Authenticate an Image under DCT Domain with Attack Recovery

Chien-Chang Chen and Husan-An Ke

Department of Computer Science
Hsuan Chuang University
Hsinchu 300, Taiwan
E-mail: cchen34@hcu.edu.tw

Abstract- Image authentication techniques verify the integrity of an image from malicious manipulations. In this paper, a DCT-based image authentication approach with attack recovery, which recovers some attacked blocks, is proposed. Two quantization properties DQP and FQP are presented to embed authentication feature. These embedded features are tolerant to JPEG compression with quantization step less than two times of the pre-determined quantization step, but is sensitive to other malicious attacks. The attacked blocks are indicated after verifying a protected image and then the embedded recovery feature is extracted to recover these damaged blocks. Moreover, in case of the damage of recovery feature, an edge-based interpolation recovery approach (EIRA) is proposed to enhance recovery results. Experimental results show that the attacked blocks can be detected and recovered efficiently by the proposed approach.

Keywords: JPEG compression, image authentication, DCT quantization, image recovery.

1. Introduction

The internet is popular because of its inexpensiveness and efficiency. However, the rapid growth of digital media over the internet has led to an urgent demand for the copyright and integrity protection because digital media can be easily replicated and modified. The existing approaches for right protection are to embed robust digital watermarks into multimedia data. Differing from robust watermarking approaches, the main purpose of fragile watermark is to indicate illegal temper of an image rather than to verify its ownership. Such techniques are very sensitive to every manipulation so that as long as the image is tampered, they can identify the damaged areas accurately. Unlike the sensitivity of fragile-watermark techniques, semi-fragile watermarking techniques detect malicious attacks while allowing specific manipulations such as JPEG. Some important works about this paper are discussed as follows.

In 2001, Lin and Chang [2] proposed that the relationship of two DCT coefficients locating at the same position of two different DCT blocks is invariant before and after JPEG compression. In order to increase authenticity, they also obtained several relationships between different thresholds and difference of two DCT coefficients. Maeno *et al.*[3] further presented a method which can record the relationship of two coefficients more precisely. They also showed that difference between two coefficients after quantization can be limited by quantization steps. Their approach requires one more bit than Lin and Chang’s work to record each relationship so as to prevent collisions during authentication procedure. Above methods have some drawback on requiring extra file to store authentication feature. Furthermore, Chen and Lin [1] proposed a tolerant system which extracts a signature from the original image and embeds this signature back into the image without additional signature files. They presented a property that difference of two coefficients at the same position in different DCT blocks will move within a fixed interval after quantization while their difference is equal to a given value *D*. When the difference is equal to one or three times of *D*, the difference after quantization can be distinguished. In order to fill up blank blocks in an image, Park *et al.* [4] presented a spectral robust interpolative image-restoration method based on projections onto convex sets. This method is efficiently for image recovery when information of attacked blocks is lost but the number of its surrounding blocks is enough. Uehara *et al.* [5] presented a method of recovering DC coefficients from AC coefficients with reasonable image quality.

In this paper, a DCT-based image authentication approach with attack recovery is proposed. The relationship of important DCT coefficients between blocks is embedded into LSB1 of these blocks. Scaling information of blocks are embedded into LSB2 of others blocks by a mapping function for recovering the attacked blocks. These two kinds of information is tolerant to JPEG compression with quantization step less than two times of the pre-determined quantization step but is sensitive to other malicious attacks. However, for a serious attack, above scaling information may be erased. Thus, for those blank blocks, an edge-based interpolation recovery algorithm (EIRA) is presented to recover a blank blocks from its neighboring blocks.

The rest of the paper is organized as follows. In Section 2, the embedding algorithm is introduced, includes two quantization surviving properties, which extract and embed image feature. Section 3 shows the proposed authentication with recovery algorithm. Some experimental results are shown in Section 4. Finally, brief conclusion is given in Section 5.

