Detecting Copy move Forgery using DCT

Ashima Gupta[1], Nisheeth Saxena[2], S.K Vasistha[3]

Computer Science and Engineering Department
Faculty of Engineering and Technology Mody Institute of Technology and Science
Lakshmangarh,Sikar(Rajasthan)
[1]ashima1412@gmail.com, [2]nsaxena.et@mitsuniverstiy.ac.in, [3]skvasistha@gmail.com

Abstract- The use of digital photography has increased over the past few years, a trend which opens the door for new and creative ways to forge images. Now a day's several software's are available that are used to manipulate image so that the image is look like as original. Images are used as authenticated proof for any crime and if these image does not remain genuine than it will create a problem. Detecting these types of forgeries has become serious problem at present. To determine whether a digital image is original or doctored is a big challenge. To find the marks of tampering in a digital image is a challenging task. A copy-move image forgery is done either for hiding some image entity, or adding more minutiae resulting in forgery. In both the case, image reliability is lost. Although this technology brings many advantages but it can be used as a confusing tool for hiding facts and evidences. In this paper we detect region duplication forgery by applying Discrete Cosine Transform. We divide the image into overlapping blocks and then search for the duplicated blocks in the image.

Index Terms- Image forgery, Copy move forgery, PCA, Wavelet Transform, Region Duplication Detection.

I. INTRODUCTION

In today's world it is easy to manipulate the image by adding or removing some elements from the image which result in a high number of image forgeries. Using the manipulation tools that are available on internet it is easy to tamper the digital images without any trace. Therefore verification of originality of images has become a challenging task. An image can be manipulated with a wide variety of manipulation techniques such as scaling, rotation, blurring, resampling, filtering, cropping, etc. We need image forgery detection technique in many fields for protecting copyright and preventing forgery. The verification of originality of images is required in variety of applications such as military, forensic, media, scientific, glamour, etc. Image tampering is a digital art which needs understanding of image properties and good visual creativity. Detection of image tampering deals with investigation on tampered images for possible correlations embedded due to tampering operations. Detecting forgery in digital images is an rising research field with important implications for ensuring the credibility of digital images.

Digital image forgery detection techniques are classified into active and passive approaches. In active approach, the digital image requires some pre-processing such as watermarking, signature, etc. Passive approach is different to active approach; this approach does not need any watermark embedded in advance.

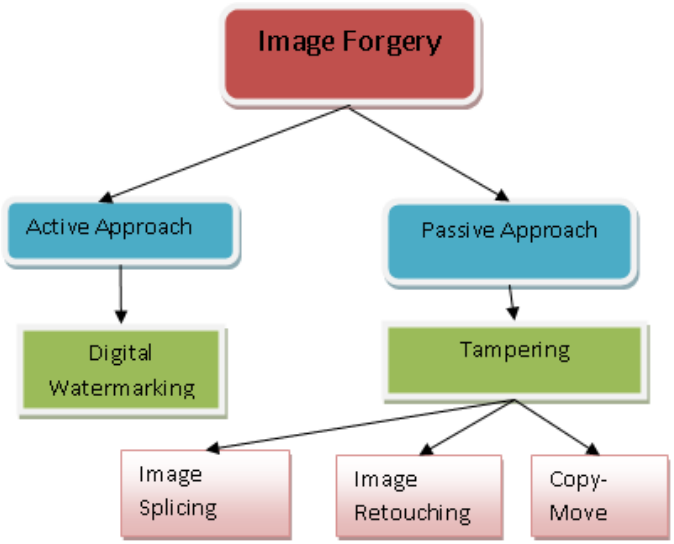


Fig. 1 Classification of Image Forgery

The copy move forgery is one of the difficult forgery. This is the most common kind of image tampering technique used, where one needs to cover a part of the image in order to add or remove information. Copy-Move is a special type of image manipulation technique in which a part of the image itself is copied and pasted into another part of the same image. Image-splicing is defined as a paste-up produced by sticking together photographic images. In a copy-move attack, parts of the original image is copied, moved to a desired location, and pasted. Detecting copy-move in an image indulges broad search of local pattern or region matches.

