Fast and Efficient Region Duplication Detection in Digital Images Using Sub-Blocking Method

Vivek Kumar Singh and R.C. Tripathi

Indian Institute of Information Technology, Allahabad
vivekkr.singh@hotmail.com

Abstract

Powerful image editing tools are very common these days. By use of such tools, image tampering is also becoming common. It is becoming very common to remove or add some information on the images mostly for the purpose of some forgery. The focus of this paper is to detect "copy move" type of forgery. In this type of forgery, one portion of image is copied and pasted somewhere else in the same image. The motive of this type of image forgery is to hide some important features from the original image. As may be the case, in an criminal evidencing system or to show large crowd in a scene having sparse population etc. In this paper, we propose a method which is more efficient and reliable in comparison to previous methods. This method is good enough even for some manipulations/attacks like for scaling, rotation, Gaussian noise, smoothing and JPEG compression etc.

Keywords: *Image tampering, Forgery, Lexicographic Sorting, Radix sort.*

1. Introduction

In present scenario it is very easy to edit any pre-existing photographs by using freely available commercial image editing tools. Any alteration in an original image in bad faith is regarded as image forgery. To detect digital image forgery is a challenging task in the field of crime, journalism etc. Fake photos many a times are used to publicize in magazines or news papers. Now days, many cases are noted in regard to the defaming business as well as political opponents by using fake photographs and videos. This makes, it very essential to know about the integrity of the photos and frames in the video clippings so as to detect the truth.

In the last decade, any photographs were generally accepted as a proof for any crime. Computers today however are being used in almost all fields of business, banking, agriculture, health and many other domains to up- keep records in the form of digital images. But due to easy availability of efficient tools, no one today is sure for the integrity of images. Presently there is no efficient method to check the authenticity and integrity of any digital image which can be put as evidence in a court. Due to a vast range of image tampering methods and tools, it has become very difficult to have a single tool which can handle detection of all facets of image forgery.

Detecting image forgery is an emerging field of research. In the last decades, many image manipulations were seen on the cover of magazines, news papers, and other media resources. Figure 1 is showing a sample case of image forgery. A part of newspaper indicates that three photos are used for creating a composite image. Herein, the White house is tampered to create a background for composite image, consisting of photos of Bill Clinton and Saddam copied from two different images and pasted over the composite image with White House in the background.


INTERNET

Spies turn to high-tech info ops

PCs, Internet used for manipulating images, public opinion

ALTERED IMAGE

1 2 3

Altered Egos
The top photo, of a fictitious meeting between President Clinton and Saddam Hussein, was generated by digitally altering and combining elements from three photos, shown below the altered image. Intelligence agencies plan to use similar techniques to create images and then disseminate them via the Internet in their efforts to influence events in foreign countries, such as Iraq.

BY DANIEL VERTON

Federal intelligence agencies are studying ways to use computers and the Internet, rather than just leaflets and radio broadcasts, to shape and disseminate information designed to sway public opinion in the world's hot spots.

As part of its so-called "perception management" program, the intelligence community has for decades created misinformation to trigger political change without direct political or military involvement in countries where the United States has vested interests, such as Iraq and North Korea.

Acting on congressional recommendations to bolster research and development in information technology, intelligence agencies are turning to PCs to develop more sophisticated means of manipulating and delivering digital photos, video clips and recorded sound to portray fictitious events in hopes of provoking desirable outcomes.

Figure 1 Sample of Image Forgery

In respect of cases being currently reported, three approaches are noted as commonly being used for image forgery. These are i) Image Enhancement (e.g. blurring the portions, brightness, Contrast or Color etc), ii) Image Compositing (Mixing up different features from two or more different images) and iii) Copy move forgery (Copying some part of information from image itself and pasting it in the same image elsewhere.). The current paper focuses on the last type of forgery.

2. Problem definition and Motivation

Copy-Move is a type of forgery in which a part of image (Fig 2(a)) is copied and then pasted on to another portion of the same image (Fig 2(b)). The main intention of such forgery is to hide some information from the original image.


