iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** VIII **Month of publication:** August 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue VIII, August 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Study and Analysis of Copy-Move Forgery Detection in Digital Image using MATLAB

Rachana[1], Ashok Kumar[2], H.L.Mandoria[3], B.K.Pandey[4]
[1]M .Tech Student, [2,4]Assistant Professor, [3]Professor and Head of Information Technology
Department of Information Technology, G. B. Pant University of Agriculture & Technology, Pantnagar, India

Abstract- with the rapid development of ubiquitous availability of imaging tools and software, it is not difficult to tamper or forge the digital image. In today's digital age, it is feasible to add or remove important features from an image without any clear traces of alteration. So there is an imperative issue to identify the authenticity of digital images in various fields such as forensics, criminal investigation, surveillance system, intelligent system, medical imaging and Journalism. Digital Image Forensic is rising and swiftly growing field of image processing area to find the authenticity of digital image. Copy-Move attack is very common type of tampering technique, where a part of an image is copied and pasted elsewhere in the same image to conceal a special object in the original image. Many block based methods have been suggested to detect duplicated region (Copy-Move forgery).One of the major challenge of these block based is the time complexity. As the image size increases the execution time of such algorithm is also increases. In the proposed method, PCA is applied to the suspected image to reduce its dimensionality. Thus, Principal Component Analysis is for digital image compression. I have devised and implemented a side matching approach to reduce the time complexity. This proposed algorithm improves the time complexity in detection of Copy-Move Forgery.

Keywords: Image forgery, digital image forensics, copy- move forgery, image tampering

I. INTRODUCTION

In the current era, digital images play important role in various field, in daily life applications in the area of military, news, medical diagnosis and media. With the enrichment of technology and ubiquitous availability of image processing tools, Digital images are vulnerable in the sense that, it can be easily the change the meaning of visual message. Sometimes it is challenging task to identify whether the image is tampered or not by the naked eyes. So, digital image is not authentic as it may be. Digital image forensic is fast growing field of image processing area to find the authenticity of the digital images. Digital image forgery detection technique is subjected to test for integrity and authenticity in many areas-forensic investigation, criminal investigation, surveillance system, intelligent system, medical imaging and journalism. These techniques are grouped into two approaches as shown in (fig1.1): a) active; and b) passive approach.

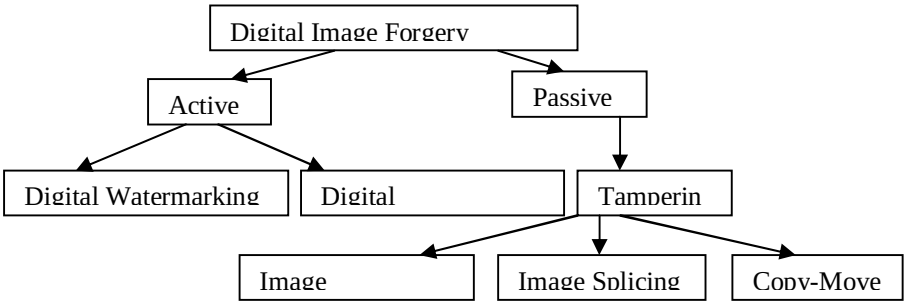
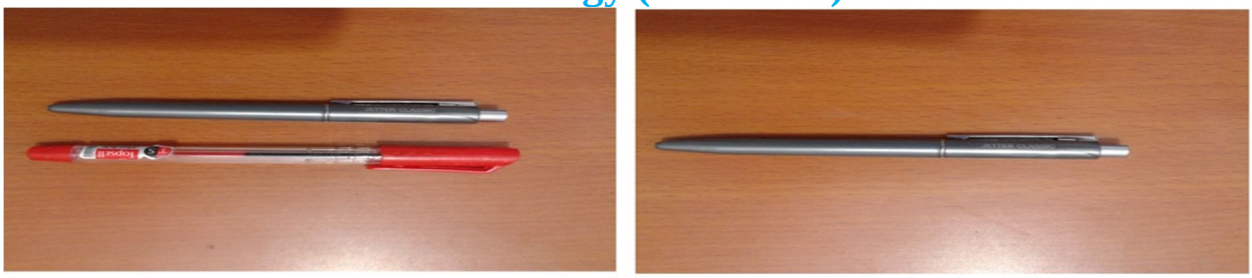


