Multimedia Tools and Applications (2021) 80:25107–25119
https://doi.org/10.1007/s11042-021-10879-z

Fragile watermarking for image authentication based on DWT-SVD-DCT techniques

Thai-Son Nguyen [1]

Received: 24 August 2020 / Revised: 19 November 2020 / Accepted: 30 March 2021 /
Published online: 13 April 2021

Abstract
Many fragile watermarking schemes for image authentication have been proposed to protect the integrity of digital images. However, these schemes still yielded unsatisfactory image quality of the watermarked images and low accuracy of tamper detection. In this paper, we propose a new, fragile watermarking scheme for image authentication based on the combination of discrete wavelets transform (DWT), singular value decomposition (SVD), and discrete cosines transform (DCT) algorithms. The feature coefficients are extracted and are used to embed the authentication code by using the quantization index modulation (QIM) process. To guarantee that the extracted authentication code is correct, the Gram-Schmidt process is used to adjust the feature coefficients. The experimental results demonstrated that the proposed scheme provides good quality watermarked images and achieves high accuracy of tamper detection under different attacks, i.e., direct cropping and object insertion attacks.

Keywords High quality · Image authentication · Tamper detection · Fragile watermarking · DWT-SVD-DCT

1 Introduction

With the rapid development of the Internet and multimedia applications, a great amount of digital data, i.e., images, videos, audio, and text, is transmitted through the Internet each second. Such transmitted data can be easily infringed by illegally copying, editing, or tampering with the data using image processing software. Therefore, protecting the integrity

Highlights
- The feature coefficients are extracted and are used to embed the authentication code.
- The scheme provides good quality watermarked images.
- High accurate tamper detection is achieved under various attacks.

✉ Thai-Son Nguyen
thaison@tvu.edu.vn

[1] School of Engineering and Technology, Tra Vinh University, Tra Vinh, Tra Vinh Province, Vietnam

and the privacy of digital images has become an increasingly important issue in both academia and industry [8, 10–12, 21, 22]. Digital watermarking is a popular technique that is used to protect the integrity and the privacy of digital images [27], and it can be classified into three categories, i.e., robust, semi-fragile, and fragile watermarking. Robust watermarking [1, 9, 19] is used to resist intentional and accidental malicious attacks, while semi-fragile watermarking [2, 15, 18, 24, 26] is used to counter to some content-preserved manipulations, i.e., Gaussian noise and JPEG compression. Fragile watermarking [3–7, 13, 14, 16, 17, 20, 25] is very sensitive to any modifications. Even performing a minor operation on the image will destroy the embedded watermark. Two of many important applications of robust watermarking are to protect copyrights and digital forensics. In contrast, the main use of the other two techniques is to protect the integrity of digital images. The major purpose of this paper is to concentrate on fragile watermarking for image authentication.

In the last few decades, several fragile algorithms for image authentication have been proposed in both the spatial and transform domains to detect tampered regions in watermarked images [3–7, 13, 14, 16, 17, 20, 25]. The schemes based on the spatial domain embed the watermark into pixels of the host images by directly modifying a group of pixels with the goal of preserving the high image quality of the watermarked images. However, schemes based on the transform domain, i.e., vector quantization (VQ), block truncation coding (BTC), discrete cosines transform (DCT), and discrete wavelets transform (DWT), transform the host images into coefficients and use them to carry the watermark. Many of the earlier studies were performed in the spatial domain [4, 16]. In 2011, Chan [4] utilized hamming code for image authentication. He rearranged the bits of pixels to construct parity check bits that can be used to reconstruct the value of the pixel exactly when a pixel was modified by an attacker. To further improve the quality of watermark images, a new fragile watermarking scheme was proposed by Qin et al. that used both image hashing and the folding operation [16]. The low-frequency component of the non-subsampled contourlet transform coefficients is used to encode the restoration bits in their scheme, and they obtained good quality reconstructed images.

In addition to schemes based on the spatial domain, some recent fragile watermarking studies also were implemented in the transform domain [3, 5–7, 13, 14, 17, 20, 25]. In 2011, Chuang and Hu [5] used vector quantization as an image authentication scheme to verify tampered regions in the watermarked images. In this scheme, two sets of authentication codes are used to verify the modifications and achieve accurate tamper detection. Qin et al. [17] combined traditional VQ and inpainting techniques to restore watermarked VQ-compressed images after tamper detection. The complexity of each block is calculated to determine whether the VQ technique or the inpainting technique was used to generate the restoration bits. Hu et al. [6, 7] proposed two new schemes for block truncation coding-compressed (BTC-compressed) images instead of using VQ-compressed images for fragile watermarking and tamper detection. However, the image quality of these two schemes was unsatisfactory; the PSNR values for various images were always less than 41 dB. To increase the quality of the watermarked BTC-compressed images in [6, 7], Nguyen et al. [13] used a reference table to embed the authentication code into BTC-compressed images. This reference table also is required in the watermark extraction phase. The quality of the watermarked images was increased significantly. Nguyen et al.'s scheme maintained PSNR values greater than 42 dB for various test images. Later on, Tiwari et al. [20] proposed new image authentication and tamper detection algorithm by using VQ mechanism. In Tiwari et al.'s scheme, to obtain the high localization accuracy, the robust zero level watermark using properties of indices of vector quantized image is embedded into the cover image. Then, the watermark is embedded

