Computers and Electrical Engineering 39 (2013) 2019–2030

Contents lists available at SciVerse ScienceDirect

Computers and Electrical Engineering

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

Dual-purpose semi-fragile watermark: Authentication and recovery of digital images ☆

Rafi Ullah [a,b,*], Asifullah Khan [c], Aamir Saeed Malik [a]

[a] Department of Electrical and Electronic Engineering, University Technology PETRONAS (UTP), Tronoh, Perak, Malaysia
[b] Department of Computer Science, COMSATS Institute of Information Technology, Park Road, Chak Shahzad, Islamabad, Pakistan
[c] Department of Computer and Information Sciences, Pakistan Institute of Engineering and Applied Sciences (PIEAS) P.O Nilore, Islamabad, Pakistan

ARTICLE INFO

Article history:
Received 2 November 2011
Received in revised form 29 April 2013
Accepted 29 April 2013
Available online 3 June 2013

ABSTRACT

This paper presents a framework based on a single dual-purpose semi-fragile watermark to verify the integrity of digital image along with the recovery of distorted image. The watermark is correlated to the host image for detecting the collage attack and then embedded in their respective wavelet subbands. Unlike the conventional block-based approaches, this work has the ability to determine the unverified regions concisely. Huffman and BCH coding are utilized while generating the watermark. Integer DCT has been exploited as it can be highly compressed by Huffman coding as compared to the conventional DCT contents. The proposed technique exhibits the flexibility between imperceptibility, robustness, and capacity. In addition, integer wavelet transform has been used to reduce the computational complexity of the algorithm. Evaluation of experimental investigation shows the performance of dual-purpose semi-fragile watermark.

1. Introduction

Seeing Is Believing is unreliable in today's digital world because the availability of powerful tools can easily duplicate and manipulate the content without leaving any trace. Thus, protection of digital content against illegal manipulation and duplication is essential. Digital watermarking is used to protect the integrity of the content. Authentication/integrity-verification, broadcast monitoring, ownership assertion, transaction tracking, and copyright protection are very common and interesting applications of watermarking [1].

Generally, robust, fragile and semi-fragile watermarking techniques are used to make the digital content secure. A large number of robust watermarking techniques are proposed that are used to protect the copyrights of the digital images. In [2,3], the mid to high frequencies in wavelet transform are modified to embed watermark in the image. In [4–8], perceptually tuned DCT-based robust watermarks are employed for protecting digital images. In [9], a robust watermarking technique based on invariant pattern recognition has been utilized to protect the copyrights of digital image. This scheme can also have useful applications in the medical imaging. Similarly, Liu et al. [10] have developed a robust watermarking approach based on wavelet transform using original image and its reference image for watermark embedding.

Robust watermarking technique resists the alterations and it is difficult to detect the friendly manipulations like JPEG compression as well as malicious manipulations. Thus, fragile watermarking approaches have been developed which are sensitive to all kinds of alterations. The core application of fragile watermarking is authentication. Wavelet based fragile watermarking technique has been proposed in [11], where the authors embed the watermark by quantizing wavelet coef-

☆ Reviews processed and approved for publication by Editor-in-Chief Dr. Manu Malek.

* Corresponding author at: Department of Electrical and Electronic Engineering, University Technology PETRONAS (UTP), Tronoh, Perak, Malaysia.
E-mail address: chamlawi@gmail.com (R. Ullah).

0045-7906/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.compeleceng.2013.04.024

ficients. Similarly, DCT, quantization index modulation, non-deterministic, block wise dependence, image structure, and CRT (Chinese Remainder Theorem) based fragile watermarking approaches have been proposed that are capable to authenticate digital images and detect tampering either incidental or malicious [12–14].

The main issue towards fragile watermark is its destruction against legitimate or illegitimate manipulation. Thus, semi-fragile watermarking techniques are the only solutions that make the system robust against the legitimate manipulation and fragile against illegitimate manipulations [15–17]. These approaches are fragile against malicious manipulations and have some tolerance against friendly manipulations like JPEG compression, which is the basic requirement in the communication system. Pre-defined parameters are used to define the strength of compression. In [17], two semi-fragile watermarks are used. One of them is used to authenticate the image and the other one is used to recover the image after distortion. A block-based approach is presented in [18], where at least two bits are embedded in 8×8 block. JPEG compression is used in watermark generation and thus, has the ability to resist the compression. This scheme is also applicable for color images where the luminance channel is used for watermark embedding. DCT and wavelet based fragile watermarking techniques have been presented in [19–21] to authenticate the digital image.

Besides authentication, recovery of tampered image at receiving end is also important. Now a day the researchers have proposed number of watermarking techniques that can protect the content as well as recover it if the content is distorted. There are two ways to recover the image: confined recovery and self-recovery. Many techniques [19,22–26] are proposed to protect the image and recover it where watermarked image has been tampered. The techniques discussed in [25,26] embed two semi-fragile watermarks to authenticate the image and recover it, if tampered. One watermark is used for authentication purpose and other one is used for the recovery. Both the techniques have the ability of authentication and recovery of the image but at the cost of imperceptibility. However, the issue with these techniques is the use of two watermarks, which affect the imperceptibility of the watermark. Similarly, in [30], the author is using semi-fragile watermark for authenticating and recovering the images but with cost concise authentication. This approach is unable to authenticate the content concisely.

The technique proposed in this paper has the ability to authenticate and recover the image by using single semi-fragile watermark. In this paper, embedding of a blind dual-purpose semi-fragile watermarking technique is presented. This technique is capable to resist the friendly manipulation like JPEG compression up to some extent and detect malicious manipulations. Unlike conventional block-based approaches, the proposed scheme precisely determines the region where the integrity of the image fails. The original image is compressed losslessly by employing Huffman coding for watermark generation. The compressed image then correlated with the approximation of original image to make it fragile against collage attack. Finally, an error correcting code (BCH encoder) is applied and then embedded in the suitable subband coefficients.

Rest of the paper is organized as follow: In Section 2, the proposed technique is briefly described. Section 3 provides the simulation results in detail. Analysis with respect to tamper detection, localization, and recovery has been presented in Section 4. Finally, we conclude the paper in Section 5.

