Wu *EURASIP Journal on Image and Video Processing* (2017) 2017:13
DOI 10.1186/s13640-017-0163-8

EURASIP Journal on Image
and Video Processing

RESEARCH Open Access

Quantization-based image authentication scheme using QR error correction

Wen-Chuan Wu

Abstract

Image authentication, which is provided with capabilities of tamper detection and data recovery, is an efficient way to protect the contents of digital images. Vector quantization (VQ) is a data compression method. A VQ-compressed code is not only a significant image authentication feature but also applicable in restoring possibly damaged pixels. However, if an image is tampered with, the necessary recovery information disappears. To solve this problem, this paper proposes a quantization-based image authentication scheme using two-dimensional (2D) barcodes to protect important features. Compared with older linear barcodes, 2D barcodes are a machine-readable representation of binary data that possess capabilities of location and tolerance. This paper presents a method for incorporating VQ-compressed code into 2D barcodes and embedding those barcodes into the image itself. Experimental results showed that VQ codes can be completely reserved during data recovery even though quick response codes sustain certain perceptible distortions. Moreover, the proposed scheme provided higher quality authenticated and recovered images compared with previous methods.

Keywords: Image authentication, Tamper detection, QR code, Error correction, Vector quantization coding

1 Introduction

Because of the extremely rapid advancements in computer technology and the Internet, an increasing number of people use digital devices, mobile phones, and tablets for data communication. As a result, more and more image and video data are emerged [1]. People cannot only deliver but access multimedia data anywhere on the Internet in a short time. These multimedia data, especially the images and videos, are frequently used in computer vision application, for instance, feature detection, object recognition [2], visual surveillance [3], photo clustering, and virtual navigation in photos [4, 5]. However, some security issues exist because of open unsafe networks. Data transmitted over networks are regularly subject to active attacks [6], such as the erasing and tampering of documents or images. Destructive modifications often cause the content of multimedia data to be inaccurate and further incur the difficulty or considerable errors for subsequent computer vision application.

In general, cryptographic methods are applied to protect the security of digital data by using encryption keys. Without the correct key, illegal attackers cannot acquire the original data. However, encryption and decryption procedures are time-consuming processes, and they are thus not suitable for high-volume multimedia data [7], digital images, and videos. Image authentication [7, 8] is one of the techniques for protecting the content integrity of digital images from malicious and unauthorized modification. Image authentication technology can detect and indicate any changes or tampered regions in a tampered image. Image authentication schemes are classified into two categories: active authentication [8–18] and passive authentication [19–21] schemes. The active authentication scheme involves extracting particular features of the image beforehand and then concealing them within the image itself, whereas the passive authentication scheme entails authenticating images with no prior information requirement. The active image authentication approach is also called fragile watermarking [12], which involves hiding a watermark in an image. The hidden watermark is highly sensitive to any modifications in the image such that it becomes fragile and even unrecognizable when the image is modified. Hence, specific locations that have been illegally modified can easily be indicated using these broken areas.

Correspondence: au4387@au.edu.tw
Department of Computer Science and Information Engineering, Aletheia University, 32 Zhenli St., Taipei 25103, Taiwan

Wong and Memon [16] proposed the public key fragile watermarking scheme for image authentication. This scheme applies block pixels, block index, and other related information to produce a signature as authentication data. Chen and Wang [12] applied a fuzzy c-means clustering technique to build the relationship between blocks for image authentication. In addition, Wu and Ren [8] proposed a scheme that entails using distinctive rules of a Sudoku puzzle to create authentication data. Chan [9] rearranged image pixel bits by using the hamming code technique for detecting tampered regions. Subsequently, Chen and Chen [10] employed the coefficients in low-frequency wavelet subbands for preventing malicious tampering. The schemes that have been proposed in [14] and [15] involve applying block truncation coding and singular value decomposition, respectively, on image blocks to obtain authentication data. The aforementioned schemes are self-embedding methods of embedding the authentication data of an image into each spatial pixel bits. Moreover, all schemes provide tamper detection ability.

In addition to the described schemes, other methods with data recovery abilities are available, and such methods can restore possibly damaged regions to a state close to the original. Wang and Tsai [17] presented an automatic image authentication and recovery method applying a fractal encoding technique to the region of importance. This approach further uses the image inpainting technique to recover tampered areas for improving the quality of the recovered image. Yang and Shen [18] drew an index table through vector quantization (VQ) from the image content and used it as the important authentication and recovery data. In 2001, Wu and Hsieh [13] also used VQ coding to improve the embedded image quality. Chuang et al. [11] acquired the VQ indices for an image and then embedded multiple copies of them into other image blocks. When the image is to be authenticated, particular forward and backward detection mechanisms are designed to detect tampered regions more precisely.

In contrast to earlier studies, Chen and Chen [10] offered a distinct solution for image authentication in 2012. They employed a fashionable quick response (QR) code to protect the authentication data from being damaged or going missing. A QR code, an extension of the traditional linear barcode, is a type of two-dimensional (2D) matrix code. It introduces the vertical dimension, thus enabling the encoding of more data. Figures 1 and 2 depict images of a traditional barcode and novel QR code, respectively. Notably, a QR code consists of black and white dots arranged in a square; it also contains special position detection patterns placed in three corners [22] that enable it to be scanned from any direction and still be decoded correctly. QR codes are usually used to represent concise text, product information, and web hyperlinks. A QR code has not only a large capacity for data storage but also four levels (L, M, Q, and H) of error correction. The higher the level of error correction is, the larger the QR code size is and the greater the error correction becomes. This property enables QR codes to be read correctly even if slightly soiled or damaged. Thus, error correction renders QR codes more powerful and useful.

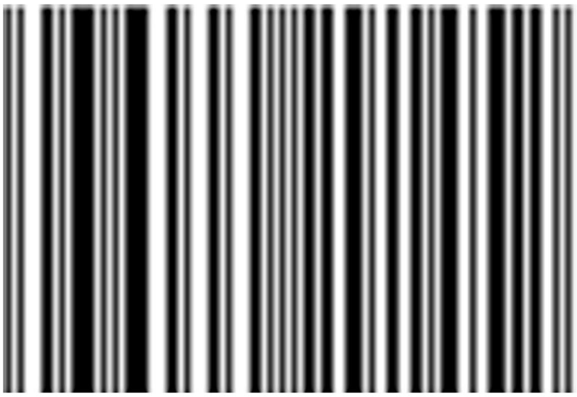


Fig. 1 Traditional barcode

Through QR codes, Chen and Chen's scheme can obtain correct authentication data to verify image integrity. However, the scheme requires the original image to indicate the tampered regions. Moreover, the scheme does not have data recovery ability. Therefore, the scheme does not make good use of the error correction property of QR codes. In this study, we developed a QR code-based image authentication scheme that applies VQ

Fig. 2 QR code for the URL "http://au.edu.tw"

indices to address this problem and improve the embedded image quality. The rest of this paper is organized as follows. Section 2 provides a review of VQ coding and some previous relevant schemes [10, 18]. Section 3 presents the proposed image authentication scheme. Section 4 presents the experimental results showing the improvement associated with using the proposed scheme. The final section presents our conclusions.