2. The Embedding Algorithm

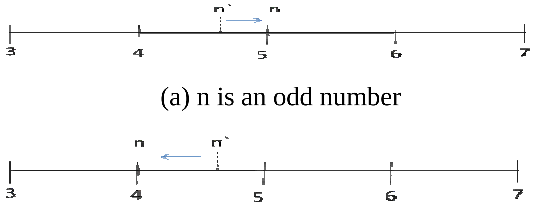
The proposed image feature extraction procedures include authentication feature extraction, recovery feature extraction, authentication feature embedding and recovery feature embedding. Authentication feature is extracted from DCT coefficients by the proposed Double Quantization Property (DQP) to survive after JPEG compression, and the authentication feature is embedded into DCY middle frequency coefficients by the proposed Further Quantization Property (FQP). Recovery feature is extracted from the most important DCT coefficients. Embedding the recovery feature is also based on DQP. Therefore, these two important properties are introduced in next section firstly.

2.1 Double Quantization Property (DQP)

DQP defines that the quantized coefficient after quantization locates within a fixed range. This property shows that only one integer exists at this range after further quantization. The proposed DQP is defined as follows. Assume *P* is a DCT coefficient, *P'* is its quantization result defined as $P' \equiv \left[\frac{P}{T}\right]\cdot T \equiv n\cdot T$, where *T* denotes the pre-determined quantization step, and $n \in Z$. Assume *Q* denotes the further quantization step satisfying $Q < 2\cdot T$, we obtain the DQP as follows.

$$(n-1) < \left[\frac{P'}{Q}\right]\cdot\frac{Q}{T} < (n+1) \qquad (1)$$

Equation (1) shows that the re-quantized coefficient $\left[\frac{P'}{Q}\right]\cdot Q$ divided by *T* locates within the range of *n-1* and *n+1*. Thus, *P'* can be perfectly reconstructed by assuming it being an odd or even number. For example, assume $n = \left[\frac{P'}{Q}\right]\cdot\frac{Q}{T} = 4.6$, and *n* is an odd number, *n* can be determined as 5 and so as to reconstruct *P'* by *5T*. Otherwise, *P'* denotes *4T* when *n* is an even number.



(a) n is an odd number

(b) n is an even number

Figure 1. An example of determining *n* from *n'* with *n'*=4.6.

Figure 1 shows that a re-quantized coefficient *n'*=4.6 can be adjusted to 4 or 5 according to being an odd or even number. Thus, parameter *n* can be perfectly reconstructed when even or odd number of $\lfloor n' \rfloor$ is equal to *n*, where $\lfloor\ \rfloor$ is the floor operation. Therefore, we use *n* to generate feature codes of the image. All extracted features by DQP are embedded into the host image by the FQP that illustrated at next section.

2.2 Further Quantization Property (FQP)

The FQP defines the relationship between the difference *D* of two coefficients and the further quantization step *Q* under the restriction *Q<2D*. The FQP is defined as follows. Assume *p* and *q* are two DCT coefficients at different blocks with the same position, and *p'* and *q'* are coefficients quantized by *Q*, respectively. For any further quantization step *D* satisfying *Q<2D*, the difference change after quantization varying within the following interval.

$$p' - q' = \begin{cases} 0 \le \text{difference} \le 2\text{D} & \text{if } \ p-q=D \\ 2D < \text{difference} < 6D & \text{if } \ p-q=4D \end{cases} \qquad (2)$$

Equation (2) shows that the difference after quantization can be distinguished when the difference before quantization is *D* or *4D*. Furthermore, *Q* limits the acceptable interval more precisely. Hence, we acquire the following equations.

If $p-q=D$ then

$$s\cdot Q\le\left[\frac{p}{Q}\right]\cdot Q-\left[\frac{q}{Q}\right]\cdot Q\le(s+1)\cdot Q \qquad (3)$$

If $p-q=4\cdot D$ then

$$s\cdot Q\le\left[\frac{q+D}{Q}\right]\cdot Q-\left[\frac{q}{Q}\right]\cdot Q\le(s+1)\cdot Q<\left[\frac{p}{Q}\right]\cdot Q-\left[\frac{q}{Q}\right]\cdot Q \qquad (4)$$

where $s=\left\lfloor\frac{D}{Q}\right\rfloor$, Q is further quantization step, $[\ ]$ is the round-off operation.

