International Journal of Signal Processing, Image Processing and Pattern
Vol. 2, No.1, March, 2009

A New Public-key Oblivious Fragile Watermarking for Image Authentication Using Discrete Cosine Transform

Chin-Chen Chang
Feng Chia University Feng Chia University, Taichung 40724, Taiwan
ccc@cs.ccu.edu.tw

Henry Chou
National Chung Cheng University, Chiayi 62102, Taiwan
chch90@cs.ccu.edu.tw

Abstract

In this paper, a new oblivious fragile watermarking using discrete cosine transform is proposed. It is inspired by Wong's public key watermarking scheme proposed in 1998 and aims to improve its vulnerability towards possible attacks indicated by Barreto and Holliman. Instead of making use of contextual information and making it an inter-block dependent scheme, as suggested by Barreto, we adopt another approach to retain its blockwise independent property. Our scheme can avoid the conditions necessary for such attacks to be feasible. Furthermore, our scheme extracts the inherent image features and embeds them into this image as the watermark. This relieves users from having to maintain a database of watermarks from various sources. Experimental results show that the watermark insertion procedure has little effect on the visual quality of the watermarked image. They also show our scheme can locate the modifications made to the watermarked image, including image scaling, cropping, geometric distortion, pixel value changes, etc.

1. Introduction

Invisible watermarking can be classified into two categories: "robust" and "fragile". Robust watermarks, intended for copyright and ownership verification, are generally designed to survive from malicious attacks such as image scaling, cropping, geometric distortions, and lossy compression. Fragile watermarks, on the other hand, are for authentication and integrity verification. They are designed to be ruined once the watermarked image is tampered with.

In this paper, we propose a new method to improve Wong's scheme while maintaining its blockwise independence. To reduce the possibility of cut-and-paste attack, an identification code unique to each image should also be embedded along with the watermark. We suggest taking advantage of the image feature itself, instead using another logo image, for watermark. This relieves the burden for the recipients to administer and maintain a database of watermark images from different sources due to requirement of the original watermark image. The experiments demonstrate the watermarking scheme retains image quality and achieves validness.

The rest of this paper is organized as follows. In Section 2, we briefly discuss the theories employed in our scheme, including DCT, which will be used for image feature extraction. Then it is followed by our proposed scheme in Section 3, followed by experimental results and some discussions on security issues in Section 4. Some concluding remarks will be given in Section 5.

2. Related theories

To begin with, we briefly review the discrete cosine transform (DCT) in our scheme.

2.1 Discrete Cosine Transform (DCT)

Images, besides being represented in the spatial domain by a two dimension array of pixel values, can also be transformed into the frequency domain. Discrete Cosine Transform ([1], Chapter 8) uses the cosine wave forms to represent the original image in its frequency domain. The energy of the original image tends to concentrate into the upper-left corner, which can be viewed as the essence of the original image. This makes a desirable property for extraction of the important features from the images and compression of digital images. For example, JPEG [2] is one of the most well known compression standard based on DCT.

The two-dimensional DCT is defined as the following formula

$$C(p,q)=\alpha_p\alpha_q\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}f(m,n)\cos\left[\frac{\pi(2m+1)p}{2M}\right]\cos\left[\frac{\pi(2n+1)q}{2N}\right], \quad (1)$$

where M and N are the numbers of rows and columns, respectively, of the two-dimensional array representing the original image, f(m, n) is the pixel value of the n-th element in the m-th row, and C(p, q) is the transformed coefficient of coordinate (p, q) in the transform domain.

In practice, however, we often partition the original image into non-overlapping blocks of the same size and apply Equation (1) to each block, substituting the height and width of the blocks into M and N.

To convert a DCT block back to its spatial domain representation, the following inverse DCT (IDCT) is applied:

$$f(m,n)=\sum_{p=0}^{M-1}\sum_{q=0}^{N-1}\alpha_p\alpha_q C(p,q)\cos\left[\frac{\pi(2m+1)p}{2M}\right]\cos\left[\frac{\pi(2n+1)q}{2N}\right]. \quad (2)$$

Without truncation error, the result block of IDCT would be the same as the original. αp and αp in (1) and (2) are defined as follows:

$$\alpha_p=\begin{cases}\sqrt{\frac{1}{M}} & \text{for } p=0,\\ \sqrt{\frac{2}{M}} & \text{for } p=1,2,\ldots,M-1.\end{cases}, \quad (3)$$

$$\alpha_q=\begin{cases}\sqrt{\frac{1}{N}} & \text{for } q=0,\\ \sqrt{\frac{2}{N}} & \text{for } q=1,2,\ldots,N-1.\end{cases}. \quad (4)$$

In practice, DCT blocks of size 8×8 are most widely used, including by the JPEG compression.