2 Related methods

The proposed scheme integrates VQ coding and QR codes to achieve image tamper detection and data recovery. Therefore, this section first reviews the basic concepts of VQ in Section 2.1. Subsequently, two relevant schemes [10, 18] of image authentication are presented in Sections 2.2 and 2.3.

2.1 VQ coding

VQ [23] is a prominent lossy data compression technique that guarantees the achievement of a satisfactory balance between image fidelity and compression ratio. Because of its easy implementation and simple decoding structure, the VQ technique has been widely used in a variety of research fields [24]. The concept of this technique is to replace original image blocks with representative patterns for the purpose of data compression. VQ comprises three procedures: (1) visual codebook generation, (2) image block quantization, and (3) index decoding. The codebook $CB = \{C_1, C_2, \ldots, C_{Nc}\}$ is a set of representative visual image vectors derived from the Linde-Buzo-Gray training algorithm [23], and each significant vector C_i is called a codeword. The generation of the codebook determines the performance of the VQ coding. VQ-based image quantization involves partitioning an image into numerous fixed-sized blocks and then comparing them with codewords in the codebook to find the closest pattern for each input vector. On the side of the VQ encoder, each of the input blocks is compressed into an index of the codebook. That index is associated with the codebook during the index decoding procedure to rapidly reconstruct the corresponding block through a table lookup operation.

Figure 3 shows the flowchart of VQ image encoding and decoding. Consider, for example, a grayscale image I of $W \times H$ pixels subjected to VQ coding. Initially, it is necessary to prepare the codebook CB containing Nc representative codewords, in which each element $C_i = (c^i{}_1, c^i{}_2, \ldots, c^i{}_k)$ is a k-dimensional vector. Next, image I is divided into several non-overlapping blocks with size $n \times n$ pixels, where $k = n \times n$, and each image block is then transformed into a vector $X = (x_1, x_2, \ldots, x_\mathrm{k})$. For block encoding, the vector X is matched with the codebook CB with the lowest distortion, which can be simply computed as follows:

$$d(C_{bt}) = \underset{\forall i}{\mathrm{Min}}\left(d(C_i) \,\middle|\, d(C_i) = \left\| c^i{}_j - x_j \right\|^2,\right.$$
$$\left. i = 1, 2, \ldots, Nc \,\mathrm{and}\, j = 1, 2, \ldots, k\right).$$

Notably, C_{bt} denotes the best-matched codeword with the shortest distance for the vector X. Therefore, the index value bt of the winner C_{bt} is recorded to replace the associated input block in order to achieve the aim of compression. The other image blocks are subsequently encoded through the same operation. The VQ encoder eventually produces a set of indices, also called an index table, to become the compressed codes of the original image I. On the opposite side, the VQ decoder uses the same codebook to translate the received index back for rebuilding the corresponding image block. That is, the decoder is required to perform only a simple table lookup operation to fetch the codewords in accordance with the indices. VQ has excellent performance with a low bit rate and a fast decoding process.

2.2 Yang and Shen's scheme

In 2010, Yang and Shen [18] proposed an image authentication scheme for recovering the tampered image using VQ indexing. This scheme regards the VQ-compressed result, which is the index table, as important recovery information and then embeds it along with authentication data into the original image. Figure 4 illustrates the flowchart of Yang and Shen's embedding procedure. At the beginning, an image is processed to clear the least significant 3 bits of each pixel into zero. Subsequently, that result is partitioned into non-overlapping $n \times n$ image blocks. Each block is sequentially compressed using a VQ encoder to produce its corresponding VQ index. Because the codeword corresponding to that index is highly similar to the image block, it can be the recovery data of that block in the later recovery procedure. To protect the security of the authentication and recovery data, Yang and Shen adopted pixel permutation to permute the embedding sequence randomly and then embedded these VQ indices into other pixel bits. Consider, for example, Fig. 4: supposed that the index value of the first block is 156, the value of which in binary is $(10011100)_2$. The eight binary bits are hidden into the permuted random pixels 12, 242, 159, and 90. Each pixel carries two binary bits of a VQ index into the second and third least significant bits (LSBs). In fact, Yang and Shen's scheme can hide t copies of a VQ index, where $t = (2 \times n \times n)/(\log_2|N_c|)$. This scheme hides authentication data (a watermark) into the first LSB by using Wong and Memon's scheme [16] to create an authenticated image.

In the tamper detection and recovery procedure, the received authenticated image is verified to determine whether it is a fake. The first step is to permute

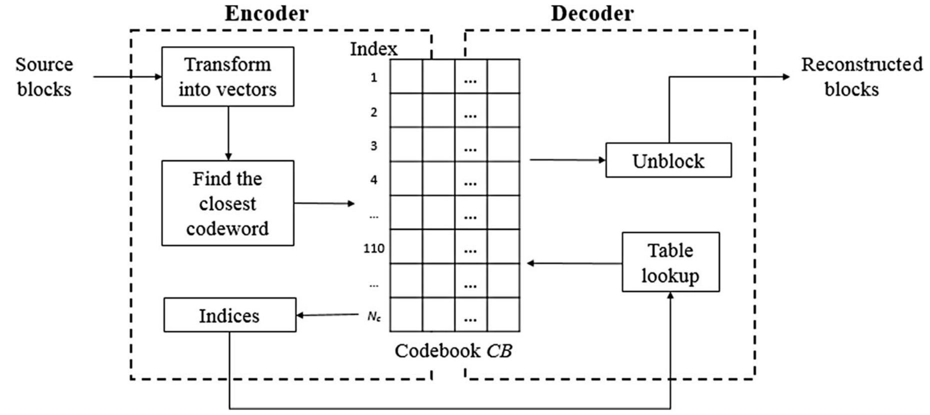
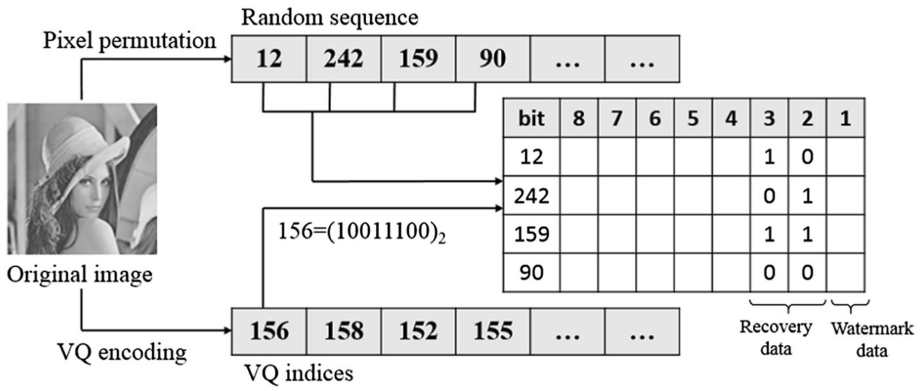


