DCT based Forgery Detection Technique in Digital Images

Reshma R. Chaudhari
Computer Engineering
Viva-Tech

Nutan C. Malekar
EXTC Department
Viva-Tech

Meena B. Vallakari
EXTC Department
Viva-Tech

Kushal Suvarna
EXTC Department
Viva-Tech

ABSTRACT
Now a day's images are tampered easily because availability of powerful image processing software and improvement of human computer knowledge. Manipulation of digital images in different fields like court of law and medical imaging create a serious problem nowadays. With rapid advances in digital image processing software, there is a widespread development of advanced tools and techniques for digital image forgery. The most common types of forgery is Copy-move forgery which copies some part of the image and pastes it to another part of the same image to cover an important scene. In this paper, the proposed method to detect Copy-Move forgery is by matching the mean and DCT low frequency coefficient components of each block with remaining all blocks. The color image is converted from RGB color space to YCbCr color space. Y-component is partitions into fixed-size overlapping blocks and, features are extracted from each image blocks. The feature vectors obtained are then lexicographically sorted to make similar image blocks neighbors and duplicated image blocks are identified using Euclidean distance as similarity criterion. The experimental results prove that the proposed method works on reasonable time and works well for gray scale and color images. In this method by using the comparison of mean value and sorting technique helps to reduced the computational complexity.

General Terms
Pattern recognition, Security, Algorithms et. al.

Keywords
Copy move detection, Image forgery, Discrete cosine transform, Image tempering, duplication of region.

1. INTRODUCTION
Any image manipulation can become a forgery, based upon the context in which it is used. An image altered for fun or someone who has taken a bad photo, but has been altered to improve its appearance cannot be considered a forgery even though it has been altered from its original capture. On the other side, some people create a forgery for gain and prestige and to make the recipient believe that the image is real and not the fake one. Three types of forgeries can be identified:

a) Using Graphical Software is one method in which a forged image can be created. It specially needs a skilful creator who can ensure that the image he is creating is realistic, e.g. that the fall of light on objects in an image is consistent right across the image, that shading is consistent, the absorption of light by an object etc. An image created using this method takes some time to develop.

b) Creating an image by altering its Content is another method. In this, the recipient is duped to believe that the objects in an image are something else from what they really are. The image itself is not altered, and if examined will be proven as so.

c) Creating an image by altering its Context is the third method. In this, objects are removed or added from an image resulting in copy-move forgeries. E.g. a person can be added or removed. The easiest way is to cut an object from one image and insert it into another image by using various image / photo editing software's.

Digital image forgery categorized in three groups; Copy-Move, Image splicing and Image retouching. Copy-Move forgery or Region-Duplication forgery is the most important type of forgery, in Copy-Move some part of the image copies and pastes into another part of the same image to create a new thing or to hide an important scene [1]. Image splicing is the procedure of creating a fake image by cutting one part of an image and paste it to another image. It works on combining few images to create one tampered image. One of the problems is that, when the backgrounds in the images are different the objects in result may appear unclear [2]. Image Retouching doesn't obviously change the image, so it can be considered as the less corrupting type of digital image forgery, it just enhance some features of image. It is famous among magazine photo editors and most of magazine covers use this technique to change some features of an image but it is ethically wrong [2].

Detection of copy-move forgery invented to search the copied regions and their pasted ones, but detection may vary based on whether there has been any post-processing on copied part before paste it to another part. Usually attackers will do some operations such as rotation, filtering, JPEG compression, resizing and noise addition to the original part before pasting, and these operations make it difficult to detect copy-move forgery, therefore forgery detector should be robust to all manipulations. The Copy-Move image forgery is illustrated in the Fig 1.

The cloned regions can be of any shape and location, it is computationally impossible to search all possible image locations and sizes. Several methods have been developed to detect copy-move forgeries. In [3], Fridrich et al first described the exhaustive search indicating that its applicability is limited mainly because of its exponential complexity and the fact that it fails in case of any distortion. In the same paper, they proposed a more effective approach, which uses a robust representation of the block that consists of quantized discrete cosine transform (DCT) coefficients.

Popescu et al. proposed a resembling method [4], which used principal component analysis (PCA) instead of DCT to generate the block representation. They went further by reducing by half the numbers of features used in [3] and therefore improving the efficiency. Despite these improvements, their method has some weaknesses, among which its failure in case of slight rotation of the copied region. Later, Weiqi Luo et al. [5] presented a technique robust to various forms of post region duplication processing, including blurring, noise contamination and lossy compression. They represented each block by 7 characteristics extracted from both the RGB color image and the YCbCr corresponding image. Li Kang et al. [6] suggested applying improved singular value decomposition to each image block to yield a reduced dimension representation and then lexicographically sort the feature matrix formed by the singular values. Their method was proven to be robust against noise distortion. Weihai Li et al. [7] proposed a rotation-robust algorithm based on the Fourier-Mellin Transform of image's blocks with features extracted along radius direction. Recently, Y. Huang et al. [8] proposed an improved DCT-based method. In their approach, DCT is applied to each block to represent its features and then truncating it yields a reduced dimension representation of the features. Their method has been proven to be robust to JPEG compression, blurring or AWGN distortions but they failed to consider the multiple copy-move forgery. Most recently, Yanjun Cao et al. [9] proposed an approach based on improved DCT that has the advantages to be robust to various attacks, such as multiple copy-move forgery, Gaussian blurring, and noise contamination; and also to have a lower computational complexity.

