HIDDEN SIGNATURES IN IMAGES

Chiou-Ting Hsu and Ja-Ling Wu

Communication and Multimedia Lab.
Department of Computer Science and Information Engineering
National Taiwan University, Taipei, Taiwan, R. O. C.
E-mail: f0506010@csie.ntu.edu.tw

ABSTRACT

In this paper, an image authentication technique by embedding each image with a signature so as to discourage unauthorized copying is proposed. The proposed technique could actually survive several kinds of image processing and the JPEG lossy compression.

1. INTRODUCTION

As the increasing of the electronic publishing, the data distribution is becoming faster, and requiring less effort to make copies. One of the major challenges is that of discouraging unauthorized copying and distributing electronic documents [2]-[5]. In order to trace the unauthorized copies, it has been suggested to sign the image with a signature or copyright message [3]. Such message must be secretly embedded and no visible difference between the coded image and the original image could be perceived. Besides, a robust signature coding approach should survive several possible attacks, such as image processing and lossy image compression.

To invisibly embed the signature message (i.e. embed into the higher frequency components) and to survive the lossy data compression (i.e. embed into the lower frequency components) is contradictory. Therefore, a reasonable trade-off is to embed the signature message in the middle band of the image [1].

2. EMBEDDING APPROACH

In this paper, a DCT-based algorithm is used to implement the middle -band embedding.

Let X be the original gray-level image and the digital signature data S be a binary image, where the marked pixels are valued as 1's, and the others are 0's. The resolution of a signature image S is assumed to be half of that of the original image X:

$$X = \{x(i,j),\ 0 \le i,j < N\},\ x(i,j) \in \{0,\cdots,2^L\}$$

where L is the number of bits used in each pixel.

$$S = \{s(i,j),\ 0 \le i,j < N/2\},\ s(i,j) \in \{0,1\}$$

2.1 Permutation of the signature data

A fast two-dimensional (2-D) pseudo-random number traversing method is used to permute the signature image.

$$s_1(i,j) = s(i',j')$$

where (i',j') is permuted to (i,j) in the pseudo-random order.

2.2 Block transformation of the image

The input image X is divided into blocks of 8×8, and then each block is DCT transformed.

$$Y_{m,n} = \{y_{m,n}(k,l),\ 0 \le k,l < 8\}$$

$$Y_{m,n} = FDCT(X)$$

2.3 Choice of middle-band coefficients

For each block, only the coefficients of middle-band are pick up to produce the 2-D residual pattern. Since the resolution of the signature image is half of that of the input image, the residual image are preferred to be of the same resolution with the signature image in order to simplify the embedding procedure.

$$z_{m,n}(u,v) = Reorder(y_{m,n}(k,l))$$

where $0 \le u,v < 4$ *and* $(k,l) \in$ *middle band*

An example is shown in Figure 1.

2.4 Produce the residual pattern

Then, a 2-D sub-block mask is used to compute the residual pattern from the chosen middle-band coefficients. For example, in Figure 2, if a=b=c=0, d=-1, x=1, then the residual image is the sub-block difference of current and previous block.

0-7803-3258-X/96/$5.00 © 1996 IEEE

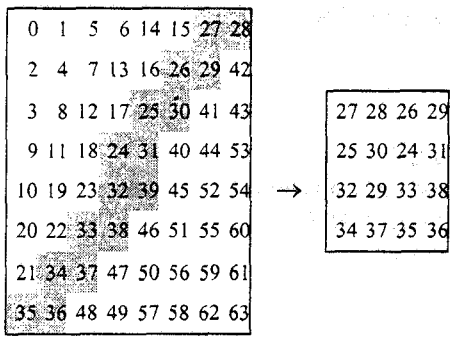


Figure 1: An example of middle-band coefficients, which are pick up in zigzag-scan order and then reorder into block of 4×4.

a	b	c
d	x	

Figure 2: The residual mask, where each square includes a reduced-resolution block of 4×4, and position x means the current reduced block.

$$R=\{r(i,j)=r_{m,n}(p,q),\ 0\le i,j<N,\ 0\le p,q<4,\ i=m\times4+p,\ j=n\times4+q\}$$

$$r_{m,n}(p,q)=sign[z_{m,n}(p,q)-z_{m-1,n}(p,q)]$$

2.5 Modification of DCT coefficients

After the residual pattern is obtained, for each marked pixel of the permuted signature data, modify the DCT coefficients according the residual mask, so that the corresponding residual value is reversed.

$$\forall\ s_1(i,j)=1$$

$$y_{m,n}(k,l),\ y_{m-1,n}(k,l)\ \text{are modified into}\ y'_{m,n}, y'_{m-1,n}$$

$$s.t.\ \ r'(i,j)=1-r(i,j)$$

$$\text{where } r'(i,j)=r'_{m,n}(p,q)=sign[z'_{m,n}(p,q)-z'_{m-1,n}(p,q)]$$

$$z'_{m,n}(p,q)=Reorder(y'_{m,n}(k,l))$$

2.6 Inverse block transform

Finally, inverse DCT to obtained the embedded image.

