Journal of Korea Multimedia Society Vol. 16, No. 4, April 2013(pp. 411-417)
http://dx.doi.org/10.9717/kmms.2013.16.4.411

Fast Detection of Copy-Move Forgery Image using DCT

Yong-Dal Shin†

ABSTRACT

In this paper, we proposed a fast detection method of copy-move forgery image based on low frequency coefficients of the DCT coefficients. We proposed a new matching criterion of copy-moved forgery image detection (MCD) using discrete cosine transform. For each 8×8 pixel block, the DCT transform is calculated. Our algorithm uses low frequency four (DC, 3 AC coefficient) and six coefficients (DC, 5 AC coefficients) of DCT per 8×8 pixel block. Our algorithm worked block matching for DCT coefficients of the 8×8 pixel block is slid by one pixel along the image from the upper left corner to the lower right corner. Our algorithm can reduce computational complexity more than conventional copy moved forgery detection algorithms.

Key words: DCT, copy-move forgery image, matching criterion

1. INTRODUCTION

Advanced digital cameras and photo-editing software packages (such as PhotoShop, Paintshop pro) make it relatively easy to create digital image forgeries [1-3]. There has been some effort in the digital signature or watermarking communities to detect and locate image manipulation. But the limitation in digital signature or watermarking technology is that the media data must be pre-processed when it is established, such as calculating hash values, or embedding watermark in the images [4].

Recently, various techniques for tamper or forgery detection or even recovery have been proposed in the literature [5,6]. Some techniques have been proposed for image tamper detection [7]. Various watermark techniques [8] have been proposed in recently years, which can be used not only for authentication, but also for being an evidence for the tamper detection [5]. Watermark techniques embedded watermarks consisting of the authentication data and the recovery data into image blocks for image tamper detection and recovery in the future [5].

A common form of digital tampering is Copy-Move forgery, in which a part of the image itself is copied and pasted into another part of the same image to conceal an important object [4]. Because the copied part come from the same image, its important properties, such as noise, color and texture, will be compatible with the rest of the image and thus will be more difficult to distinguish and detect. Several researchers have developed techniques for detection this form of image forgery [4]. Since the key characteristics of Copy-Move forgery is that the copied part and the pasted part are in the same image, a direct method, this forgery is exhaustive search [1], but it is computationally complex. J. Fridrich [1] proposed exact match for detection and an effective blocking approach, in which the image blocks are represented by quantized DCT (discrete cosine transform) coefficients, and a lexicographic sort is adopted to detect the Copy-Move blocks [1,2]. A. C. Popescu [2] worked by applying a principal component analysis (PCA) on small fixed size image blocks to yield a reduced dimension repre-

※ Corresponding Author : Yong-Dal Shin, Address : 12-1 Seolgye-ri Youngdong-eup Youngdong-gun Choongbuk Korea, TEL : +82-43-740-1145, FAX : +82-43-740-1139, E-mail : ydshin@yd.ac.kr
Receipt date : Dec. 22, 2011, Revision date : Feb. 15, 2012
Approval date : Mar. 26, 2012
† Dept. of IT & Securities, Youngdong University, Korea

sentation. Jeong [7] developed detection of copy-move forgery image in wavelet transform domain.

In most methods of copy-move forgery detection, the detected image is divided into overlapping blocks, which are then represented as vectors, which are then lexicographically sorted for later detection. Suppose a detected image of size N×N is divided into $(N-b+1)^2$ overlapping blocks of size b×b, which are represented as vectors of b^2 dimension, and sorted in a lexicographically order [5].

In this paper, we proposed a fast detection method of copy-move forgery image based on low frequency coefficients of the DCT coefficients. We proposed a new fast detection algorithm using matching criterion of copy-moved forgery image detection (MCD). The proposed method used DCT (Discrete Cosine Transform) with 8×8 pixel block. For each 8×8 pixel block, the DCT transform is calculated, DCT coefficients of the 8×8 pixel block is slid by one pixel along the image from the upper left corner to the lower right corner. MCD of our algorithm uses low frequency four (DC, 3 AC coefficient) and six coefficients (DC, 5 AC coefficients) of DCT per 8×8 pixel block. Our algorithm can reduced computational complexity more than conventional copy move forgery detection algorithms.