The structure of the paper is as follows. In section II we review the work which is already done in detection of forgery in digital images. In section III we proposed the method to detect copy-move forgery in digital images. Experimental results are shown in section IV. Lastly, we conclude the paper in section V.

II. RELATED WORK

There were several techniques proposed to detect image forgery in the literature of digital image forensics. Copy move forgery is one of the popular method to create the image forgery in which the part is copied and moved to the other place in the same image. There are so many techniques to detect such type of forgeries. One approach to detect copy-move forgery detection, proposed by Fridrich et al. [3], basically performs a rigorous search by comparing the image to every cyclic-shifted versions of it. But the complexity of this approach is very high, it requires $(mn)^2$ steps to execute for a image of size M×N so it is difficult to implement it practically.

There is a technique based on the Radon transform and phase correlation in order to improve the robustness in forgery detection. In this the proposed technique can detect forgeries even if the forged images were undergone some image processing operations such as rotation, scaling, Gaussian noise addition, etc [7]. Popescu et al [4] proposed a copy-move image forgery detection algorithm using block matching approach and Principal Component Analysis (PCA). In order to detect images through rotation, scaling and other operations quickly and efficiently, image tamper detection based on Radon and Fourier-Mellin transform is presented [5]. M. sridevi attempt to verify the authenticity of image using the image quality features like markov and moment based features. They are found to have their best results in case of forgery involving splicing [6].

One of the distinguish property of copy move forgery detection is the feature extraction process. Some methods are based on dimensionality reduction [4], [8], moments [9], [10], color properties [11], frequency domain transform [3].

Other technique to detect copy move forgery is by using Discrete Cosine Transform (DCT). Junfeng He et.al. proposed the method that can detect forged jpeg image and locate the doctored part by applying the DCT transform on images. This method has many other advantages like fast speed etc.

III. PROPOSED APPROACH

There is an approach that can detect doctored JPEG images and further locate the doctored parts, by examining the double quantization effect hidden among the DCT coefficients. Our method detects region duplication forgery by dividing the image into overlapping blocks and then we search for the matching region in the image. We show the effectiveness of this technique on credible forgeries and compute its robustness also. We can check the efficiency of algorithm for noisy figure too.

A. Region Duplication Detection

The detection of copy move forgery in digital images is done as:

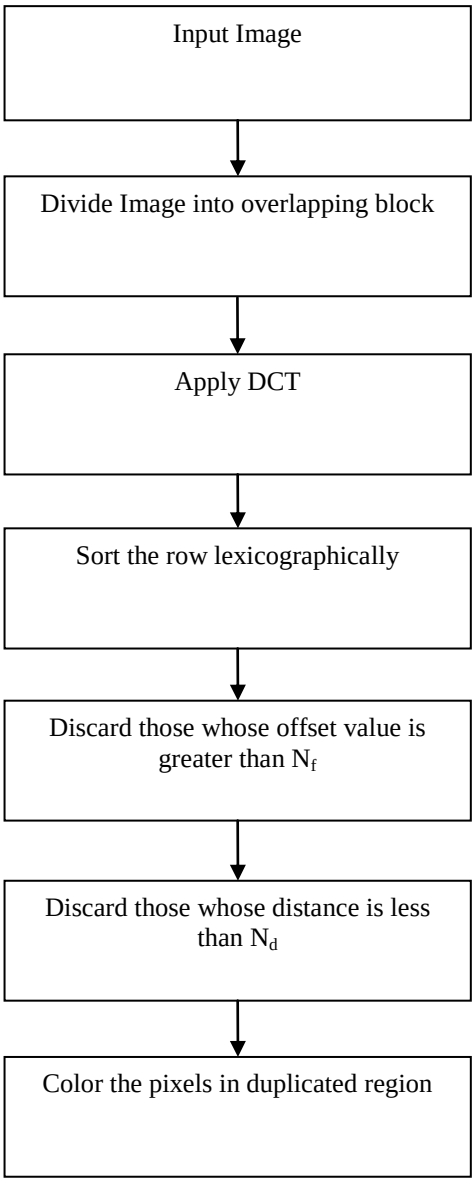


Fig. 2 Duplication Detection Algorithm

This research aims to prove that the use of DCT to detect forgery is better for jpeg images than using a predefined method PCA. We have further tried in this approach to make the program efficient by applying DCT instead of PCA. Since the PCA does not detect the forgeries for jpeg image efficiently, we apply DCT so that we detect forgery on jpeg image too. After that we compare both the approaches and find out the results and compare the results.

An experiment will be conducted to prove that the algorithm works and can be used to detect duplicated regions on a highly textured image. Once we've located the possible modified region, we need to estimate the size o the modified region and later execution time in a copy-move attack detection algorithm. We have chosen algorithm that detects copy move forgery in images of any format.

IV. EXPERIMENTAL RESULTS

We see that earlier method does not detect the forgery for jpeg format image, there is another method to detect image forgery. We can detect image forgery by using DCT also which

result in good detection for jpeg images as shown in figure. There are various steps of detecting Forgery in digital images. Here we detect region duplication image forgery in which part of image is copied and pasted. Shown in figures are original and tampered images. The tampering consisted of copying and pasting a region in the image to conceal a person or object. Shown other figures are the outputs of our detection algorithm as applied to the tampered image. In each map, the duplicated regions are shown with gray scale values.

Image 1

(a) INPUT IMAGE (.JPG)

Now we do some modification or changes in the input image and make the image tampered.

(b) TAMPERED IMAGE

After applying the algorithm we get the output image

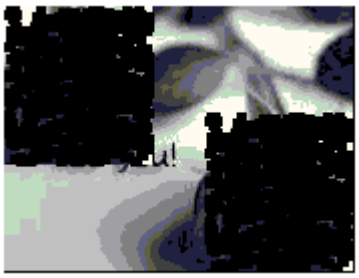
(c) OUTPUT IMAGE

Fig. 3 Forgery detection result (a) Original image (b) Tampered image (c) Detection result(Output)

Image 2

(a) INPUT IMAGE

(b) TAMPERED IMAGE



(c) OUTPUT IMAGE

Fig. 4 Forgery detection result (a) Original image (b) Tampered image (c) Detection result(Output)

A. *Experiment Configuration*

The experiment is run on a 32-bit dual core machine with a processor speed of 3.2GHz using 1GB of DDR2 RAM. The research is run using Matlab since all of the algorithms are coded in Matlab. All images are converted into grayscale. We opt for grayscale since it is simpler to handle. We coded an algorithm to randomly create a copy-move attack on all of these images.

B. *Result Analysis*

TABLE I
Comparison of execution time when block size = 4×4 (Using DCT)

Size of image	Avg. detection result	Execution time (seconds)	Execution time (using MEX function - seconds)
160×120	100%	58.2	10.85
174×132	99.9%	82.88	16.68
128×128	99%	21.86	3.96
208×144	70%	93.2	23.07

TABLE II
Comparison of execution time when block size = 8×8 (Using DCT)

Size of image	Avg. detection result	Execution time (seconds)	Execution time (using MEX function - seconds)
160×120	100%	67.2	22.8

174×132	99.9%	201.22	29.18
128×128	99%	26.21	8.22
208×144	70%	184.3	29.10

C. *Efficiency of Algorithm*

The graph shows that when the block size is increases the efficiency of detecting the forged image correctly decreases. Therefore to detect the forgery correctly we should keep the size of block small.

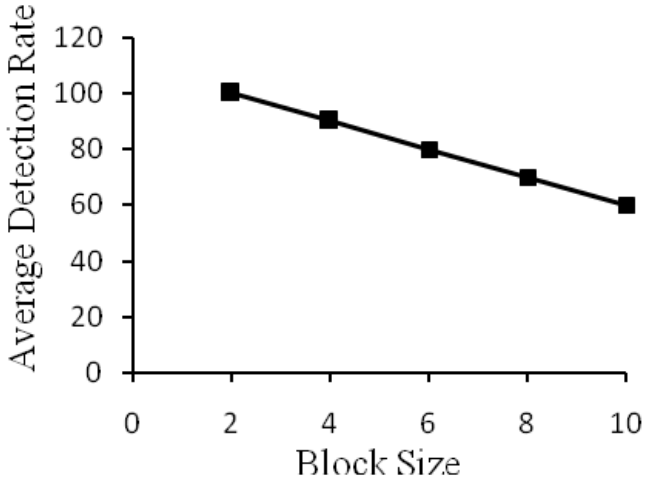


Fig. 5 Graph between Avg. Detection Rate and Block size

This graph shows that when block size is increase the average execution time of detecting the forged part of image is also increased.