$$X'=IDCT(Y'_{m,n})$$

3. EXTRACTING METHOD

The extraction of signature requires both the original image and the embedding images. The extraction steps are as follows:

3.1 Block transformation

Both the original image X and the embedded image are DCT transformed.

$$Y_{m,n}=FDCT(X)$$

$$Y'_{m,n}=FDCT(X')$$

3.2 Produce their residual patterns

Make use of the middle-band DCT-coefficients to produce the residual patterns.

$$z_{m,n}(p,q)=Reorder(y_{m,n}(k,l))$$

$$z'_{m,n}(p,q)=Reorder(y'_{m,n}(k,l))$$

$$\Downarrow$$

$$r(i,j)=r_{m,n}(p,q)=sign[z_{m,n}(p,q)-z_{m-1,n}(p,q)]$$

$$r'(i,j)=r'_{m,n}(p,q)=sign[z'_{m,n}(p,q)-z'_{m-1,n}(p,q)]$$

3.3 Extract the permuted data

Take the exclusive-or (XOR) operation on these two residual pattern to obtain a permuted binary data.

$$s_1(i,j)=r(i,j)\oplus r'(i,j)$$

3.4 Reverse-permutation

Reverse-permute S_1 to get the signature data S,

$$s(i,j)=s_1(i',j')$$

where (i',j') is reverse-permuted to (i,j) according to the pseudo-random order.

Figure 3 shows an example of embedding and extracting results.

4. DISCUSSION

Figure 4 and 5 shows the example of the proposed method under the attack of the image enhancement and JPEG compression.

In order to provide different embedding results, the "magic key" will be introduced into this algorithm. A "magic key" is considered as an additional feature that can be implemented to serve various embedding process by using the same embedding technology. For example, it could be used to

- designate different seed of the pseudo-random number generator,
- designate different reorder pattern of the middle-band coefficients,
- designate different pattern of the residual mask, and
- designate the specific bands that will be used to embed the signature data.

5. CONCLUSION

The simulation results of the proposed signature approach indicate that the middle-band embedding technique can actually survive the general image processing attacks, such as image enhancement, and the JPEG lossy compression.

REFERENCES

[1] E. Koch and J. Zhao, "Towards Robust and Hidden Image Copyright Labeling," Proc. IEEE Nonlinear Signal and Image Processing, pp. 452-455, June 1995.

[2] J. T. Brassil, S. Low, N. F. Maxemchuk, and L. O'Gorman, "Electronic Marking and Identification Techniques to Discourage Document Copying," *IEEE J. Selected Areas Commum.*, vol. 13, no. 8, Oct. 1995.

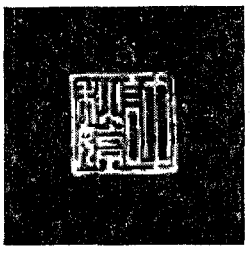
[3] B.M. Macq and J. J. Quisquater, "Cryptology for Digital TV Broadcasting," *Proc. IEEE*, vol. 83, no. 6, June 1995.

[4] O. Bruyndonckx, J. J. Quisquater and B. Macq, "Proc. IEEE Nonlinear Signal and Image Processing, pp. 456-459, June 1995.

[5] I. Pitas and T. H. Kaskalis, "Applying Signatures on Digital Images," Proc. IEEE Nonlinear Signal and Image Processing, pp. 460-463, June 1995.

(a) Original image "Lena".

(b) The signature data.



(c) The coded image.

(d) Decoded signature.

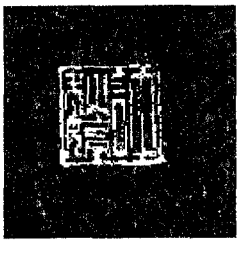


Figure 3: An embedding example of the proposed signature approach.

(a) Enhanced results of Fig. 3(c)

(b) Extracted signature of Fig. 3(a).

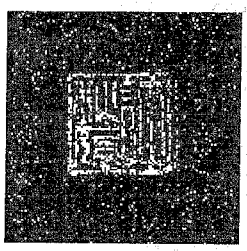


Figure 4: The results of the proposed signature approach under the attack of image enhancement.

(a) JPEG compressed image of Figure 3(c).

(b) Extracted signature of Figure 5(a).

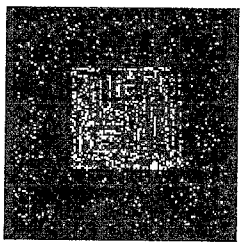


Figure 5: The results of the proposed signature approach under the attack of the JPEG lossy compression with compression ratio of 5.76.