ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(8), DOI: 10.17485/ijst/2016/v9i8/87900, February 2016* ISSN (Online) : 0974-5645

A Novel Method to Detect Copy-move Tampering in Digital Images

V. Thirunavukkarasu and J. Satheesh Kumar*

Department of Computer Applications, Bharathiar University, Coimbatore-641046, Tamil Nadu, India;
arasu_mca3@yahoo.com, jsathee@rediffmail.com

Abstract

Background/Objectives: Copy-move is one of the familiar and crucialimage tampering techniques. To develop a method that automatically detect and locate the copy moved region is a primary objective. **Methods/Statistical analysis:** A novel method that employs Discrete Cosine Transform (DCT) to transform image spatial co-ordinates into frequency co-efficientis introduced. The 2D-DCT is applied to each sub blocks of tampered image and the high frequency co-efficient of each sub-blocks are extracted as a feature vector. These feature vectors are matched and tampered regions are located. **Findings:** The proposed method effectively detects and locates the tampered region in an image without using any authentication code or signatures. It also detects very small and multiple copy-move region. The efficiency of proposed method is evaluated on several test images. The results indicate that the accuracy of the method is high, number of false matches and dimension of feature vectors are reduced over the existing methods. **Application/Improvements:** The proposed method can be applied to criminal investigation, journalistic photography, law-enforcement,and medical imaging. The dimension reduction techniques may be implemented to reduce computation complexity and improve accuracy.

Keywords: Copy-move, Dimension Reduction, False Matches, Feature Vector, Tampering

1. Introduction

Images and videos are the main sources of evidence in forensic investigation, the reliability of these sources are questioned due to simplicity in counterfeit its original content. Tampered images will destroy someone's solitude and reputation. It will deceive the public opinion and cause serious threats in security of digital images. Developing a robust and consistent method to ensure the truthfulness and legitimacy of digital images is one of the growing areas of research in image processing[1]. Active and passive are the two approaches used in image tamper detection. In active approach authentication code is inserted in to an image,by verifying the authentication code reliability can be ensured, digital watermarking and digital signatures are the two active techniquesemployed in image tamper detection[2,3]. Passive approach does not contain any authentication code or signature rather user specified algorithms are used for tamper detection[4,5].

Among the other techniques,copy-move is one of the common image tampering techniques. Since the duplicated regions are from the same image, it has similar properties like color, noise and texture. Figure 1 shows an example for copy-move image tampering[6].

(a) Original image (b) A copy-move tampered image

Figure 1. An example for copy-move tampering.

Organization of this paper includes section IIwhich describe related works on copy-move tamper detection, section III introduce the proposed work, experiments and result are discussed in section IV and section V draws conclusion.

* *Author for correspondence*

2. Related Works

Many passive techniques have been proposed to detect copy-move forgery, which can be categorized in to two groups namely block based and feature based approaches. Fridrichet al.analyzed exhaustive search,autocorrelation method and proposedDiscrete Cosine Transform (DCT) based method to detect copy-move forgery. The method effectively detects copy-moved region even the tampered region is enhanced or retouched but the algorithm detects false matches in flat and uniform areas[7].Popescuet al. introduced an efficient technique which employsPrincipal Component Analysis (PCA) for fixed size blocks to reduce the feature dimension. The accuracy of the method is improved over DC Thowever it is not efficient for small block size, low Signal Noise Ratio (SNR) and low JPEG qualities[8]. Zhao et al.implements a robust method based on DCT and Singular Value Decomposition (SVD). The method detects copy-move region even the source image is affected by Gaussian noise, blurring and JPEG compression[9].Qiuminet al. proposed log-polar based method to revel copy move region even the tampered region is influenced with scaling and rotation however it is more expensive when computing Discrete Fourier Transformation to every block (DFT)[10]. Weihaiet al. implements block artefact grid extraction method to detect the copy-move region which includes multi-compression and truncation. The computational load and clarity of the grid map is the most important challenge in this method[11]. The accuracy and computational complexity are thekey factors in tamper detection algorithm. The proposed method exactly detects small and multiple copy-move tampered regions with reduced dimension over the existing methods.