a **b**

Fig 1: a) original image b) copy-move forgery image

The authors Popescu has apply a principal component analysis (PCA) on small fixed size image blocks to yield a reduced-dimension representation [10]. This representation robust to minor variations in the image due to additive noise or lossy compression. Li et al. calculated the similarity of blocks based on discrete wavelet transform and singular vector decomposition (DWT-SVD) and Luo et al. measured block characteristics vector from each block [11,12].

In this paper, we propose a mean and DCT-based approach, which is not only robust to multiple copy-move forgery, noise contamination, but also to rotation with an angle up to 5 degrees. The rest of the paper is organized as follows: Section 2 described the proposed method and Section 3 presents the experimental results and finally conclusion is drawn in Section 4.

2. PROPOSED METHOD

In copy-move forgery, since the copied regions come from the same image, at the end of the process, we will have relatively similar areas in the image. The detection of such forgery will therefore consist in finding wide relatively similar areas in an image. The easiest way to detect those areas is the exhaustive search but this can only be done for very small images because it is computationally costly. Moreover, it fails when the copied region is further processed. To make the detection more efficient, we will use the most common approach that starts by dividing the suspected image into overlapping blocks. Once the division is done, robust features must be extracted from the blocks in order to have an efficient detection rate. At last, the features are sorted to make a sufficiently reliable decision based on the similarity of consecutive pairs [13].

The different steps of our method are presented as follows:

1. Convert the RGB image to YCbCr colour space. If the given image is grey image then keep it as it is.

   $Y = 16 + (0.299*R) + (0.587*G) + (0.114*B)$

   $C_b = 128 – (0.168736 *R) – (0.331264*G) + (0.5*B)$

   $C_r = 128 + (0.5*R) – (0.418688*') – (0.081312*B)$

2. Extract the Y-Component from the YCbCr colour space.
3. Partition an Y plane image into blocks of each size 8 x 8 (Consider the pixel as top-left pixel of the corresponding block). For example a M x N is the size of Y plane, (M-7) x (N-7) blocks will be created by selecting overlap block with one pixel shift in horizontal and vertical direction.
4. Compute 2-Dimensional DCT for each and every block sequentially of Y plane image.
5. Consider the first 6 lowest frequency component values ((0,0),(0.1),(1,0),(2,0),(2,1),(0,2)) of each DCT block, as they contribute more information to the image.
6. Compute the Mean of each block in the Y plane.

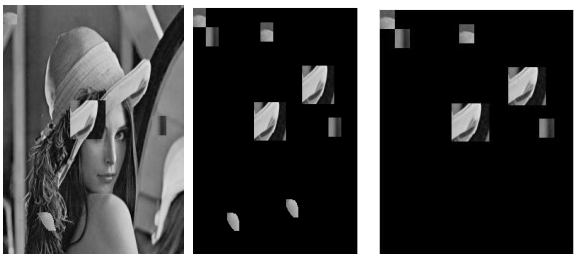
$$Mean = \frac{1}{m*n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} x(i,j)$$

7. Create a feature matrix (V) using 6 low frequency components star from (0,0) position of each block in zigzag manner and one mean value from step 6.
8. Search for the blocks with the absolute difference of the Mean within the Threshold Region ($0<\tau_1$) lexicographically (carefully neglecting the comparison with the same block).
9. If the absolute difference of Means lies within the Threshold Region ($0<\tau_1$) then compare the 6 lowest frequency values of both the blocks for matching (carefully neglecting the comparison with the same block).
10. The absolute difference of all these frequencies components are added and this value is checked for lying in the Threshold Region ($0<\tau_2$).
11. If all the above mentioned conditions are met then it is decided that the particular block of the image is forged.
12. If the image is forged then copy the contents of the forged region in a blank image so that the forged region is highlighted.

3. EXPERIMENTAL RESULTS

In this section, the performance of the proposed method on a set of forged images generated using Adobe Photoshop CS6 is evaluated and it has been implemented using Matlab 7.9. The original images are generated from different sources. Gray

scale and colored images with different size of duplication regions were considered for experimental purpose. Performance of this method is evaluated by varying the both thresholds value and block size from 8x8 to 16x16. Fig 2 shows the tempered image and corresponding detection results with different block sizes.



