

Compact and Robust Fingerprints Using DCT Coefficients of Key Blocks

Sheng Tang^{1,2}, Jin Tao Li¹, and Yong Dong Zhang¹

¹ Institute of Computing Technology, Chinese Academy of Sciences
100080, Beijing, China

{ts,jtli,zhd}@ict.ac.cn

² Graduate School of the Chinese Academy of Sciences
100039, Beijing, China

Abstract. In this paper, we present a novel fingerprinting method for image authentication, the fingerprint length of which is very short (only 81 bytes) and independent on image sizes. First, we extract features based on the block DCT coefficients of images, and binarize the feature map to get key blocks. Then we apply Principal Components Analysis (PCA) to the DCT Coefficients of key blocks. Finally, we take the quantized eigenvector matrix (9×9) as fingerprints. Experimental results show that the proposed method is discriminative, robust against compression, and sensitive to malicious modifications.

1 Introduction

Fingerprints are perceptual features or short summaries of a multimedia object [1]. They can be used for identifying contents just as human fingerprints are used for identification. The aim of fingerprinting (also known as multimedia identification, robust hashes, robust signatures, or passive watermarking) is to provide fast and reliable methods for content identification [1]. It is an emerging research area that is receiving increased attention.

A number of applications of multimedia fingerprinting such as multimedia authentication, indexation of content, and management of large database, were detailed in [1–3]. A typical example of application is multimedia authentication, the key issue of which is to protect the content itself instead of the particular representation of the content without access to the original signals [2, 4, 7]. This renders traditional cryptographic schemes using bit-sensitive hash functions not applicable [1, 2, 5], for multimedia signals can be represented equivalently in different forms, and undergo various manipulations during distribution that may carry the same perceptual information. Therefore, fingerprints should be both discriminative and robust [1].

Researchers have paid great efforts on fingerprinting techniques. Up to now, many image fingerprinting methods have been proposed [1–8]. Schneider and Chang [4] proposed a scheme based on image-block histograms to authenticate the content of an image. Although their scheme is compression tolerant, it has two main drawbacks: considerably large storage requirement of histograms and

its security due to the easy way to modify an image without changing its histogram. Bhattacha and Kutter [5] proposed a method based on the locations of salient feature points by using a scale interaction model and Mexican-Hat wavelets. Although the extracted fingerprints are very short, the selection process, relevance of the selected points and its robustness to lossy compression are unclear [8]. Moreover, the feature points are too few and separate to capture the major content characteristics from a human perspective. Thus the method is not discriminative and may be inadequate for detecting some modifications inside the objects. Lou DC and Liu JL [6] proposed a method based on quantization and compression of means of all blocks. Because blocks can be easily modified without changing their means, security problem similar to that of [4] still exists. Queluz [7] proposed techniques to generate fingerprints based on moments and edges. Because moments ignore the spatial distribution of pixels, different images may have same or similar moments. Consequently, moment features are not discriminative enough. Additionally, it is easy to modify an image without changing its moments. Several issues have to be further solved such as the reduction of fingerprint length, the consistency of edge detector, and the robustness to color manipulations [8]. Ching-Yung Lin and Shih-Fu Chang [3, 8] present an effective technique for image authentication which can prevent malicious manipulations but allow JPEG lossy compression. However, their extracted fingerprints are not very compact compared with our method, and largely depend on the image sizes and the number of DCT coefficients compared in each block pair. Recently, a compact and robust fingerprinting method based on radon transform has been proposed in [1]. But the method is not intended for authentication, and is not based on the DCT domain. Hence it can not directly extended to compressed video stream.

In this paper, we present a novel fingerprinting scheme based on the DC and low-frequency AC terms of block DCT coefficients. The procedure for generating fingerprints is shown in Fig.1. First, we extract features based on block DCT coefficients, and binarize the feature map to get key blocks. Then we apply PCA to the DCT Coefficients of key blocks (data matrix A in Fig.1). Finally, we take the eigenvector matrix as fingerprints. Experiments show that the proposed method is discriminative, robust against compression, and sensitive to malicious modifications.

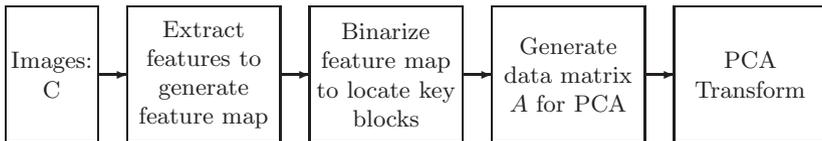


Fig. 1. Procedure for generating fingerprints

As we quantize each element of the eigenvector matrix (9×9) to an one-byte integer, the length of extracted fingerprint is very short (only 81 bytes) and independent on image sizes. Since fingerprint lengths of most existing meth-

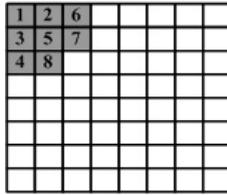


Fig. 3. 8×8 block-DCT coefficients used to compute HTS. The upper-left element of this figure corresponds to the DC term of each 8×8 block DCT. The shaded elements indicate the set of coefficients used in our method, and the numbers indicate the column indices in the data matrix for PCA

JPEG compression process, and place them into a $N \times 8$ matrix in zigzag order, where N is the total number of blocks. This can be represented as (1), where D_{ij} denotes the j^{th} DCT coefficients of the i^{th} block of the image C .