All printed material, including text, illustrations, and charts, must be kept within the parameters of the 8 15/16-inch (53.75 picas) column length and 5 15/16-inch (36 picas) column width. Please do not write or print outside of the column parameters. Margins are 1 5/16 of an inch on the sides (8 picas), 7/8 of an inch on the top (5.5 picas), and 1 3/16 of an inch on the bottom (7 picas).

3. The Proposed Scheme

In this section, we shall introduce our blockwise independent public-key watermarking scheme for image authentication. This scheme consists of two procedures, which are the watermark insertion procedure and the extraction procedure. Note the feature of the original image, instead of a pre-designed logo image, is extracted and used as the watermark. The details go as follows.

3.1 Watermark Insertion Procedure

The purpose of the insertion procedure is to extract the local feature of the original image, or the content-based watermark, and compose a watermarked image. Suppose X is the original grayscale image of size M × N, where M and N are the height and width of the image, respectively.

Step 1: Partition X into n blocks Xr and Br ($0 \le r < n$) of 8 × 8 pixels.

Step 2: For each block Xr, clear the least significant bits all pixels in Xr to obtain the block Xr.

Step 3: Calculate the DCT block Cr from Xr. Cr is a two-dimensional array whose element Cr(p, q) is the transformed coefficient of coordinate (p, q) in the transform domain.

Step 4: Use a cryptographic secure one-way hash function h(·) to compute the hash value Hr ≡h(M, N, Cr). In practice, the bit length of Hr is longer than the number of pixels in each block, which is 64 in our scheme. Here only a predefined number of bits from the bit stream are preserved.

Step 5: Encrypt with the public key cryptosystem to generate the digital signature $S_r \equiv E_{SK}\left(ID \| m \| n \| h\right)$, where E(·) is the encryption of the public key system, SK denotes the private key, ID is a unique identification code assigned to the image by the original publisher, and m and n denote row and column number of block Xr, respectively. The notation || denotes the concatenation operator.

Step 6: Embed Sr into the LSBs of Xr to form block X'r of the watermarked image.

Step 7: Repeat Step 3 through Step 6 until all the blocks in the original image has been processed.

Now we have the watermarked image X', which then can be safely distributed over the electronic media.

3.2 Watermark Extraction Procedure

The watermark extraction is for verifying whether or not an image X' has been tampered with. When a user wonders if her image has been illegally modified, the following steps can be performed.

Step 1: Partition X' into n blocks X'r ($0 \le r < n$) of size 8 × 8.

Step 2: Split the LSBs from X'r to get S'r, and decrypt it to get the decrypted block W'r ≡ DPK(S'r). Here PK is the public key corresponding to the private key SK used in watermark insertion.

Step 3: Zero out the LSBs of all pixels in X'r to obtain X′r, and calculate its DCT block C′r.

Step 4: Use the same one-way hash function h(·) as in the insertion procedure to compute H'r ≡ h(M, N, C′r), where M and N are the image height and width of X', respectively.

Step 5: Verify W'r = ID || m || n || h. If the equation holds, the watermarked is verified. Otherwise, output that r-th block of X' has been counterfeited.

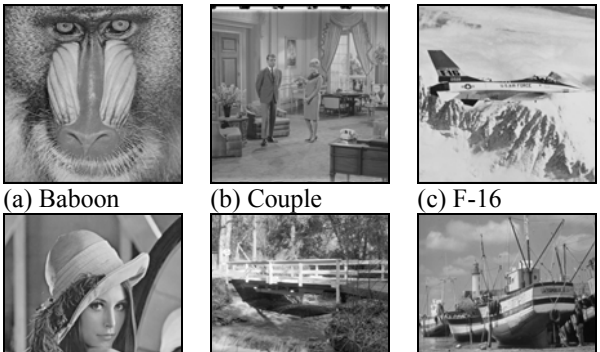
Step 6: Repeat Step 2 through Step 6 until all the blocks in the received image X' has been processed.

As shown in the insertion and extraction procedures above, the feature of the original image is used for watermark insertion. This adoption of a content-based watermark differs from the scheme proposed by Wong, relieving the burden for the end users to maintain a database of watermark images – a desirable advantage.

