Detecting Copy Move Forgery In Digital Images

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)

Abstract

In today's world several image manipulation software's are available. Manipulation of digital images has become a serious problem nowadays. There are many areas like medical imaging, digital forensics, journalism, scientific publications, etc, where image forgery can be done very easily. 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. The detection methods can be very useful in image forensics which can be used as a proof for the authenticity of a digital image. In this paper we propose the method to detect region duplication forgery by dividing the image into overlapping block and then perform searching to find out the duplicated region in the image.

Keywords— **Image forgery, Copy move forgery, Block matching, PCA, Region duplication detection.**

I. INTRODUCTION

Apparently, the photo manipulation has a long and rich history. 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. Digital images offer many attributes like brightness and color of individual pixel for a tamper detection algorithm. An image is generally accepted as a proof of occurrence of any depicted event. Because of the availability of low cost software it is easy to manipulate image. As a result, we lost authenticity of image. We need image forgery detection technique in many fields for protecting copyright and preventing forgery. The applications in which image forgery detection technique is used are journalism, scientific publications, forensic science, glamour photography etc. Therefore, how we find out the image is true or not is very important [1]. Thus image forgery detection technique become important and emerging area in research. Image forgery refers to malicious image manipulation with intent to mislead the perception of observers [2].

The image forgery approaches are basically classified as active and passive approaches as shown in fig. 1. Both approaches use different techniques and they are further classified as:

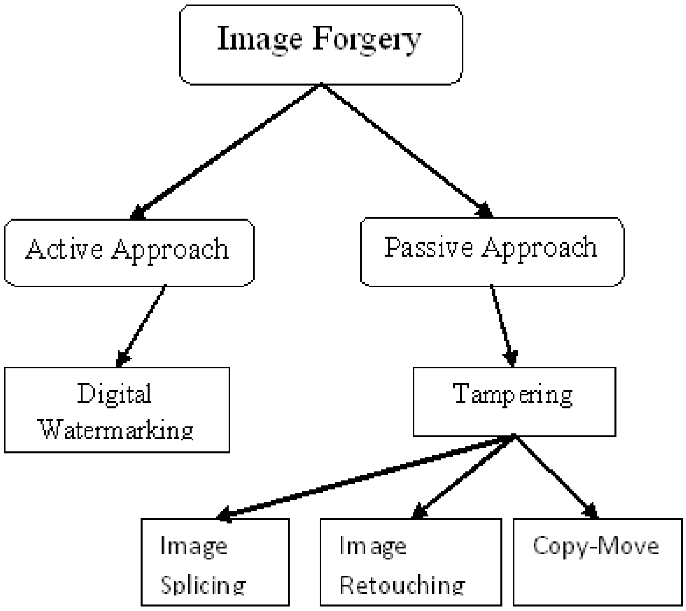


Fig. 1 Classification of image forgery

The copy move forgery is one of the difficult forgery. In a copy-move attack, parts of the original image is copied, moved to a desired location, and pasted. This is usually done in order to conceal certain details or to duplicate certain aspects of an image. Because the copied part come from the same image, its important properties, such as noise, color palette and texture, will be compatible with the rest of the image and thus will be more difficult to distinguish and detect these parts.

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.

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] .

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]. 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].

III.PROPOSED APPROACH

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 can check the efficiency of algorithm for noisy image too. We show the efficiency of this technique on credible forgeries and quantify its robustness also.

A. Region duplication detection

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

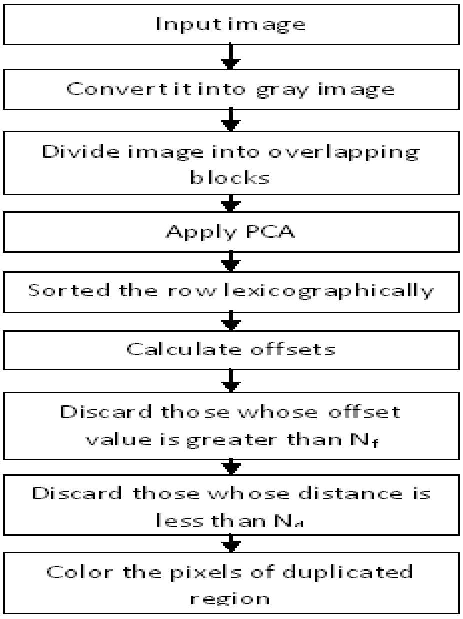

Input image
Convert it into gray image
Divide image into overlapping blocks
Apply PCA
Sorted the row lexicographically
Calculate offsets
Discard those whose offset value is greater than N_f
Discard those whose distance is less than N_d
Color the pixels of duplicated region