2. RELATED COPY-MOVE FORGERY [1,9]

In a Copy-Move forgery, a part of the image itself is copied and pasted into another part of the same image. This is usually performed with the intention to make an object "disappear" from the image by covering it with a segment copied from another part of the image [1]. Textured areas, such as grass, foliage, gravel, or fabric with irregular patterns, are ideal for this propose because the copied areas will likely blend with the background and the human eye cannot easily discern any suspicious artifacts [1]. Because the copied parts come from the same image, its noise component, color palette, dynamic range, and most other important properties will be compatible with the rest of the image and thus will not be detectable using methods that look for incompatibilities in statistical measures in different parts of the image [1]. To make the forgery even harder to detect, one can use the feathered crop or the retouch tool to further mask any traces of the copied-and-moved segments [1].

Any Copy-Move forgery introduces a correlation the original image segment and the pasted one. This correlation can be used as a basis for successful detection of this type of forgery. The algorithms for detection of the Copy-Move forgery are developed -one that uses an exact match for detection and one that is based on an approximate match [1].

Before describing the best approach based on approximate block matching that produced the best balance between performance and complexity, two other approaches were investigated-Exhaustive search and Autocorrelation [1].

The Exhausted search is most obvious approach method. In this method, the image and its circularly shifted version are overlaid looking for closely matching image segments. Let us assume that x_{ij} is the pixel value of a gray scale image of size M× N at the position i, j. In the exhaustive search, the following difference are examined [1]:

$$|X_{i,j}-X_{i+k \bmod(M) j+l \bmod(N)}|, \quad k=0,1,\cdots.M-1,\ l=0,1,\cdots.N-1 \text{ for all I, and j,} \tag{1}$$

The autocorrelation of the image xof the size M×N is defined by the formula [1]:

$$r_{k,l}=\sum_{i=1}^{M}\sum_{j=1}^{N} X_{i,j}X_{i+k,j+l}, \quad i,k=0,\cdots M-1,\ j,l=0,\cdots,\ N-1. \tag{2}$$

The correlation can be efficiently implemented using the Fourier transform utilizing the fact that $r=x*\hat{x}$, where $\widehat{x_{ij}}=x_{M+1-i,N=1-j}$, $i=0,\cdots$, M-1, $j=0,\cdots$, N-1. Thus we have

$$R=F^{-1}F(x)F(\widehat{x}) \tag{3}$$

where F denotes the Fourier transform [1].

S. Kahn et. Al [9] proposed an efficient method for detection of copy-move forgery using discrete wavelet transform. The work on "Detection of copy-move forgery in digital images"is implemented in two phase as described below. The first phase deals with detection of reference and matching blocks on the lowest level of wavelet transform compressed image. The second phase deals with checking on different discrete wavelet transform (DWT) levels to produce more robust output. The first phase is expressed as described that [9].

Red Green Blue color input image, Gray scale conversion, Discrete Wavelet Transform, Overlapping block pixel into a matrix, Maximum contrast blocks selection, Matrix sorting, Phase correlation calculation between rows, Candidate block coordinates into a new matrix, Find Candidate blocks.

The second phase is expressed as described that [9]. Candidate block, Candidate blocks as regions in LL_{L-1} image, Region dividing into blocks and comparison, Region comparison directly on LL_{L-2} image, Region comparison directly on original image and duplicated blocks detection.

The related conventional algorithms [1,2,9] need more computational complexity.

3. THE PROPOSED METHOD

Any copy-moved forgery introduces a correlation between the original image segment and the pasted one. This can be used as a basis for a successful detection of this type of forgery.