4. Experimental Results and Discussions

In our experiments, several standard images, including Baboon, Couple, F-16, Lena, Bridge, and Fishing Boat were used to test our watermarking scheme, as shown in Fig. 1. These are all 8-bit grayscale images of 512 × 512 pixels. We adopted MD5 as the one-way hash function and RSA [3] as the public-key cryptosystem in our watermark insertion and extraction procedures. The bit-lengths of fields mentioned in Step 5 of our insertion procedure, ID, m, n, and h, are 16, 8, 8, 32 bits, respectively. Only the first 32 out of the 128 bits of the MD5 output are used.

The insertion and extraction procedures, altogether, take less than 5 seconds on an AMD Duron-750 running Windows XP. With more efficient DCT algorithms, the required time can be further shortened.

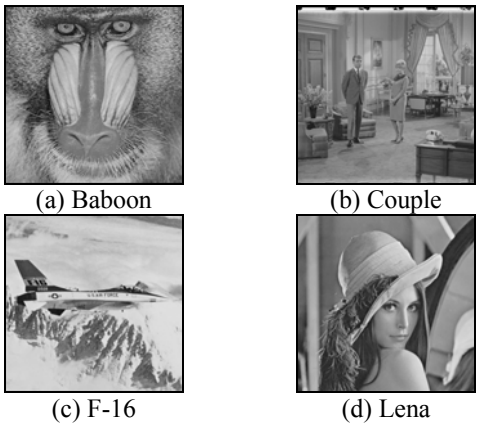


(a) Baboon (b) Couple (c) F-16

(d) Lena (e) Bridge (f) Fishing Boat

Figure 1. Six test images of 512 × 512 pixels

Figure 2 shows the corresponding watermarked images of the original images in Fig. 1. Due to the limitation of space, only four of them were included for our illustration. Table 1 shows the PSNR values of all the six watermarked images. Because the watermark is embedded in the LSBs, it's not surprising to share the common property of high PSNR values (> 51 dB) as other data hiding schemes that make use of LSBs.



(a) Baboon (b) Couple

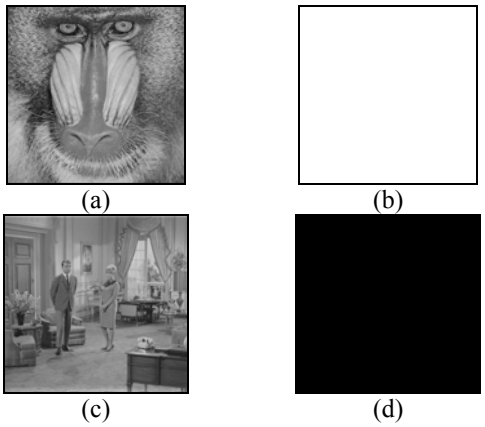
(c) F-16 (d) Lena

Figure 2. The watermarked images

Table 1. The PSNR values of the watermarked images of our scheme

Image	Baboon	Couple	F-16	Lena	Bridge	Fishing Boat
PSNR	51.15	51.13	51.14	51.15	51.15	51.13

Suppose the receiver suspects a watermarked image has undergone some transmission error or malicious modification, our watermark extraction procedure would indicate these changes. For comparison, an intact watermarked image is shown in Fig. 3(a) and the watermark extraction output is shown in Fig. 3(b). Now we first consider changes to image sizes like scaling and cropping. Figure 3(c) and 3(d) shows a cropped watermarked Couple image and its watermark verification result, respectively. A cropped watermarked image would generate the similar output. In fact, since the image height M and width N are used in watermark insertion and extraction procedures of every block, any change in image size would be detected and responded in every block of the image. In addition, the extraction of watermark using a wrong public key would decrypt all watermarked blocks incorrectly. The result is an entirely black image, as in case of change in image size.