2. Authentication framework

The proposed framework is based on a single dual-purpose semi-fragile watermark that is blindly embedded in the appropriate coefficients of wavelet subbands. The technique makes it possible to secure the digital image against any kind of attack applied on the to-be-checked image either in spatial domain or in transform domain without having any sacrifice on the imperceptibility. Entire wavelet subbands are involved in either watermark generation or embedding.

2.1. Generation and embedding of semi-fragile watermark

The general block diagram for generating and embedding watermark is shown in Fig. 1.

2.1.1. Watermark generation

A grayscale original image (to-be-authenticated image) is specified by $M \times N$ matrix and decomposed into approximation ($LL1$) and detailed subbands ($HL1$, $LH1$ and $HH1$) using integer wavelet transform (*IntWT*). A full-frame integer DCT (*IntDCT*) is applied on the image approximation to compress it at high ratio as given in Eq. (1). Block distortions take place by using block-based DCT and it can be resolved by applying full-frame DCT. However, it is difficult to adapt quantization to local image structure [27]

$$IntDCT\_image\_approx = Int\_DCT(LL1) \tag{1}$$

where *IntDCT_image_approx* shows the integer DCT coefficients of the image approximation. Huffman coding is then applied to compress the *IntDCT_Image_approx* losslessly using Eq. (2). In this technique, the quality of the recovered image will exactly match the approximation of the original image because of lossless compression of the image approximation.

$$Huffman\_image\_approx = huffmanenco(IntDCT\_image\_approx) \tag{2}$$

where *Huffman_image_approx* is the compressed $LL1$ in binary pattern. The $LL1$ subband has been selected for correlating the resultant of Eq. (2). The subbands other than $LL1$ are used to embed the watermark, because the $LL1$ coefficients severely affected by watermark embedding. Thus, the $LL1$ is free for correlation without introducing any conflict [28]. The four adja-

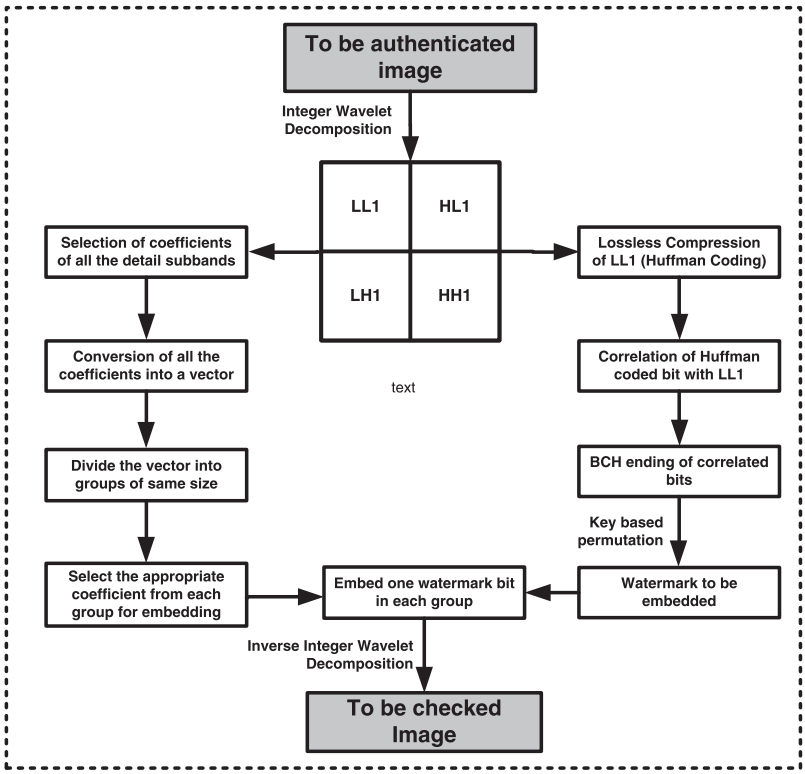

Fig. 1. Generation and embedding of watermark.

cent coefficients (i.e. $(LL1(m+1,n+1), LL1(m+1,n), LL1(m,n+1), LL1(m,n))$) of $LL1$ are averaged and quantized using Eq. (3). The quantized values are then *XORed* with the *Huffman_image_approx*.

$$Correlated\_binary\_pattern = \left\lfloor \frac{average}{QC} \right\rfloor mod2 \oplus Huffman\_image\_approx \tag{3}$$

where *average* is the average value of the four adjacent coefficients in $LL1$, and QC is the quantization parameter which deals with the sensitivity of the proposed technique against collage/counterfeiting attack. On the receiving side, if the image is compressed then the parameter QC will make sure the de-correlation of the extracted watermark with the approximation of the watermarked image. The *Correlated_binary_pattern* is then passed through an error correcting code called BCH encoder using the following equation:

$$BCH_{pattern} = bchenco(Correlated\_binary\_pattern) \tag{4}$$

The $BCH_{pattern}$ is then permuted based on a secret key to obtain the ultimate watermark for embedding as given in Eq. (5). The permutation of $BCH_{pattern}$ makes the watermark secures.

$$Watermark_{final} = permute(BCH_{pattern}) \tag{5}$$

where *permute* is used for key based random permutation. $Watermark_{final}$ is now ready to be embedded in the respective subbands of the to-be-authenticated image.