Equation (3) shows that if the difference of two coefficients *p* and *q* is equal to *D*, the quantization difference is *sQ* or *(s+1)Q* with *Q<2D*. If the difference between two coefficients *p* and *q* is equal to *4D* with *Q<2D*, the quantization difference is larger than *(s+1)Q* as an upper bound of Equation (4). This property not only embeds authentication information into DCT coefficients, but also helps us to extract the embedded authentication feature without extra file.

2.3 Recovery Feature Extraction

To keep good image quality, the embedded quantity of recovery feature must be restricted. However, a significant characteristic in DCT locates that some significant DCT coefficients keep important information of an image. Fig. 2 shows that only ten coefficients remained in every DCT block reconstruct 'Lena' efficiently.

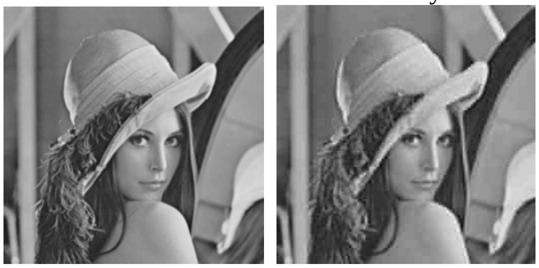

(a) (b)

Figure 2. (a) Original image 'Lena', (b) only remained ten DCT coefficients of (a)

In order to decrease the size of recovery information, the recovery information is extracted from the reduced original image. One reduced block is divided to four parts and the extracted feature is then embedded into four blocks of other corresponding areas in original image.

A series of bits generated by a secret number determines the coefficients quantized to even or odd times, and then embed into LSB1 of other quantized coefficients. The recovery information acquired from the reduced original image is embedded into the LSB2 of selected parameters. Because of DQP, we ensure that every selected parameter can be reconstructed exactly. Therefore, the recovery feature embedded in these parameters can also be extracted correctly.

2.4 Feature extraction procedure

The proposed image authentication and recovery approaches are completely compatible to quantization-based lossy compressions because of using above two properties. The DQP extracts robust authentication features from important DCT coefficients, and the FQP embeds the extracted authentication features into middle frequency coefficients. Furthermore, the DQP is also used to embed recovery information via its characteristic of rebuilding coefficients. Figure 3 depicts the flowchart of the proposed embedding algorithm and is introduced as follows.

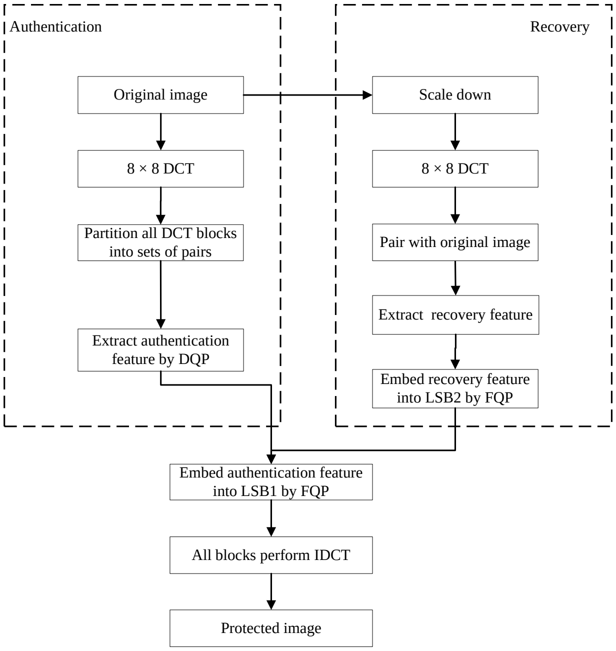

Authentication
Recovery
Original image
Scale down
8 × 8 DCT
8 × 8 DCT
Partition all DCT blocks into sets of pairs
Pair with original image
Extract recovery feature
Extract authentication feature by DQP
Embed recovery feature into LSB2 by FQP
Embed authentication feature into LSB1 by FQP
All blocks perform IDCT
Protected image

Figure 3. Flowchart of the proposed embedding steps.