(a) (b)

(c) (d)

Figure 3. Watermark verification outputs of intact and modified images

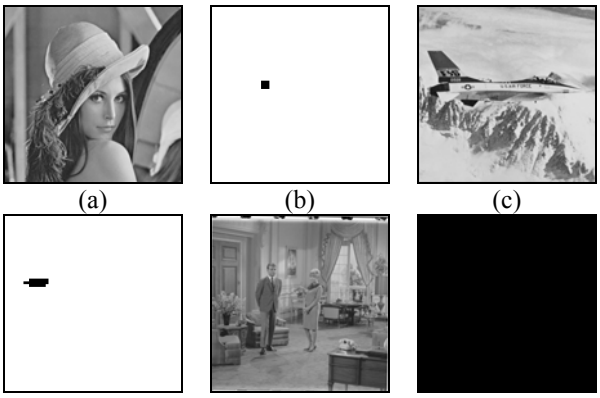


Figure 4. Watermark verification outputs of modified images

Figure 4 shows more watermark verification results of watermarked images which has been tampered with. In Fig. 4(a), there is an extra ornament added to the brim of the hat, and the watermark extraction procedure detects and localizes the modification as shown in Fig. 4(b). In Fig. 4(c), local distortion was applied to the F-16 logo on the fin of the fighter, and it resulted in the output in Fig. 4(d), which indicated the region covering the affected pixels. Finally, Fig. 4(e) shows the rotated Couple image by 1° clockwise. Every block of the image was affected, and therefore an entirely black result was generated.

Before closing this section, we shortly discuss the security of our watermarking scheme. Since we included an identification code (ID) unique to each image, and the location of the block (m and n), the possibility of cut-and-paste is ruled out because it's impossible to find a candidate block for counterfeiting that shares the same (ID, m, n)-tuple as the block intended to be replaced. As for birthday attack on our scheme, it requires 232 trials to succeed in breaking a single block with high probability. If one still doesn't consider it secure enough, it can still be mended by enlarging the block size. A block size of 12×12 or 16×16, requiring 264 or 2128 trials for the attacker to counterfeit a particular block, respectively, should be enough for most practical applications.

5. Conclusions

This paper has presented a new oblivious fragile watermarking technique for embedding fragile digital watermarks into images. The insertion and extraction algorithms have been illustrated. As we have argued, the blockwise independence property can be retained while maintaining its security against cut-and-paste attacks and birthday attacks. Because it uses the image features as the watermark to be embedded, a logo image is not required. Hence the users do not have to maintain a large database of watermark images from vendors. Experiments have shown that the proposed scheme can report modifications to the watermarked images, including image scaling, cropping, pixel value changes, etc. The results also demonstrate high quality of the watermarked images – better than 51 dB for all of our experimental images.

6. References

[1].R. C. Gonzalez, and R. E. Woods, Digital Image Processing, 2nd Ed., Prentice Hall, New Jersey, 2002.

[2] W. B. Pennebaker, and J. L. Mitchell, JPEG: Still Image Data Compression Standard, Van Nostrand Reinhold, New York, 1993, pp. 34–38.

[3].R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, Feb. 1978, pp. 120–126.

Authors

Chin-Chen Chang received his Ph.D. degree in computer engineering from National Chiao Tung University. His first degree is Bachelor of Science in Applied Mathematics and master degree is Master of Science in computer and decision sciences. Both were awarded in National Tsing Hua University. Dr. Chang served in National Chung Cheng University from 1989 to 2005. His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. Prior to joining Feng Chia University, Professor Chang was an associate professor in Chiao Tung University, professor in National Chung Hsing University, chair professor in National Chung Cheng University. He had also been Visiting Researcher and Visiting Scientist to Tokyo University and Kyoto University, Japan. During his service in Chung Cheng, Professor Chang served as Chairman of the Institute of Computer Science and Information Engineering, Dean of College of Engineering, Provost and then Acting President of Chung Cheng University and Director of Advisory Office in Ministry of Education, Taiwan. Professor Chang has won many research awards and honorary positions by and in prestigious organizations both nationally and internationally. He is currently a Fellow of IEEE and a Fellow of IEE, UK. And since his early years of career development, he consecutively won Outstanding Talent in Information Sciences of the R. O. C., AceR Dragon Award of the Ten Most Outstanding Talents, Outstanding Scholar Award of the R. O. C., Outstanding Engineering Professor Award of the R. O. C., Distinguished Research Awards of National Science Council of the R. O. C., Top Fifteen Scholars in Systems and Software Engineering of the Journal of Systems and Software, and so on. On numerous occasions, he was invited to serve as Visiting Professor, Chair Professor, Honorary Professor, Honorary Director, Honorary Chairman, Distinguished Alumnus, Distinguished Researcher, Research Fellow by universities and research institutes. His current research interests include database design, computer cryptography, image compression and data structures.

Henry Chou was born in Taiwan. He received his M.S. degree in Computer Science and Information Engineering in 2003 from National Chung Cheng University. He is presently a Ph.D. student of University of Florida, U.S.A. His research interests are in digital image processing, information hiding and watermarking technique.