Fig 1.1: Digital Image Forgery Classification

Active approach requires some pre-processing operations, like attaching watermark and signature when producing digital images. Inserting some known information in the image at the capturing end and extracted it at authentication end to examine the authenticity of image. On the other hand, passive approach is the process of authenticating digital image without using and additional information aside from the picture themselves. More regular type of digital image forgery is copy move forgery in which a part of an image itself is one copied and pasted into another location of the same image to conceal certain details or alter the meaning of the visual message. An example of copy-move forgery is shown in (fig 1. 2).

Volume 4 Issue VIII, August 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)



(a) Original Image (b) Forged Image (Copy-Move)

Fig1. 2: Example of Copy –Move Forgery

Copy-Move forgery detection technique is used to find out the duplicated regions, some post processes such as edge smoothing, blurring and noise addition has been done which makes digital image forgery detection difficult. We focus on espy copy-move forgery in digital image. Copy-Move forgery detection method is fall under the two categories: a) Block based method; and b) key point based method.

Block based method- In this method, the suspected image is divided into overlapping blocks & then makes a comparison in blocks to detect duplicated region. Key point-based methods operate on whole image. Instead block based methods, Key point based methods compute their features only on image regions with high entropy. One of the most frequently used methods to detect such type of forgery is to use block based method.

This paper is organized into five sections. The rest of the thesis is organized as follows: The present section is followed by section 2, which provides a review of the previous work done in the field of copy –Move forgery detection. Section 3 describes the proposed method, a common workflow graph of digital image forgery detection is exercised and step by step representation of the proposed method is given. Section 4 discusses the experimental results with the proposed method and the comparison of obtained results with the previous algorithm proposed by **Sunil *et al.* (2013).** Section 5 presents the research conclusions and the suggestions for further studies.

II. RELATED STUDIES

There have been a lot of work in recent years; there are several techniques for detection of copy-move forgery in digital image. Firstly, there is a technique to espy copy move forgery, proposed by Fridrich et al. [1]. First analyzed the exhaustive search and then suggested a block matching method to espy copy move forgery. This method was based on Discrete Cosine Transformation (DCT), and lexicographic sorting is used and neighboring blocks are taken as possibly forged area. Thus these considered neighbor region are compared in the matching step .This technique in some complicated manipulation techniques like blurring or random noise addition it is not easy task to detect the forgery. To make the computation faster, Popescu et al. [2] proposed a method based on Principal Component analysis (PCA).Due to the characteristics of PCA the number of features required to present a block were reduced as the half of the numbers of the features used by Fridrich. This method has better immunity to random noise and JPEG compression. But this method is not robust to enough adequate small rotation of duplicated regions. There are some other methods proposed that can detect the copy-move forgery in the presence of more sophisticated processing, like blurring & noise addition. Mahadian [3] proposed a method based on detection of blur moments invariant, PCA and kd-tree. Li et al.[4] proposed a method based on Discrete Wavelet transform (DWT) and Singular Value Decomposition (SVD). This method works well even if the image is extremely compressed. There is a technique based on randon transformation and phase correlation is suggested by Nguyen and Katzenbeisser [5]. In order to detect images through some post processes like rotation, scaling and Gaussian noise addition. Many block based method have been introduced to determining the duplicated region in doctored image. Most of the block based methods of copy move forgery detection is precise and accurate but the computational cost is very much high and the experimental results show that the performance of the method has improved in terms of execution time There are three major approaches which may be employed to reduce time complexity of block matching methods namely decreasing number of instances, reducing feature vector dimension and improving block matching algorithm.

III. PPOPOSED METHOD

A. Workflow Structure of Copy-Move Forgery Detection Techniques

For detection of image forgery, we perform a particular series of operations on image. In this passive technique takes every image as a forged or tampered image. After we go through a particular series of operations image is categorized into two categories:

Volume 4 Issue VIII, August 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

authentic images and forged images. We describe here a typical procedure of passive detection techniques of digital image forgery has been followed as shown in Fig 3.1.