2.1.2. Watermark embedding

The watermark is now ready to be embedded in the suitable feature of the to-be-authenticated image. The suitable features of $HL1$, $LH1$ and $HH1$ subbands are selected for embedding purpose. The block diagram of the embedding procedure is given in Fig. 1. The selected subbands are used by taking into consideration the trade-off between the robustness and imperceptibility. The entire coefficients of the selected subbands are converted into a single sequence/vector V. Coefficients with the same coordinates are concatenated adjacently in the new vector V. The vector is scrambled based on a secret key for security purposes, and then divided into same size of groups g. One watermark bit is embedded in each group, and this single bit is capable to control all coefficients within a group. If group size is large, then number of embedded bits will be low and hence the imperceptibility will be high, and vice versa. Increase in imperceptibility will not affect the detection resolution. The watermark is embedded by modifying the weighted mean of each group. The weighted mean m_j of each group can be calculated using the following equation:

$$m_j = \sum_{i=1}^{g_s-1} p_i |f_j(i)| \tag{6}$$

where g_s is the group size, $f_j(i)$ is the ith coefficients of jth group, and p is the key based bipolar random sequence with uniform distribution $p \in \{1, -1\}$. The groups are further quantized using the following equations:

$$g_j = \left\lfloor \frac{m_j}{Q} \right\rfloor \cdot Q \cdot \Delta_j \tag{7}$$

$$Quantized_g(g_j) = \begin{cases} 0 & if \left\lfloor \frac{g_j}{Q} \right\rfloor \ is \ even \\ 1 & if \left\lfloor \frac{g_j}{Q} \right\rfloor \ is \ odd \end{cases} \tag{8}$$

where Q is the quantization step and it can be set according to the compression ratio on the watermarked image, Δj is the quantization residue, and the $Quantization_g$ is the resultant binary lattice.

The $Watermark_{final}$ is then embedded by modifying the weighted mean of each group in such a way that the $Quantization_g$ becomes equal to $Watermark_{final}$. The number of groups should be equal to the number of watermark bits so that every watermark bit can be embedded in their respective group. The largest coefficient is selected in a group to embed the watermark bit, which causes less noticeable artifacts. In detail subbands, the high magnitude coefficients represent more texture contents in the corresponding spatial location, and vice versa. Thus, the proposed approach is performed efficiently for high textured images instead of low textured images. The modification in the weighted mean is performed in Eq. (9). Random permutation of vector V makes sure that there will be at least one high magnitude coefficient in every group.

$$m'_j = \begin{cases} \lfloor m_j + Q/2Q + \frac{Q}{2} \rfloor, & if \ Quantized_g(m_j + \frac{Q}{2}) = Watermark_{final}(j) \\ \lfloor m_j + Q/2Q - \frac{Q}{2} \rfloor, & if \ Quantized_g(m_j + \frac{Q}{2}) \neq Watermark_{final}(j) \end{cases} \tag{9}$$

g'_j is the expected weighted mean of jth group. Let δ be the difference in the original and expected weighted means given in the following equation:

$$\delta_j = m_j - m'_j \tag{10}$$

The suitable (largest) coefficient in each group is modified according to the following equation:

$$f'_{j,maximum} = f_{j,maximum} + pi \cdot sign(f_{j,maximum}) \cdot \delta_j \tag{11}$$

If sign of the largest coefficient in a group $f_{j,maximum}$ changed after applying Eq. (11), then the second largest coefficient is selected by using $\delta_{j,residue}$ instead of $\delta_j \cdot \delta_{j,residue}$ is calculated using the following equation:

$$\delta_{j,residue} = sign(\delta_j) \cdot |\delta_j| - |f_{j,maximum}| \tag{12}$$

The process is repeated until $\delta_{j,residue} = 0$. The author in [29] assign zero to the sign-changing coefficient after applying Eq. (11). This practice causes serious modifications in the watermarked (to-be-checked) image.

The entire watermark is embedded in the suitable coefficients of permuted vector V. The vector is inversely permuted based on the same key. The entire vector coefficients are placed in their respective subbands. Inverse IntWT is then applied to obtain the to-be-checked image.

2.2. Watermark extraction and image recovery

2.2.1. Watermark extraction

The extraction of the embedded watermark is the inverse procedure of watermark embedding and generation as shown in Fig. 2. After decomposing the to-be-checked image, the respective subbands are selected, where the watermark is embedded. The keys and the wavelet types used in the watermark generation and embedding process are supposed to be available at the receiving end. The coefficients in the respective subbands are concatenated, permuted, and divide into groups in the similar way by using the same keys. The weighted mean of each group is calculated and the watermark bits are extracted by quantizing the weighted mean of each group using the following equation:

$$Watermark'_{final} = Quantized_g(m'_j) \tag{13}$$

where g'_j is the recalculated weighted mean of jth group. The groups m_j and m'_j are then compared for integrity verification. If both match, then the watermarked work in not manipulated, otherwise manipulated. The detail of tampering detection and localization will be discussed in Section 2.2.3.

2.2.2. Image recovery

After extracting the watermark bits, the procedure of decompression is applied to obtain the required image approximation. Similar to the previous approach [26], the technique proposed in this paper use the self-embedding approach for recov-

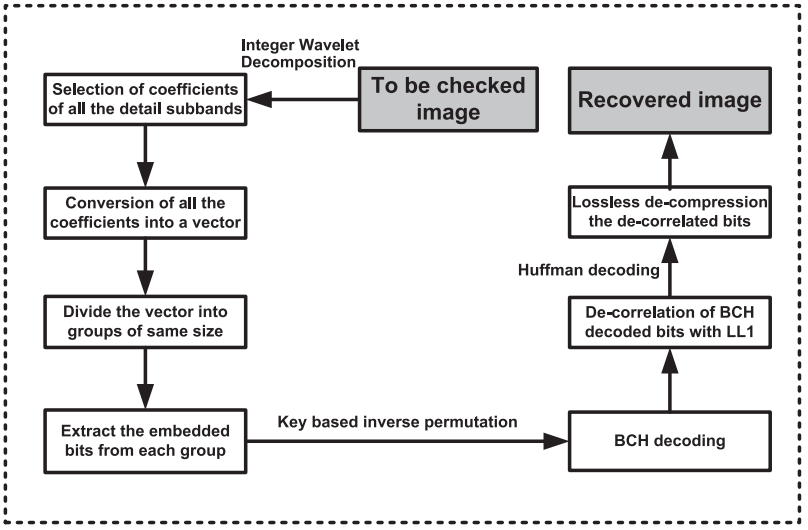

Fig. 2. Extraction of watermark.

ering the image but with the difference that this technique is able to recover the exact version of the original image approximation i.e. the embedded image will be recovered exactly even after JPEG compression or any tiny malicious manipulation. Lossless compression (Huffman coding) method and BCH coding have been utilized before embedding the watermark. On receiving side, the reverse procedure of generating and embedding the watermark is applied to obtain the original image approximation ($LL1$). The extracted watermark is permuted BCH encoded bit pattern. Thus, the inverse permutation is applied to get the BCH coded bits back using the following equation:

$$Inv\_permuted\_watermark = inv\_permute(Watermark_{extracted}) \tag{14}$$

where $Watermark_{extracted}$ is the extracted watermark from their respective subbands. The BCH decoding is then performed to obtain the correlated Huffman coded bit pattern using the following equation:

$$BCH_{decoded} = bchdeco(Inv\_permuted\_watermark) \tag{15}$$

After de-correlation of $BCH_{decoded}$ with image approximation, the resultant is decoded by using Huffman decoder as given in Eq. (16). The image approximation of watermarked image will be similar that original un-watermarked image because the approximation subband has not been used for embedding purpose and this make sure that the contents in the approximation are similar. However, if the watermarked image is tampered either maliciously or incidentally, then the required bits cannot be obtained and this shows that the image manipulated.

$$Huffman_{decoded} = huffmandeco(D\_BCH_{decoded}) \tag{16}$$

where $D\_BCH_{decoded}$ is the de-correlated bit pattern. Finally, the inverse *IntDCT* is applied on $Huffman_{decoded}$ to obtain the required approximated image ($LL1$) using the following equation:

$$Recovered_{LL1} = inv\_IntDCT(Huffman_{decoded}) \tag{17}$$

The quality of the recovered approximation exactly matches the approximation of the original image because of using the error correcting code i.e. BCH codes. The BCH sequences of bit pattern (watermark before BCH encoding) with size greater than the original bit pattern (watermark after BCH encoding) include the error correcting bits. Different pairs of BCH codes produce different size of the watermark. In final experiments of our technique, the BCH code pair i.e. (31, 16, 3) where 16 are actual bits, 31 are physical bits and 3 bits are to be corrected for each 31 bits, produces better results compared to the other BCH codes that are used throughout in our experiments. The codes (31, 16, 3) and (127, 64, 10) gives almost same result. A trade-off between the imperceptibility and error correction strength has been made while selecting the BCH codes. The strength of the watermark in the proposed technique varies according to the selection of BCH codes as shown in Table 1. The *Lena* image is used as test image.

2.2.3. Tamper detection and localization

The affected coefficients in the altered watermarked image are scattered in the detail subbands. If the erroneous/affected coefficient belongs to group x then all the other non-affected coefficients of group x are also considered as erroneous coefficients. The locations corresponding to the tampered region will have high density as shown in Fig. 3.

Table 1
Behavior of the proposed approach by using different BCH codes.

BCH code pairs	PSNR	Survival level against JPEG compression (%)
(31, 16, 3)	43.24	85
(31, 11, 5)	36.18	80
(127, 64, 10)	42.20	90
(127, 43, 14)	35.27	80
(255, 187, 9)	42.75	95
(255, 179, 10)	39.43	85

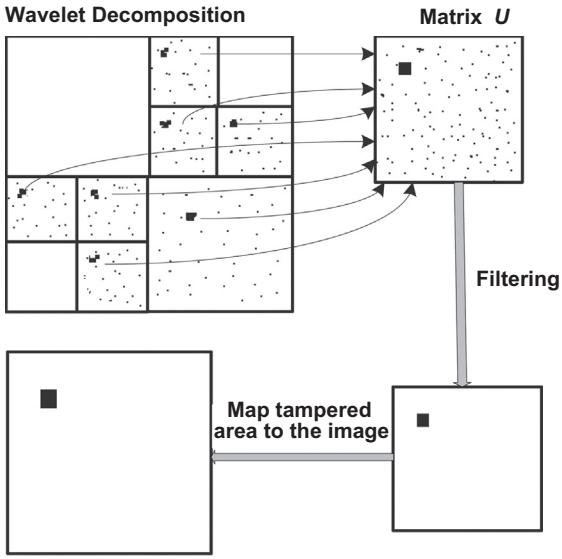

Fig. 3. Illustration of authentication process.

This is because when the sequence map back to the original position in the subbands, the tampered/unverified coefficients converges together and all other, correct coefficients, which are considered as unverified coefficients, are scattered sparsely. The matrix U is constructed and $U(m, n)$ is considered as unverified coefficients according to the following equation:

$$U(m,n) = \begin{cases} 0 & \textit{if any of } HL1(m,n), LH1(m,n) \textit{ and } DD1(m,n) \textit{ is unverified} \\ 1 & \textit{otherwise} \end{cases} \tag{18}$$

where $HL1(m, n)$, $LH1(m, n)$, and $DD1(m, n)$ are the detailed subbands at first level wavelet decomposition as shown in Fig. 4. The black pixels are erroneous pixels i.e. '0', and the white are correct pixels i.e. '1'. The two parameters *Dense* and *Sparse* pixels are used to differentiate the incidental and malicious manipulation. The *Dense* pixels are the error pixels whose one of its neighboring pixels is also an error pixel. On the other hand, the *Sparse* pixels are the error pixels whose neighboring pixels are correct pixels. If the matrix U contains no black (error) pixel, then to-be-checked image has not been altered. On the other hand, if the matrix U contains *sparse* pixels then the image is tampered incidentally otherwise maliciously. In Fig. 3,

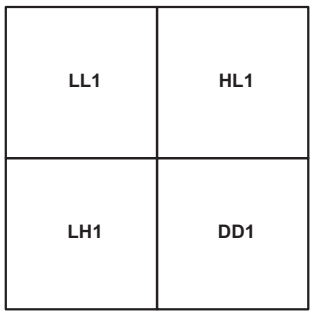

Fig. 4. The wavelet subbands after first decomposition.

high density unverified coefficients correspond to the tampered regions and all other black pixels are correct but belongs to the unverified groups. The noise filter is then applied to pick out the tampered regions. If the attacker attacked on the to-be-authenticated image in transform domain, then our technique is able to detect the tampering but localization of tampering region is not possible because the transform domain have one-to-many relationship with spatial domain.