Fig. 3 Flowchart of vector quantization encoding and decoding

the pixel sequence by using the same random key and then extract three LSBs from each pixel value. The first LSBs are grouped to form an output binary watermark, which is then compared with the original watermark, just as in Wong and Memon's scheme. If the received image is modified in any way, either by changing pixel values or using an inappropriate secret key, then the extracted watermark bitmap becomes incorrect and consequently resembles random noise. The invalid block pixels can be recovered by fetching the hidden VQ indices from the preceding second and third LSBs and then decoding them. Because of lossy VQ compression, the restored image blocks are very close to the original contents. To avoid the loss of the hidden VQ bits, this scheme uses t copies of them to improve the image restoration result. However, the original watermark may be required for checking image integrity and performing the image recovery process. Moreover, the process damages three LSBs of each image pixel such that the authenticated image quality is drastically reduced.

2.3 Chen and Chen's scheme

In 2012, Chen and Chen [10] proposed a different solution to image tamper detection. They efficiently utilized the properties of data storage and strong error correction of QR codes to secure the authentication data of an image. A QR code can hold up to 700 times more data than a typical barcode can, and it can be produced in four error correction levels. With the help of error correction, the authentication data, even when tampered with, can still be completely restored without error. Figure 5 depicts the flowchart of Chen and Chen's embedding procedure. Initially, an original image is used to perform a discrete wavelet transform to extract a subband of the LL_3 block representing a coarse scale of that image. The LL_3 block is then expressed in QR code format. The authors suggested using the M error correction level and removing a few regular areas, (e.g., position detection pattern, alignment pattern, and timing pattern) to generate a smaller QR code. The remaining areas serve as the authentication data. The original image is also partitioned into several small and non-overlapping



bit	8	7	6	5	4	3	2	1
12						1	0	
242						0	1	
159						1	1	
90						0	0	

Fig. 4 Flowchart of Yang and Shen's embedding procedure

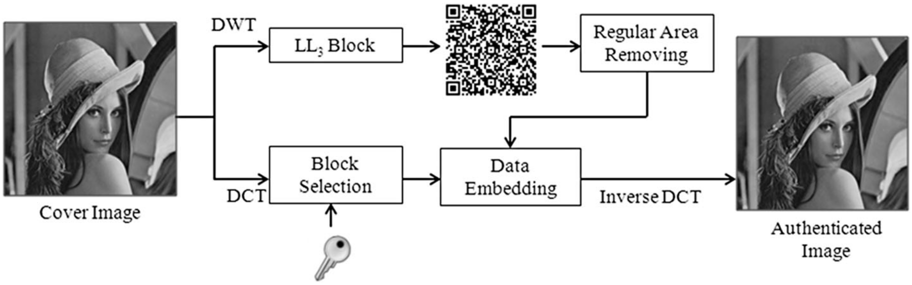


Fig. 5 Flowchart of Chen and Chen's embedding procedure

blocks, and a discrete cosine transform (DCT) is performed on each block. This scheme applied a secret key to randomly select block for data embedding. For each chosen block, only five high-frequency DCT coefficients are employed to conceal the aforementioned authentication data. After the embedding process, these blocks are finally restored to a pixel-domain authenticated image by using an inverse DCT process.

During tamper detection, this scheme mainly adopts the readability of a QR code to verify that the received authenticated image is not a fake. First, that image is processed using a DCT and the same secret key is used to retrieve the block coefficients that were already carried with authentication data. Subsequently, the extracted bits and the regular areas that were removed earlier are filled into the look of a standard QR code. If the recovered QR code is not readable, the image may have been modified maliciously. By contrast, if it is readable, the data drawn out from that code must be compared with the LL_3 block of the received authenticated image. If the two are identical, the image has not been tampered with; otherwise, that image has been modified before. Because of the advantage of error correction in QR codes, Chen and Chen's scheme can be used to verify image integrity. However, it cannot accurately locate the exact regions where the image has been tampered with, and it exhibits weak recovery capability.

3 Proposed scheme

To address the problems of the two aforementioned schemes, this section presents the proposed image authentication scheme for exploiting QR codes to protect the integrity of significant VQ authentication data. The proposed scheme involves of authentication data generation procedure, image tamper detection procedure, and content reconstruction procedure. Before the authentication data generation procedure is executed, it is necessary to prepare a grayscale image I, called the cover image, with $W \times H$ pixels to be authenticated and a VQ codebook CB with Nc codewords.

3.1 Authentication data generation procedure

The purpose of this procedure is to generate authentication data from the cover image I and then conceal them underneath. For clarity, a flowchart of this procedure is presented in Fig. 6. An LSB elimination operation is first performed to clear the least significant 1 bit (1-LSB) of each pixel to zero for future data embedding. The resulting image I is then encoded using the VQ technique, where each image block is the size of $n \times n$ pixels. The encoding result is an index table, consisting of VQ indices, and a VQ index idx_i corresponding to the ith image block. That index table is regarded as the major authentication and recovery data that must be embedded into image I. Next, an operation of block grouping is introduced to reduce the volume of the VQ index table. A group G_i is defined by

$$G_i = \{idx_m, idx_{m+1}, idx_{m+c}, idx_{m+c+1}\},$$

where

$$m = \left(\left\lceil \frac{i-1}{t} \right\rceil - 1\right) \times 2 \times c + (i-1)\%t \times 2 + 1,\ c = W/n, t = c/2.$$

Notably, each index value idx_i belongs to only one group. For example, for a 256×256 image and 4×4 blocks, there are four indices, namely idx_3, idx_4, idx_{67}, and idx_{68} in group G_2. That is, four adjacent blocks are included in the same group. From each group G_i, the value idx_m is selected and collected in a set of authentication data Au_1, whereas the value idx_{m+c+1} is collected in a set of authentication data Au_2. Subsequently, the two sets Au_1 and Au_2 are encoded into the corresponding QR code formats Q_1 and Q_2, respectively, by using a dedicated code generator. Because the capacity of QR codes is limited, the block grouping operation must be designed in the proposed scheme.