by using modified index key based algorithm. However, this scheme suffered the image quality limitation, approximately 42 dB. To improve the image quality of watermarked image, Azeroual and Afdel [3] proposed novel tampered detection scheme based on fragile watermarking and Faber-Schauder wavelet. Their scheme obtained the average PSNR greater than 51 dB. To improve the accuracy of tamper detection and the quality of watermarking image, Peng et al. [14], applied two identical host images, where one image contains the secret data while the other image is used to embed the distortion information. In Peng et al.'s scheme, the SOS algorithm [23] is used construct the reference matrix for embedding watermark. However, this scheme offered low image quality, when the average PSNR is smaller than 50 dB.

In this paper, a fragile watermarking scheme for image authentication is proposed to improve the image quality provided by previous schemes and to achieve highly accurate tamper detection. Three algorithms, i.e., the DWT algorithm, the SVD algorithm, and the DCT algorithm, were considered carefully to extract the feature coefficients for carrying the authentication code. The authentication code is generated by a pseudo-random generator with a secret key K. Then, quantization index modulation (QIM) is used to embed the authentication code into the feature coefficients. To guarantee that the same authentication code is extracted in the watermark extraction, the Gram-Schmidt process is used to adjust these coefficients. The experimental results indicated that the proposed scheme achieved high visual quality of watermarked images and provided highly accurate tamper detection under different attacks, i.e., direct cropping and object insertion attacks.

The rest of this paper is organized as follows. Section 2 provides the details of the proposed fragile watermarking scheme. Our experimental results and the performance of the proposed scheme are presented in Section 3. In Section 4, our conclusions are presented to summarize the main contributions of the proposed scheme.

2 The proposed scheme

The proposed scheme consists of two main phases, i.e., the watermark embedding phase and the watermark extraction phase. These two phases are discussed in detail in Subsections 2.1 and 2.2, respectively.

2.1 Watermark embedding phase

In this subsection, the host image is partitioned into non-overlapping 8×8 blocks. Then, we use 1-level DWT [25] to decompose each of the image blocks into four different coefficient sub-bands, i.e., *LL, HL, LH*, and *HH*, as shown in Fig. 1. In principle, most of energy of a grayscale image is concentrated on the low-frequency sub-band, thus the authentication code is embedded into this sub-band to protect it against to accidental modifications. However, altering the *LL* sub-band for embedding authentication degraded the host image significantly. To avoid this shortcoming, we use both SVD and DCT to extract suitable features from the *LL* sub-band for the embedding authentication code.

The *LL* sub-band is divided into non-overlapping blocks with the size of 4×4. Then, the SVD algorithm is used to decompose each block further by using Eq. (1).

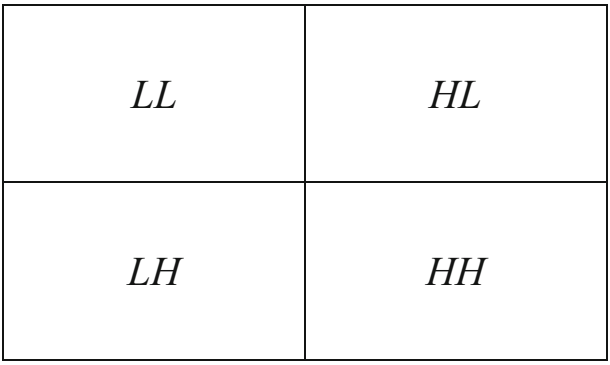

Fig. 1 Discrete wavelet transform algorithm

$$\mathrm{A} = \mathrm{USV}^{\mathrm{T}} = \begin{bmatrix} | & | & | & | \\ u_1 & u_2 & \mathrm{u}_3 & u_4 \\ | & | & | & | \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ 0 & 0 & \lambda_3 & 0 \\ 0 & 0 & 0 & \lambda_4 \end{bmatrix} \begin{bmatrix} | & | & | & | \\ v_1 & v_2 & v_3 & v_4 \\ | & | & | & | \end{bmatrix}^T, \quad (1)$$

where S is a diagonal matrix that contains all non-negative, real, singular values $\lambda_k{}'$s, and U and V are the left and right unitary matrices, respectively, that consist of the singular vectors u_k *and* v_k. Since the image layer with the larger singular value, i.e., λ_1 $u_1 v_1^T$, is less affected by digital signal processing (DSP) attacks, it is used to embed the authentication bits. Then, we use a one dimensional (1-D) DCT on both matrices, i.e., U and V, by using Eq. (2):

$$\begin{gathered} \mathrm{DCT(i,j)} = \mathrm{C(i)} \times \mathrm{C(j)} \times \sum_{x=1}^{N} \sum_{y=1}^{N} pixel(x,y) \times \cos\left[\frac{(2x+1)i\pi}{2N}\right] \cos\left[\frac{(2y+1)j\pi}{2N}\right]; \\ N = 8; pixel(x,y) \text{ are values of matrix } U \text{ or } V \\ \mathrm{C(i)}, \mathrm{C(j)} = \begin{cases} \sqrt{\dfrac{1}{N}} & for\ i,j = 1 \\ \sqrt{\dfrac{2}{N}} & for\ i,j = 2,3,\ldots,N. \end{cases} \end{gathered} \quad (2)$$