3. Experimental results

A set of grayscale test images has been chosen for experimental work. The technique is implemented in MATLAB 2009b environment. The group size *g*, the quantization parameter used for correlation purpose *QC* and quanta used in watermark generation and embedding *Q* are set according to the requirement of the application. Large group size means low strength watermark and thus high imperceptibility, and vice versa. Similarly, quanta *Q* vary according to the survival of the technique against JPEG compression i.e. large quanta means survival against high compression and vice versa. Quantization parameter *QC* makes sure the correlation of the extracted watermark with approximation of the to-be-checked image. The visual quality of to-be-authenticated and to-be-checked images is very similar because of watermark with low capacity watermark and the selection of appropriate wavelet coefficients for embedding watermark bits.

The proposed technique has been compared with the previous approaches [17,26] with respect to watermark strength (PSNR). These approaches use dual watermarks and are able to detect the manipulations and make the recovery possible from the altered image, but at the cost of imperceptibility. Similarly, in [30], the author use single semi-fragile watermark for the authentication and recovery, but the single watermark has high strength as well as it cannot authenticate the image concisely. However, in the proposed approach, accurate authenticity and high quality recovery had been made by using single dual-purpose semi-fragile watermark. Table 2 demonstrates the comparison of our approach with [17,26,30].

Table 2
Prominent features and performance comparison with previous approaches.

Features	Ref. [17]	Ref. [30]	Ref. [26]	Proposed approach	Supporting results
Watermark payload	High	Low	Low	Very low	Section 2.1.1
Watermark security	Satisfactory	No	Satisfactory	Highly secure	Section 2.1.1
Tamper detection	Good	Satisfactory	Block-based	Good	Figure ure9, Section 2.2.2
Localization	Accurate	Inaccurate	Block-based	Highly accurate	Figure ure9, Section 2.2.2, 2.2.1
PSNR	Reasonable	Good	Good	Better	39 + db – 43 + db
Compression acceptance	Yes	Yes	Yes	Yes (user control)	*Q* is defined
Collage attack resiliency	No	No	No	Yes	Eq. (3)
Attack classification	Yes	No	Yes	Yes	Section 2.2.3
Image recovery	Yes	Yes	No	Yes	Section 2.2.2

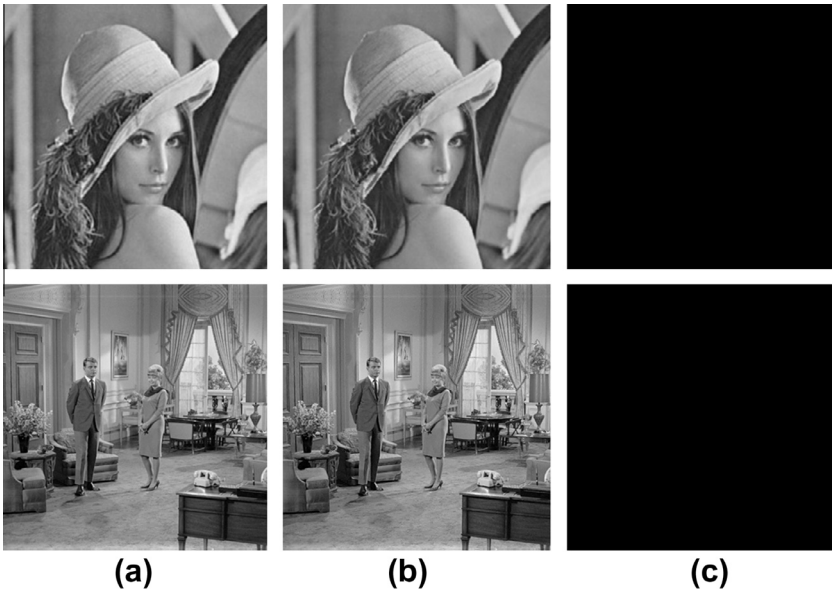

Fig. 5. (a) JPEG compressed watermarked images, (b) recovered approximation images, and (c) difference images, the difference have been taken between the extracted and the original authentication watermarks.

3.1. Effect of JPEG compression

Fig. 5 shows the watermarked images that are compressed (85%) and then recovered. The difference between $Watermark_{final}$ and $Watermark'_{final}$ are shown correspondingly. The usefulness of the approach presented in this paper is that, the embedded watermark is semi-fragile with low payload and has tolerance towards JPEG compression. The watermark $Watermark_{final}$ checks the authenticity and proves that the image is not being tampered maliciously. In addition, $Watermark_{final}$ is used to recover the exact version of the image approximation as well. The detail is given in Section 2.2.2. It can be observed that proposed approach can obtain the exact version of the compressed host image even when the watermarked image is attacked with JPEG lossy compression. A single semi-fragile watermark is used to authenticate and recover the image instead of using two watermarks as discussed in [25,26].

3.2. Authentication/recovery verses imperceptibility

The proposed approach is compared with the [25,30] based on imperceptibility. The image can be authenticated accurately and can be recovered but with the cost of imperceptibility, because two watermarks are used independently for both

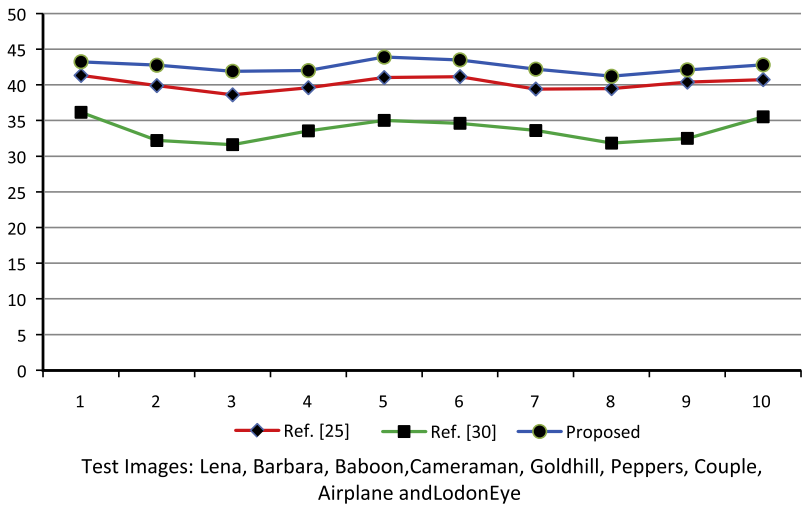

Fig. 6. Comparison of proposed approach with [25] and [30] based on PSNR. Ten different test images are used in this experiment.