Before data embedding in image I, image blocks must be rearranged arbitrarily according to a random sequence RS by using a secret key SK. This means that the seventh image block could be first used to embed QR codes, then the fourth image block, and so on; that is, the sequence RS could be {7, 4, 15, 11, …}. This approach can increase the security of the authentication data and ensure that

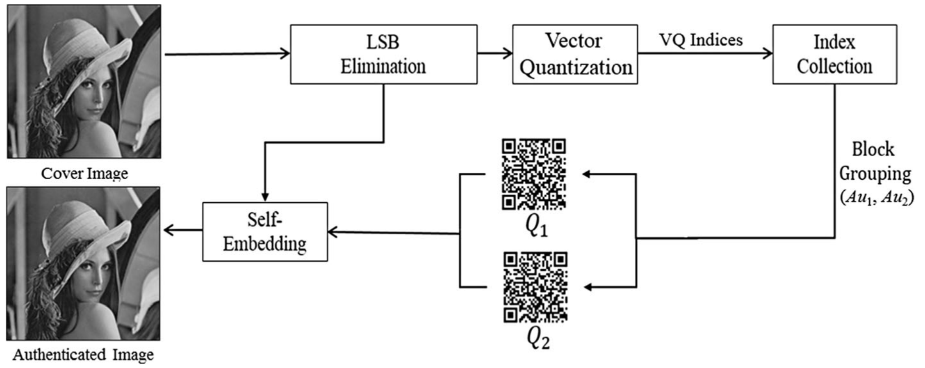


Fig. 6 Flowchart of the proposed authentication data generation procedure

modifications are widely distributed over QR codes. During the data embedding process, QR codes Q_1 and Q_2 are hidden into the 1-LSB of all pixels. If a module in QR codes is black, then an image pixel in I remains unchanged; otherwise, the 1-LSB of an image pixel is set to 1. The preceding data hiding processes are repeated until all the modules of the two QR codes are hidden into image I. Finally, an authenticated image $\bar{I}$ corresponding to the original image is generated. Only the 1-LSB of each pixel is modified; hence, the acquired image $\bar{I}$ is highly similar to the original image I. Conventionally, a QR code carrying more data capacity has a larger size. Because the size of QR modules is not proportional to the size of the cover image, we extend QR codes to enlarge part of the quiet zone so that the size of the QR codes is equal to that of the cover image.

3.2 Image tamper detection procedure

The main purpose of the tamper detection procedure is to accurately detect and mark the suspected modified regions of an authenticated image $\bar{I}^*$. Figure 7 shows the flowchart of the proposed tamper detection procedure. The first process entails dividing image $\bar{I}^*$ into numerous non-overlapping $n \times n$ blocks. These blocks are then scrambled chaotically by using the same sequence RS through key SK. The next process involves extracting the hidden data from the 1-LSB of each pixel and then combining them to form two QR codes Q_1^* and Q_2^*. The codes Q_1^* and Q_2^* carry authentication data Au_1 and Au_2, respectively, and these data can be easily acquired by subjecting Q_1^* and Q_2^* to QR decoding. Simultaneously, our scheme is also to execute the identical data generation procedure on image $\bar{I}^*$ in order to get its specific data Au_1^* and Au_2^*, where $Au_1^* = \{idx_m^*\}$ and $Au_2^* = \{idx_{m+c+1}^*\}$. Note that an index value appears only in none or one of two sets. By comparing values in the sets Au_1^* and Au_2^* with values in the sets Au_1 and Au_2 one by one, we could easily discover where the suspected tampered blocks are. If idx_m^* in Au_1^* is not equal to idx_m in Au_1, it means that the m-th block might have been tampered with already; otherwise, the m-th block is very likely correct and clear. Also, if idx_{m+c+1}^* in Au_2^* is not equal to idx_{m+c+1} in Au_2, it means that $m + c + 1$-th block might be damaged; otherwise, that block is an undamaged and clear one.

In a detected result, clear blocks are marked in white intensity whereas damaged ones are marked in black intensity. However, not all of blocks are able to be detected for content integrity. The main reason is that we introduced block grouping operation in the prior data generation procedure. Half of VQ indices is recorded only in two QR codes. Hence, an additional stage is required to detect the other blocks in $\bar{I}^*$ more accurately. The following six conditions are used to check an image block not including in

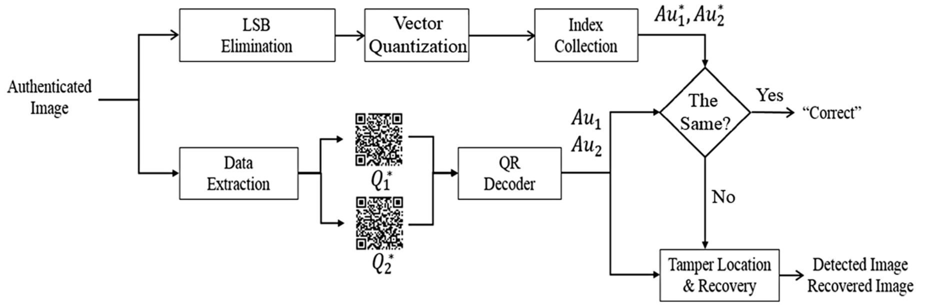


Fig. 7 Flowchart of the proposed tamper detection procedure

the two sets Au_1 and Au_2 has been modified or not. As long as one condition meets, this block will be regarded as a tampered one and marked in black intensity. Finally, we will derive a detected image of binary format. Figure 8 shows three detecting examples for different tampered blocks, in which the block drawn in black is damaged one. In case 1 of Fig. 8, they are detected as tampered ones because the fifth block meets condition 3 and the second block meets condition 4. In addition to the second and fifth blocks, for case 2, the seventh one is also tampered block on account of condition 5.

Condition 1: Neighboring blocks on left and right are both tampered.
Condition 2: Neighboring blocks on top and bottom are both tampered.
Condition 3: Neighboring blocks on top and right are both tampered.
Condition 4: Neighboring blocks on left and bottom are both tampered.
Condition 5: Neighboring blocks on top and left are both tampered.
Condition 6: Neighboring blocks on right and bottom are both tampered.