Figure: 2(a) **Figure 2 (b)**
(http://blogs.techrepublic.com/security/?p=554)

The most commonly used method for detecting this type of forgery is "Block matching". Each block is matched with all other possible blocks in the same image. However, this method is most compute intensive and full of complexity. Each block corresponds to some features, some of which are extracted as representative of such blocks for matching with the other blocks. At last the result is concluded on the basis of matched blocks considering some distance threshold. There are various other approaches in block matching. For example Fridrich and Lucas[1] used DCT(discrete Cosine transform) for block matching. The main benefit of using it is strong energy compaction property of DCT. The advantage is that any type of manipulations such as noise addition and compression will not affect energy coefficients. However the above method fails for any type of geometrical transformations of the query block e.g. rotation, scaling etc.

A.C. Popescu et al. [2] proposed a principal component analysis (PCA) on image blocks to give a reduced dimension representation. After that, lexicographical sorting algorithm is applied on each block to get duplicated region. H. Huang et al. [3] first calculated SIFT descriptors of an image, which do not depend on illumination and rotation etc. These descriptors are matched with each other to detect copy move forgery in the image; the results are shown in fig 3. Luo et al. [4], applied color information for blocks. The whole block is divided into four sub blocks and one considers average of red, blue and green color values. Results show this method to be very robust to attacks like, JPEG compression, Gaussian blurring and additive noise. Li [5] proposed a method using DWT (Discrete Wavelet Transform) and SVD (Singular Value Decomposition) .This method however cannot overcome with the problem of high computational complexity and time complexity.

Figure 3 Result of SIFT Descriptor Method

In fact, an efficient copy-move technique should be robust to attacks like losses due to compression, addition of Gaussian noise, rotation and scaling. Till now, no method seems to have been reported which is efficient with all above manipulations in proper time. Edoardo [11] suggested a block based approach in which texture is extracted from the block as a feature. Analysis showed that the statistical descriptor is yielding better result.

In the present paper we are detecting copy move forgery which can give accurate result even in wake of Gaussian noise, jpeg compression, rotation and smoothing conditions. The approach proves to be fast and accurate by dividing blocks in sub blocks and some sort of mathematical functions are applied to get some feature values. These values are then sorted by using radix sort. Our experimental results show that this approach is good enough to detect copy move forgery even for manipulations like JPEG compression, rotation (up to some limit), Gaussian Noise and smoothing. The use of radix sort followed by count sort makes our approach more efficient and less time consuming. There after we use some post processing techniques like erosion and then dilation to remove false matches.

The rest of this paper is organized as follows. Related work is discussed in Section II. In Section III, the proposed method is described in details. In Sections IV. Some experimental results of the current investigation are reported and conclusion is given in section V.

3. Proposed Method

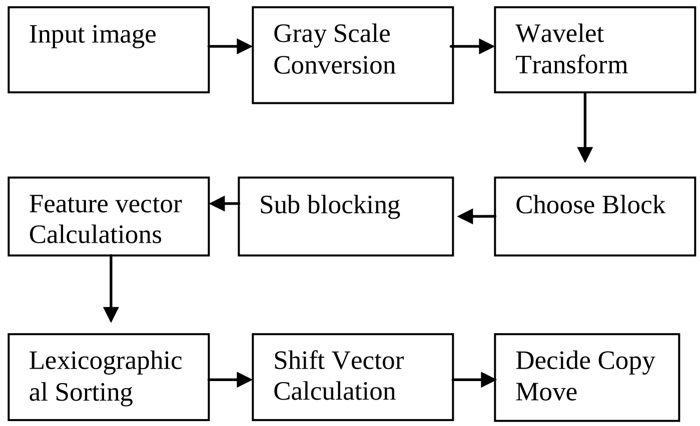


Figure 4 Flow Chart of Proposed Method

Our algorithm takes an image as an input and then it checks that whether it is RGB or gray. If the input image is RGB, it converts the same into corresponding gray scale image. This processed image is then divided into various blocks. These blocks are matched to detect if there is any copy move forgery.