The HTS values of all blocks compose the feature map. After the HTS feature map is formed, we binarize it to get key blocks. Before binarization, we quantize each element HTS_i of HTS to an integer $HTS_q \in [0, 127]$ according to (2):

$$HTS_q = \lfloor \frac{127(HTS_i - HTS_{min})}{HTS_{max} - HTS_{min}} \rfloor \tag{2}$$

where HTS_{max}, HTS_{min} mean the maximum and minimum values of HTS.

After quantization, all the HTS values can be classified into two categories $C_1: \{0, k\}$ and $C_2: \{k + 1, 127\}$, where k is the threshold of binarization. Thus, we can define the between-class variance as (3).

$$\sigma_b^2 = [u_1(k) - u_2(k)]^2 (\sum_{i=0}^k P_i) (\sum_{i=k+1}^{127} P_i) \tag{3}$$

where, P_i is the probability defined as (4), n_i is the number of blocks whose quantized HTS_q equal $i (i = 0, \dots, 127)$,

$$P_i = \frac{n_i}{N} \tag{4}$$

and u_1, u_2 are means of C_1 and C_2 defined as (5) and (6).

$$u_1(k) = \frac{\sum_{i=0}^k iP_i}{\sum_{i=0}^k P_i} \tag{5}$$

$$u_2(k) = \frac{\sum_{i=k+1}^{127} iP_i}{\sum_{i=k+1}^{127} P_i} \tag{6}$$

Consequently, we can determine the HTS threshold k_b for binarization by (7), and take the blocks whose HTS_q are greater than k_b as the key blocks.

$$k_b = argmax\{\sigma_b^2\} \tag{7}$$

5 Experimental Results

In evaluating our proposed method, we tested it on the well-known “F14” image (732×500) and the 2000 test images randomly selected from the Corel Gallery database including many kinds of images (256×384 or 384×256). Prior to extracting fingerprints, we normalized all the images by taking the luminance component although it can be applied to other components. Resizing is not necessary because fingerprint lengths are independent on image sizes. To do experiments, we first extracted fingerprints from the 2000 images.

To test robustness of the method, we used StirMark [10] to compress the 2000 images to various JPEG images with different quality levels Q ranging from 10% to 90%, and calculated S between images and their corresponding JPEG images. The mean and standard deviation (Std) of the measured S were shown in Table.1. It shows that our method is fairly robust against compression.

Table 1. Mean and Std of the measured S between images and corresponding JPEG images for 2000 test images

JPEG Compression	Mean	Std
JPEG(Q=10%)	0.8361	0.1367
JPEG(Q=20%)	0.9167	0.0970
JPEG(Q=30%)	0.9411	0.0821
JPEG(Q=40%)	0.9554	0.0688
JPEG(Q=50%)	0.9631	0.0635
JPEG(Q=60%)	0.9664	0.0533
JPEG(Q=70%)	0.9751	0.0467
JPEG(Q=80%)	0.9856	0.0375
JPEG(Q=90%)	0.9887	0.0306

For image authentication, since obvious degradation exists in many images of JPEG(Q=10%), we can set the mean S (0.9167) of JPEG(Q=20%) as the threshold T , or even greater according to various applications.

We made small modifications of “F14” as shown in Fig.4. The measured S between the original image and the tampered images (b), (c) and (d) are 0.8409, 0.7830 and 0.8077 respectively. All those values are below the threshold $T = 0.9167$. Thus, we successfully detected that the three images were tampered. It shows that our method is sensitive to malicious modifications of images.

To test discriminability of the method, we randomly selected 262140 pairs of fingerprints of the 2000 test images, and calculated S between each pair. The histogram of the measured S was shown in Fig.5. All the measured S were in the range between 0.0710 and 0.8440. The mean and standard deviation were 0.3723, 0.1005. We can see that the histogram closely approaches the ideal random i.i.d. case $N(0.3723, 0.1005)$. The mean of the measured S was far below $T = 0.9167$. Thus we can arrive at very low false alarm rate (the probability that declare two different images as similar or authentic): 3.0318×10^{-8} . The above results show that our method is discriminative.