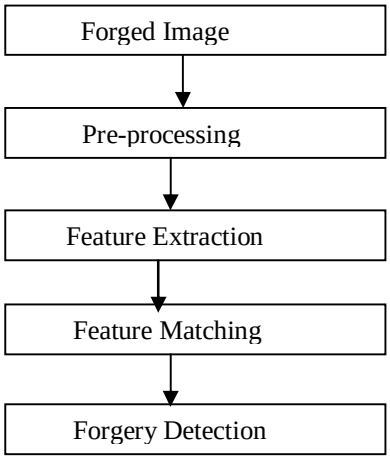


Fig 3.1: Block diagram of Copy-move forgery detection algorithm.

1) *Image preprocessing:* In this step inputted the color image and then convert it to grayscale image. Copy Move Forgery Detection method can either block based and keypoint based approach. Block based method- In this method, the suspected image is divided into overlapping blocks & then makes a comparison in blocks to detect duplicated region. Key point-based methods operate on whole image. Instead block based methods, Key point based methods compute their features only on image regions with high entropy.
2) *Feature extraction:* feature is extracted after pre-processing step. It is the process of finding a new representation of the data (image) in terms of features. The main aim of this step is to extract discriminate features that represent the data well. Avoiding redundancy and reducing the dimensionality of the data are two requirements for good features.
3) *Matching:* After feature extraction, detection of the copy move forgery method looking for the similar blocks. In this step feature vectors are matched to obtain duplicated regions in suspected image. Now is the point at which determining the duplicated block of inputted suspicious image based on their feature vectors.
4) *Forgery Detection:* In this final step of detection of duplicated region in the suspected image, the algorithm outputs a black map image; regions which are taken as duplicated region are marked with a black color.

B. Algorithm Framework

The proposed algorithm based on PCA is presented below. Aim is to find the image areas that are same or extremely similar. Methods for detecting the Copy-Move Forgery can be divided into four steps. Details are as follows:

Step 1: Converting the colored image into grayscale image:

The inputted the suspected image of size m x n, we assuming this is grayscale image. If this image is not grayscale image convert this to grayscale image from RGB color image by the luminosity method: I = 0.228R + 0.587G + 0.114B. To reduce the time complexity of overall algorithm, we use grayscale image.

Step 2: Feature Extraction (PCA):

1) Feature extraction is a process of taking out informative and non-redundant data from the image. PCA or Principal component analysis is a type of feature extraction process which deals in bringing out strong patterns in a dataset.
2) Feature extraction is a type of dimensionality reduction that efficiently represents interesting parts of an image.

PCA is applied on the grayscale image to reduce the dimension of grayscale image.

Step 3: Dividing image into blocks & Side-matching technique:

Image is divided into blocks with an initial size of 2 * 2 which keeps on increasing with a multiple of 2 (i.e. 4*4, 8*8 etc.). These blocks are then compared using side matching technique which is a successor of block matching technique. In this technique we instead of matching the entire block of image, we compare either the row side or the column side of the image. Each block is compared and their standard deviation is stored in an array. These standard deviation values are then compared with each other. The lowest standard deviation value will be the duplicate/forged region.

Step 4: Highlight the blocks that shows repetition

Volume 4 Issue VIII, August 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Those regions that show the repetition must be highlighted in such a way that the forged/tampered area is visible to human eye. This is the last step of the algorithm, in this step both, the original and duplicated region are marked with black color in order to highlight the forged region.

IV. EXPERIMENTAL RESULTS

The algorithm is implemented in MATLAB R2013a programming tools on a PC with Windows 7 and the following features:
Processor: Intel(R) Core(TM) i3-3110M CPU @ 2.40 GHz 2.40 GHz
Installed Memory (RAM): 2.00 GB
System Type: 64-bit operating system

A. Visual Results

This experiment is designed to validate the proposed method for detection of copy-move forgery. In experiment, we first forged tested images, and then detected forged images by using one method. Fig.4.1 shows the experimental results, the duplicated regions can be detected.

Fig4.1 Visual Result to show copy-move forgery detection

B. Efficiency Testing

In order to test the efficiency of the proposed method, we tested the detection time. In experimental, tested images are different in size. Table 4.1 shows statistical average values of the time cost.