Detailed procedure is divided into seven parts.

1. **Discrete Wavelet Transform: -** Wavelet decomposition of the images is advantageous to inherit multi resolution characteristics of images. The process of discrete wavelet transform is reduction of the size of the image at each level. At each level, the image is divided into four small images. These sub images can be combined together to restore the original image. This step includes reducing the size of image using DWT. Further steps will be performed for the resulting image of this step.

2. **Sub Blocking**: - The image reduced in step 1 is divided into all possible blocks of $b \times$ b pixels. Thus for an image of size $M \times$ pixels, there will be $B = (M - b + 1)x(N - b + 1)$ blocks

We have divided blocks diagonally separately for both diagonals as shown in figure 5.

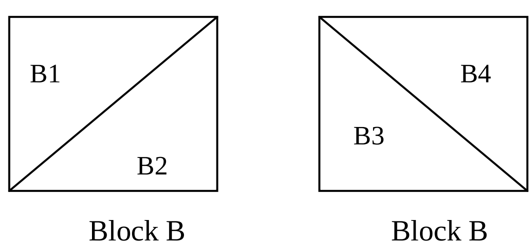


Figure: 5

By dividing a block in such manner we get some good features which are highly related. For each block

B_i $(i = 1,2,3, \dots\dots,$, there are nine features V= $v_i(i = 1,2,3 \dots$ which we shall calculate.

Features are calculated according to following equations:-

$$v_i = \begin{cases} Average\ of\ middle(B) & i = 1 \\ average(B_{i-1}) \div (average(B)) & 2 \le i \le 5 \\ average(B_i) & 6 \le i \le 9 \end{cases}$$

First feature $_1$is calculated by averaging pixels of sub block middle (B). These pixels are those which reside in a square block with side b*I and with center same as of the original block where I is a real number between 0 and 1 (We have used I=2/3). There is no hard and fast rule of calculating the optimum value of I but this is expected to be between 0.65 and 0.99. By doing so we can have a better result because generally border of copied area is more tampered. Features $v_2, v_3, v_4,$ are calculated by taking the ratio of the average of pixel value of sub block and the average of pixel value of block B.

These features are efficient for certain operations. It is good for Gaussian Noise addition. Next features $v_6, v_7, v_8,$ can be calculated by taking difference between average of pixel values of each sub block and whole block. These features help in giving very good results for constant smoothing.

After calculating all the feature vectors, it should be normalized in the range of (0,255). Radix sort is applied on these features. We used count sort as a stable sort for this purpose.

3. Lexicographical Sorting:- For each block we get nine feature vectors $V = v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8$. All these are stored in an array A. This array will contain features of blocks as well as the row and column indices of the starting pixel of this block. That means, this array has (9+2) columns and $d \quad (M - b + 1) * (N - b +$ rows. First nine columns will be used in sorting. Since features are normalized for the integers so Radix sort is efficient method [12]. The highest priority is given to feature V_1, then the features from V_2 to V_5 and least for the features V_6 to V_9. The main advantage of sub blocking the blocks in the form of diagonals is that one pixel is contributing in two different sub blocks. So it gives strongly correlated features.

4. Detection of suspected copied regions: - Array A is successfully sorted, hence the rows, representing blocks with very similar features, are arranged nearby. For every pair of contiguous rows which are representing the features of the two respective blocks, we find logical distance between these two feature sets as given in (1) where each feature is considered as an independent dimension. When the logical distance is found to be less or equal to a preset threshold T_1 and the physical distance between the block regions is greater of equal to a preset threshold T_2, a copy move activity in the corresponding blocks is suspected.

$$D_i(r_i, r_{i+1}) = \sqrt{\sum_{j=1}^{9} [r_i(j) - r_{i+1}(j)]^2} \quad \ldots. (1)$$

Where, $r_i($ is the j^{th} feature of i^{th} row.