The authentication code is embedded by modifying either the DCT coefficients of $DCT_{u_1}(k)$ *or* $DCT_{v_1}(k)$ in the middle index range, e.g., $k = 2$ or 3, by using the QIM technique. It is noted that, in the proposed scheme, thanks to the value of k a embedding set E is generated by four elements, i.e.,$DCT_{u_1}(2), DCT_{v_1}(2), DCT_{u_1}(3)$ and $DCT_{v_1}(3)$, defined as $E = (E_0, E_1, E_2, E_3)$. Therefore, to improve the security of the proposed scheme, one more secret key SK is needed for generating a pseudo random number generator R. Then, one element E_{pos} is selected from the embedding set E for containing the authentication code, where $pos = R_i \bmod 4$. By doing so, the security of the proposed scheme is guaranteed. Figure 2 shows the main processes of the proposed watermark embedding phase.

The input variables are a grayscale host image H and a secret key K. The output is a watermarked image. The watermark embedding phase consists of seven steps as followings:

Step 1: Partition the image H into 64×64 non-overlapping blocks $B_{m,n}(i,j)$ for $i = 1, 2, \cdots, 8$ and $j = 1, 2, \cdots, 8$, and each block consists of 8×8 pixels. The authentication code

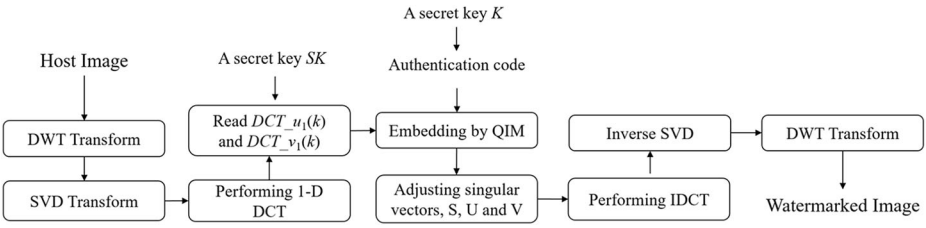

Fig. 2 Main processes of the watermark embedding phase

W in binary form is generated randomly by a pseudo-random number generator with the secret key K.

Step 2: Apply the 1-level 2-D DWT transform to generate four sub-bands, i.e., *LL, LH, HL*, and *HH*. Then, Eq. (1) is used to decompose each 4 × 4 block of low-frequency sub-band *LL* further by SVD algorithm, thereby obtaining two matrices, i.e., U and V.

Step 3: Apply 1-D DCT of u_1 and v_1 to get two DCT sequences, i.e., $DCT_{u_1}(k)$ *and* $DCT_{v_1}(k)$.

Step 4: Use the QIM technique to embed the authentication code bit w_b = {0, 1} into the coefficient $DCT_{u_1}(k)$ *or* $DCT_{v_1}(k)$, where $k = 2$ or 3:

$$\begin{aligned} \widehat{DCT_{u_1}}(k) &= 2\left\lfloor \frac{DCT_{u_1}(k)}{2} \right\rfloor + w_b, \\ \widehat{DCT_{v_1}}(k) &= 2\left\lfloor \frac{DCT_{v_1}(k)}{2} \right\rfloor + w_b. \end{aligned} \tag{3}$$

Step 5: Adjust the singular vectors as follows. After embedding, the inverse DCT is used to obtain two new singular vectors, $\widehat{u_1}$ *and* $\widehat{v_1}$. Since coefficients u_1 and v_1 are modified to $\widehat{u_1}$ and $\widehat{v_1}$, leading the orthogonal relationship in two matrices U and V is also altered. To ensure that $\widehat{u_1}$ *and* $\widehat{v_1}$ are extracted exactly in order to determine the corrected embedded authentication code, the Gram-Schmidt algorithm is used according to the value of $\{\widehat{u_1}, u_2, u_3, u_4\}$ and it is defined in Eq. (4).

$$\begin{aligned} \breve{u_j} &= \frac{\widehat{u_j}}{\sqrt{\left(\widehat{u_j^T} \cdot \widehat{u_j}\right)}}; \quad j = 1,2,3,4; \\ \widehat{u_i} &= u_i - \sum_{j=1}^{i-1} \left(u_i^T \cdot \breve{u_j}\right) \cdot \breve{u_j}\,; i = 2,3,4. \end{aligned} \tag{4}$$

Because the orthonormal property had to be held for matrix V, Eq. (4) is applied to $\{\widehat{v_1}, v_2, v_3, v_4\}$ as well. Before decomposing by SVD, let A *b*e sub-band *LL*,

$$\beta_1 = \lambda_1 \sqrt{\widehat{u_1^T u_1}} \sqrt{\widehat{v_1^T v_1}} \text{ , and } B = A - \beta_1 \widetilde{u_1} \widetilde{v_1^T}.$$