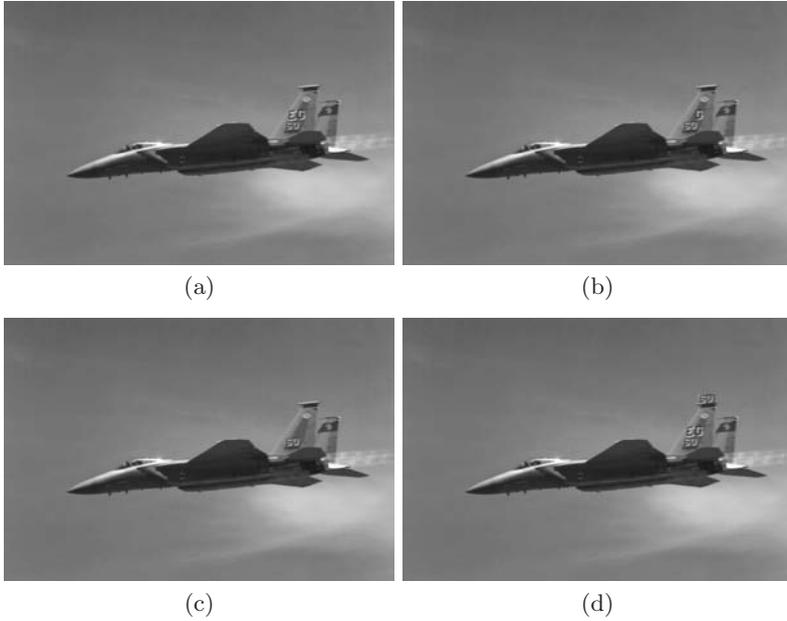


Fig. 4. Authentication test on the image “F14”: (a) Original image “F14”; (b) Remove the char “E” on the empennage; (c) Remove the two chars “EC” on the empennage; (d) Copy the two chars “GO” onto the top of the empennage

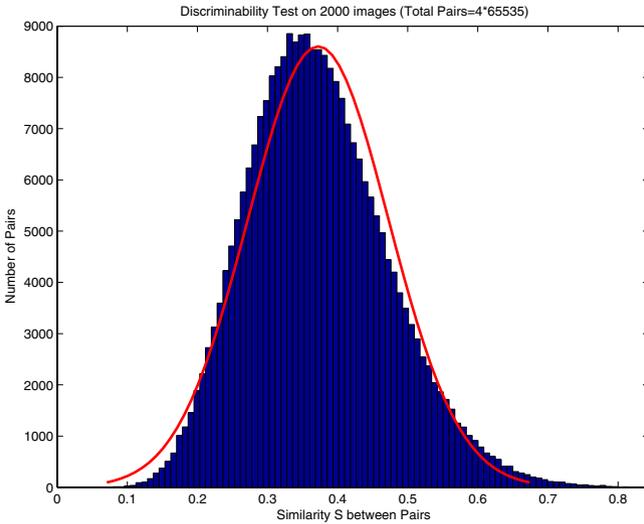


Fig. 5. Histogram of the measured S between 262140 pairs of images randomly selected from 2000 images. The red line represents the ideal random i.i.d. case $N(0.3723, 0.1005)$

6 Summary and Conclusions

In this paper, we present a novel image fingerprinting method for authentication based on PCA of the DCT coefficients of key blocks determined by the HTS threshold. Experiments show that the proposed method is discriminative, robust against compression, and sensitive to malicious modifications. It is convenient to extend our method to verify compressed video streams without DCT transforms. Furthermore, since the fingerprint length is only 81 bytes long regardless of image sizes, and the middle-frequency terms of block DCT coefficients are not adopted by our method, combining our method with semi-fragile watermarking and embedding fingerprint there may be feasible.

Acknowledgement

This work is supported by National Nature Science Foundation of China under grant number 60302028.

References

1. J.S.Seoa, J.Haitsmab, T.Kalkerb, C.D.Yoo, "A robust image fingerprinting system using the Radon transform," *Signal Processing: Image Communication*, 19(4):325-339, April 2004.
2. B.B.Zhu, M.D.Swanson, A.H.Tewfik, "When seeing isn't believing - multimedia authentication technologies", *Signal Processing Magazine, IEEE*, 21(2):40-49,2004.
3. C.-Y. Lin and S.-F. Chang, "Robust digital signature for multimedia authentication", *Circuits and Systems Magazine, IEEE*, 3(4):23-26, 2003.
4. M. Schneider, S.-F. Chang, "A robust content based digital signature for image authentication", *In: Proceedings of IEEE ICIP 96, Lausanne, Switzerland*, Vol.3:227-230, October 1996.
5. S. Bhattacharjee, M. Kutter, "Compression tolerant image authentication", *In: Proceedings of the IEEE ICIP 1998, Chicago, IL*, October 1998.
6. Lou DC, Liu JL. "Fault resilient and compression tolerant digital signature for image authentication", *IEEE Transactions on Consumer Electronics*, 46(1):31-39, 2000.
7. M.P. Queluz, "Authentication of digital images and video: generic models and a new contribution", *Signal Processing: Image Communication*, 16(5):461-475, Jan. 2001.
8. C.-Y. Lin and S.-F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation", *IEEE Trans. Circuits Syst. Video Technol.*, 11(2): 153-168, 2001.
9. J. Edward Jackson, *A User's Guide to Principal Components*, John Wiley & Sons, Inc., pp. 1-25, 1991.
10. Fabien A. P. Petitcolas, "Watermarking schemes evaluation", *IEEE Signal Processing*, 17(5):58-64, September 2000.