\widehat{W}\right)$. The random bits are generated using the same secret keys (K for binary signature, K' for image digest) that were used during the time of watermark permutation at encoder. The symbol $\widehat{W}$ represents the extracted binary signature or image digest, i.e., $\widehat{W} \in \{W''_{bs}, W''_{md}\}$.

To determine whether a modification is malicious or incidental, the following tamper detection rule (TDR) is used. For an image of block size ($a \times b$), the TDR is defined as follows:

$$TDR\left(W^b_{bs}, W^{b''}_{bs}\right) = \frac{1}{N_w}\left(\sum W^b_{bs} \oplus W^{b''}_{bs}\right) \tag{12}$$

where N_w is the length of the extracted watermark, $\oplus$ is the *XOR* operator, and W^b_{bs} and $W^{b''}_{bs}$ are, respectively, the embedded and the extracted watermark bits from a block of size ($a \times b$), i.e. $W^b_{bs} \in W_{bs}$ and $W^{b''}_{bs} \in W''_{bs}$. The presence of tampering is detected if $TDR\left(W^b_{bs}, W^{b''}_{bs}\right) \geqslant T$, where $T(0 \leqslant T \leqslant 1)$ is an appropriate threshold. The value of T is determined using the Neyman–Pearson criterion (i.e. by minimizing the probability of missing the watermark subject to a fixed false alarm probability P_F) [41]. The probability of false alarm is computed as follows [42]:

$$P_F = \sum_{k=((T+1)/2)N_w}^{N_w} \binom{N_w}{k} P_e^{N_w-k}(1-P_e)^k \tag{13}$$

where P_e is the probability of bit error i.e., $P_e = Prob\left(W^b_{bs} \neq W^{b''}_{bs}\right)$. Note that P_F depends on P_e, N_w and T. In the case that the underlying image block ($a \times b$) is simplified not to be a watermarked copy, it is reasonable to assume $P_e = 0.5$. The selection of threshold (T) value is based on applications. If a high quality of received image is required, a smaller threshold (T) value would be chosen. In this work, the threshold value $T = 0.625$ is chosen such that it has an associated probability of false alarm less than 10^{-8}. A block size of (64×64) is used in zero level (host image) for tamper detection, as it provides a good trade-off between the robustness to image distortion and the size of the smallest detectable feature tampering [43]. Practically, the value of $T = 0.625$(=10/16) implies that a (64×64) block is declared as tampered if it's ten or more (16×16) sub-blocks (out of 16 such sub-blocks) are tampered.

Difference in the original and reconstructed watermark image $D(i,j)$ is now calculated as follows:

$$D(i,j) = |W_{bs}(i,j) - W''_{bs}(i,j)| \quad (1 \leqslant i,j \leqslant n) \tag{14}$$

If $D(i,j) = 1$, the pixel at (i,j) location in the binary difference signature image is white and represents watermark extraction error. Contrarily, if it is black, it represents an accurate watermark extraction. Here, tamper correction is based on the assumption that if the attack is intentional, most of the watermark error pixels are closed to the difference image. The watermark difference $D(\cdot)$ is used as a mask to find the tampered region, which is recovered by the marker (W''_{md}). To achieve this goal, inverse Floyd halftoning is applied with image digest (W''_{md}) and LL subband of received (damaged) image $\left(h_w^{LL_2}\right)$ as input, to get a low resolution image ($\boldsymbol{m}'$). The tampered coefficients in the 2nd LL subband $\left(h_w^{LL_2}\right)$ of the received image is recovered using the following rule:

$$h_w^{LL_2}(r,c) = \begin{cases} m'(r,c) & \text{if } D(i,j) = 1 \\ h_w^{LL_2}(r,c) & \text{otherwise} \end{cases} \tag{15}$$

where $\langle r,c\rangle = \langle i : i+b, j : j+b\rangle$ and b is the block size used for embedding one bit of signature (watermark). The LL subband $h_w^{LL_2}$ and the watermark difference D are now resampled to the original size ($N \times N$) of the host image using the bilinear interpolation. The 2-level IWT is then calculated on the resultant resampled image of $h_w^{LL_2}$ i.e. $h_w^{R_l}$ and D. The tampered coefficients in the subsequent subbands *i.e.* $R \in \{HL, LH, HH\}$ of level l are corrected using following rule:

$$h_w^{R_l}(i,j) = \begin{cases} h_{w,z}^{R_l}(i,j) & \text{if } D_z^{LL_l}(i,j) = 1 \\ h_w^{R_l}(i,j) & \text{otherwise} \end{cases} \tag{16}$$

where $h_{w,z}^{R_l}$ represents the subband R (except the LL subband) of level 'l' for the zoomed version of $h_w^{LL_2}$, and $D_z^{LL_l}$ represents LL subband of level 'l' for the zoomed version of D. Inverse IWT is then performed to get back the corrected image.

Fig. 3 shows a visual schematic of the watermark encoding, forgery attack, watermark decoding and tamper detection and correction process. The proposed algorithm, although presented for gray scale images, can easily be extended for color images by considering each color channel as a gray-scale image. For efficient implementation, the RGB coordinate can first be transformed to YC_rC_b coordinate. The watermarks can then be embedded in appropriate color channels (luminance or chrominance).