Along with the modification of matrices U and V, the singular values in matrix S must be modified as follows:

$$\beta_i = arg \min_{\lambda_i'} \left\{ \left\| A - \left(\beta_1 \widetilde{u_1} \widetilde{v_1^T} + \sum_{i=2}^{4} \lambda_i' \widetilde{u_i} \widetilde{v_i^T} \right) \right\|_F^2 \right\}$$

$$= arg \min_{\lambda_i'} \left\{ \left\| B - \sum_{i=2}^{4} \lambda_i' \widetilde{u_i} \widetilde{v_i^T} \right\|_F^2 \right\};$$

$$\beta_i = \widetilde{u_i^T} B \widetilde{v_i}, for\ i = 2,3,4,$$

where ||.|| is the Frobenius norm. After adjustment with the values of

$$\widetilde{u_i}'s,\ \widetilde{v_i}'s, and\ \beta_i's$$

, the reconstructed image block is computed by Eq. (7):

$$A' = \sum_{i=1}^{4} \beta_i \widetilde{u_i} \widetilde{v_i^T} = \lambda_1 \widehat{u_1} \widehat{v_1^T} + \sum_{i=2}^{4} \beta_i \widetilde{u_i} \widetilde{v_i^T}.$$

Step 6: Replace each block in *LL* by the value of A'.

Step 7: Obtain the watermarked image by using the 1-level inverse DWT with the new *LL* sub-band, and the three original sub-bands, i.e., *LH, HL*, and *HH*.

2.2 Watermark extraction phase

When an image, which is suspected to have been tampered from the watermarked image, is published on the Internet, the watermark extraction algorithm is used to detect whether or not any regions in this image have been tampered. The watermark extraction algorithm is designed to be as simple as possible and to represent a replica of the watermark embedding algorithm. Figure 3 shows the flowchart of the proposed watermark extraction phase.

In the watermark extraction algorithm, the three first steps are done in the same manner that was used in the watermark embedding algorithm. Then, two DCT coefficients, i.e., $\widehat{DCT_{u_1}}(k)$ and $\widehat{DCT_{v_1}}(k)$, are determined, and the authentication code bits w_b's are extracted by Eq. (8):

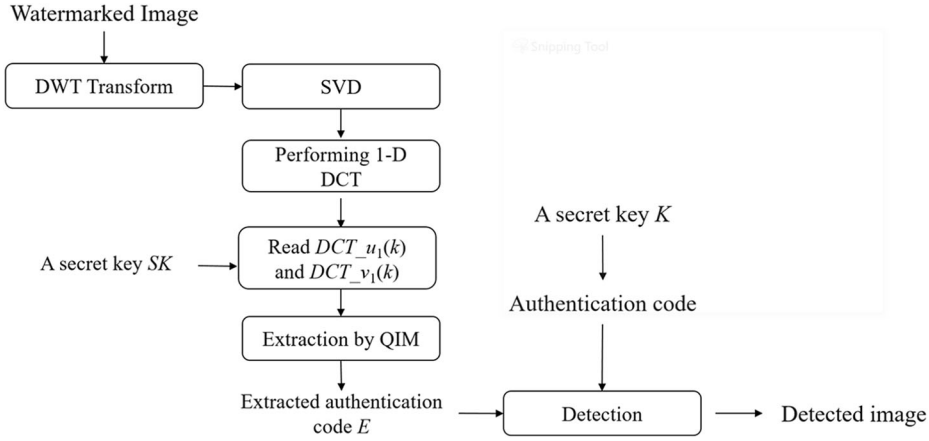

Fig. 3 Flowchart of the watermark extraction phase

$$w_b = \widehat{DCT}_i \; mod \; 2, \tag{8}$$

where $\widehat{DCT}_i$ denotes the DCT coefficient, that is determined based on the secret key SK as was done in the watermark embedding phase.

After obtaining the extracted authentication code bit w_b, according to the secret key K, we reconstruct the original authentication code W to detect whether or not the watermarked image block has been tampered. Then, the corresponding authentication code bit w of W is read and compared with the extracted authentication code bit w_b. If $w_b = w$, the current block is marked as a legal block, meaning that no modifications have been performed in the current block; otherwise, it is marked as an illegal block.

The mentioned processes discussed above are implemented repeatedly until the entire image is detected completely. The detected image is obtained by gathering all the legal and illegal blocks.