3.3 Content reconstruction procedure

After tamper detection procedure, the next process of the proposed scheme is content reconstruction procedure so as to restore the image block, especially for the suspected tampered blocks. This procedure mainly aims at the blocks marked black in the prior detected image. Initially, it is necessary to separate detected image into lots of non-overlapping $n \times n$ blocks. If an image block is black, it indicates that the block has been modified and it needs to be restored. Such modified blocks are classified into two categories: type 1 and type 2. Type For each block in type 1, its VQ index was taken down in QR codes. Owing to error correction capability of a QR code, the encoded data, VQ indices still can be restored completely and losslessly even though that code suffered from tolerable dirtied and damaged. Therefore, we can simply use the corresponding VQ indices to reconstruct the tampered blocks of type 1.

On the contrary, it is a bit hard to recover these damaged blocks in type 2 since their VQ indices are not recorded beforehand. Here, we introduced a side-match prediction to reconstruct those blocks approximately. The concept of side-match prediction is shown in Fig. 9, where the middle block X is what we want to restore and its four adjacent blocks on top, bottom, right, and left directions are U, D, R, and L, respectively. Among them, pixel values in blocks U, D, R, and L are clear or have been reconstructed already. The first step to restore block X is to predict its surrounding twelve pixels, that is x_1, x_2, x_3, x_4, x_5, x_8, x_9, x_{12}, x_{13}, x_{14}, x_{15}, and x_{16}. The computational formula about prediction are listed below:

$$x_1 = avg(l_4, u_{13}), x_2 = u_{14}, x_3 = u_{15}, x_4 = avg(r_1, u_{16}), x_5 = l_8, x_8 = r_5,$$

$$x_{13} = avg(l_{16}, d_1), x_9 = l_{12}, x_{12} = r_9, x_{16} = avg(r_{13}, d_4), x_{14} = d_2, x_{15} = d_3.$$

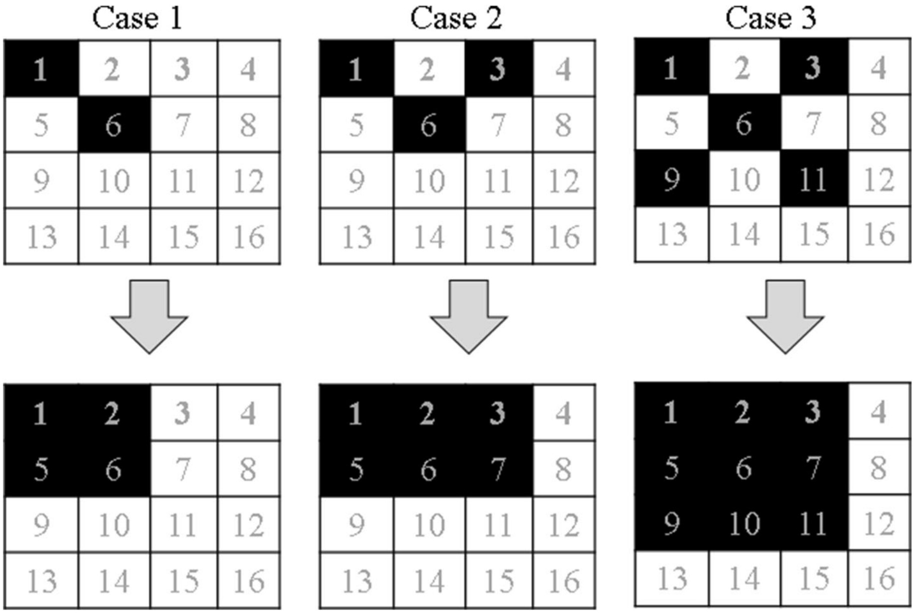


Fig. 8 Detecting example for tampered blocks

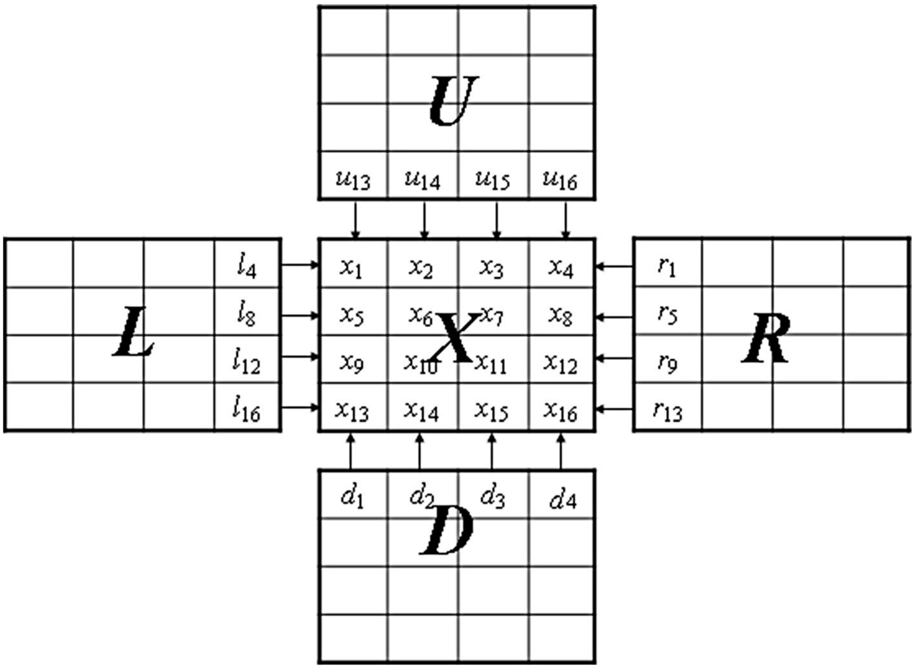

U
u_{13} u_{14} u_{15} u_{16}
L
l_4 l_8 l_{12} l_{16}
X
x_1 x_2 x_3 x_4
x_5 x_6 x_7 x_8
x_9 x_{10} x_{11} x_{12}
x_{13} x_{14} x_{15} x_{16}
R
r_1 r_5 r_9 r_{13}
D
d_1 d_2 d_3 d_4

Fig. 9 A diagram of side-match prediction

Note that notation $avg(S)$ is an average function to return the average of the arguments in the set S. Next step is for the middle four pixels, x_6, x_7, x_{10}, and x_{11}, to calculate by using the surrounding known or reconstructed pixels. Their corresponding formulas are shown below:

$$x_6 = avg(x_2, x_5), x_7 = avg(x_3, x_8), x_{10} = avg(x_9, x_{14}), x_{11} = avg(x_{12}, x_{15}).$$

Due to the image characteristic that neighboring pixels have extremely similar values, the prediction technique is considerably able to recover image content. It is