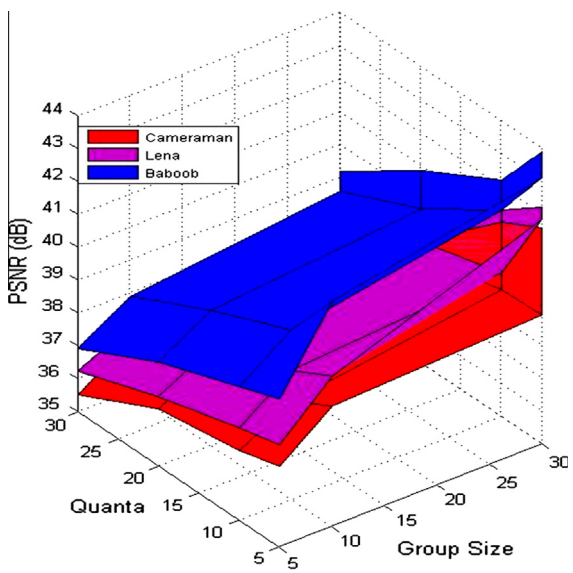

Fig. 7. PSNR versus ***Quanta***, with different ***Group Size*** on three different images i.e. ***Camereman***, ***Lena*** and ***Baboon***.

the purposes. In [30], a single watermark is used to authenticate and recover the image but at the cost of imperceptibility and authentication. In the proposed approach, a single watermark is used to authenticate and recover the image without any cost of imperceptibility and authenticity. We can accurately authenticate and recover the image. Fig. 6 shows that the PSNR (Peak Signal to Noise ratio) is much better as compared to other approaches.

3.3. Imperceptibility against different parameters

Variations in PSNR against different *Quanta* and *Group size* is illustrated in Fig. 7. The PSNR is determined empirically. One can see that when the *Group size* increases, the PSNR increase, while increasing *Quanta*, PSNR decreases and vice versa.

Moreover, as the watermarks are embedded in high magnitude wavelet coefficients of a group, the PSNR for highly textured images i.e. *Baboon* image is high. The embedding strength of the watermarks for the proposed scheme is lower than the other approaches proposed in [25,26,30].

3.4. BER - Bit Error Ratio

BER against different JPEG quantization factors is demonstrated in Fig. 8. The comparison is performed with Kundur's method [11] and Liu's method [29]. All the approaches are subjected to JPEG compression with different quality factors. We observe that the number of erroneous bits is low for the proposed approach until a high JPEG compression of 30%. The reason for this is that the suitable image features have been selected for embedding the watermark bits.

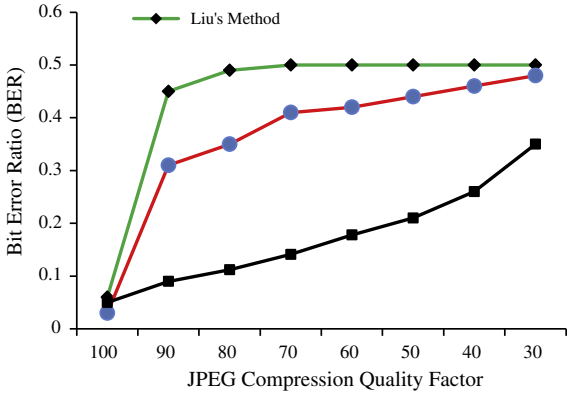

Fig. 8. BER against different JPEG quantization factors for Kundur and Hatzinakos [11], Liu and Steinebach [29] and proposed approach.

Table 3
Number of dense and sparse pixels using different frequency content based images. Corresponding JPEG quality factor (QF) is given.

Quanta	QF	Camereman		Lena		Baboon	
		Dense	Sparse	Dense	Sparse	Dense	Sparse
$Q = 30$	60	3014	765	517	1646	23	56
	65	2743	987	313	1609	0	80
	70	1732	1029	170	1524	0	47
	75	454	1310	24	1340	0	27
	80	79	829	15	1115	0	16
	85	23	584	0	818	0	11
	90	0	212	0	506	0	6
	95	0	89	0	199	0	2
	100	0	7	0	26	0	0
$Q = 20$	60	3312	471	560	1688	34	67
	65	2987	762	431	1635	12	76
	70	1723	1241	297	1583	0	34
	75	562	1421	89	1399	0	23
	80	123	1285	36	1120	0	12
	85	23	756	15	830	0	4
	90	2	412	0	517	0	1
	95	0	178	0	265	0	0
	100	0	37	0	147	0	0