The detected image should be processed further by the refinement method to enhance its accuracy. Specifically, the refinement method is performed on the detected image several times. Each time, the refinement method divides the detected image into non-overlapping 3×3 blocks. Then, each white block is tested to see whether or not its color has been changed to black color. Fig. 4 shows four conditions, i.e., Con1, Con2, Con3, and Con4, that may occur in this refinement method, with B being the current white test block. Taking Con1 in Fig. 4a as an example, if the top-left and bottom-right adjacent blocks of B are black, the color of B will be

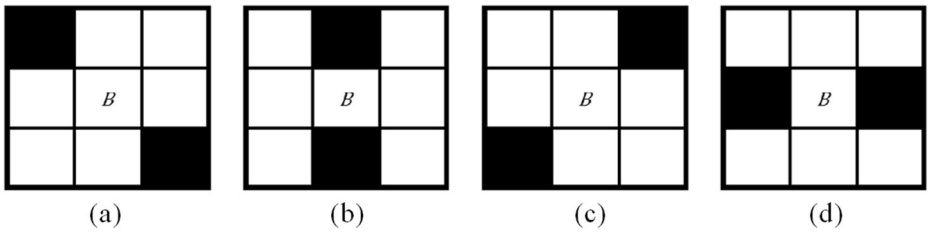

Fig. 4 Four conditions of the refinement method. **a** Con1, **b** Con2, **c** Con3, **d** Con4

modified to black. The refined detected image cannot be obtained until all of the white blocks in the detected image have been tested.

3 Experimental results

In this section, five 512 × 512 images, i.e. Lena, Peppers, Boat, Barbara, and Airplane serve as the host images to illustrate the performance of the proposed scheme.

The peak signal-to-noise ratio (PSNR) was used to measure the image quality of watermarked images and PSNR is calculated as

$$PSNR = 10\log_{10}\left(\frac{255^2}{(1/M)\sum_{i=1}^{M}\left(I_i - I_i'\right)^2}\right), \tag{9}$$

where M is the size of the watermarked image, and I_i and I'_i are the pixel values of the original image and the watermarked image, respectively.

Figure 5 shows the five test images before and after embedding the authentication code. It is obvious that the watermarked images of the proposed scheme have great quality, the values of PSNR always were greater than 84 dB for the images.

To evaluate the proposed scheme's accuracy of tamper detection, the watermarked images were subjected to two different attacks, i.e., a cropping attack and an object insertion attack. The results are shown in the following two subsections.

3.1 Results of direct cropping

To simulate this attack, a certain region was deleted from the watermarked image. Figure 6 shows examples of the direct cropping attack on three watermarked images, i.e. Lena, Airplane, and Peppers. Figures 6a, c, and e depict the enlarged part of three watermarked images with cropped blocks with the sizes of 8 × 8, 16 × 16, and 32 × 32, respectively. Figure 6 shows that the proposed scheme succeeded in detecting this type of attack, and the detected images are shown clearly in Figs. 6b, d, and f, since a normalized correlation coefficient (NCC) always was greater than 0.99. Even when the cropped block is very small in size (Fig. 6a), the proposed scheme presented highly precise localization capacity, as shown in Fig. 6b.

3.2 Results of object insertion

A common attack is the cut-and-paste attack, which also is referred as the object insertion attack. In this attack, the attacker intentionally can cut one region from another image and paste it somewhere in the wall of watermarked images. Figure 7 shows the results of object insertion attacks with various sizes of tamper objects. Figures 7a and b illustrate the case in which relatively small-sized objects (a pepper or a flower) were inserted into the watermarked images, Peppers and Lena. These insertions, resulted in a normalized correlation coefficient (NCC) larger than 0.85. NCC is used to measure the similarity between the refined detected image and the tampered image, and it is defined by Eq. (10):