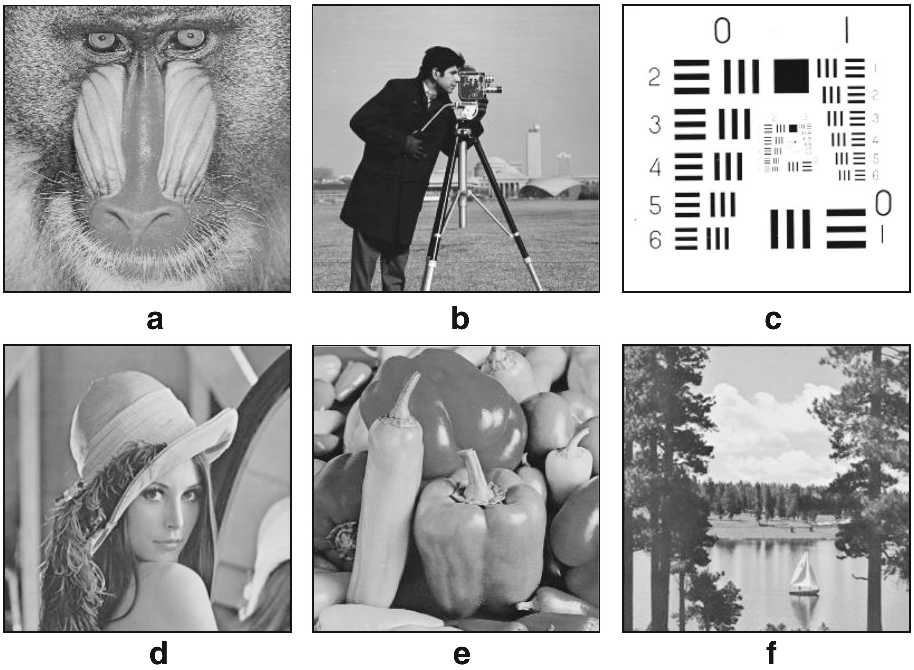


Fig. 10 Six 256 × 256-pixel test images. **a**. Baboon, **b**. Cameraman, **c**. Chart, **d**. Lena, **e**. Pepper, **f**. Sailboat

Table 1 Results for the image "Pepper" under distinct tampering attacks

Size (pixels)	Schemes	Authenticated image (dB)	Tampered image (dB)	Recovered image (dB)
15 × 15	Yang and Shen's scheme	43.13	24.92	43.00
	The proposed scheme	51.09	35.19	43.99
20 × 20	Yang and Shen's scheme	43.13	23.02	40.37
	The proposed scheme	51.09	31.24	41.45
25 × 25	Yang and Shen's scheme	43.13	21.69	39.55
	The proposed scheme	51.09	26.99	39.63
30 × 30	Yang and Shen's scheme	43.13	20.65	39.20
	The proposed scheme	51.09	26.80	37.53

evident that the predicted pixels are inexact and injured, but they are very similar to the original values in general. This way is merely unsuitable to the situation of larger tampering regions. Our scheme is necessary to repeat the two steps as mentioned above until all the tampered blocks are reconstructed and a recovered image being obtained eventually.

4 Experimental results and discussion

In our experiments, six grayscale 256 × 256-pixel images were served as test images, which are "Baboon," "Cameraman," "Chart," "Lena," "Pepper," and "Sailboat" shown in Fig. 10. Each image was performed on LSB elimination and vector quantization operations in order to generate its index table of 4096 indices, where the size of image blocks is 4 × 4 and the codebook size N_c is 256. Then, we took 2048 indices from those as the authentication code to create two QR codes (Q_1 and Q_2) of 175 × 175 pixels, where an error correction level is L. Afterward, our proposed scheme embeds two QR codes into the 1-LSB bits of that image. In order to evaluate the qualities of authenticated, tampered, and recovered images, here, the ruling metrics of peak-signal-to-noise ratio (PSNR) is adopted in the experiments. The PSNR value indicates the fidelity between original image and modified image. In general, a higher PSNR value means that the modified image has better quality. In another word, that image is extremely similar to the original image.

Tables 1 and 2 show the experimental results of two schemes for images "Pepper" and "Baboon," respectively. The authenticated images generated by using Yang and Shen's scheme [18] and our proposed scheme are all modified under distinct single tampering attacks. As shown in the two tables, the size of $m \times m$ pixels is a modifying area in a tampered image. No matter which one scheme is adopted, the larger the modifying area is, the worse the quality of tampered and recovered images will be, and vice versa. The results explicitly show that the qualities of the authenticated image in our proposed scheme reached as high as 51 dB, which is better than that of Yang and Shen's scheme. The main reason is that Yang and Shen's scheme embeds authentication data into three LSB bits of each pixel, but the proposed scheme only embeds them into one LSB bit of each pixel. On the average, in addition, our proposed scheme also produces better recovered image quality than that of Yang and Shen's scheme, especially for small

Table 2 Results for the image "Baboon" under distinct tampering attacks

Size (pixels)	Schemes	Authenticated image (dB)	Tampered image (dB)	Recovered image (dB)
15 × 15	Yang and Shen's scheme	43.45	27.76	38.67
	The proposed scheme	51.11	38.83	48.75
20 × 20	Yang and Shen's scheme	43.45	25.80	38.30
	The proposed scheme	51.11	35.59	47.25
25 × 25	Yang and Shen's scheme	43.45	24.39	35.99
	The proposed scheme	51.11	32.23	44.47
30 × 30	Yang and Shen's scheme	43.45	23.14	31.41
	The proposed scheme	51.11	30.08	40.87

Table 3 Comparisons of the schemes under two modifying artifacts

Test images	Yang and Shen's scheme [18]		The proposed scheme	
	Authenticated image (dB)	Recovered image (dB)	Authenticated image (dB)	Recovered image (dB)
Baboon	43.45	36.00	51.11	37.64
Cameraman	42.88	41.07	51.15	47.15
Chart	42.08	34.13	50.78	37.55
Lena	43.24	42.09	51.39	47.11
Pepper	43.13	41.86	51.09	37.44
Sailboat	44.14	39.79	50.98	43.88
Average	43.15	39.16	51.08	41.80

modifying areas. But, our proposed scheme will obtain a little degraded recovered results when the modifying area is getting bigger. For this reason, the proposed scheme is more suitable for small tampering areas. This is because our proposed scheme is performed based on block grouping and prediction recovery operations.

In addition to a single tampering attack, we also try to add more irregular region artifacts to the authenticated image in order to evaluate the tolerance of QR codes. Tables 3 and 4 show the comparative results of six test images using Yang and Shen's scheme and the proposed scheme, where there are two and three artifacts in each test image of Tables 3 and 4, respectively. It is obvious that the proposed scheme yields better image fidelity with higher PSNR value than the previous scheme [18] in terms of authenticated images and recovered images. Figures 11 and 12 present the subjective results based on visual quality of test images "Pepper" and "Cameraman," respectively, by using the proposed scheme. Figures 11b and 12b are the corresponding tampered image of Figs. 11a and 12a, in which we modified three irregular image areas. We observed from Figs. 11c to 12c that our scheme is able to detect and indicate tampered locations accurately without misjudgments occurred. Even though the two QR codes extracted from tampered image are a little damaged, VQ index values hidden in it still can be acquired completely to restore suspected tampered regions as well shown in Figs. 11f and 12f.