3. The Proposed Detection Algorithm

Transform coding is a primary component in modern image and video processingapplications. The proposed algorithm employs DCT to transform the image element from spatial domaintofrequency domain.

3.1 Discrete Cosine Transform

DCT is an important transformation technique used in image and video compression standards.Itexhibits excellent de-correlation and energy compaction characteristics which helps to remove the redundancy and bundle the energy withfew coefficients. The separable property of DCT aids to apply 1-D transformation to rows and columns. The DCT root functions are orthogonal which assist to reduce computational complexity. The one dimensional and two dimensional DCT are described as follows.

3.1.1 TheOne Dimensional DCT

The one dimensional discrete cosine transformation can be represented as

$$c(u)=\alpha(u)\sum_{x=0}^{N-1} f(x)\cos\left(\frac{(2x+1)u\pi}{2N}\right) \quad \text{for u=0,1,2,\&..N-1}$$

where,

$$\alpha(u)=\begin{cases}\sqrt{\frac{1}{n}} & for\ u=0\\ \sqrt{\frac{2}{n}} & for\ u=1,2,...,N-1\end{cases}$$

The value of c(u) is called one dimensional DCT coefficient of spatial gray scale value f(x).

3.1.2 The Two Dimensional DCT

The two dimensional discrete cosine transformations can be represented as

$$c(u,v)=\alpha(u)\alpha(\mathrm{v})\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)[\cos\left(\frac{(2x+1)u\pi}{2N}\right)\cos\left(\frac{(2x+1)\,\mathrm{v}\,\pi}{2N}\right)]$$

for u=0, 1, 2….N-1 and v=0, 1, 2…..N-1
where,

$$\alpha(u)\ or\ \alpha(v)=\begin{cases}\sqrt{\frac{1}{n}} & for\ u\ (or)v=0\\ \sqrt{\frac{2}{n}} & for\ u\ (or)v=1,2,...,N-1\end{cases}$$

The value of c (u, v) is called two dimensional DCT coefficient of spatial gray scale value f (x, y).

3.2 Algorithm Framework

The proposed copy-move tamper detection algorithm framework is shown in Figure 2. The whole detection framework includes six steps:(1) Preprocessing the suspected image (2) Dividing the preprocessed image into fixed size overlapping blocks (3)Dividing each overlapping blocks into non-overlapping sub blocks (4)

Apply 2D-DCT to each sub block (5) Extracting features from each sub-block (6) Matching and locating the tampered region.

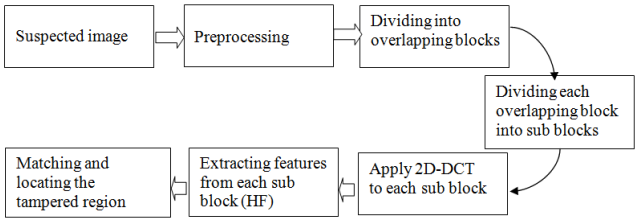

Figure 2. The algorithm framework of proposed method.

Step 1: In the first step check the suspected image is gray scale or color image, if it is color image convert to gray scale using the standardformula

$Y = 0.299\ R + 0.587\ G + 0.114\ B$

where, R,G, and B are the three colour channels of suspected image.

Step 2: After pre-processing the input image is divided into overlapping blocks of fixed size b X b.Each adjacent overlapping blockhas one different row and column. The size of the overlapping blocks should not exceed the size of the tampered region. Each overlapping blocks are denoted by $OB_{ij}$where i and j denotes starting position of row and column of a particular block. The total number of overlapping blocks are (M-b+1)(N-b+1). WhereM, Ndenotes the size of the suspected image and b denotes the block size, here the sizes of the overlapping blocks are assumed as 8 X 8.