Image size	128x128	256x256	384x 384	424 x424	512 x512	656 x656	832 x832
Detection time (s)	9.098	10.243	12.168	14.714	20.981	44.653	50.421

Table 4.1: Time taken to detect copy move forgery

C. The performance of the proposed system is given in terms of accuracy

The performance of the proposed system is given in terms of accuracy in Equation (4.1)

$$\text{Accuracy} = \frac{Tp + Tn}{Tp + Tn + Fn + Fp} \times 100 \qquad 4.1$$

Where:

1) T_p (True Positive) is the number of forged images, which are classified as forged images.
2) T_n (True Negative) is the number of authentic images, which are classified as authentic images.
3) F_p (False Positive) is the number of authentic images, which are classified as forged images.
4) F_n (False Negative) is the number of forged images, which are classified as authentic images.
5) The performance of the proposed method is compared with other related method namely F_DCT that is proposed by Sunil et al. (2013).

To compare the speed of the proposed algorithm with the existing method, a database of more than 50 images is developed. The database consists of images with different contrasts and resolutions.

In the first case, a low contrast image is shown in Fig. 4.2. In this image the forgery is created in this image. The proposed method successfully locates the copied and the pasted region and colors both of them as black to highlight it. In Fig. 4.3 a high contrast image, in Fig. 4.4 a low resolution image and in Fig. 4.5 a high resolution image is shown and in Table 4.2 the comparison result of

Volume 4 Issue VIII, August 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

corresponding image's computational time is represented. It revealed that the proposed method is faster than the existing methods. Thus, the proposed algorithm is the improved version of the block matching algorithms.

The proposed method detected the forgery with 100% success rate. Also the efficiency of the proposed method is highly dependent upon the size of copy-moved region.

(a) Original image (b) Forged image (c) Forgery Detection

Fig.4.2: Copy-move forgery detection in a low contrast image

(a) Original image (b) Forged image (c) Forgery Detection

Fig.4.3: Copy-move forgery detection in a high contrast image

(a) Original image (b) Forged image (c) Forgery Detection

Fig.4.4: Copy-move forgery detection in a low resolution image

(a) Original image (b) Forged image (c) Forgery Detection

Fig.4.5: Copy-move forgery detection in a high resolution image

	Time taken by (in sec.)F_DCT method	Time taken by (in sec.)Proposed method
Low contrast Image	33.728	11.664
High contrast Image	34.773	13.728
Low resolution Image	30.554	10.1063
High resolution Image	26.768	9.898

Table 4.2: Execution time comparison

The above comparison shows that the proposed method is far better than the existing method.

V. CONCLUSION AND FUTURE WORK

In block matching algorithm, I found that in the most of the block methods of copy move forgery detection is precise and accurate but the computational cost is very much high. The proposed method has less time complexity. The proposed method is evaluated on a number of original and forged images. According to experimental results the proposed method is quite attractive in comparison to previous method. The proposed method obtains 100% accuracy to detect copy-move forgery (just copy-move) without post processing operations such as scaling, rotation, reflection, noise addition and JPEG compression. According to the performance of the proposed method to detect copy-move forgery in digital images, robustness against post processing may be studied further.

REFERENCES

[1] J. Fridrich, D. Soukal, and J. Lukas, “Detection of copy-move forgery in digital images,” Proceedings of the Digital Forensic Research Workshop. Cleveland OH, USA, 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] B. Mahdian and S. Saic, “Detection of copy-move forgery using a method based on blur moment invariants,” Forensic science international, vol. 171, no. 2, 2007, pp. 180–189.