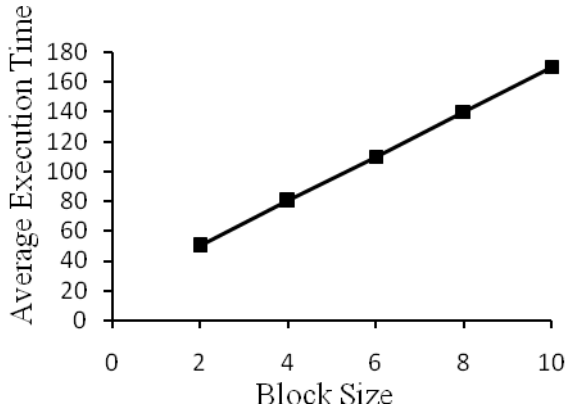


Fig. 6 Graph between Avg. Execution Time and Block size

[11] W. Luo, J. Huang, and G. Qiu, "Robust Detection of Region-Duplication Forgery in Digital Image," 18th International Conference on Pattern Recognition (ICPR'06), pp. 746-749, 2006.

[12] Junfeng He, Zhouchen Lin, LifengWang, and Xiaoou Tang," Detecting Doctored JPEG Images Via DCT Coefficient Analysis", LNCS, pp. no. 423-435, Springer, 2006.

V. CONCLUSION

Copy-move forgery is one of the most frequently applied forgery technique. In this we use a robust method to detect the duplicated region in the digital image. We have conducted some test on the algorithm against sample images from the internet. The result of the test is very encouraging since we got improvements in the detection rate and the detection time of the copy-move attack detection algorithm that we used. We are happy that the project is able to meet the outlined objectives proved that the use of DCT is better than using PCA for detecting copy-move attacks in highly textured images.

We can improve the efficiency of forgery detection by applying wavelet transform. For future work, we plan to further optimize the data structures to gain additional query performance and further improve accuracy. The process can be further extended to different formats and works for binary scale, gray scale and color images also.

REFERENCES

[1] Tao Jing Xinghua li, Feifei Zhang, Image Tamper Detection Algorithm Based on Radon and fourier-Mellin Transform",pp 212-215 IEEE 2010.

[2] Sarah A. Summers, Sarah C. Wahl"Multimedia Security and Forensic Authentication of Digital images, "http://cs.uccs.edu/~cs525/studentproj/proj52006/sasummer/doc/cs525projsummersWahl.doc".

[3] J. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images", in Proceedings of Digital Forensic Research Workshop, August 2003.

[4] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," Technical Report, TR2004-515, Department of Computer Science, Dartmouth College, pp. 758-767, 2006.

[5] Guoqiang Shen, Lanchi Jiang, Guoxuan Zhang, "An Image Retrieval Algorithm Based on Color Segment and Shape Moment Invariants," Second International Symposium. Computational Intelligence and Design vol. 10, no.2, pp. 517-521,2009.

[6] M .Sridevi, C.Mala and S.Sandeep "Copy – move image forgery detection", Computer Science & Information Technology (CS & IT) , Vol. 52 pp. 19–29, 2012.

[7] Hieu Cuong Nguyen and Stefan Katzenbeisser"Detection of copy-move forgery in digital images using Radon transformation and phase correlation" ,Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, pp. 134-137,2012.

[8] X. Kang and S. Wei, "Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics," International Conference on Computer Science and Software Engineering, pp. 926-930, 2008.

[9] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants.," Elsevier Forensic Science International, vol. 171, no. 2-3, pp. 180-189 Sep. 2007..

[10] S.-jin Ryu, M.-jeong Lee, and H.-kyu Lee, "Detection of Copy-Rotate- Move Forgery Using Zernike Moments," IH , LNCS 6387, vol. 1, pp. 51-65, 2010.