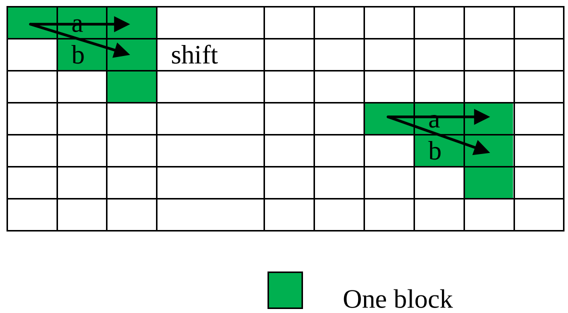
5. Neighbor Shift Matching:

For a suspected pair of blocks, the system compares features of nearby blocks of both of the blocks of a pair which are at the same vector distance from the corresponding block.

Neighbor Shift value is calculated by subtracting two corresponding feature vectors. Shift vector of the entire suspected duplicate region will be same. As in 2.

$$\text{Shift}\,(B_1(i), B_2(i)) = \text{Shift}\,(B_1(j), B_2(j)) \qquad \ldots. (2)$$

Two copied and then moved areas will yield some pair of identical features. This feature will yield same shift vector. This shift vector will be checked for a particular number of neighbors. Same shift vector will be showing the duplicated region.



6. Detection of Duplicated Region

Initially, it is not known what the size of the duplicated region is. So it becomes expedient that to detect even small size patches, much smaller block size be selected. However, with every small block size, chances of catching even small similar regions become substantial. As a result, there may be various false matches. To remove such false matches we perform erosion followed by dilation. Erosion shrinks the boundary of the matched block and after one or two erosions; it removes the small unwanted blocks. Then dilation is performed same number of times to get the original shape of the forged area.

7. Detection of Copy-Rotate-Move (CRM) Forgery

We propose a simple and fast method of detecting CRM forgery. We take overlapped blocks same as used in previous steps. If size of the block is $b \times b$, b must be an odd number. Nine pixels ($p_{i=0to8}$) in a block i.e. center pixel and its 8-adjecent pixels are numbered as centered pixel as 0^{th} pixel and others in clockwise direction 1to 8 starting from top left corner of these nine pixels as shown in figure.

We made an array G with 20 columns. First nine of these had values of pi with sorted order. Next nine pixels are indices of the respective pixels in pi. Last two columns are representing the left top pixels x,y coordinate in the image.

1	2	3
8	0	4
7	6	5

Array G is lexicographically sorted with respect to first nine values in the array with zeroth column at the highest priority and so on. Now adjacent rows of array G are compared with respect to first nine values. When any two rows are found having nearly same at least seven values in first nine values, ninth to seventeenth elements should also be in same circular sequence. If the sequence is found to be same, the two blocks are declared as a portion of CRM type forgery. The circular sequence will give the angle of rotation of the region. In the found angle we checked for the neighbor shift value in that angle only upto 4 or 5 steps. If these values are found to be same then CRM is declared at corresponding blocks. This process is continued for each suspected region.

This CRM method will not work for JPEG compression and Gaussian noise.

4. Experimental Results

The entire process is proposed in the preceding section was implemented in Matlab 7.0 and executed on a computer of CPU 3.0GHz with main memory 1GB and secondary storage memory of 160 GB. The test images used are free from any type of other tamperings which we proposed in this approach. Tests were conducted on such hundred images. In the present study, all these hundred images are copy moved forged images without any further modifications. We made another Set of images containing Gaussian noise. Other uniformly smoothed images, JPEG compressed images, and some predefined rotations were also tested. We have considered a square block of size 16*16 pixels and checked for different threshold values of discrimination say 50, 100 and 150.