Our algorithm is as follow. For each 8×8 pixel block, DCT transform is calculated. DCT coefficients of the 8×8 pixel block are slid by one pixel along the image from the upper left corner to the lower right corner.

DCT algorithm [10] transforms signal/image data from the spatial/time domain to the frequency domain. For most images, much of the signal energy lies at low frequencies; these appear in the upper left corner of the DCT such as DCT six coefficients of Fig. 1. Compression is achieved since the lower right values represent higher frequencies, and are often small - small enough to be neglected with little visible distortion. DCT transform algorithm is equation (4) [10].

$$II(u,v) = C(u)C(v)\sum_{i=0}^{B-1}\sum_{j=0}^{B-1} I(i,j)\cos\left[\frac{(2i+1)u\pi}{2B}\right] \cos\left[\frac{(2j+1)v\pi}{2B}\right] \quad (4)$$

$C(u) = \sqrt{\frac{1}{B}}$ for $U=0$, $C(u) = \sqrt{\frac{2}{B}}$ for $otherwise$, B is a block size of DCT.

Inverse DCT (IDCT) is

$$I(u,v) = C(u)C(v)\sum_{i=0}^{B-1}\sum_{j=0}^{B-1} II(u,v)\cos\left[\frac{(2i+1)u\pi}{2B}\right] \cos\left[\frac{(2j+1)v\pi}{2B}\right] \quad (5)$$

The Transform coefficients for U=0 is the average value of the B×B pixel block. This value is the referred to as the DC coefficients. All other coefficients are called the AC coefficients.

The matching criterion of copy-moved forgery image detection (MCD) using DCT coefficients for block image as follow.

$$MCD = \sum |II(i,j) - II(i+m,j+n)|, \quad (6)$$

II is DCT coefficients, i=0,1, j=0,1. The i, j are DCT four coefficients of 8×8 pixel block. m, n=0,1,2 ……(N-B+1) for N×N image. II is DCT coefficients, i=0,1, j=0,1 for low 4 coefficients and i=0,1,2, j=0,1,2, for 6 coefficients, except (2,1), (1,2), (2,2). The i, j are DCT six coefficients of 8×8 pixel block. m, n=0,1,2……(N-B+1) for N×N image.

The MCD is a matching criterion of copy-moved forgery image detection. II is DCT coefficients of the 8×8 pixel block of full size image N×N at the position i, j.

Fig. 1 show DCT 4-low frequency (0,1,2,3) and DCT 6-low frequency (0,1,2,3,4,5) coefficients. Our

algorithm use four(DC, 3AC, (0,1,2,3)) and six coefficients (DC, 5 AC (0,1,2,3,4,5)) of the DCT coefficients for 8×8 block.

In order to compute MCD for full image (256×256), DCT coefficients of the 8×8 pixel block is slid by one pixel along the image from the upper left corner to the lower right corner.

The proposed algorithm for detection of copy-moved forgery image is as follows:

```
If  (MCD == 0.0)
        copy-move block
else                                    (7)
        not copy-move block
```

0	1	4					
2	3						
5							

Fig. 1. DCT four (0,1,2,3) and six (0,1,2,3,4,5) low frequency coefficients for 8×8 pixel block.

From equation (7), if the value of MCD were 0.0, the block is a copy-move forgery block. Because the equation (6) is 0, copy block image is same moved block image. If the value of MCD were not 0.0, block is not copy-move forgery block. Because te equation (6) is not 0.0, the block image is not equal copy-moved block image.

4. EXPERIMENTAL RESULTS

We have implemented the detection algorithm in C language and tested copy-moved forged some test images. The size of test images [11] are 8 bits, 256×256 pixels. The test images were cropped. We have tampered Lena, Man, 3-Car, Tank images by copy-moved one image block over another, in the same image.