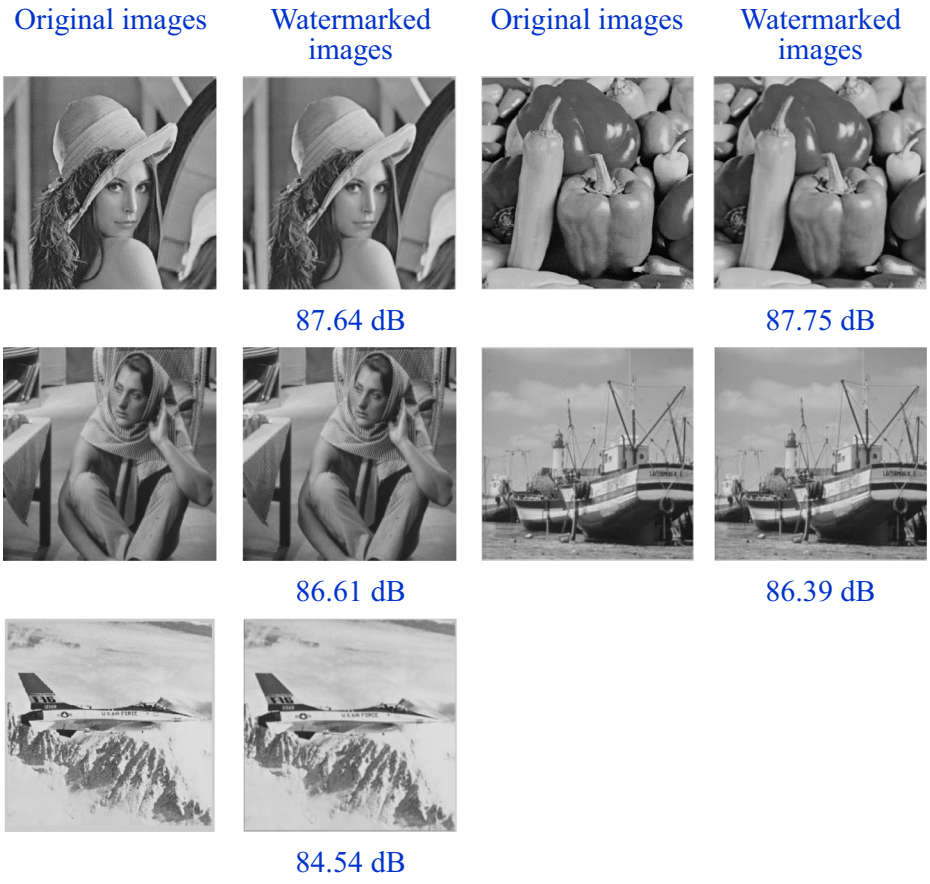

Fig. 5 Illustrations of images before and after the authentication code was embedded

$$\mathrm{NCC} = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W}\left[I_{i,j}-I_{mean}\right]\left[D_{i,j}-D_{mean}\right]}{\sqrt{\left(\sum_{i=1}^{H}\sum_{j=1}^{W}\left[I_{i,j}-I_{mean}\right]^2\right)\left(\sum_{i=1}^{H}\sum_{j=1}^{W}\left[D_{i,j}-D_{mean}\right]^2\right)}}, \tag{10}$$

where I denotes the tampered object in binary form, I_{mean} is the mean value of all of the pixels in image I. D is the refined detected image and D_{mean} is the mean value of all of pixels in image D.

Figure 7c shows the case in which a medium-sized object was added, and Fig. 7d presents the case in which a large-sized object was added. Definitely, the proposed scheme always provided the highest value of NCC. It was evident that the proposed scheme has the ability to detect all inserted objects with a high accuracy of tamper detection, as is clearly demonstrated in these figures.

To demonstrate the superiority of the proposed scheme, we compared the proposed scheme to recent image authentication schemes [14, 18–20]. In Table 1, in addition to five above mentioned images, five more general grayscale test images, i.e., Baboon, GoldHill, House, Sailboat, Elaine, are tested to further evaluate the effectiveness of the proposed scheme. It can be seen in Table 1 that first column shows different techniques are applied for either fragile or