Step3: All the overlapping blocks are further divided into non-overlapping sub blocks of size nb.

Step 4: 2D-DCT is applied to each non-overlapping sub blocks.

Step 5: Each sub blocks contains both low and high frequency DCT coefficients. The high frequency coefficients from each sub-blocks are extracted and arranged in a two dimensional matrix and the rows of a matrix are lexicographically ordered. For each overlapping block 60 high frequency coefficients are extracted.

Step 6: Each row in a two dimensional matrix is compared to match the identical blocks. If two rows are identical the algorithm stores the position of identical rows and shift vector (SV) is calculated.

$SV = (SV1, SV2) = (i_1 - j_1, i_2 - j_2)$

The algorithm removes the false matches by finding the shift vector whose occurrence exceeds user specified threshold (T).

4. Experiments and Results

The proposed method is evaluated with Intel core i5 processor and Mat lab R2013a environment.The test images are taken from three different datasets. The first dataset contains 10 different source images each of size is 200 X 200 pixels[12]. The second image dataset holds 24 PNG color images of size 768 X 512 pixels released by Kodak Corporation for unrestricted research usage[13]. The third data set contains different uncompressed PNG images of different sizes[14]. In the experiment the parameters are set as b=8, nb=4 and T=5[15]. The result of proposed method is shown in Figure 3 and Figure 4.

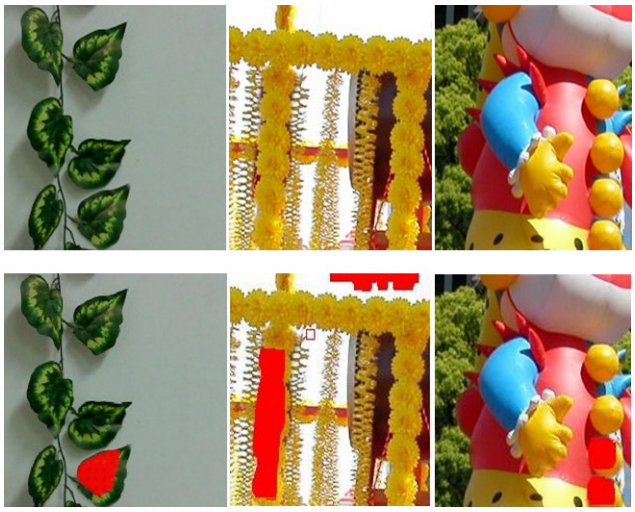

Figure 3. The top row exhibitsthe three tampered images with different sizes, the bottom rowistheir corresponding detection results.

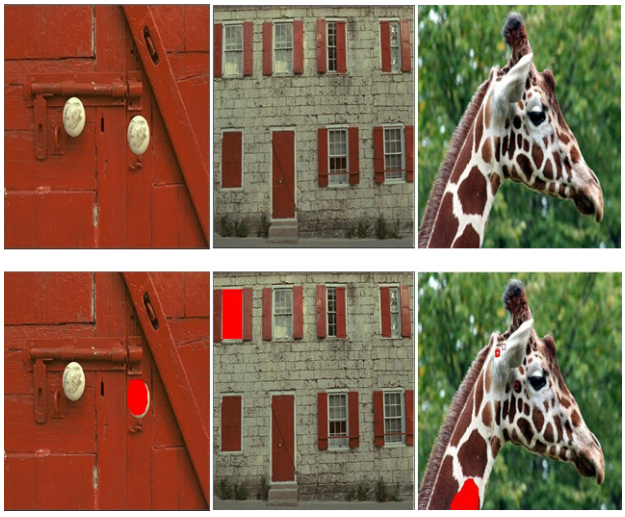

Figure 4. The first two tampered images in the top roware in size 768 X 512, third tampered image Of size 800 X 533, the bottom row shows the corresponding detection result.