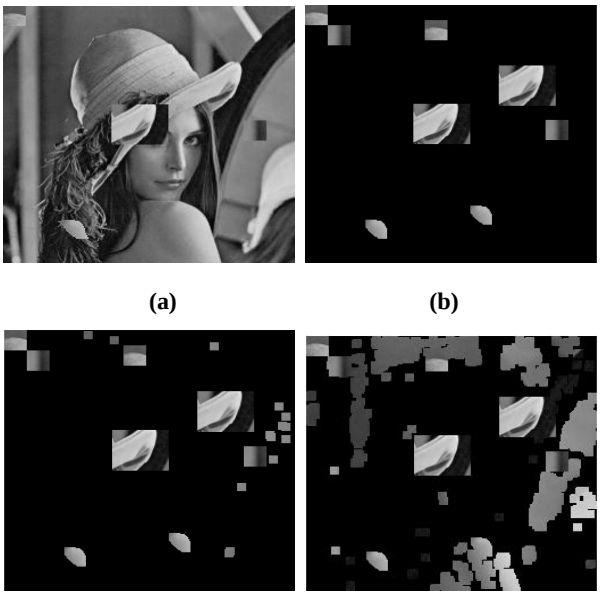
(a) (b) (c)

Fig 2: (a) Tempered image, (b) Detection result with 8x8 blocks and (c) Detection result with 16x16 blocks.

Fig 3 shows the color tempered image and its detection results with different block sizes. Fig 4 shows the quality of detection with various thresholds. If the size of forged portion is greater than or equal to block size then detection result is more accurate.

(a) (b) (c)

Fig 3: (a) Tempered color image, (b) Detection result with 8x8 blocks and (c) Detection result with 16x16 blocks.



(a) **(b)**

(c) **(d)**

Fig 4: (a) Tempered image, (b) Result with T_1=2,T_2=1, (c) Result with T_1=2,T_2=3 and (d) Result with T_1=3,T_2=7

4. CONCLUSION

In this paper algorithm for Copy-Move forgeries is presented. This algorithm falls under the category of passive methods as it does not require any prior information on the suspicious image to proceed. Experimental results show multiple copy move forgeries can be done in the same image and also is relatively robust to some common distortions. If the size of the forged part is less than that of the block used then the accuracy of this method is slightly degraded.

5. REFERENCES

[1] C. L. Jing, "Image copy-move forgery detecting based on local invariant feature," Journal of Multimedia, vol. 7, 2012.

[2] Q. S. W. Chen and W. Su, "Image splicing detection using 2-d phase congruency and statistical moments of characteristic function," E. J. Delp and P. W. Wong, editors, Proceedings of SPIE: Security and Watermarking of Multimedia Content IX, vol. 6505, p. 65050, 2007.

[3] J. Fridrich, D. Soukalm, J. Lukáš, "Detection of copy-move forgery in digital images", In proceedings of the Digital Forensic Research Workshop, Cleveland, pp. 19–23, 2003.

[4] Alin C. Popescu, H. Farid, "Exposing Digital Forgeries By Detecting Duplicated Image Regions", Technical Report TR2004-515, Dartmouth College, 2004.

[5] Li Kang, Xiao-pin Cheng, "Copy-move forgery detection in digital image", 3rd International Congress on Image and Signal Processing (CISP), vol. 5, pp. 2419 – 2421, 2010.

[6] Weiqi Luo, Jiwu Huang, Guoping Qiu, "Robust Detection of Region-Duplication Forgery in Digital Images", In proceedings of the International Conference on Pattern Recognition, Washington, DC, pp. 746-749, 2006.

[7] Weihai Li and Nenghai Yu, "Rotation Robust Detection of Copy-move Forgery", In proceedings of the IEEE 17th nternational Conference on Image Processing, Hong Kong, 2010.

[8] Yanping Huang, Wei Lu, Wei Sun and Dongyang Long, "Improved DCT-based Detection of Copy-Move Forgery in Images", Forensic Science International, vol.206, pp. 178-184, 2011.

[9] Yanjun Cao, Tiegang Gao, Li Fan, Qunting Yang, "A robust detection algorithm for copy-move forgery in digital images", Forensic Science International, vol. 214, pp.33–43, 2012.

[10] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Computer. Science, Dartmouth College, Tech. Rep. TR2004-515, 2004.

[11] Li G., Wu, Q., Tu, D., Sun, S.: A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. In: Proc. of ICME. (2007).

[12] Luo W., Huang, J., Qiu, G.: Robust detection of region-duplication forgery in digital image. In: Proc. of ICPR. (2006).

[13] N. Diane Wandji, S. Xingming, M. Fah Kue: "Detection of copy-move forgery in digital images based on DCT", IJCSI International Journal of Computer Science, Issues, Vol. 10, Issue 2, No 1, March 2013.