1. Scale down an image for extracting recovery information.
2. Divide both the original and downscaling images into 8×8 non-overlapping blocks, and then each block is transformed by DCT individually.
3. Partition all blocks into pairs by a mapping function.
4. All blocks from downscaling image pair with original image blocks by the other mapping function. One block from downscaling image is corresponding to four

blocks of original image.

5. For each pair of blocks in the authentication procedure
   5.1 Obtain authentication feature codes by DQP.
   5.2 Embed above authentication feature into original image by FQP.
6. For each pair of blocks in recovery procedure
   6.1 Extract recovery information from each DCT block of the downscaling image.
   6.2 Embed them into corresponding blocks of the original image by FQP.
7. All blocks transform by IDCT to obtain the protected image.

3. Authentication with Recovery Algorithm

This section introduces the method to authenticate the verification of the image and recover the attacked blocks if necessary. In embedding procedure, watermarks are embedded into LSB1 of quantized coefficients and important DCT information is embedded into other DCT blocks for block recovery. In authentication procedure, the first step verifies the correctness of each block. The maliciously attacked blocks are detected in this step. Then, those attacked blocks, if exist, are recovered from other blocks' embedded information. At last, the proposed EIRA recovers the attacked blocks that cannot be recovered in previous procedure. Sections 3.1, 3.2, and 3.3 illustrate the proposed authentication procedure, recovery procedure, and EIRA, respectively

3.1 Authentication Procedure

Authentication procedure first reconstructs the quantized coefficients. Then image feature codes calculated from these quantized coefficients and authentication bits extracted by the FQP are compared. The consistent result shows that the selected pair of blocks is correct, otherwise, they have been tampered with.

From the FQP, we define

If $sQ \le p' - q' \le (s+1)Q$ then z=1

If $p' - q' > (s+1)Q$ then z=0

where *p'* and *q'* are two DCT coefficients after JPEG quantization at different blocks with the same position. *S* denotes $\left\lfloor \frac{D}{Q} \right\rfloor$, where *Q* is JPEG quantization step, $\lfloor\ \rfloor$ is the floor operation, and z denotes extracted authentication bit.

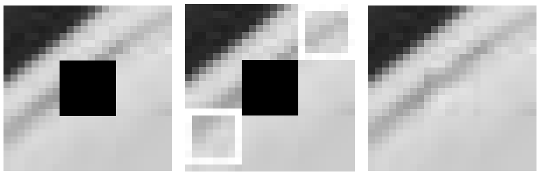
3.2 Recovery Procedure

After performing above authentication procedure, the maliciously attacked blocks are detected. The recovery procedure obtains the recovery information from LSB2 of corresponding blocks of the attacked blocks. Then extract the embedded bits and recover to their positions in DCT domain and perform IDCT. After performing the recovery procedure, the following EIRA is required when any block is blank.

3.3 Edge-based Interpolation Recovery Algorithm (EIRA)

In order to guarantee the integrity of recovery image, an edge-based interpolation recovery algorithm (EIRA) is proposed to estimate the attacked blocks whose recovery feature is lost. The EIRA selects the best edge form of the attacked block. Therefore, according to edge information which gathered from its surrounding blocks, the most suitable pair of blocks is selected to recover the attacked block. Figure 4 show an example of applying EIRA and the algorithm is described as follows.

1. Select all surrounding blocks of the attacked block and then divide them into groups of pair blocks according to their own locations and directions which the edges may pass through the attacked block.
2. Detect edges on these pair of blocks.
3. Transform them by Hough Transform to obtain angles of these edges.
4. Find out the most suitable pair of blocks and their edge direction.
5. Extend the pair of blocks along the selected direction.
6. Adjust the pixel values in the attacked block by a scanline whose angle is equal to the selected direction.
7. Finally, we can obtain an approximation of the original image.