The images are scanned from the upper left corner to the lower right corner while sliding a 8×8 block. For each block, the DCT transform is calculated. The matching criterion of copy-moved forgery image detection (MCD) used equation (7) based on DCT four coefficients and DCT six coefficients (Fig. 1). From equation (7), if the value of MCD were 0.0, the block is a copy-move forgery block. Because sum of difference for block is 0, copy block image is same moved block image. If the value of MCD were not 0.0, the block is not copy-move forgery block. Because sum of difference for block is not 0.0, the block image is not equal copy-moved block image.

In this paper, the computation number of the DCT coefficients need four and six, and the block computation number per one block in order to detect copy-move forgery block is (N-B+1)× (N-B+1) for N×N image.

Fig. 2 and 3 show original Lena and Man original images, copy-move forgery image, detection of copy-move forgery image. From figure 2(c), 3(c), upper black rectangular (64×64) is copied block, the

(a) Original Image (b) Copy-Move forgery (c) Detection Copy-Move forgery (Black box)

Fig. 2. Lena image

(a) Original Image (b) Copy-Move forgery (c) Detection Copy-Move forgery (Black box)

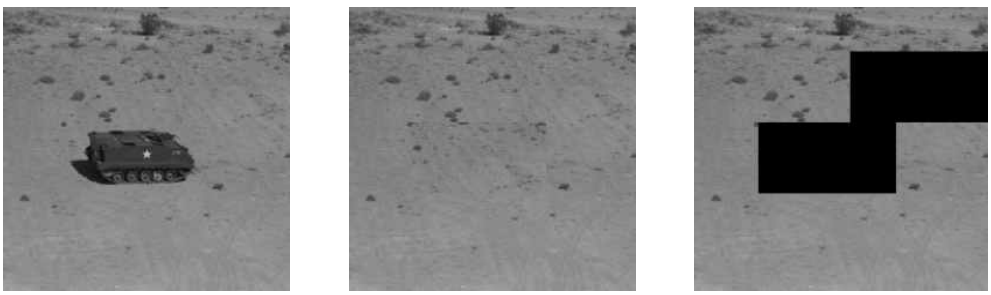
Fig. 3. Man image

other black rectangular (64×64) is a moved forgery image. The figure 2(c) and 3(c) used four (01,2,3) low frequency DCT coefficients of 8×8 pixel block. From figure 2(c), 3(c), the duplication image show copy-move forgery images perfectly (100% forgery image detection).

Fig. 4 and 5 show original 3-Car and Tank original images, copy-move forgery image, detection of copy-move forgery image. From figure 4(c), 5(c), upper black rectangular is copied block, the lower black rectangular is a moved forgery image. The figure 2(c), 3(c), 4(c), and 5(c) used four (0,1,2,3) low frequency DCT coefficients of 8×8 pixel block. From figure 2(c), 3(c), 4(c), and 5(c), the duplication images show copy-move forgery images perfectly (100% forgery image detection). Because the proposed MCD used four (0,1,2,3 of Fig. 1, DCT-4 low frequency of Table 1) and six (0,1,2,3,4,5 of Fig. 1, DCT-6 low frequency of Table 1) low frequency coefficients of DCT. If the value of 8×8 pixel block MCD was 0.0, the 8×8 pixel block is a copy-move forgery block. Because sum of dif-

(a) Original Image (b) Copy-Move forgery (c) Detection Copy-Move forgery (Black box)

Fig. 4. 3-Car image



(a) Original Image (b) Copy-Move forgery (c) Detection Copy-Move forgery (Black box)

Fig. 5. Tank image

Table 1. Comparison results of other methods for test images

Algorithms	Image representation	Block size	Block number	Feature dimension	Computation complexity (reference [1])
Fridrich[1]	DCT	8×8	$(256-8+1)^2$	64	100.0 %
Popescu[2]	PCA	8×8	$(256-8+1)^2$	32	50.00%
Kahn[9]	DWT	8×8	$(128-8+1)^2$	64	26.01%
Proposed-1	DCT-6 low frequency	8×8	$(256-8+1)^2$	6	9.37%
Proposed-2	DCT-4 low frequency	8×8	$(256-8+1)^2$	4	6.25 %

ference for 8×8 pixel block is 0, copy block image is same moved block image.