4.1 PerformanceEvaluation of Proposed Method

The performance of proposedmethod is evaluated in two levels such as image level and pixel level. In image level it identifies whether the image is tampered or not. In the pixel level it shows how accurate the method will detect the tampered region. Accuracy rate and false positive are used to evaluate the performance.

$$AR = \frac{CDB}{TTB}$$

where, TTB is total tampered blocks and CDB is number of correctly detected blocks

$$FP = \frac{DGR}{TNB}$$

where, TNB is total number of blocks and DGR refers detected genuine region as tampered region. The detection performances of proposed method for various test images are shown in Table 1.

Table 1. Detection performance for different images

Image	Size	Accuracy Rate (AR%)	False Positive (FP%)	Time (seconds)
Leaves	200 X 200	100	-	23.996
String of flowers	200 X 200	95	4.1	21.880
Toy	200 X 200	100	-	21.358
Door knob	768 X 512	100	-	225.275
Building	768 X 512	100	-	229.919
Giraffe	800 X 533	99.5	0.03	264.598

5. Conclusion

In this paper a novel passive method using DCT is presented to detect copy-move forgery in digital images without using watermarking and digital signatures. Taking advantage of high frequency components of DCT coefficients,the tampered regions were automatically detected. The experimental results show that proposed method is efficient even tampered region is enhanced or retouched. It alsodetects small and multiple forged regions. Comparing with existing methods proposed method has lower computational complexity and high accuracy rate.This work can make a little contribution in the area of image forensics.

6. References

1. Farid H.Exposing digital forgeries in scientific images. Proceedingsof the 8th workshop on Multimedia and Security; 2006. p. 29–36.
2. Khan A, Siddiqa A, Munib S, Malik S A.A recent survey of reversible watermarking techniques. Information Sciences. 2014; 279:251–72.
3. Tong X, Liu Y, Zhang M, Chen Y. A novel chaos-based fragile watermarking for image tampering detection and self-recovery. Signal Processing and Image Communication. 2013; 28(3):301–08.
4. Thirunavukkarasu V, Satheesh Kumar J. Evolution of blind methods for image tamper detection-A review. International Journal of Applied Engineering Research. 2014; 9(21):5069–76.
5. Thirunavukkarasu V, Satheesh Kumar J.Intrusive and non-intrusive techniques for detecting fake images. International Journal of Business Intelligence. 2014; 3(01):374–79.
6. Farid H. A survey of image forgery detection. IEEE Signal Processing Magazine. 2009; 2(26):6–25.
7. FridrichAJ, SoukalmBD, Lukas AJ. Detection of copy-move forgery in digital images. Proceedings of Digital Forensic Research Workshop; 2003. p. 19–23.
8. Popescu AC, Farid H. Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing. 2005; 53(10):3948–59.
9. Zhao J, Guo J. Passive forensics for copy-move image forgery using a method based on DCT and SVD. Forensic Science International. 2013; 233(1–3):158–66.
10. Wu Q, Wang S, Zhang X. Log-polar based scheme for revealingduplicated regions in digital images. IEEE Signal Processing Letters. 2011; 18(10):559–62.
11. Li W, Yu N, Yuan Y.Doctored JPEG image detection.IEEE International Conference on Multimedia and Expo; Hannover; 2008. p. 253–56.
12. Muhammad G, Hussain M, Khawaji K, Bebis G. Blind copy move imageforgery detection using dyadic un-decimated-wavelet transform. Proceedings of 17th Digital Signal Processing (DSP) Conference; Corfu: Greece; 2011 Jul.
13. Kodak Lossless True Color Image Suite [Internet]. [Cited 2013 Jan 27]. Available from: http://r0k.us/graphics/kodak.
14. Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E. An evaluation of popular copy-move forgery detection approaches. IEEE Transactions on Information Forensics and Security. 2012; 7(6):1841–54.
15. Park H-J, Seo S-T, Song B-S. Clinical decision support system for patients with cardiopulmonary function using image processing.Indian Journal of Science and Technology. 2015 Apr; 8(S8):83–88. doi: 10.17485/ijst/2015/v8iS8/64331.