(a) (b) (c)

Figure 4. An EIRA example (a) attacked image (b) pair to extend (c) recovery result

3.4 Authentication with Recovery Algorithm

The authentication with recovery algorithm adopts above three procedures in order to get the authentication result first and then recover the attacked blocks, if necessary. Figure 5 depicts the proposed authentication with recovery algorithm. The algorithm is composed of above three procedures and introduced as follows.

1. Divide the test image into 8╳8 non-overlapping blocks, and then each block is transformed by DCT individually.
2. Partition all DCT blocks into sets of pairs blocks by the mapping function used in embedding algorithm.
3. For each pair of blocks,
   3.1 Obtain image feature code by the DQP.
   3.2 Extract authentication feature from pre-determined DCT middle frequent coefficients.
   3.3 Verify validity of these two blocks by comparing above two results.
4. When difference is detected at step 3.3, recover the attacked blocks by extracting recovery information from corresponding blocks.
5. In step 4, if the recovery information embedded in corresponding blocks is also tampered with, the attacked block is estimated by the proposed EIRA algorithm.
6. Acquire the recovery image.

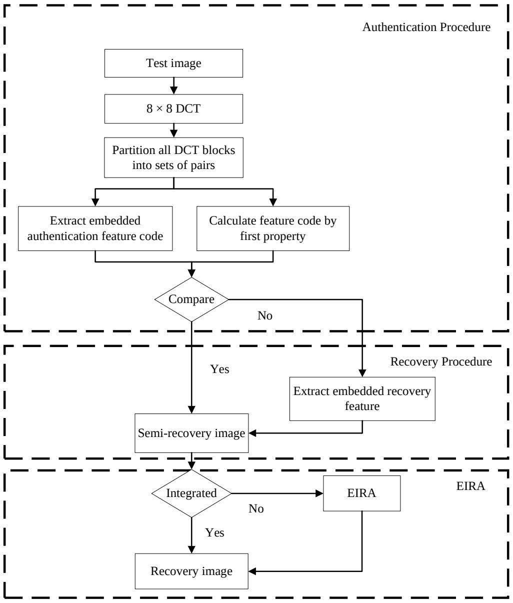
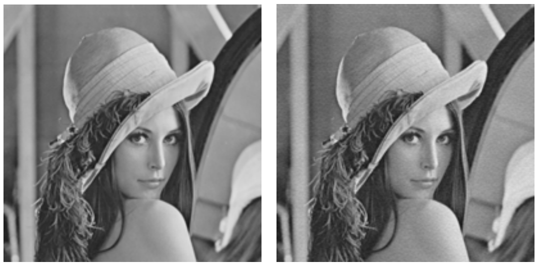

Authentication Procedure
Test image
8 × 8 DCT
Partition all DCT blocks into sets of pairs
Extract embedded authentication feature code
Calculate feature code by first property
Compare
No
Yes
Recovery Procedure
Extract embedded recovery feature
Semi-recovery image
EIRA
Integrated
No
EIRA
Yes
Recovery image

Figure 5. Authentication with recovery algorithm.

4. Experimental Results

This section demonstrates some experimental results of the proposed authentication with recovery algorithm, in which some attacks including copy and paste, and cropped are applied to the protected image. The image "Lena" with size 512×512 is tested. Image feature codes are calculated from six coefficients at a pair of blocks. Three coefficients in these two DCT blocks are at positions (0,1), (1,0) and (1,1). These coefficients are quantized by standard JPEG quantization table. Moreover, the average length of recovery information is about 32 bits per block in the scaled image and the recovery bits are embedded into AC coefficients by replacing with the closest values whose LSB2 are the same as recovery bits to keep image quality.