Table 5 compares the numerical results of the six test images processed using Chen and Chen's scheme [10] and the proposed scheme. The results indicate that the quality of authenticated image generated from our scheme on average is superior to that generated from Chen and Chen's scheme. Moreover, the previous scheme yields rather degraded quality for the image "chart" due to the usage of DCT frequency operation. That means that Chen and Chen's scheme is inappropriate for binary images. In addition, we also attempted to modify the authenticated images in the same manner and then perform the two schemes in order to recover image content. From Table 5, it can be clearly seen that the recovered image quality of our scheme is 41.80 dB on average, whereas Chen and Chen's scheme failed in the recovery procedure. The reason for this situation is that the previous scheme [10] adopted LL_3 subband, which represents rough contours of an image, of DWT as the authentication data. That scheme can neither locate tampering regions nor recover them. In contrast, our scheme is not only capable of accurately detecting the suspected modified areas, but almost restoring to their original states.

Table 4 Comparisons of the schemes under three modifying artifacts

Test images	Yang and Shen's scheme [18]		The proposed scheme	
	Authenticated image (dB)	Recovered image (dB)	Authenticated image (dB)	Recovered image (dB)
Baboon	43.45	34.30	51.11	35.37
Cameraman	42.88	40.54	51.15	47.05
Chart	42.08	32.63	50.78	35.98
Lena	43.24	42.04	51.39	46.99
Pepper	43.13	41.74	51.09	37.29
Sailboat	44.14	37.41	50.98	41.88
Average	43.15	39.16	51.08	40.76

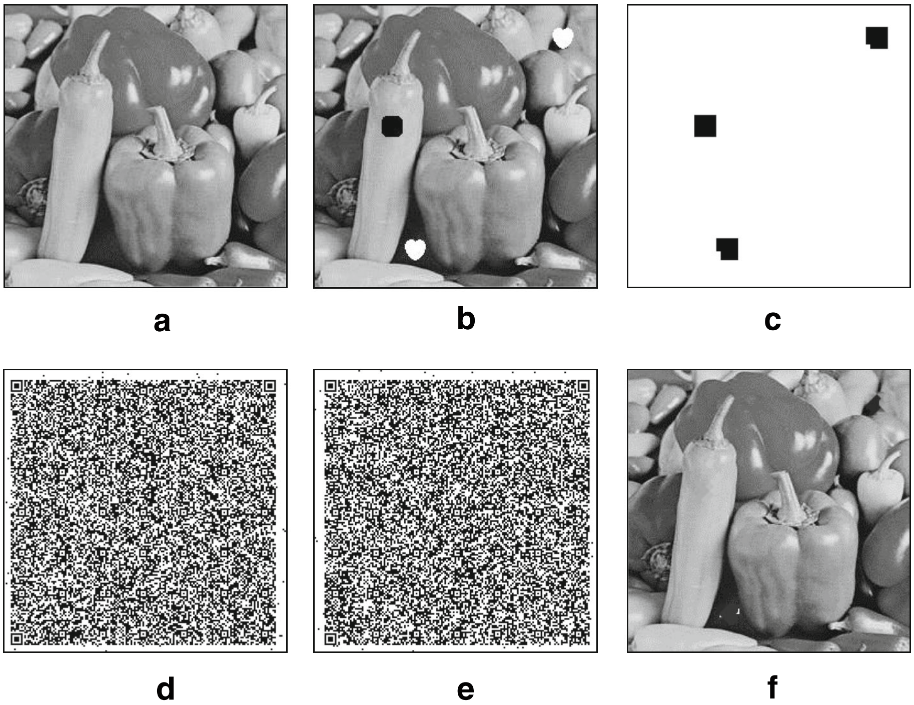


Fig. 11 Visual results of the proposed scheme for the image "Pepper". **a**. Authenticated image (PSNR=51.09dB), **b**. Tampered image (PSNR=21.05dB), **c**. Detected result, **d**. Extracted QR code, **e**. Extracted QR code, **f**. Recovered image (PSNR=37.29dB)

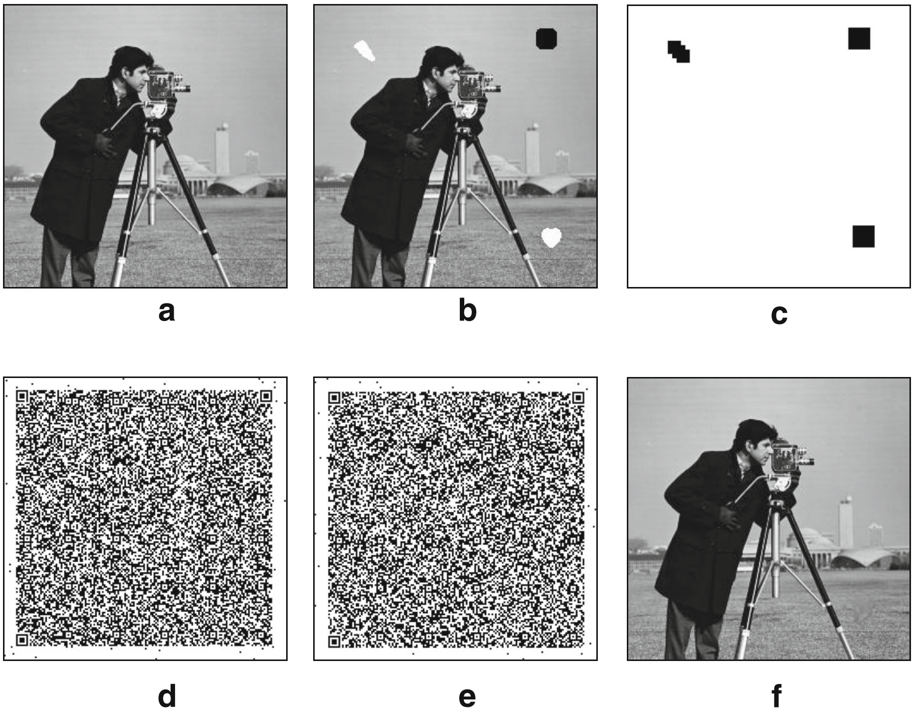


Fig. 12 Visual results of the proposed scheme for the image "Cameraman". **a**. Authenticated image (PSNR=51.15dB), **b**. Tampered image (PSNR=24.59dB), **c**. Detected result, **d**. Extracted QR code, **e**. Embedded QR code, **f**. Recovered image (PSNR=47.05dB)