Figure 8: Original Image

For example, the image taken in figure 8 is an original image without having any forgery. Image size is 479×319. Block size selected by us was 16×16. In the image, the truck is hidden by pasting some portion of tree groves onto truck area. There was no other after manipulation except copy move. (Please see Figure 9a). Fig 9b is showing the result of detection of copy moved region. The result obtained is very accurate and fast. The final image is found after performing erosion and dilation. Count for shift vector is taken 2. We performed various attempts on the same image with different threshold values and with different counts for shift vectors.

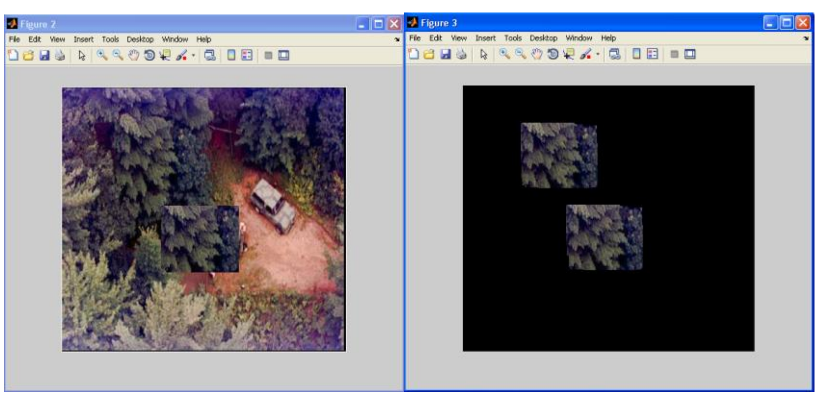


Figure 9 Result of Copy move without any Modifications

The result shown accordingly is very accurate. There were no modifications after performing copy move. Threshold set for above experiment is 150.

Figure 10 (a) Image with Gaussian noise at SNR = 35db

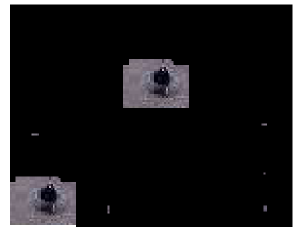


Figure 10 (b) Detected Region

The figure 10(b) shows the detected results over image shown in figure 10(a) with Gaussian noise.

For SNR as 35db (signal to noise ratios). Threshold value considered is 100 in this case. Copied and pasted area are detected accurately again in this case as well. The method is effective to withstand attacks with various such SNR values.

Figure 11 shows the results of images which have undergone another type of attack i.e. some compressions. The results are checked on various others QF (Quality Factors). Please see figures 11a and 11b respectively.

Figure 11 (a) Original image t with QF 70

Figure 11 (b) Result

We performed some experiments on rotation problem too. We assumed a rotation of 45 degree. The result obtained is quite accurate but it is taking long time for the execution. Figure 12 (b) is the tampered image wherein the light pole is rotated by 45 degree. The blocks are taken from original image and after performing various rotations the results are checked. Figure 12 (c) is showing the resultant image.

(a) **(b)** **(c)**

Figure 12 (a) original image (b) Rotated copy pasted image. (c) Resulting images

In order to describe the result accuracy of the algorithm, two elements can be defined as Equation (3), (4).

Let us assume, R_i is the copy area, $R_i{}'$ is the forged region. With respect to these area, D_i and D_i' are found as copy and the forged area respectively. The element *r* is the ratio of correct detection, whereas *w* is the ratio of false detection.

EQUATION

$$r = \frac{\sum_i(|R_i \cap D_i|) + (|R_i{}' \cap D_i{}'|)}{\sum_i(|R_i| + |R_i{}'|)} \quad \text{..................3}$$

$$w = \frac{\sum_i(|R_i \cup D_i|) + (|R_i{}' \cup D_i{}'|)}{\sum_i(|R_i| + |R_i{}'|)} - r \quad \text{..................4}$$

In our experiment we found result in the terms of r and w as shown in table 1:

Tempering size	r	w
2 %approx	0.9558	0.0904
4%approx	0.9766	0.701
6%approx	0.9814	0.365

The results shown in table 1 describes that the proposed algorithm is working effectively. When the copied area is more, the w (detection ratio) increases while false ration reduces means larger copied area increase accuracy.