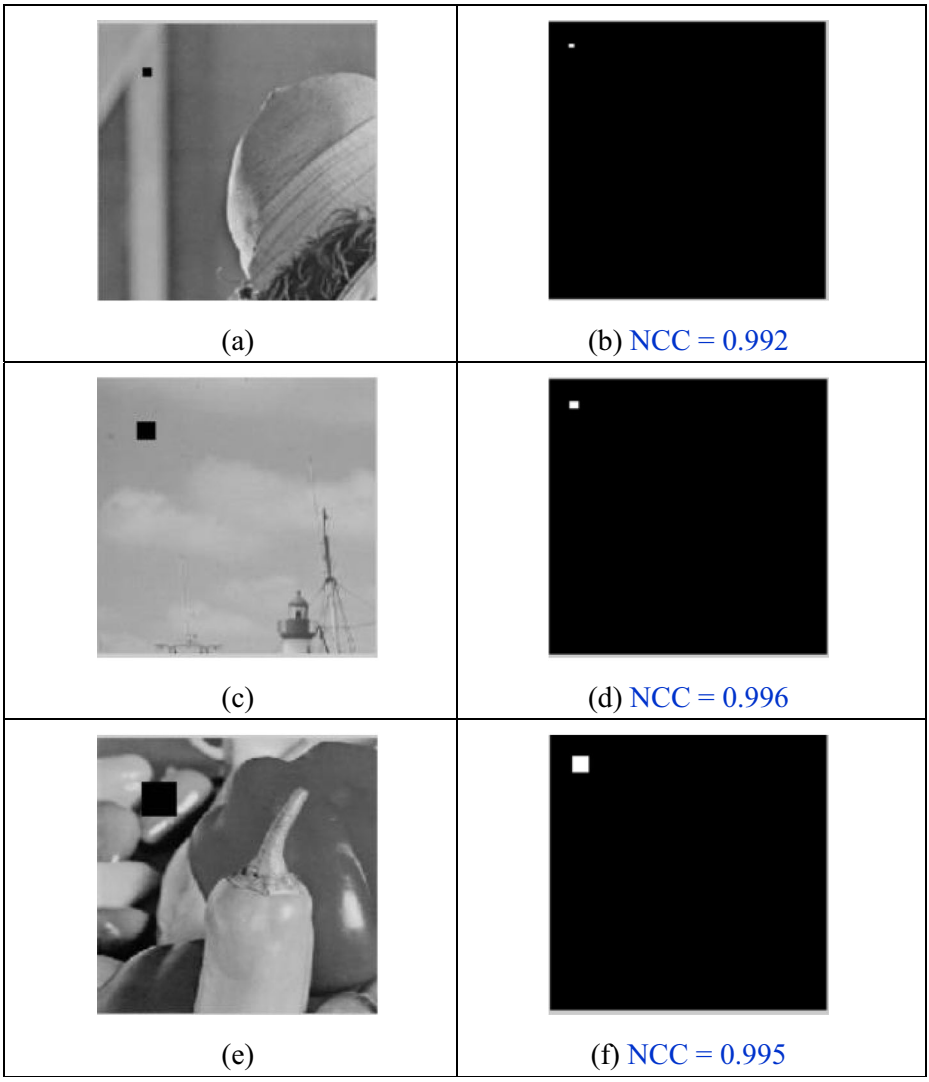

Fig. 6 Illustration of direct cropping attack and tamper detection results

semi fragile watermarking algorithm. Subsequently performance evaluation matrices such as average PSNR of watermarked images, similarity between the refined detected image and the tampered image and localization capacity are compared. The proposed scheme obtained average PSNR = 84 dB, NCC = 0.893, very high efficiency of tamper detection /localization. The schemes proposed by other authors achieved good PSNR, but the average PSNR obtained by the proposed scheme is dramatically higher than those of other four schemes. All algorithms are able to locate tamper but Tiwari et al.'s scheme [20] obtained the highest average NCC among five schemes. However, the average NCC of the proposed scheme is still better than other three schemes [14, 18, 19]. Moreover, average execution time is measured while all computing was performed on a computer with Intel i3 processor @ 1.7 GHz, 4GB DDR RAM and Windows 10 OS. In the Table 1, the average execution times required by our scheme and

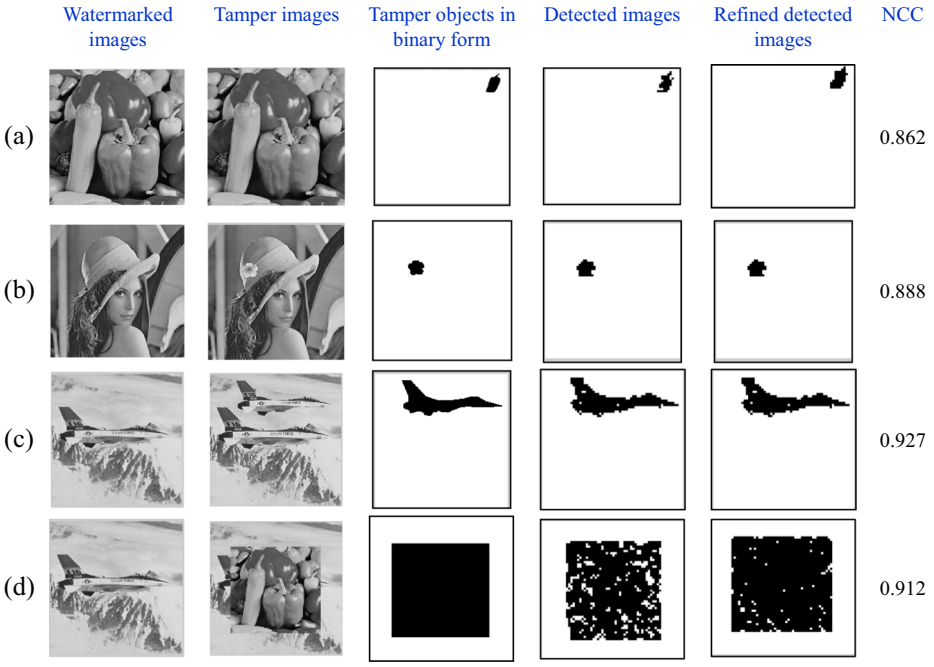

Fig. 7 Illustration of object insertion attack and tamper detection results

the four existing schemes [14, 18–20] are presented. Obviously, Tiwari et al.'s scheme [20] requires the highest computation time, followed by the proposed scheme, Shojanazeri et al.'s scheme [18], Singh et al.'s scheme [19], and then Peng et al.'s scheme [14]. Tiwari et al.'s scheme is the worst one. This is because Tiwari et al.'s scheme takes much more time than others for two stage VQ coding. However, overall proposed algorithm is having superiority in terms of imperceptibility, exact extraction of embedded watermark, high accuracy in tamper detection.

Table 1 Performance comparison of the proposed scheme with four recent image authentication schemes [14, 18–20]

Schemes	Techniques	Average PSNR(dB) of watermarked image	Similarity factor (Average NCC)	Tamper detection/ Accuracy	Average execution time (in second)
Singh et al. [19]	DCT based technique	39	0.727	Medium	2.92
Shojanazeri et al. [18]	DWT and Zernike moments	41	0.765	Medium	3.14
Tiwari et al. [20]	Two stage VQ technique	42	0.908	High	6.03
Peng et al. [14]	SOS technique	48	0.876	High	1.19
Proposed scheme	DWT-SVD-DCT techniques	84	0.893	High	5.67

4 Conclusions

A novel fragile watermarking scheme for image authentication was proposed in this paper. The advantages of using the DWT, SVD, and DCT algorithms were explored to select the features coefficients. Then, the authentication code was generated and embedded in these features using the QIM technique. The Gram-Schmidt process was used to adjust these coefficients to ensure that the embedded authentication code was extracted exactly. The experimental results indicated that the proposed scheme provided highly accurate tamper detection under different attacks, i.e., direct cropping and object insertion attacks. In addition, the proposed scheme achieved watermarked images with dramatically high visual quality while maintaining the high accuracy of tamper detection.