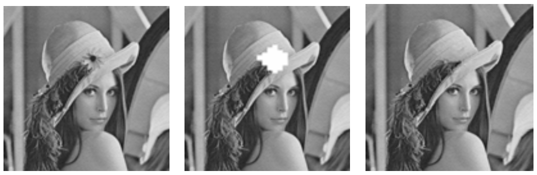
Figure 6.(a) shows the original image: 'Lena' and (b) is the protected image of (a) with PSNR=35.39dB.



(a) (b)

Figure 6.(a) Lena with size 512╳512, (b) the protected image of (a).

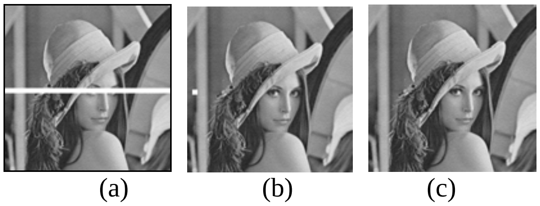
Experiment of "copy and paste" attack is also applied to the protected image as shown in Fig. 6.(b). The attacked image is illustrated in Fig. 7.(a). The authentication result is shown in Fig. 7.(c), where the white blocks denote the attacked blocks. Figure 7.(c) shows the recovery result with PSNR 34.75dB.



(a) (b) (c)

Figure 7. (a) The "copy and paste" attacked image, (b) the authentication result, (c) the recovery result.

Experiment of "cropped" attack is also demonstrated. The attacked image with PSNR 19.47dB is illustrated in Fig. 8.(a). Figure 8.(b) shows the recovery result by extracting the embedded recovery information. The result of the proposed authentication with recovery algorithm is shown in Fig 8.(c) with PSNR 32.37 dB.



(a) (b) (c)

Figure 8.(a) The “cropped” attacked image, (b) the recovery result, (c)the EIRA result.

Table 1 shows the comparison with the Lin and Chang’s method [2]. The proposed method requires no extra file and has the attack recovery property. Especially in the attack recovery, no previous literatures, like [2] or [3], have presented works with this property.

Table 1. The comparison between the proposed method and important works.

	Require no extra file	Attack recovery
The proposed method	√	√
Lin and Chang’s method	×	×

5. Conclusion

This work presents a DCT-based image authentication approach with attack recovery. This scheme detects and recovers the tampered region by two proposed algorithms, namely DQP and FQP. The DQP reconstructs DCT quotients based on pre-determined even or odd numbers. The FQP distinguishes between the quantized and further quantized images after further quantization. These two proposed properties survive after the quantization step. Experimental results show that the proposed scheme is tolerant to JPEG compression with a quantization step less than twice the pre-determined quantization step. The proposed approach reconstructs an approximate version of the original image after authentication. The attacked blocks can be efficiently recovered. Future study should focus on improving the quality of the protected image.

References

[1]. C.C. Chen and C.S. Lin, “Toward a Robust Image Authentication Method Surviving JPEG Lossy Compression,” ***Journal of Information Science and Engineering,*** vol. 23, no. 2, 511-524, 2007.

[2]. C. Y. Lin and S. F. Chang, “A robust image authentication method distinguishing JPEG compression from malicious manipulation,” ***IEEE Transactions on Circuits and Systems of Video Technology***, vol. 10, pp. 153-168l, 2001.

[3]. K. Maeno, Q.B. Sun, S.F. Chang, and M. Suto, “New Semi-Fragile Image Authentication Watermarking Techniques Using Random Bias and Nonuniform Quantization,” ***IEEE Transactions on Multimedia***, vol. 8, no.1, pp.32-45, 2006

[4]. J. Park, D.C. Park, R.J. Marks and M.A. EI-Sharkawi, “Recovery of Image Blocks Using the Method of Alternating Projections,” ***IEEE Transactions on image processing***, vol.14, no.4, pp. 461-467, 2005

[5]. T. Uehara, R. Safavi-Naini, O. Philip, “Recovering DC Coefficients in Block-Based DCT,” ***IEEE Transactions on Image Processing***, vol. 15, no. 11, pp. 3592-3596, 2006.