Time performance: Computational cost reduced in this method as we have used only nine features for each blocks. The results are improved from two directions one is decomposition of image and another is by using less features of blocks. The result is faster and with in few minutes it give the result.

5. Conclusion

In this study, we proposed a new method based on efficient feature selections. Our method is more efficient than previous methods. Copy move forgery is detected by the use of sub blocking method. Our method withstands to detect the duplicated region of original image attacked by way of Gaussian noise, JPEG compression, rotation (up to some extent). Results are not only much accurate but also efficient in terms of processing time. Use of shift vector and erosion followed by dilation made the results very effective. The method is yet to be improved to withstand attacks like of rotation by an arbitrary degree and for scaling.

Table 2. Comparison with Previous work (on our Database):

Methods	False Detection(w)	Right Detection(r)
[1]	0.222	0.643
[2]	0.721	0.8771
[12]	0.622	0.9411
Present Method	0.365	0.9814

References

[1] J.Fridrich, D. Soukal, and J. Lukas. Detection of Copy-Move Forgery in digital Images. *Proc. Of Digital Forensic Research Workshop*, Aug. 2003.

[2] A.C. Popescu and H. Farid. Exposing digital forgeries by detecting duplicated image regions. *Technical Report TR2004-515*, Dartmouth College, Aug. 2004.

[3] H. Huang, W. Guo, and Y. Zhang, "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm," *in Proceedings of IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, Vol. 2,2008, pp. 272-276.

[4] W .Luo, J. Huang, and G. Qiu, "Robust Detection of Region Duplication Forgery in Digital Image," in Proceedings of the 18th International Conference on Pattern Recognition, Vol. 4, 2006, pp. 746-749.

[5] G. Li, Q. Wu, D. Tu, and S. Sun, "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries based on DWT and SVD," in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing China, July 2-5, 2007, pp. 1750-1753.

[6] Rafael C. Gonzalez, Richard E. Woods, Steven L. Eddins,"Digital Image Processing using MATLAB",Second Edition, Pearson Publications, 2004.

[7] T. E. Boult and G. Wolberg, "Correcting Chromatic Aberrations Using Image Warping," *in Proceedings of Computer Vision and Pattern Recognition*, 1992, pp. 684-687.

[8] M. K. Johnson and H. Farid, "Exposing Digital Forgeries Through Chromatic Aberration," *in Proceedings of the 8th workshop on Multimedia and security*, 2006, pp. 48-55.

[9] J. Lukas, J. Fridich, and M. Goljan, "Detecting Digital Image Forgeries Using Sensor Pattern Noise," *in Proceedings of the SPIE Conference on Security, Steganography, and Watermarking of Multimedia Contents*, Vol. 6072, January 2006, pp. 362-372.

[10] N. Khanna, A. K. Mikkilineni, G. T. C. Chiu, J. P. Allebach, and E. J. Delp, "Scanner Identification Using Sensor Pattern Noise," *in Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX*, Vol. 6505, No. 1, 2007, pp. 65051K.

[11] Edoardo Ardizzone, Alessandro Bruno, Giuseppe Mazzola, "Copy-Move Forgery Detection via Texture Description," Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence,2010 pp. 59-64.

[12] Hwei-Jen Lin, Chun-Wei Wang, Yang-Ta Kao, "Fast Copy-Move Forgery Detection," WSEAS TRANSACTIONS on SIGNAL PROCESSING, Issue 5, Volume 5, May 2009, pp. 188-197.

[13] W. Q. Luo, J. W. Huang and G. P. Qiu, "Robust detection of region duplication forgery in digital image", *Journal of Computers, vol. 30, no. 11, 2007, pp. 1998-2007.*