Fig. 2 Detection of duplicated region

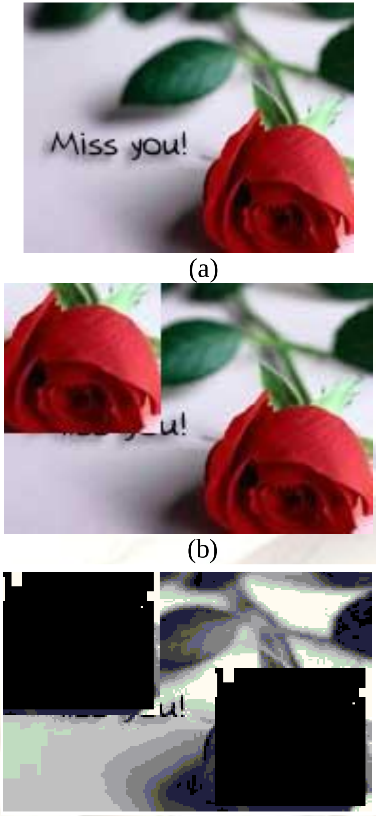
B. **Algorithm**

We start with an input image of size M×N having n number of pixels. Our task is to find out the duplicated region of unknown location and shape.

1. Read the image chosen by user.
2. If the input image is not grayscale then first convert it into grayscale image.
3. Initialize parameters:
   b – Number of pixels per block – there are $N_b = (\sqrt{N}-\sqrt{b}+1)^2$ such blocks.
   N_n – Number of neighboring rows to search in a lexicographically sorted matrix
   N_f - Minimum frequency threshold
   N_d – Minimum offset threshold
4. After that divide the image into overlapping blocks.
5. Apply PCA to reduce the dimension of image and build N_b×b matrix.
6. Now rows are sorted lexicographically. Let S be the sorted matrix and s_i denote the row of sorted matrix and (x_i,y_i) denote the position of block's image coordinate.
7. For every pair of rows s_i and s_j from S such that $|i – j| < N_n$, place the pair of coordinates $(x_i; y_i)$ and $(x_j; y_j)$ onto a list.
8. Compute offsets:
   (x_i-x_j,y_i-y_j) if $x_i-x_j >0$
   (x_j-x_i,y_i-y_j) if $x_i-x_j <0$
   $(0,|y_i-y_j|)$ if $x_i = x_j$
9. Discard pairs whose offset frequency is less than N_f.
10. Discard those pairs whose offset magnitude, $\sqrt{((x_i-x_j)^2 – (y_i-y_j)^2)}$ is less than N_d.
11. From the left over blocks, color all pixels in a duplicated area with a unique grayscale intensity value.

IV.EXPERIMENTAL RESULT

In our experiments we have tampered several internet downloaded images by copying one part of image and paste it on same image only. Our data set consist of 50 tampered images. This algorithm detects copy move forgery on these images correctly and efficiently. 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 is an original and tampered image. The forgery consisted of copying and pasting a region in the image to hide a person or object. Shown figures are the outputs of our detection algorithm which applied to the tampered image. In each representation, the duplicated regions are shown with grayscale values. Truncation of the PCA basis generally reduces the dimension from 64 to 32. We applied the procedure for different images and get the output. The outputs of some images are shown below:-



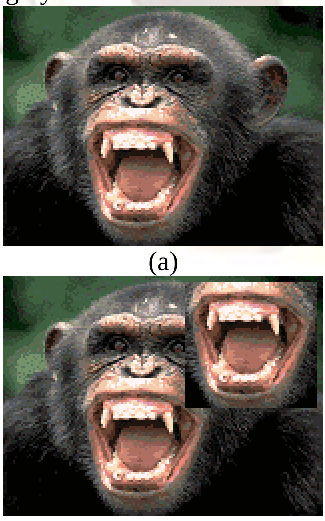
(a)