4. Performance evaluation

This section presents simulation results to show the performance of the proposed data hiding technique in the context of tamper detection and correction in a digital image. The efficiency of the proposed technique is evaluated over 25 benchmark images [44,45] including the popular test images such as Water Lilies, Lena, Cameraman, Baboon, Fishing Boat, Opera, Pueblo bonito, F16 and Pepper shown in Fig. 4. This set of images is chosen in order to demonstrate the efficacy of the proposed algorithm over varied characteristics such as smooth areas, edges, texture, curvature and regular and irregular geometry of objects. All of the test images are 8 bit/pixel gray scale images with size 512×512. The step size for dither (Δ) is set to 15. Note that this corresponds to the watermark power (WP) of 12.73 dB, which is calculated as follows [46].

$$WP = 10\log_{10}\frac{\Delta^2}{12}\,dB \tag{17}$$

In the proposed technique, one bit of W'_{bs} is embedded into two (4×4) blocks, one each obtained from HL2 and LH2. At the same time, one bit of W'_{md} is embedded into two (2×2) blocks, one each obtained from HL1 and LH1. The bits of W'_{md} are embedded in level-1 wavelet subbands as these subbands offer high embedding capacity. The tamper detection performance is evaluated using the probability of false alarm (P_F) and the probability of miss (P_M), which are defined below:

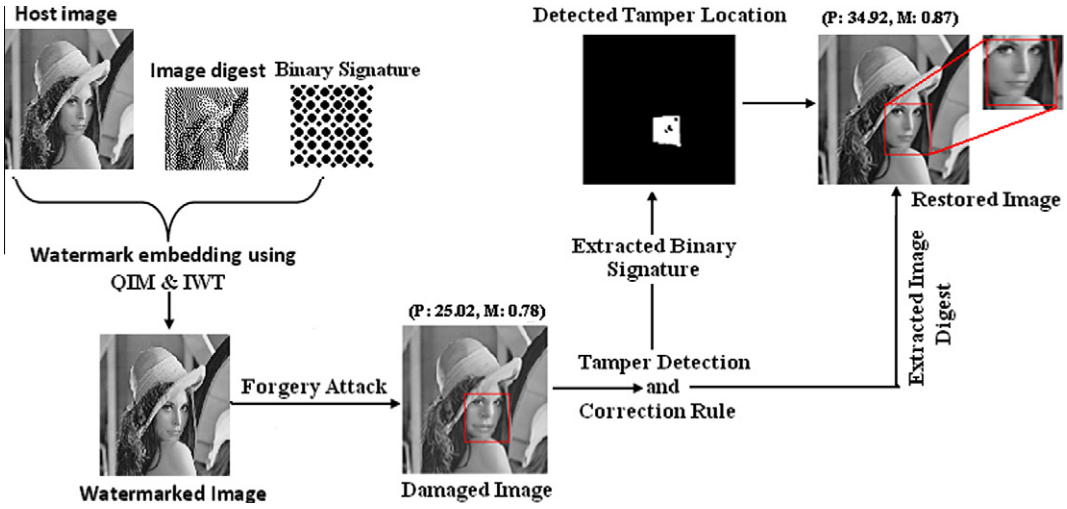

Fig. 3. Graphical schematic of the watermarking, encoding, forgery attack, watermark decoding, and tamper detection and correction process.

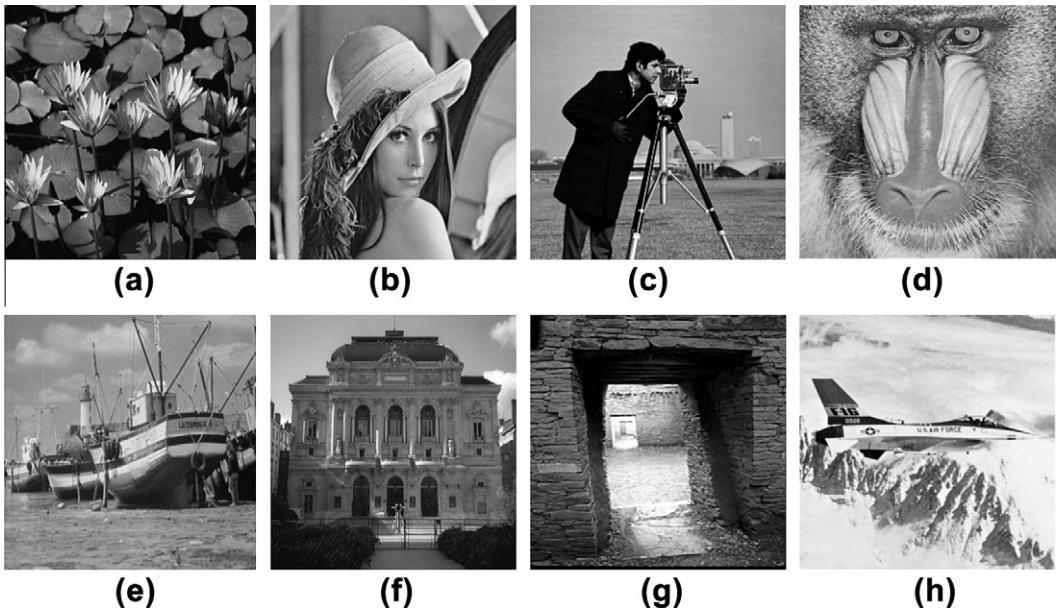

Fig. 4. Test images, (a): water lilies, (b) lena, (c) cameraman, (d) baboon, (e) fishing boat, (f) opera, (g) pueblo bonito, (h) F16.

$$P_M = \left[\frac{1}{\bar{n}}\sum_{i=1}^{\bar{n}} TDR\left(W_{bs}^{b}, W_{bs}^{b''}\right) < T\right] \times 100 \tag{18}$$

$$P_F = \left[\frac{1}{\bar{n}}\sum_{i=1}^{\bar{n}} TDR\left(W_{bs}^{b}, W_{bs}^{b''}\right) > T\right] \times 100 \tag{19}$$

where $\bar{n}$ is the number of image blocks, and W_{bs}^{b} and $W_{bs}^{b''}$ are respectively the embedded and extracted watermark bits from a block.

In this study, we use peak-signal-to-noise-ratio (PSNR dB) and mean-structure-similarity-index-measure (MSSIM) [47] as the objective measures to quantify the watermarked image quality. For an 8-bit/pixel gray scale image, the PSNR (in dB) is defined as follows:

$$PSNR(in\ \mathrm{dB}) = 10\log_{10}\left[\frac{255^2}{\frac{1}{X\times Y}\sum_{r=1}^{X}\sum_{c=1}^{Y}[P(r,c)-\tilde{P}(r,c)]^2}\right] \tag{20}$$

where $P(r,c)$ represents the pixel value at coordinate (r,c) in the original undistorted image, and $\tilde{P}(r,c)$ represents the pixel value in the watermarked (stego) image, and X and Y are, respectively, the number of rows and columns. The MSSIM is defined as follows:

$$MSSIM(P,\bar{P}) = \frac{1}{M'}\sum_{j'=1}^{M'} SSIM\left(P_{j'},\bar{P}_{j'}\right) \tag{21}$$

where

$$SSIM(P,\bar{P}) = [l(P,\bar{P})]^{\delta}.[c(P,\bar{P})]^{\beta}.[s(P,\bar{P})]^{\gamma}. \tag{22}$$

The functions $l(P,\bar{P}), c(P,\bar{P})$ and $s(P,\bar{P})$ are the luminance comparison, contrast comparison and structure comparison function, respectively, and δ, β and $\gamma\{\delta,\beta,\gamma > 0\}$ are the parameters used to adjust the relative importance of the components. Note that the value of MSSIM satisfies $0 \leqslant MSSIM(P,\bar{P}) \leqslant 1$, and $MSSIM(P,\bar{P}) = 1$, if $P = \bar{P}$. The symbols $P_{j'}$ and $\bar{P}_{j'}$ are the image contents at the j'th local window, and M' is the number of samples in the quality map.

Note that the PSNR is a simple measure of image quality based on average error without considering the local content or structure of image or video signal. Although, it does not always correlate well with the subjective quality, the PSNR is still widely used as it is easy to compute and represent visual quality relatively well in most situations. On the other hand, the MSSIM index has been shown to be more accurate for measuring the quality of images [48], as this measure consists of human visual characteristics as well as structure of the content. More recent works incorporates entropy masking to include neighborhood contributions and statistical pattern that play important roles in human perception [49,50].

4.1. Data imperceptibility

In this section, we evaluate the fidelity of the watermarked images obtained using the proposed data hiding technique and is compared with existing techniques in the literature. The size of the binary signature (W_{bs}) is 64×64, while the size of the message digest (W_{md}) is 128×128. The PSNR and MSSIM values are shown in Table 2. The high numerical values indicate that the visual quality of watermarked image is well maintained. It is also observed that for a given watermark power, although the visual quality in PSNR (dB) for the watermarked image does not vary much, high value of structural similarity is observed for the images having high texture image such as Baboon and Pueblo Bonito. This demonstrates the fact that the data embedding causes less visual degradation for the high texture image such as Baboon and Pueblo Bonito than the low texture image such as Lena.

Table 3 compares the data imperceptibility performance of the proposed technique with the techniques proposed by Lu et al. [28], Li [29], Lin et al. [30], and Adsumilli et al. [36] for the same watermark payload. The entries in Table 3 were obtained by averaging the results from 100 independent experiments conducted over 25 benchmark images. The relatively high values of PSNR (dB) and MSSIM indicate that better invisibility of the hidden data is achieved by the proposed technique. This is due to the use of the IWT that offers low loss in image information for QIM data embedding.

The comparison of DWT and IWT with respect to image fidelity for different watermark powers (WP) is shown in Table 4. It is observed that the IWT, as expected, provides a superior performance compared to the DWT. Note that the increase in the WP causes degradation in the visual fidelity, which is indicated by the lower values of both PSNR and MSSIM. It is also observed that change in PSNR values are not smooth, while the MSSIM values decrease smoothly. This is primarily because PSNR is expressed in dB and logarithm is a nonlinear function. Fig. 5 shows a few selected watermarked images, and Fig. 6(a)–(d) show the corresponding image digests (which are embedded and used for recovery of the tampered region). Fig. 6(e)–(f) show the corresponding inverse halftoned images. Fig. 7(a)–(d) show example of a binary signature, processed binary signature, the extracted signature, and the extracted binary signature using incorrect key. Without the true key, the extracted signature looks like noise. It demonstrates that the proposed scheme is sensitive to key (K) and hence it is secured.

Table 5 shows the variation in image quality for different watermark payload i.e., the number of watermark bits. It is observed that as the payload increases, the quality of the watermarked image decreases, as expected. In addition, it is also seen that the IWT offers better performance in terms of MSSIM and PSNR values than DWT. This is due to large correlation between the coefficients in IWT than the traditional DWT [51]. The large values of correlation indicate low randomness and high redundancy in the coefficients. Data hiding technique takes the advantage of this redundancy to embed more bits of watermark for a given embedding distortion.

Table 2
PSNR (dB) and MSSIM of the watermarked image corresponding to the watermark power 12.73 dB.

	Water lilies	Baboon	Lena	Cameraman
PSNR (dB)	35.27	35.13	35.02	35.57
MSSIM	0.90	0.95	0.87	0.86
	Fishing boat	Opera	Pueblo bonito	F16
PSNR (dB)	35.16	35.16	35.30	35.16
MSSIM	0.90	0.89	0.94	0.86

Table 3
The PSNR (dB) values of the watermarked images for the proposed technique and related works [28–30,36]. Watermark payload is 20,480 bits.

	PSNR (dB)	MSSIM
Proposed technique	35.27	0.90
Lu et al. [28]	30.11	0.86
Li [29]	32.23	0.87
Lin et al. [30]	33.79	0.89
Adsumilli et al. [36]	32.25	0.87

4.2. Performance evaluation under various non-malicious operations

To evaluate the P_e and to quantify the P_F for the proposed techniaque, some typical common signal processing operations such as filtering, sampling, histogram equalization, various noise addition, dynamic range change, and lossy JPEG compression are performed on the watermarked images. Performance is also evaluated against shifts, rotations, and other geometric attacks such as affine transformation, since the QIM-based schemes reported in the literature show relatively poor performance for such kind of operations. The BER is important as the value of P_F is directly related to P_e. Smaller the value of P_e, the better is the system performance in term of P_F as shown in Eq. (13). For image scaling operation, before watermark extraction, the attacked images are rescaled to the original size. For rotation operation, the rotation angle undergone by the watermarked images is estimated by control point selection method with the help of the host images. The rotated watermarked images are then inverse rotated and is corrected by linear interpolation. These corrected watermarked images are then used for the watermark detection. This is done to compensate for the effect of loss in the data due to the rotation operation. The numerical values of BER are averaged and are shown in Table 6. It is observed that the values of P_e, corresponding to the most common signal processing operations, are low for integer wavelet based data hiding compared to the same for traditional DWT. It is also observed that the proposed algorithm can successfully resist attacks such as filtering, scaling, cropping, random removal of some rows and columns, combination of scaling and small rotation.

Table 7 shows the performance measure for lossy JPEG compression as the operation is common to any band limited broadband transmission channel. The objective here is to test the degree or extent of compression operations by the watermarked image rich with varied contents and characteristics. It is seen that the scheme is robust for moderate JPEG compression up to quality factor 70. It is also observed in Table 7 that the increase in payload size for a fixed embedding space increases the BER values. As embedding space is fixed, then due to the increase in payload, the number of host signal points that are used for embedding of a watermark bit would be less. This leads to poor detection performance and high BER.

Tables 8 and 9 show the P_F against several common image processing operations and geometric attacks such as small rotation

Table 4
Variation of PSNR (dB), MSSIM values for different WP (dB).

	WP (dB)	9.20	10.03	10.79	11.48	12.13	12.73	13.29	13.81	14.31	14.78
IWT	PSNR (dB)	38.55	37.66	37.04	36.36	35.78	35.18	34.76	34.28	33.82	33.29
	MSSIM	0.94	0.92	0.91	0.90	0.89	0.87	0.86	0.85	0.84	0.82
DWT	PSNR (dB)	36.21	35.55	35.14	34.67	33.67	33.25	32.86	32.34	31.76	31.12
	MSSIM	0.92	0.90	0.89	0.88	0.87	0.86	0.85	0.84	0.83	0.81

Fig. 5. Watermarked images (a) water lilies, (b) lena, (c) cameraman, (d) baboon. (*P*,*M*) above each image represents the PSNR (in dB) and MSSIM values of the image.

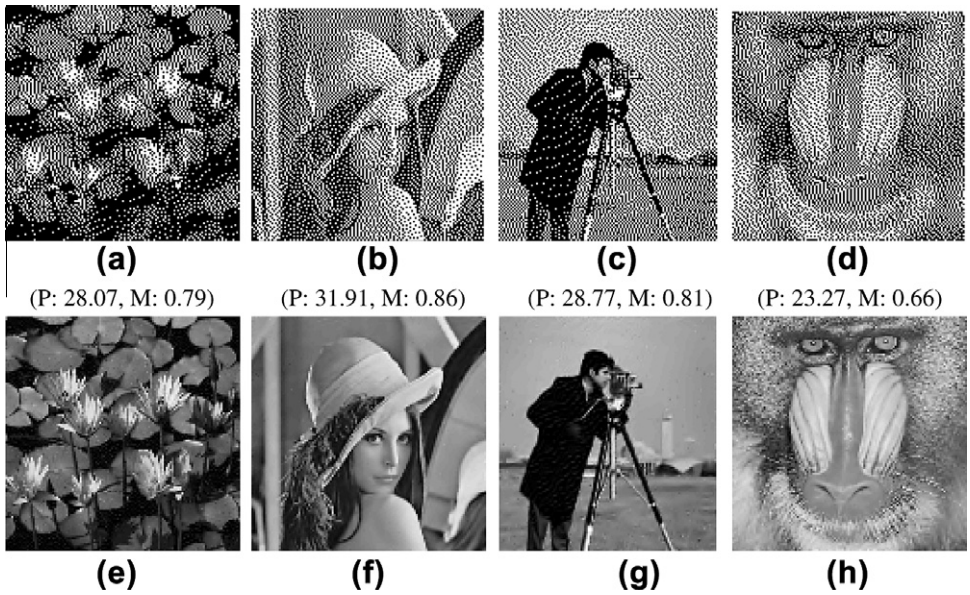

Fig. 6. (a)–(d) Image digest (a) water lilies, (b) lena, (c) cameraman, (d) baboon. (e)–(f) inverse halftoned image (e) water lilies, (f) lena, (g) cameraman, (h) baboon. *P*: PSNR value (in dB) of the image and *M*: MSSIM value of the image.

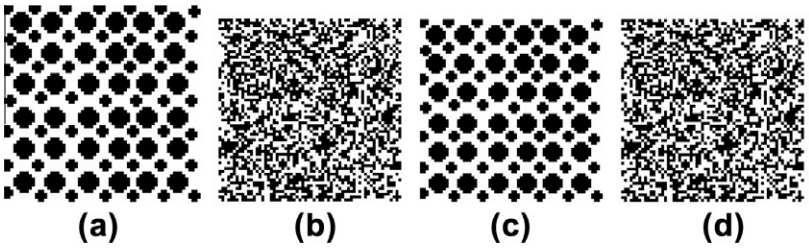

Fig. 7. (a) Sample signature for all test images, (b) processed signature, (c) extracted binary signature with BER = 0 for all test images, (d) extracted watermark using fake key.

and affine transform available in benchmark StirMark 4.0 [52–54]. Numerical values shown in Tables 8 and 9 are obtained by averaging the values of 100 independent experiments conducted over the large number of benchmark images. It is observed that for majority of the operations the P_F has a small value. In the case of histogram equalization the gray levels of the watermarked images are modi-

Table 5
Results of variation of the image quality for different watermark size (payload). Watermark power 12.73 dB.

	Watermark payload (in bit)	10,000	12,000	15,000	20,480
IWT	PSNR (dB)	47.02	42.56	38.05	35.27
	MSSIM	0.98	0.96	0.92	0.90
DWT	PSNR (dB)	44.15	39.86	35.67	33. 25
	MSSIM	0.94	0.93	0.89	0.86

Table 6
Bit error rate (P_e) for normal and integer DWT (**A**: Median (3 × 3); **B**: Mean (3 × 3); **C**: High pass (3 × 3); **D**: Down & Up (0.9); **E:** Histogram; **F**: Dynamic Range; **G**: Salt & Pepper (0.009); **H**: Speckle (0.009); **I**: Gaussian (0.009); **J**: Random Bit Error (1%); **K**: Rotation (3 degree)), **L**:Affine (2).

	A	B	C	D	E	F	G	H	I	J	K	L
DWT	0.64	0.74	0	0.78	0.52	0	0	0.14	0.40	0.16	0.25	0.39
IWT	0.31	0.39	0	0.19	0.33	0	0	0.12	0.38	0.12	0.15	0.10

Table 7
Bit error rate (P_e) values for different watermark size (payload) in case of lossy JPEG compression.

Watermark payload (in bits)	10,000	12,000	15,000	17,400
BER (JPEG 70)	0	0	0	0.11
BER (JPEG 60)	0	0	0.13	0.15
BER (JPEG 50)	0.12	0.14	0.17	0.19

Table 8
Probability of false alarm (P_F) in % for various signal processing attacks. **A:** JPEG70; **B:** Mean Filtering (3 × 3); **C:** Median Filtering (3 × 3); **D:** Histogram Equalization; **E:** Down and Up Sampling (by factor 0.75); **F:** Dynamic Range Change (50–200); **G:** Salt & Pepper Noise (variance 0.05); **H:** Random Bit Error (1%); **I:** Rotation (3 degree); **J:**affine (2).

	A	B	C	D	E	F	G	H	I	J
IWT	0	0.84	0.70	7.72	0.39	0	0	0	0	3
Normal DWT	0	6.64	0.64	16.4	1.56	6.25	0	0	0	8.25

fied significantly, and this results in a high value of P_F. It is also observed that the IWT provides a superior performance compared to classical DWT.

4.3. Performance evaluation under various malicious attacks

To evaluate the probability of miss (P_M) for the proposed technique, various malicious operations such as editing (e.g., copy-move, copy-paste) and random bending attacks are performed in Adobe Photoshop 7 and the results are shown in Fig. 8 along with zoom of the recovered areas. The rectangular boxes shown inside the images in column (a) indicate the tampered regions. The images shown in column (b) show the detected tampered regions (as white). The non-tampered regions are shown as black. The corrected images are shown in column (c). It is observed that the technique finds the tampered region correctly with $P_M = 0$ as well as restores tampered regions effectively, even if, the quality of the tampered image is as low as 20 dB. Moreover, the technique can also correct the damaged regions effectively as long as the percentage loss in the watermarked image is below 40%.

We have also investigated situations where the extracted image digest is also corrupted due to tampering. Note that the recovery capability will be weakened in such a scenario as some of the bits corresponding to the extracted image digest would be wrong. The average simulation results are shown in Table 10. It is observed that the present scheme can recover the maliciously tampered image (with PSNR >27 dB and MSSIM >0.80) as long as the tampered region is not more than 40%. The scheme is unable to recover the image when the total tampered region is greater than 45%.

Table 11 shows the performance comparison of the proposed technique with several existing techniques based on both data hiding [27,31–33] and digital signature [6,7] with respect to P_M and P_F. It is observed that the proposed technique has a comparable performance to most existing techniques [27,31–33,6,7] and offers low values of P_M and P_F. However, the exception is seen for Hu technique [27] and Yang technique [33] for *smoothing* and *histogram equalization* operations. Although Hu and Yang techniques provide better performance for these operations in term of P_M and P_F, they fail to recover the forgery part. On the other hand, the proposed technique efficiently resolves that problem with a marginal sacrifice on P_F value. In Table 11, it is also observed that the Lin technique [31] and Queluz technique [32] offer high value of P_F for both smoothing and histogram equalization. This is because the Lin technique [31] embeds watermark bit by making ordinal relation of DCT coefficients that are *order invariance* and *coefficient invariance*. As a result, the algorithm offers superior performance in term of P_M for only JPEG. This is due to the fact that JPEG is a DCT based compression scheme. On the other hand, the Lin technique [31] fails to provide improved performance for other image processing operations such as smoothing and histogram equalization. Queluz et al. [32] embed watermark bits using even/odd quantization, which is very fragile in nature, and hence the technique shows high value of P_F for smoothing and histogram equalization. On the other hand, the proposed technique uses the QIM, and hence superior performance in terms of fidelity and BER is achieved over the embedding strategies used in both [31,32] and consequently results in low values of P_M and P_F. Finally, the technique proposed in [18] uses image feature as a reference watermark (authentication mark) and can be altered after common image processing operations like smoothing, histo-

Table 9
Probability of false alarm (P_F) in % for lossy JPEG and JPEG 2000 operations in case of IWT.

	Lossy JPEG (quality factor)									JPEG 2000 (bpp)			
	100	95	90	85	80	75	70	65	60	0.80	0.60	0.40	0.20
P_F	0	0	0	0	0	0	0	0.01	0.02	0	0.21	0.90	1.10

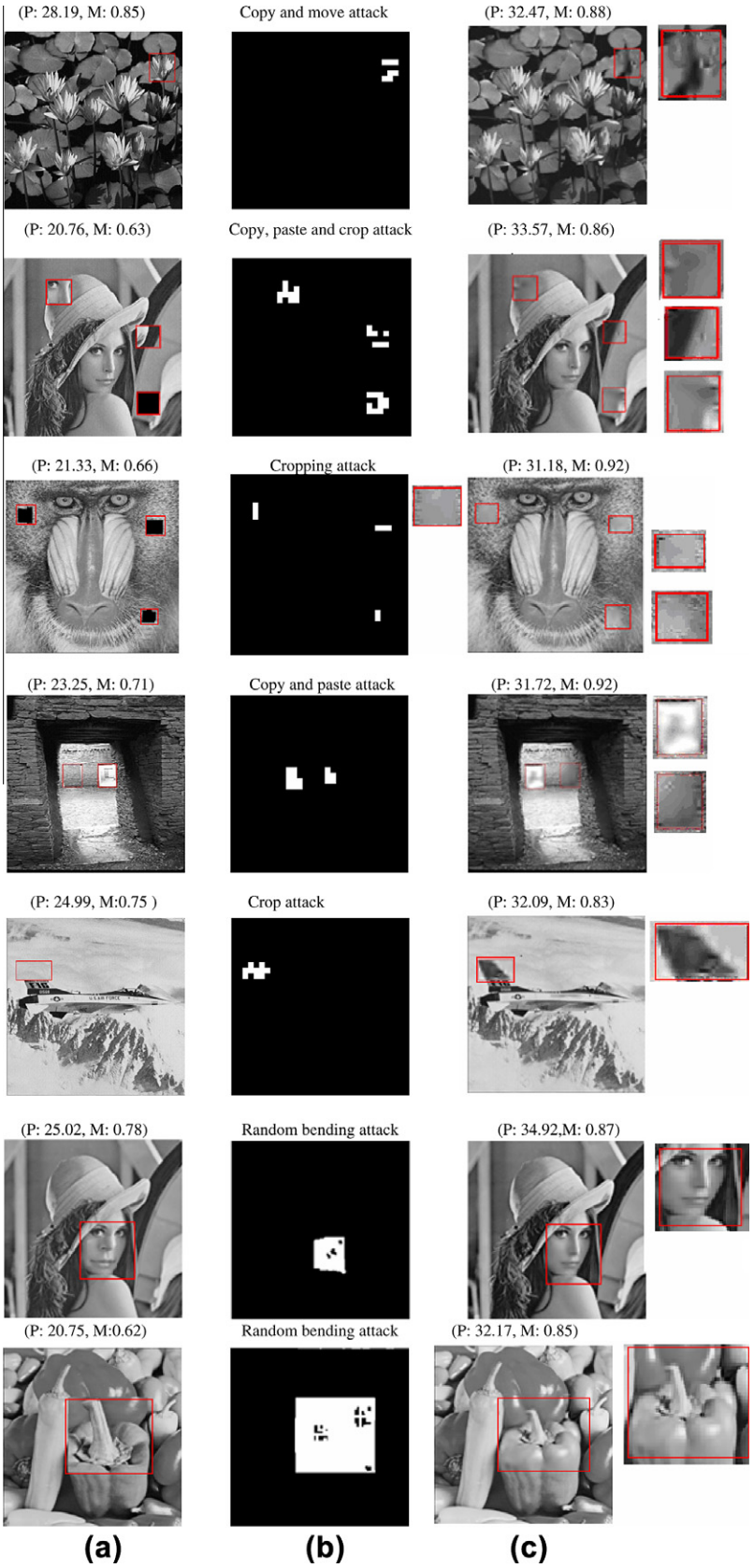

Fig. 8. Results for several selected test images. (a) Tampered images, (b) detected tampered regions, and (c) restored images. *P*: PSNR value (in dB) of the image and *M*: MSSIM value of the image. The type of attack is mentioned on top of the column b images.

gram equalization and random noise. This ultimately leads to a poor performance in P_F.

Table 12 presents the comparative results of the proposed technique with other recovery techniques [20–24,36]. The evaluation is

Table 10
PSNR (dB) values before and after recovery of tampered region, when embedded image digest is also lost.

% of the image digest lost	% of the image corrupted	Tampered image		Recovered image	
		PSNR (dB)	MSSIM	PSNR (dB)	MSSIM
0	23	20.76	0.63	33.57	0.86
1	28	19.42	0.61	32.32	0.83
2	35	18.35	0.60	31.01	0.82
5	40	17.42	0.59	27.35	0.80

Table 11
Performance comparison with other techniques with respect to P_M and P_F. DS: Digital signature. DH: Data hiding. 'PT' represents average execution time in second.

Semi-fragile watermarking techniques	PT	Forgery attack P_M (%)		P_F (%) for various signal processing attacks				
				No attack	Smooth	Histog. equal.	JPEG 70	Rand. noise
Lin et al. (2001) [31]	130	0.00		0.00	100	99.0	0.00	32.3
Queluz et al. (2002) [32]	78	0.10		0.10	27.8	94.3	0.01	0.01
Hu et al. (2005) [27]	112	0.00		0.00	0.08	0.31	0.16	0.22
Yang et al. (2007) [33]	105	0.0		0.0	0.2037	0.0001	0.2157	0.15
Kang et al. (2008) [6]	120	0.00		0.00	–	–	0.18	0.20
Mendoza et al. (2008) [7]	85	DS	0.00	0.00	–	–	0.05	–
	95	DH	4.00	0.00	–	–	0.004	–
Jin et al. (2009) [18]	102	0.23		0.00	10.10	–	5.14	4.17
Proposed technique	107	0.00		0.00	0.84	7.72	0.00	0.00

Table 12
Comparison of other normal recovery techniques (PSNR (dB) & MSSIM). 'PT' represents average execution time in second.

Technique	Zhang et al. (2004) [20]	Che et al. (2008) [21]	Qiang et al. (2009) [22]	Lin et al. (2004) [23]	Yang et al. (2005)[24]	Adsumilli et al. (2005) [36]	Proposed technique
PSNR (dB)	28.80	30.21	33.41	32.94	33.40	30.12	33.68
MSSIM	0.80	0.82	0.85	0.84	0.85	0.83	0.86
PT	132	116	98	126	121	118	107

conducted with 25 benchmark images and the average results are shown in Table 12. It is observed that the proposed method provides a superior performance. This is due to the following reasons: (1) half-toning technique generates better image digest which helps to achieve superior image recovery, and (2) the IWT offers low loss in image information due to the DM-QIM watermarking and leads to better watermark decoding reliability.

Tables 11 and 12 also show a comparison of the execution time of various techniques. The experiments were conducted in Pentium IV, 2.80 GHz processor; with 512 MB RAM using MATLAB 7. It is observed that the average time required by the proposed technique is of the same order to that of other techniques. The average times required for the implementation of [32,33,7,18] techniques (see Table 11) are slightly lower compared to the proposed technique, but the P_F value of the existing techniques are much higher than the proposed technique. In addition, the schemes proposed in [32,33,7,18] are unable to recover the tamper region. On the other hand, the execution time of [22] is little lower than the proposed technique but the PSNR and MSSIM values for the former are lower than the latter.

5. Conclusions and scope of future works

In this paper, a novel semi-fragile data hiding technique, based on integer wavelet transform and QIM, has been proposed for tamper detection and correction. The experimental results show that the proposed technique can efficiently distinguish malicious changes from various common image processing operations. The technique also corrects the tampered regions effectively as long as percentage loss in watermarked image is below 40%. The proposed technique is simple, cost effective and easy to implement, and can be used as a possible solution for digital rights management. Future work would be extended for countering the attack such as collage and vector quantization (VQ) attack. Future work will also be directed for development of hardware architecture for the proposed tamper detection and correction technique through application specific integrated circuit (ASIC) or field programmable gate array (FPGA) and extension of the proposed scheme for color image.

References

[1] F.A.P. Petitcolas, H.J. Kim, Digital Watermarking, Springer, Berlin/Heidelberg, 2003.
[2] O. Ekici, B. Sankur, B. Coskun, U. Naci, M. Akcay, Comparative evaluation of semi fragile watermarking algorithms, Journal of Electronic Imaging 13 (2004) 209–216.
[3] E.T. Lin, C.I. Podilchuk, E.J. Delp, Detection of image alterations using semi-fragile watermarks, in Proc. SPIE International Conference Security and Watermarking of Multimedia Contents, San Jose, CA, 2000, pp. 152–163.
[4] S.Y. Yang, Z.D. Lu, F.H. Zou, A novel semi-fragile watermarking technique for image authentication, in Proc. 7th International Conference on Signal Processing, 2004, pp. 2282–2285.
[5] M.J. Tsai, C.C. Chien, A wavelet-based semi-fragile watermarking with recovery mechanism, in Proc. IEEE International Symposium on Circuits and Systems, Washington, USA, 2008, pp. 3033–3036.
[6] X. Kang, S. Wei, Identifying tampered regions using singular value decomposition in digital image forensics, in Proc. International Conference on Computer Science and Software Engineering, Wuhan, Hubei, 2008, pp. 926–930.
[7] J.A. Mendoza, C. Cruz, M.N. Miyatake, H.P. Meana, Content authentication schemes for digital images, in Proc. 5th International Conference on Electrical Engineering, Computing Science and Automatic Control, Mexico City, 2008, pp. 292–297.
[8] M. Costa, Writing on dirty paper, IEEE Transactions on Information Theory 29 (1983) 439–441.
[9] B. Chen, G.W. Wornell, Quantization index modulation: a class of provably good methods for digital watermarking and information embedding, IEEE Transaction of Information Theory 47 (2001) 1423–1443.
[10] B. Chen, G.W. Wornell, Digital watermarking and information embedding using dither modulation, in Proc. IEEE Workshop on Multimedia Signal Processing, Redondo Beach, CA, 1998, pp. 273–278.
[11] A. Phadikar, S.P. Maity, M-ary QIM data hiding for error concealment of digital image in JPEG pipeline, in Proc. International Conference on Advances in