Table 5 Comparisons of Chen and Chen's schemes and the proposed scheme

Test Images	Chen and Chen's scheme		The proposed scheme	
	Authenticated image (dB)	Recovered image (dB)	Authenticated image (dB)	Recovered image (dB)
Baboon	43.91	N/A	51.11	37.64
Cameraman	38.46	N/A	51.15	47.15
Chart	6.05	N/A	50.78	37.55
Lena	35.90	N/A	51.39	47.11
Pepper	27.18	N/A	51.09	37.44
Sailboat	35.63	N/A	50.98	43.88
Average	31.19	N/A	51.08	41.80

N/A means that image is not available by using the previous scheme [10]

5 Conclusions

In this paper, we proposed a simple and effective image authentication scheme based on vector quantization coding technique. It aims to extract VQ-compressed codes as the authentication and recovery data of an image and then convert them into two-dimensional QR code formats. With the capability of error correction and tolerance that QR codes have, the important confidential data can be protected completely and errorless. As shown in the simulation experiments, the performance of proposed scheme in both image quality and detected result is quite satisfactory. Moreover, it is superior to the previous schemes especially for recovered images. Even though we attempt to modify authenticated images under multiple attacks, detected results of our proposed scheme are pretty exact, and recovered image quality is over 40 dB on average. The recovered images are conducive to later application in computer vision. In future, we will extend this current work to how to authenticate an image is real even while the photo size is changed. Furthermore, it is likely to verify the authenticity from not just one but multiple images because people often take repetitive photos from the same scene and transmit them to online repositories.

Funding

This work was supported by the Aletheia University, Taiwan, Republic of China, under the Grant AU-AR-104-004.

Competing interests

The authors declare that they have no competing interests.

Received: 29 July 2016 Accepted: 21 January 2017
Published online: 02 February 2017

References

1. I.C. Shen, W.H. Cheng, Gestalt rule feature points. IEEE Trans. Multimedia **17**(4), 526–537 (2015).
2. K.E.A. van de Sande, T. Gevers, C.G.M. Snoek, Evaluation of color descriptors for object and scene recognition. IEEE Trans. Pattern Anal. Mach. Intell. **32**(9), 1582–1596 (2010).
3. C.Y. Lin, W.W. Chang, Y.C. Chou, Bidirectional background modeling for video surveillance. J. Electron. Sci. Technol. **10**(3), 232–237 (2012).
4. H.Y. Chi, W.H. Cheng, C.W. You, M.S. Chen, *What catches your eyes as you move around? On the discovery of interesting regions in the street.*, *Proceedings of International Conference on Multimedia Modeling*, (Miami, 2016), p. 4–6
5. T.H. Tsai, W.C. Jhou, W.H. Cheng, M.C. Hu, I.C. Shen, T. Lim, K.L. Hua, A. Ghoneim, M.A. Hossain, S.C. Hidayati, Photo sundial: estimating the time of capture in consumer photos. Neurocomputing 177, 529–542 (2016).
6. F. Ahmed, I.S. Moskowitz, Correlation-based watermarking method for image authentication applications. Opt. Eng. **43**(8), 1833–1838 (2004).
7. S. Jothimani, P. Betty, A survey on image authentication techniques. Int. J. Eng. Trends Technol. **7**(4), 184–186 (2014).
8. W.C. Wu and G.R. Ren, A new approach to image authentication using chaotic map and sudoku puzzle. *Proceedings of the 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, (Kyoto Japan), 628–631 (2009)
9. C.S. Chan, An image authentication method by applying hamming code. Pattern Recogn. Lett. **32**(14), 1679–1690 (2011)
10. J.H. Chen, C.H. Chen, Image tamper detection scheme using QR Code and DCT transform techniques. Int. J. Comput. Consum. Control **1**(2), 61–68 (2012)
11. J.C. Chuang, Y.C. Hu, C.C. Lo, W.L. Chen, Grayscale image tamper detection and recovery based on vector quantization. Int. J. Secur. Appl. **7**(6), 209–228 (2013)
12. W.C. Chen, M.S. Wang, A fuzzy c-means clustering-based fragile watermarking scheme for image authentication. Expert Syst. Appl. **36**(2), 1300–1307 (2009)
13. W.C. Wu and Y.P. Hsieh, Quantization- and prediction-based image authentication and recovery. *Proceedings of the 5th International Conference on Genetic and Evolutionary Computing*, (Kinmen Taiwan), 188–191 (2011)
14. C.M. Wu, Y.C. Hu, K.Y. Liu, J.C. Chuang, A novel active image authentication scheme for block truncation coding. Int. J. Signal Process. Image Process. Pattern Recognit **7**(5), 13–26 (2014)
15. W.C. Wu and Z.W. Lin, An image content protection and tampering localization scheme using singular values. *Proceedings of the 3rd International Scientific Conference on Engineering and Applied Sciences*, (Okinawa Japan), 238–247 (2015)
16. P.W. Wong, N. Memon, Secret and public key image watermarking schemes for image authentication and ownership verification. IEEE Trans. Image Process. **10**(10), 1593–1601 (2001)
17. S.S. Wang, S.L. Tsai, Automatic image authentication and recovery using fractal code embedding and image inpainting. Pattern Recogn. **41**(2), 701–712 (2008)
18. C.W. Yang, J.J. Shen, Recover the tampered image based on VQ indexing. Signal Process. **90**(1), 331–343 (2010)
19. S. Amtullah, A. Koul, Passive image forensic method to detect copy move forgery in digital images. J. Comput. Eng. **16**(2), 96–104 (2014)
20. Y.L. Chen, C.T. Hsu, Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection. IEEE Trans. Inf. Forensics Secur. **6**(2), 396–406 (2011)
21. W. Luo, Z.H. Qu, F. Pan, J. Huang, A survey of passive technology for digital images forensics. Front. Comput. Sci. China **1**, 166–179 (2007)
22. K.H. Pandya, H.J. Galiyawala, A survey on QR codes: in context of research and application. Int. J. Emerg. Technol. Adv. Eng. **4**(3), 258–262 (2014)
23. Y. Linde, A. Buzo, R.M. Gray, An algorithm for vector quantizer design. IEEE Trans. Commun. **28**(1), 84–95 (1980)
24. C. Karri, U. Jena, Fast vector quantization using a bat algorithm for image compression. J. Eng. Sci. Technol. **19**(2), 769–781 (2016)