(b)

(c)

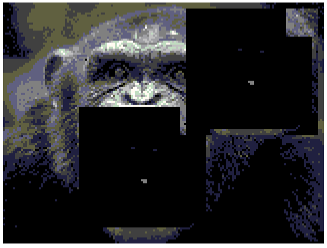
Fig. 3 Forgery detection result (a) Original image (b) Tampered image (c) Detection result(Output)

To measure the robustness and sensibility of our algorithm we constructed a database of 50 color images having different sizes. These images were taken randomly from anywhere and saved with different format like bmp, jpeg, png etc with varying signal to noise ratios (SNR). In each image, a stochastic square region was copied and pasted onto a random non-overlapping place in the image. The result of forgery detection on another image:



(a)

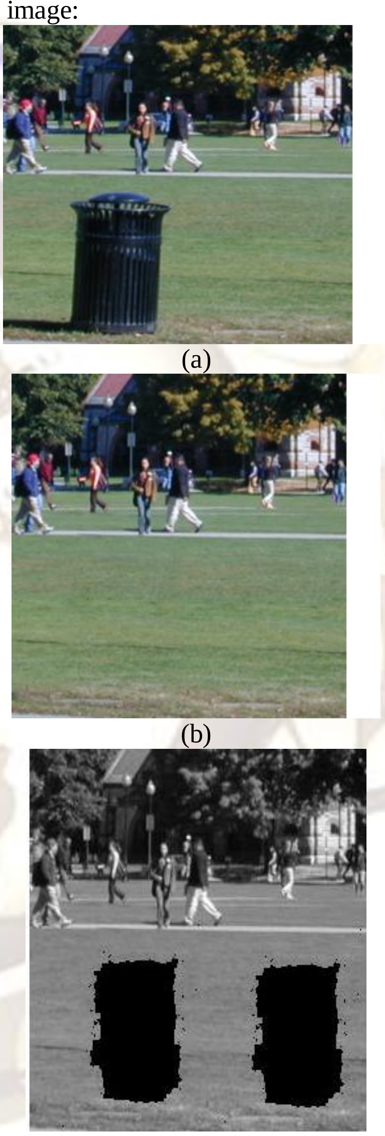
(b)



(c)

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

Another image:



(a)

(b)

(c)

Fig. 5 Forgery detection result (a) Original image (b) Tampered image (c) Detection result(Output)

Shown on the top images with duplicated regions of random sizes. In these examples, all parameters were set. It is notable that the accuracy is generally very good, except for small block sizes and low JPEG factors. It is also notable that the average number of false positives (regions incorrectly labelled as duplicated) is comparatively low.

TABLE 1

Size of image (M×N)	**Block size (b)**	**Execution time(seconds)**	**Distance of copy-move block(N_d)**
174×132	4×4	92.860214	45
	8×8	250.544609	
	4×4	106.634706	25
	8×8	271.963953	
160×120	4×4	62.987334	45
	8×8	161.275506	
	4×4	71.718857	25
	8×8	176.005020	
282×256	4×4	843.962759	45
	8×8	2263.309443	
	4×4	861.856422	25
	8×8	2352.73821	

V. CONCLUSION

Copy-move forgery is one of the most frequently applied forgery technique. In this paper, we use a efficient method to detect the duplicated region in the digital image. Firstly, the given image is divided into overlapping rectangular blocks where overlapping blocks are created. Secondly , to reduce the search area and to make the search unit as robust as possible to post processing like compression, Gaussian noise, scaling and rotation, some transformation technique is used like DCT, PCA, DWT,SVD, etc. Thirdly feature vectors, after transformation are sorted lexicographically. The neighbouring vectors are compared against the similarity parameters to hint the duplication of region which are located in the image.

For future work, we plan to further optimize the data structures to gain query performance and to improve accuracy. This approach works even if the pasted region has undergone transformations like translation and rotation.

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.

[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.