Acknowledgements This research is funded by Tra Vinh University for Science and Technology Development under grant number **207**/HĐ.HĐKH-ĐHTV.

References

1. Abdelhakim AM, Saleh HI, Nassar AM (2017) A quality guaranteed robust image watermarking optimization with artificial bee Colony. Expert Syst Appl 72:317–326
2. Al-Otum HM (2014) Semi-fragile watermarking for grayscale image authentication and tamper detection based on an adjusted expanded-bit multiscale quantization-based technique. J Vis Commun Image Represent 25(5):1064–1081
3. Azeroual A, Afdel K (2017) Real-time image tamper localization based on fragile watermarking and Faber-Schauder wavelet. AEU Int J Electron Commun 79:207–218
4. Chan CS (2011) An image authentication method by applying hamming code on rearranged bits. Pattern Recogn Lett 32(14):1679–1690
5. Chuang JC, Hu YC (2011) An adaptive image authentication scheme for vector quantization compressed image. J Vis Commun Image Represent 22(5):440–449
6. Hu YC, Chen WL, Lo CC, Wu CM (2013) A novel tamper detection scheme for BTC compressed images. Opto-Electron Rev 21(1):137–146
7. Hu YC, Lo CC, Chen WL, Wen CH (2013) Joint image coding and image authentication based on absolute moment block truncation coding. J Electron Imag 22(1):1–12
8. Kumar C, Singh AK, Kumar P (2020) Dual watermarking: An approach for securing digital documents. Multimed Tools Appl 79:7339–7354
9. Liao X, Li K, Liu K. J. R (2020) Robust Detection of Image Operator Chain With Two-Stream Convolutional Neural Network IEEE J Sel Top Sig Process, vol. 14, no. 5
10. Liao X, Yin JJ. Chen ML, Qin Z (2020) Adaptive payload distribution in multiple images steganography based on image texture features IEEE Transactions on Dependable and Secure Computing
11. Luo L, Chen Z, Chen M, Zeng X, Xiong Z (2011) Reversible image watermarking using interpolation technique. IEEE Trans Infor Forens Secur 5(1):187–193
12. Mansouri A, Mahmoudi-Aznaveh A (2019) Toward a secure video watermarking in compressed domain J Inf Secur Appl, vol. 48
13. Nguyen TS, Chang CC, Chung TF (2014) A tamper-detection scheme for BTC-compressed images with high-quality images. KSII Trans Inter Infor Syst 8(6):2005–2012
14. Peng Y, Niu X, Fu L, Yin Z (2018) Image authentication scheme based on reversible fragile watermarking with two images. J Inf Secur Appl 40:236–246
15. Preda RO (2013) Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain. Measurement 46(1):367–373
16. Qin C, Chang CC, Chen PY (2012) Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism. Signal Process 92(4):1137–1150
17. Qin C, Chang CC, Chen KN (2013) Adaptive self-recovery for tampered images based on VQ indexing and inpainting. Sig Process 93(4):933–946

18. Shojanazeri H, Adnan WAW, Ahmad SMS, Rahimipour S (2017) Authentication of images using Zernike moment watermarking. Multimed Tools Appl 76:577–606
19. Singh D, Singh SK (2017) DCT based efficient fragile watermarking scheme for image authentication and restoration. Multimed Tools Appl 76:953–977
20. Tiwari A, Sharma M, Tamrakar RK (2017) Watermarking based image authentication and tamper detection algorithm using vector quantization approach. AEU – Int J Electron Commun 78:114–123
21. Vo PH, Nguyen TS, Huynh VT, Do TN (2020) A high-capacity invertible steganography method for stereo image. *Digit Media Steganography Princ Algorithm Adv Acad Press*:99–122
22. Wang XT, Chang CC, Nguyen TS, Li MC (2013) Reversible data hiding for high quality image exploiting interpolation and direction order mechanism. Digit Sig Process 23(2):569–577
23. Yin Z, Chang C, Xu Q, Luo B (2015) Second-order steganographic method based on adaptive reference matrix. IET Image Process 9(4):300–305
24. Zhang W, Frank YS (2011) Semi-fragile spatial watermarking based on local binary pattern operators. Opt Commun 284(16–17):3904–3912
25. Zheng P, Zhang Y (2020) A robust image watermarking scheme in hybrid transform domains resisting to rotation attacks. Multimed Tools Appl 79:18343–18365
26. Zhu X, Ho ATS, Marziliano P (2007) A new semi-fragile image watermarking with robust tampering restoration using irregular sampling. Signal Process Image Commun 22(5):515–528
27. Zhu BB, Swanson MD, Tewfik AH (2004) When seeing isn't believing multimedia authentication technologies. IEEE Sig Process Mag 21(2):40–49