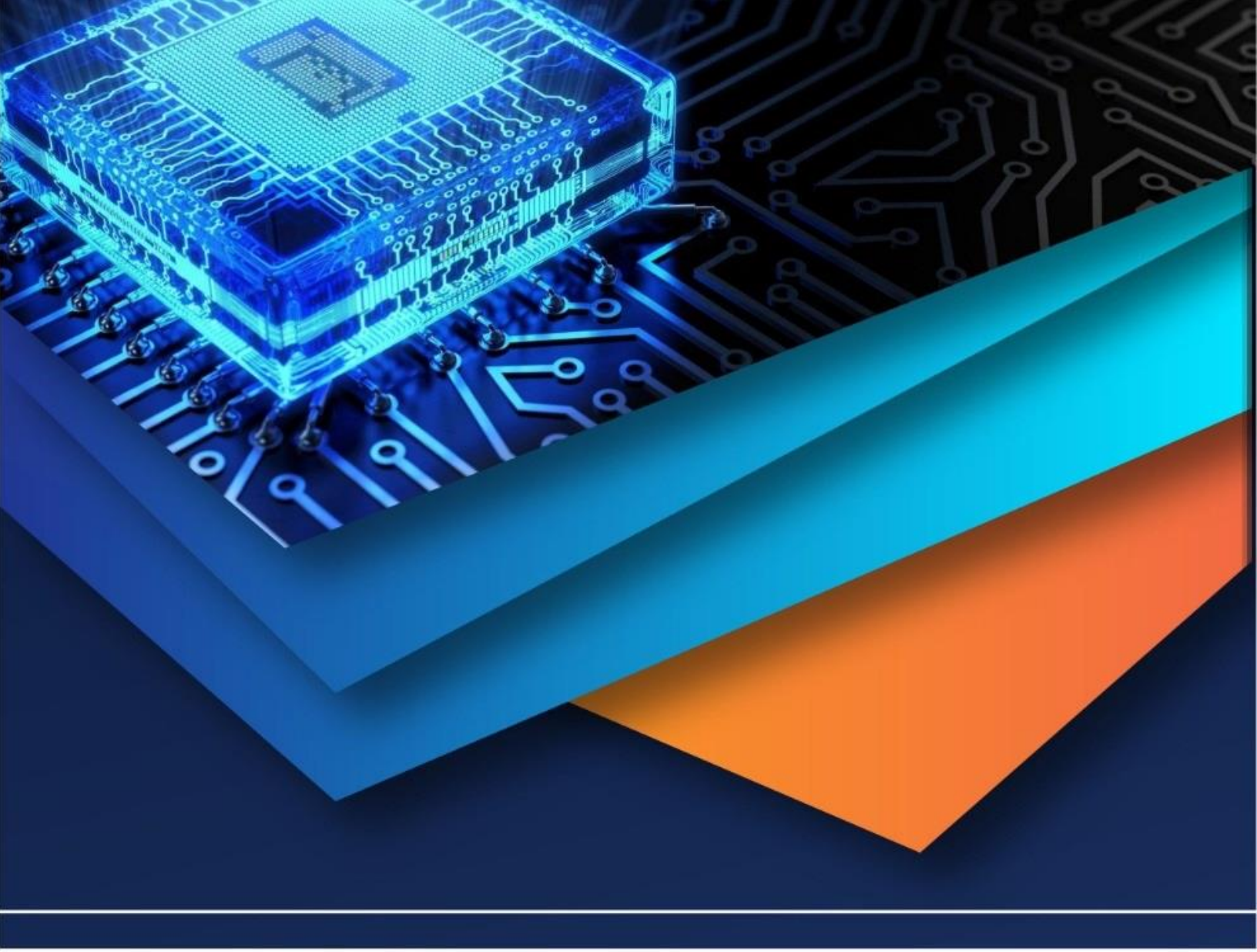
[4] G.Li, Q.Wu, D.Tu, and Shaojie Sun, “A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD,” IEEE International Conference on Multimedia & Expo, 2007.

[5] Nguyen HC, Katzenbeisser S., “Detection of copy-move forgery in digital images using radon transformation and phase correlation”. Proceedings of the 2012 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '12); July 2012; IEEE; pp. 134–137.

[6] Sunil Kumar, Jagannath Desai .“A Fast DCT Based Method for Copy Move ForgeryDetection”. Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013)

[7] Gajanan K. Birajdar, Vijay H. Mankar, “Digital image forgery detection using passive techniques: A survey,” Digital Investigation, vol. 10, no.3, 2013, pp. 226-245.

[8] O. M., Al-Qershi and B. E. Khoo, “Passive detection of copy-move forgery in digital images: State-of-the-art,” Forensic Science International, vol. 231, no. 1, 2013, pp. 284–295.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY