

# Copy-Move Forgery Detection Algorithm for Digital Images and a New Accuracy Metric

Tehseen Shahid, Atif Bin Mansoor

College of Aeronautical Engineering, National University of Sciences and Technology, Rawalpindi, Pakistan

Email: tehseen86@gmail.com

College of Aeronautical Engineering, National University of Sciences and Technology, Rawalpindi, Pakistan

Email: atif-cae@nust.edu.pk

**Abstract**— Authenticity of digital images plays important role in various fields like medical, legal, criminal, and journalism. In this paper we propose a method to detect copy move forgery by block matching in spatial domain. The algorithm is tested on a developed database. We further propose a new quantitative metric to measure the accuracy and robustness of any copy-move detection algorithm.

**Index Terms**— copy move forgery, image manipulation, image forensic, forgery detection

## I. INTRODUCTION

The U.S Office of Research Integrity reported that there were less than 2.5% of accusations of fraud involving disputed images in 1990. The percentage rose to 26% in 2001 and by 2006, it went up to 44.1% [1]. Mike Rossner of The Journal of Cell Biology assesses that at least one figure in 20% of the documents accepted in the journal is manipulated, and one out of every hundred papers has images which are deliberately manipulated [2].

Cheap and easy availability of sophisticated and powerful image manipulation tools have caused doubts on the integrity of digital images. It's a fact that many of the images we come across in our daily life are either fake or altered. There are significant number of magazines and newspapers which are publishing doctored images. Courts all over the world accept digital photographs, but in the prevalent circumstances require reliable mechanisms to assure authenticity of images.

Image manipulation has a history as long as that of photography. Many of the famous photographs in history were the altered ones, for example, the renowned portrait of Abraham Lincoln (circa 1860) was made by merging Senator John Calhoun's body and Abraham Lincoln's head [3]. Different war photographers used image manipulations to make the photographs more tempting. Even many of the leaders like Hitler, Castro, Mussolini, Stalin etc tried to modify history by manipulating photographs [3]. Though image manipulation has extensive past, advent of digital photography made the alteration of photographs so easy that even an amateur can create a forgery which is imperceptible. This demands a reliable image manipulation detection system, able to detect whether a photograph is real or altered. Though fine alterations may be indiscernible to human



Figure 1. John Calhoun's portrait (top), Abraham Lincoln's portrait created by merging his head on to John Calhoun's body (bottom) [3]

eye but these manipulations cause subtle changes in the core statistics of the image which are possible to detect.

Most common image manipulation techniques involve

- Removal of objects from the image.
- Addition of objects in the image.
- Change of appearance of objects in the image.

The most common of these three manipulations is removal of undesired objects from the image. It is

generally done by copying one part of the image and pasting it over the undesired object. This alteration is known as “copy-move forgery”. A number of methods have been proposed for the detection of copy-move forgery. Fridrich et al proposed the detection of the copied regions by matching the discrete cosine transform coefficients of the lexicographically arranged overlapping image blocks [4]. Popescu and Farid attempted the solution of the problem by employing principal component transform instead of discrete cosine transform for the overlapping image blocks and their subsequent matching [5]. B. Mahdian and S. Saic employed 24 blur moment invariants up to seventh order for the representation of overlapping blocks and kd-tree matching [6]. The technique is reported to be quite efficient even in the presence of additional noise, blur degradation or random contrast changes in the copied portions of the image.

A considerable amount of research effort is reported in literature for detection of copy move forgery, but a quantitative metric to measure and compare the effectiveness of reported algorithms is missing. In this paper we propose a method to detect copy move forgery by block matching in spatial domain. We further propose a simple but new quantitative metric to measure the accuracy and robustness of any copy-move detection algorithm.

II. PROPOSED ALGORITHM

Figure 2 depicts the flow chart of the proposed algorithm. The input image of size a×b is divided into ‘n’ blocks of size m×m pixels by moving the block point to point on the image. Each block is iteratively compared to every other block in the image. In case of complete match both blocks are marked as copied. In case of copy detection, the adjacent neighbours of the marked blocks are then compared. The algorithm confirms the

manipulation if at least three blocks in the adjacent neighbourhood of the both marked blocks are exact match of each other. In case of coloured images, the image is first converted into a matrix of size 3 times a×b by appending the RGB values of each pixel. The copy forge detection approach is subsequently applied on this modified matrix and copied blocks are marked.

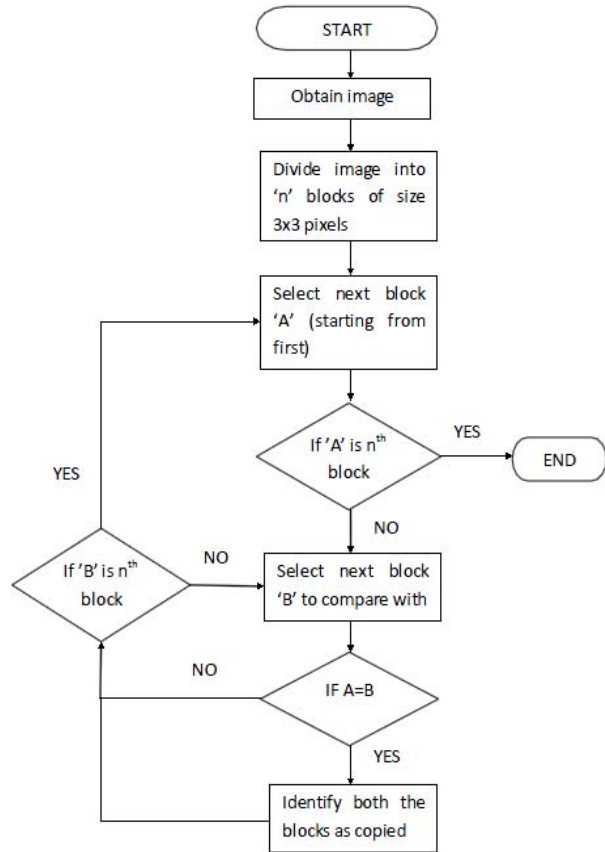


Figure 2. Flowchart of the algorithm for copy-move forgery detection

III. RELIABILITY METRIC

We propose a new metric to gauge the reliability of any copy move forgery detection algorithm. Let the total number of copied pixels is donated by ‘q’ and the total number of pixels detected as copied by ‘p’. Then percentage accuracy of any copy mover forgery detection algorithm can be calculated as:

$$Accuracy = \begin{cases} \frac{q}{p} \times 100 & \text{if } p \leq q \\ \frac{p-q}{p} \times 100 & \text{if } p > q \end{cases} \quad (1)$$

IV. EXPERIMENTAL RESULTS

We created a database of 100 manipulated images of different kinds and dimensions from the 100 original images downloaded from [7] and [8].

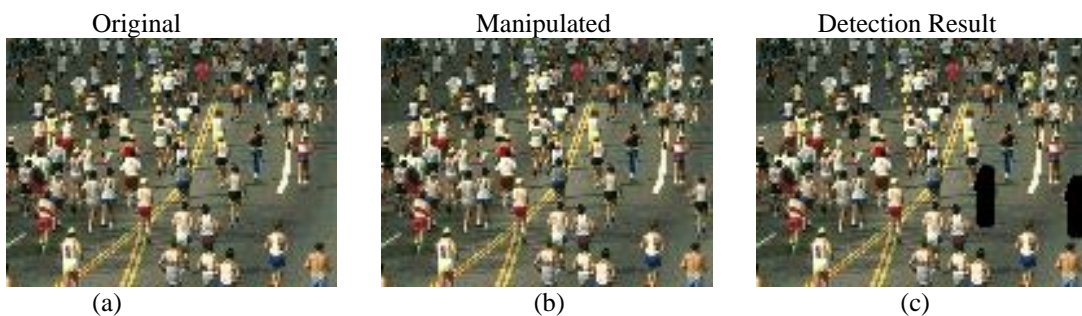


Figure 3. Marathon

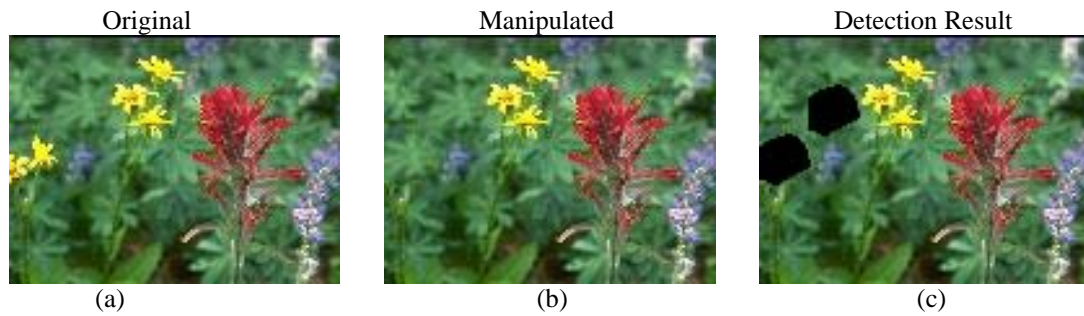


Figure 4. Flowers

The algorithm is implemented on a machine having

TABLE I.  
RESULTS SHOWING THE ACCURACY AND PROCESSING TIME OF THE  
ALGORITHM

| Image Name | Block Size (pixels) | Processing time (minutes) | Accuracy (percentage) |
|------------|---------------------|---------------------------|-----------------------|
| Marathon   | 3x3                 | 8                         | 85.93                 |
|            | 5x5                 | 12                        | 81.12                 |
|            | 7x7                 | 16                        | 76.54                 |
| Flowers    | 3x3                 | 9                         | 85.98                 |
|            | 5x5                 | 11                        | 80.37                 |
|            | 7x7                 | 13                        | 74.82                 |

Intel Core2Duo with 2 GB RAM. The dimension  $m$  of block is varied from 1 to 7 to ascertain the optimum block size. Also the processing time is recorded to determine the effect of block size. Figures 3(a) and 4(a) depict variety of images from the developed database which are altered (Figures 3(b) and 4(b)) and the result of the proposed algorithm (Figures 3(c) and 4(c)). Table 1 gives the accuracy and processing time utilized by the algorithm for various block sizes for images of size 128 x 96. It is observed that block size of 3 x 3 give the optimum performance in terms of accuracy and processing time.

## CONCLUSION

We have presented in this paper an algorithm which can effectively detect copy-move forgery. The algorithm is tested on a developed database and gave best performance for a block size of 3x3. We also propose a new metric to gauge the accuracy of different copy-move forgery detection algorithms. The metric will facilitate comparing different algorithms and their benchmarking.

## REFERENCES

- [1] Krueger, J. W. Accountabil. Res. Pol. Qual. Assur. 9, 105–125 (2002). J. Clerk Maxwell, *A Treatise on Electricity and Magnetism*, 3<sup>rd</sup> ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
- [2] <http://www.nature.com/nature/journal/v434/n7036/full/434952a.html>
- [3] <http://www.cs.dartmouth.edu/farid/research/digitaltampering/> visited on 26 July, 2009.
- [4] J. Fridrich, D. Soukal, and J. Lukas. Detection of copy-move forgery in digital images. In Proceedings of Digital Forensic Research Workshop, pages 55–61, Cleveland, OH, USA, August 2003. IEEE Computer Society.
- [5] A. Popescu and H. Farid. Exposing digital forgeries by detecting duplicated image regions. Technical Report TR2004-515, Department of Computer Science, Dartmouth College, 2004.
- [6] B. Mahdian and S. Saic. Detection of copy-move forgery using a method based on blur moment invariants. *Forensic science international*, 171(2–3):180–189, 2007.
- [7] <http://www.flickr.com>
- [8] <http://www-db.stanford.edu/~wangz/image.vary.jpg.tar>