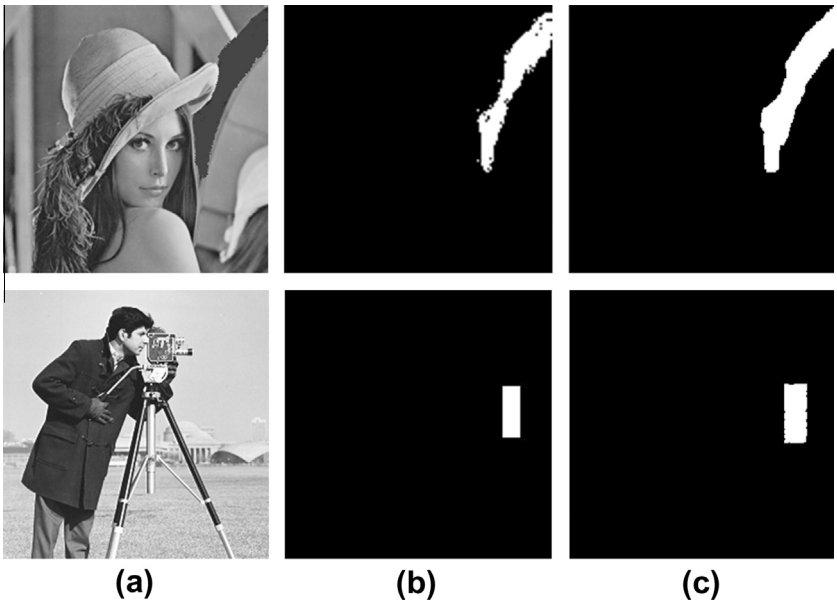

Fig. 9. (a) Tampered watermarked images of ***Lena*** and ***Camereman***, (b) tampered regions are determined and localized obviously by Proposed approach, and (c) proposed by Li and Yuan [31].

3.5. Error pixels with respect to image textures

In Table 3, we observe that, number of *Dense* and *Sparse* pixels after applying JPEG compression for *Lena* and *Cameraman* images are almost same. This is because they have roughly same amount of smooth and textured regions. However, the *Baboon* image is more textured compared to the *Lena* and *Cemeraman* images and thus gives better results. The images with high textured regions in major area can accept the high JPEG compression. The parameters; *Dense* and *Sparse* pixels have been used to check the strength and behavior of the attack (incidental or malicious). When the image is compressed beyond the defined level, then the number of *Dense* pixels becomes much higher and thus, considered as a malicious attack.

3.6. Malicious tampering and its localization

Fig. 9 shows the watermarked image that has been tampered maliciously. The *Lena* image is tampered on the right top and the building is replaced by the background color in the *Cameraman* image. The difference, Fig. 9b shows that the images are tampered maliciously. The modifications are in high strength, thus the recovery bits are modified and the recovery of the image is not possible in this case. The BCH decoder can recover the bits but up to some extent i.e. JPEG compression or tiny malicious modification. The proposed algorithm is strongly capable to localize the tampered regions instead of traditional block based approaches [19,31–33], where only blocks are located. The proposed technique is able to detect every erroneous pixel instead of erroneous block because image features are highly secured. The comparison analysis of the proposed approach is carried out with Li and Yuan [31] with respect to the resolution of tamper localization as shown in Fig. 9c. In [31], a trade-off has been made between the tamper localization, security and watermark embedding distortion. The resolution of tamper localization varies according to the watermark payload. It can be observed from Fig. 9b that the proposed

Fig. 10. (a) Original image, (b) recovered image after no distortion, (c) recovered image after JPEG compression with 80%, and (d) recovered image after jpeg compression with high ratio (the compression is beyond the pre-defined scope).

approach has more effective tamper localization resolution (No expansion of altered region as compared to Li and Yuan [31], Fig. 9c).

3.7. Exact recovery after some distortion

In Fig. 10, we see that the images are recovered after distortion and without distortion. In (b) and (c), the images are recovered after no distortion and after JPEG compression respectively. In this case, the strength of the compression is within the scope. However, in (d), the image is recovered after JPEG compression with high ratio and we see that it is not readable. In this case, the compression strength is out of pre-defined scope. We have discussed earlier that in the proposed technique, the Huffman coding is used to compress the image, therefore the quality of the recovered image will be either exactly match the original image approximation or will be unreadable.

4. Analysis

Some of the issues that affect the performance of the algorithms are g, QC and Q that can be set empirically. The imperceptibility, robustness and capacity vary according to the values of above parameters. Similarly, another issue is the availability of secret keys and type of wavelet transform on the receiving side. Both are supposed to be available at the receiving side. The technique proposed in this paper is

- able to detect tampered regions concisely and localize it accurately by using very low strength watermark (the PSNR for different images is above 42 dB. For more textured images like Baboon image, the PSNR is near to 44 dB),
- able to resist compression and recover the embedded image exactly after compression,
- able to differentiate the incidental and malicious manipulations,
- able to detect the collage/counterfeiting attack.

The performance comparison has been exhibited in Table 2, where the proposed approach is compared with some previous approaches with respect to number of features like watermark payload, watermark security, robustness, recovery, localization, and attacks resiliency.

5. Conclusion

In this paper, we have proposed a dual-purpose semi fragile watermark to authenticate the digital image along with the recovery after distortion. The watermark, which has been correlated with the host image itself, is embedded in the suitable coefficients of respective subbands. The correlation of the watermark make it capable to detect the collage/counterfeiting attacks. Unlike the conventional block-based approaches, the proposed approach has the ability to verify the digital image concisely. Before embedding, the watermark is being compressed by using the Huffman coding and then BCH code is applied on the Huffman coded coefficients for correcting the erroneous bits on the verification side. The correction rate varies according to the BCH pairs used. A trade-off between imperceptibility and robustness has been made while selecting the wavelet coefficients for embedding the watermark bits. BCH code is also selected based on imperceptibility and robustness. Integer DCT has been used because integer DCT coefficients can be compressed at high rate as compared to the conventional DCT contents. The proposed approach exhibits the flexibility between the three contradictory requirements of watermarking, i.e. imperceptibility, robustness, and capacity i.e. this approach have the ability to concisely determine the tampered region with no sacrifice on the imperceptibility. In addition, integer wavelet transform has been exploited to reduce the computational complexity of the algorithm.