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT transforms a signal or image from the spatial domain to the frequency domain. The criterion of detection of copy-moved forgery using DCT coefficients is sufficient by four and six coefficients instead of 64 coefficients for 8×8 pixel block to reduce computation complexity. The table 1 shows computation complexity for test images (256×256) [5,9].

From Table 1, the computation complexity for the proposed method compared to Fridrich[1], Popescu[2], and Kahn[9].

Total Complexity for 256×256 image of the proposed method was reduced 93.75% than Fridrich [1]. Therefore, the computation complexity of our algorithm more efficient than conventional algorithms [1,2,9].

5. CONCLUSION

In this paper, we proposed a fast detection method of copy-move forgery image based on low frequency coefficients of the DCT coefficients. We proposed a new matching criterion of copy-moved forgery image detection (MCD) using DCT. The proposed method used DCT (Discrete Cosine Transform) with 8×8 pixel block. For each 8×8 pixel block, the DCT transform is calculated. Our algorithm uses low frequency four (DC, 3 AC coefficient) and six coefficients(DC, 5 AC coefficients) of DCT per 8×8 pixel block. Our algorithm worked block matching for DCT coefficients of the 8×8 pixel block is slid by one pixel along the image from the upper left corner to the lower right corner. Our algorithm can reduce computational complexity more than conventional copy moved forgery detection algorithms.

6. REFERENCES

[1] J. Fridrich, D. Soukal, and J. Lukas "Detection of Copy-Move Forgery in Digital Images," *Proc. of Digital Forensic Research Workshop*, pp. 55-61, 2003.

[2] A.C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," *Dartmouth College, Hanover, New Hampshire, USA*:TR2004-515, 2004.

[3] J. Zhang, Z. Feng, and Y. Su, "A New Approach for Detecting Copy-Move Forgery in Digital Images," *11th IEEE Singapore International Conference on Communication Systems* pp. 362-366, 2008.

[4] E.S. Khan and E.A. Kulkarni, "An Efficient Method for Detection of Copy-Move Forgery using Discrete Wavelet Transform," *International Journal of Computer Science and Engineering*, Vol. 2, No. 5, pp. 1801-1806, 2010.

[5] H.J. Lin, C.W. Wang, and Y.T. Kao, "Fast

Copy-Move Forgery Detection," *WSEAS Transaction on Signal Processing,* Vol. 5, Issue 5, pp. 188-197, 2009.

[6] Y.D. Shin, "Fast Detection of Copy-Move Forgery Image using Three Step Search Algorithm in the Spatial Domain," *ICHIT2012, Lecture Note in Compute Science 7425*, pp. 389-395, 2012.

[7] B.G. Jeong and I.K. Eom, "Detection of Copy-Move Forgery Image Wavelet Domain," *Proc. of the 23-th Korean Signal Processing Conference*, Vol. 23, pp. 1-2, 2010.

[8] K.R. Kwon, B.H. Koo, and J.H. Kim, "Multimedia Image Processing : Adaptive Digital Watermarking for Copyright Protection of CAD Data," *Journal of Korea Multimedia Society,* Vol. 9, No. 6, pp. 709-719, 2006.

[9] S. Kahn and A. Kulkarni, "Reduced Time Complexity for Detection of Copy-Move Forgery using Discrete Wavelet Transform," *International Journal of Computer Applications,* Vol. 6, No. 7, pp. 31-36, 2010.

[10] P. Yip and K. Rao. *Discrete Cosine Transform: Algorithms, and Applications*, Academic press, Boston, 1990.

[11] SIPI Image Database http://sipi.usc.edu/database.

Yong-Dal Shin

Yong-Dal Shin is a professor in department of IT & securities at Youngdong university, Choongpook Korea. He received PH.D. degree from Kyungpook national university, Daegu Korea, 1994. He research areas include multimedia security, digital watermarking, digital forensics.