Computing, Control, and Telecommunication Technologies, Kerala, India, 2009, pp. 93–97.
[12] A. Phadikar, S.P. Maity, M.K. Mandal, QIM data hiding for tamper detection and correction in digital images using wavelet transform, in Proc. of 23nd IEEE Canadian Conference on Electrical and Computer Engineering, Calgary, Canada, 2010, pp. 1–5.
[13] A. Phadikar, S.P. Maity, ROI based quality access control of compressed color image using DWT via lifting, Electronic Letter on Computer Vision and Image Analysis 8 (2009) 51–67.
[14] A. Phadikar, S.P. Maity, Quality access control of compressed color images using data hiding, International Journal of Electronics and Communications 64 (2010) 833–843.
[15] S.P. Maity, M.K. Kundu, S. Maity, Dual purpose FWT domain spread spectrum image watermarking in real-time, International Journal of Computer and Electrical Engineering 35 (2009) 415–433 (in the special issue on real-time security and copyright protection of multimedia).
[16] P. Campisi, M. Carli, G. Giunta, A. Neri, Blind quality assessment system for multimedia communications using tracking watermarking, IEEE Transaction on Signal Processing 51 (2003) 996–1002.
[17] X. Wu, J. Hu, Z. Gu, J. Huang, A secure semi-fragile watermarking for image authentication based on integer wavelet transform with parameters, in Proc. Australasian Workshop on Grid Computing and E-research, New South Wales, Australia, 2005, pp. 75–80.
[18] C. Jin, Y. Chao, X.L. Zhang, Semi-fragile watermark based on adaptive quantization for image content authentication, in Proc. International Conference on E-business and Information System Security, China, 2009, pp. 1–5.
[19] R. Chamlawi, A. Khan, A. Idris, Z. Munir, A secure semi-fragile watermarking scheme for authentication and recovery of images based on wavelet transform, in Proc. World Academy of Science, Engineering and Technology, vol. 17, 2006, pp. 217–220.
[20] H.B. Zhang, C. Yang, Tamper detection and self recovery of images using self-embedding, Chinese Journal of Electronics 32 (2004) 196–199.
[21] S.B. Che, Z.G. Che, B. Ma, Q.B. Huang, Image self-embedding technology research based on singular value decomposition, in Proc. 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), Dalian, China,2008, pp. 1–7.
[22] S. Qiang, W. Jiawen, Z. Hongbin, Tamper detection and self-recovery of image based on self-embedding, in Proc. Asia-Pacific Conference on Information Processing, Shenzhen, China, 2009, pp.76–79.
[23] P.L. Lin, P.W. Huang, A.W. Peng, A fragile watermarking scheme for image authentication with localization and recovery, in Proc. of IEEE Sixth International Symposium on Multimedia Software Engineering, Miami, Florida, 2004, pp. 146–153.
[24] Z.L. Yang, Hierarchical fragile watermarking scheme for image authentication, Master thesis, CSIE, National Dong Hwa University, July 2005.
[25] Q. Qin, W. Wang, S. Chen, D. Chen, W. Fu, Research of digital semi-fragile watermarking of remote sensing image based on wavelet analysis, in Proc. IEEE International Symposium on Geo science and Remote Sensing, Anchorage, Alaska, USA, 2004, pp. 2542–2545.
[26] C. Yung, S.F. Chang, Semi-fragile watermarking for authenticating JPEG visual content, in Proc. SPIE Security and Watermarking of Multimedia Content, San Jose, 2000, pp. 140–151.
[27] Y.P. Hu, D.Z. Han, Using two semi-fragile watermark for image authentication, in Proc. of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 2005, pp. 5484–5489.
[28] Z.M. Lu, D.G. Xu, S.H. Sun, Multipurpose image watermarking algorithm based on multistage vector quantization, IEEE Transaction on Image Processing 14 (2005) 822–831.
[29] C.T. Li, Digital fragile watermarking scheme for authentication of JPEG images, in Proc. of IEE on Vision, Image and Signal Processing, vol. 151, 2004, pp. 460–466.
[30] C.H. Lin, T.S. Su, W.S. Hsieh, Semi-fragile watermarking scheme for authentication of JPEG images, Tamkang Journal of Science and Engineering 10 (2007) 57–66.
[31] C.Y. Lin, S.F. Chang, A robust image authentication method distinguishing JPEG compression from malicious manipulation, IEEE Transaction on Circuits System and Video Technology 11 (2001) 153–168.
[32] M.P. Queluz, Spatial watermark for image content authentication, Journal of Electronic Imaging 11 (2002) 275–285.
[33] H. Yang, X. Sun, Semi-fragile watermarking for image authentication and tamper detection using HVS model, in Proc. of International Conference on Multimedia and Ubiquitous Engineering, Seoul, 2007, pp. 1112–1117
[34] W. Sweldens, The lifting scheme: a custom-design construction of biorthogonal wavelets, Applied and Computational Harmonic Analysis 3 (1996) 186–200.
[35] W. Sweldens, The lifting scheme: construction of second generation wavelets, SIAM Journal on Mathematical Analysis 29 (1997) 511–546.
[36] C.B. Adsumilli, M.C.Q. Farias, S.K. Mitra, M. Carli, A robust error concealment technique using data hiding for image/video transmission over lossy wireled/wireless channels, IEEE Transactions on Circuits and Systems for Video Technology 15 (2005) 1394–1406.
[37] S. Voloshynovskiy, T. Pun, Capacity security analysis of data hiding technologies, in Proc. IEEE Confarence on Multimedia and Expo, Lausanne, Switzerland, 2002, pp. 477–480.
[38] P.W. Wong, Inverse halftoning and kernel estimation for error diffusion, Media Technology Laboratory, HPL-93-92, 1993, pp. 1–23.
[39] R. Floyd, L. Steinberg, An adaptive algorithm for spatial grey scale, SID International Symposium Digest of Technical Papers, 1975, pp. 36–37.
[40] C. Christopoulos, A. Skodras, T. Ebrahimi, The JPEG 2000 still image coding system: an overview, IEEE Transactions on Consumer Electronics 46 (2000) 1103–1127.
[41] M. Barni, F. Bartolini, A. Piva, Improved wavelet-based watermarking through pixel-wise masking, IEEE Transaction on Image Processing 10 (2001) 783–791.
[42] D. Kundur, D. Hatzinakos, Digital watermarking using multiresolution wavelet decomposition, in Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing, Seattle, 1998, pp. 2969–2972.
[43] J. Fridrich, Image watermarking for tamper detection, in Proc. International Conference on Image Processing, Chicago, 1998, pp. 404–408.
[44] (Test image online source) Available: <http://www.cl.cam.ac.uk/fapp2/watermarking>.
[45] (Test image online source) Available: <http://www.petitcolas.net/fabien/watermarking/>.
[46] J.P. Boyer, P. Duhamel, J.B. Talon, Performance analysis of scalar DC-QIM for watermark detection, in Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, Honolulu, Toulouse, 2006, pp. II–II.
[47] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, Image quality assessment: from error measurement to structural similarity, IEEE Transactions on Image Processing 13 (2004) 1–14.
[48] C. Li, A.C. Bovik, Content-partitioned structural similarity index for image quality assessment, Signal Processing: Image Communications 25 (2010) 517–526.
[49] A.C. Bovik, Perceptual image processing: seeing the future, in Proc. IEEE, vol. 98, no. 11, 2010, pp. 1799–1803.
[50] C. Yim, A.C. Bovik, Quality assessment of de-blocked images, IEEE Transactions on Image Processing 20 (2011) 88–98.
[51] A. Phadikar, S.P. Maity, Data hiding based quality access control of digital images using adaptive QIM and lifting, Journal Signal Processing: Image Communication 26 (2011) 646–661.
[52] F.A.P. Petitcolas, Watermarking schemes evaluation, IEEE Signal Processing 17 (2000) 58–64.
[53] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Attacks on copyright marking systems, in: Proc. Second International Workshop on Information Hiding, LNCS, 1525, Springer-Verlag, 1998, pp. 219–239.
[54] StirMark Benchmark 4.0 (Web Resources): <http://www.petitcolas.net/fabien/watermarking/stirmark/>.