References

[1] Cox J, Miller ML, Bloom JA, Fridrich J, Kalker T. Digital watermarking and steganography. 2nd ed. Elsevier; 2008.
[2] Hsieh MS, Tseng DC. Hiding digital watermarks using multi-resolution wavelet transform. IEEE Trans Ind Electron 2001;48(5):875–82.
[3] Seo YH, Choi SY, Park SH, Kim DW. A digital watermarking algorithm using correlation of the tree structure of DWT coefficients. IEICE Trans Fundam Electron Commun Comput Sci 2004;E87-A(6):1347–54.
[4] Suthaharan S, Kim SW, Lee HK, Sathananthan S. Perceptually tuned robust watermarking scheme for digital images. Pattern Recogn Lett 2000;21(2):145–9. Elsevier Science.
[5] Khan A. Intelligent perceptual shaping of a digital watermark, PhD thesis. Faculty of Computer Science and Engineering, Ghulam Ishaq Khan Institute of Engineering Sciences and Technology Pakistan; 2006.
[6] Khan A. A novel approach to decoding: exploiting anticipated attack information using genetic programming. Int J Knowl-Based Intell Eng Syst 2006;10(5):337–47.
[7] Khan A, Tahir SF, Majid A, Choi TS. Machine learning based adaptive watermark decoding in view of an anticipated attack. Pattern Recogn 2008;41:2595–610. Elsevier Science.
[8] Shieh C-S, Huang HC, Wang FH, Pan JS. Genetic watermarking based on transform-domain techniques. Pattern Recogn 2004;37:555–65. Elsevier Science.
[9] Kim HS, Baek Y, Lee HK, Suh YH. Robust image watermark using radon transform and bispectrum invariants. Lect Notes Comput Sci 2003;2578:145–59. Springer.
[10] Liu J-L, Lou DC, Chang MC, Tso HK. A robust watermarking scheme using self-reference image. Comput Stand Interface 2006;28(3):356–67. Elsevier.

[11] Kundur D, Hatzinakos D. Digital watermarking for telltale tamper proofing and authentication. Proc IEEE 1999;87(7):1167–80.
[12] Yu D, Sattar F, Barkat B. Multiresolution fragile watermarking using complex chirp signals for content authentication. Pattern Recogn 2006;39(5):935–52. Elsevier Science.
[13] Lin PL, Huang PW, Ping AW. A fragile watermarking scheme for image authentication with localization and recovery. In: Proceedings of the IEEE sixth international symposium on multimedia, software engineering (ISMSE'04); 2004.
[14] Yang Y, Bao F, Deng RH. Flexible authentication of images. In: Visual communication and image processing conference; 2003.
[15] Chi KH, Li LCT. Semi-fragile watermarking scheme for authentication of JPEG images. In: Proc international conference on information technology: coding and, computing (ITCC'04); 2004.
[16] Ko CC, Huang CH. A novel semi-fragile watermarking technique for image authentication. In: Proc 6th IASTED international conference on signal and image processing (SIP'04); 2004.
[17] Chamlawi R, Khan A, Idris A. Wavelet based image authentication and recovery. J Comput Sci Technol 2007;22(6):795–804. Springer.
[18] Campisi P, Kundur D, Hatzinakos D, Neri A. Compressive data hiding: an unconventional approach for improved color image coding. EURASIP J Appl Signal Process 2002;2002(2):152–63.
[19] Lin CY, Chang SF. Semi-fragile watermarking for authentication of JPEG visual content. In: Proc. of SPIE; 2000.
[20] Hu YP, Han DZ. Using two semi-fragile watermarks for image authentication. In: Proceedings of the fourth international conference on machine learning and cybernetics, Guangzhou, China; 2005.
[21] Liu H, Lin J, Sun J, Huang YS. Image authentication using content based watermark. IEEE; 2005.
[22] Hung KL, Chang CC, Chen TS. Secure discrete cosine transform based technique for recoverable tamper proofing. Opt Eng 2001;40:1950–8.
[23] Li KF, Chen TS, Wu SC. Image tamper detection and recovery system based on discrete wavelet transformation .In: Proceedings of the international conference on communications, computers, and signal processing, IEEE; 2001.
[24] Radhakrishnan R, Memon N. On the security of the digest function in the SARI image authentication system. IEEE Trans Circ Syst Video Technol 2002;12(11):1030–3.
[25] Chamlawi R, Khan A. Digital image authentication and recovery: employing integer transform based information embedding and extraction. Inform Sci 2010;180(24):4909–28. Elsevier.
[26] Chamlawi R, Khan A, Usman I. Authentication and recovery of images using multiple watermarks. Comput Electr Eng 2010;36(3):578–84. Elsevier.
[27] Koji S, Miki H, Hideo K. Image coding using full-frame DCT. J Joho Shori Gakkai Kenkyu Hokoku 1999;99(5):43–8.
[28] Ishihara N, Abe K. A Semi fragile watermarking scheme using weighted vote with sieve and emphasis for image authentication. IEICE Trans Fundam 2007;E90-A(5):1045–54.
[29] Liu H, Steinebach M. Semi-fragile watermarking for image authentication with high tampering localization capability. In: Proceeding of the second international conference on automated production of cross media content for multi-channel distribution, IEEE; 2006.
[30] Piva A, Bartolini F, Caldelliy R. Self recovery authentication of images in DWT domain. Int J Image Graph 2005;5(1):149–66.
[31] Li CT, Yuan Y. Digital watermarking scheme exploiting non-deterministic dependence for image authentication. Opt Eng 2006;45(12):1–6.
[32] Kilburn D. Dirty linen, dark secrets. ADWEEK; 1997.
[33] Koz A. Digital watermarking based on human visual system. Department of Electrical and Electronic Engineering, Middle East Technical University 2002.

RAFI ULLAH receives his MS degree in computer system engineering from GIKI in 2006. He receives his PhD degree in computer and information sciences from PIEAS Islamabad in 2010. He completed his post-doc research in from UTP Malaysia in 2012. He is currently working as assistant professor in COMSATS, Islamabad. His research areas include multimedia security and medical imaging.

ASIFULLAH KHAN receives his MS and PhD degrees in computer system engineering from GIK Institute Pakistan in 2003 and 2006 respectively. He completed his post-doc research in GIST South Korea in 2008. He is currently working as associate professor in PIEAS Islamabad. His research areas include image processing, machine learning, pattern recognition, and bioinformatics.

AAMIR SAEED MALIK receives his MS in information and communication and PhD degrees in information and mechatronics from GIST South Korea in 2003 and 2007 respectively. He is currently working and associate professor in the department of electrical and electronic engineering UTP Malaysia. His research areas include image processing, computer vision, pattern recognition and brain signals.