

Copy-Move Forgery Detection Utilizing Local Binary Patterns

Ramandeep Kaur
D.A.V College, Punjab, INDIA

Abstract: Digital images are extensively utilized as communication medium. Forgeries in digital images have grown to be an astringent concern with the availability of powerful image processing tools. Among various image forgery approaches, copy-move forgery is the commonly used technique in which a component of the image is facsimiled and pasted in order to hide extraneous portion of the image. Square block matching technique is utilized to detect this kind of forgery. In this paper, firstly input image is divided into overlapping chunks. Features of the small blocks are extracted by making use of Local binary pattern texture method. Further blocks are lexicographically sorted and lastly duplicated blocks are identified utilizing the similarity criterion and Euclidean distance threshold.

Keywords: Image Processing, Image Forensics, Digital Tampering

I. Introduction

Because of variants of digital cameras and utilizer-amicable image editing software people can engender and manipulate digital images facilely. A digitally transmuted photograph can be indistinguishable from an authentic photograph. So, image tampering detection is one of the major goals in image forensics.

Copy-Move forgery is carried out with the intention to make an object “disappear” from the image by covering it with a minute block facsimiled from another part of the same image. The conception of detecting this kind of forgery is to divide the image into diminutive blocks, which only have one row or one column different pixels with their neighboring blocks. Because the replicated parts come from the same image, noise components, Effulgence, the color palette, and the other properties will be well matched with the rest of the image, therefore it is very arduous for a human ocular perceiver to detect such forgery.

Figure 1: Example of Copy-move forgery (a) original image (b) tampered image



In this paper the focus is on the detection of malevolent manipulation with digital images. The rest of the paper is compiled as follows: literature review is discussed in section 2. Section 3 explains the local binary pattern using the square block matching technique. Section 4 presents the results. Conclusion for this paper is given in Section 5.

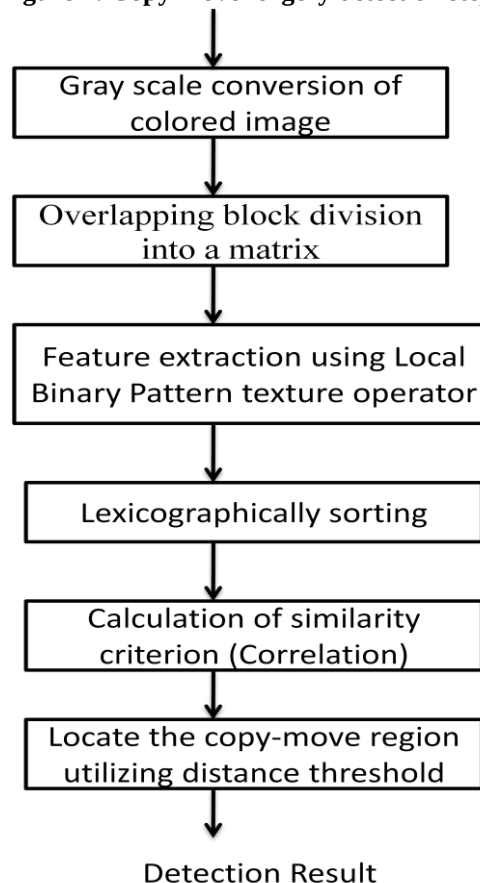
II. Literature Review

Since the key aspect of Copy-Move forgery is that the facsimiled part and the pasted part are in the same image, one method to detect this forgery is exhaustive search, but it is computationally intricate and more time is needed for detection. Therefore to increment the speed/performance of operation process many researchers use block matching approaches [1] [2]. Ramandeep et al. proposed a tool to detect the copy-move forgery on the cull of feature and kindred similarity measure. GUI tool localized only those image areas that are identical or extremely similar. Fridrich et al. [3], primarily introduced a method to espy copy-move forgery. They lexicographically sorted the discrete cosine transform coefficients of the divided blocks and then checked whether the adjusted blocks were homogeneous or not. B.L.Shivakumar and Dr. S.Santhosh Baboo [4] have proposed copy-move forgery detection method predicated on SURF, which detects duplication region with different size. Kulkarni et al. [5] and Sridevi et al. [1] proposed a copy-move forgery detection algorithm to detect the duplicated regions by making use of block matching technique. In [6], B. Mahdian capitalized on the blur invariant moments to extract the block features. These methods may fail to detect the copy move forgery, if the duplicated regions are rotated or flipped. Recently many researchers considers detecting copy move forgery utilizing the geometric transforms such as Zernike moments and scale invariant feature transform [7]. This approach was resilient to distortion and achieved a detection precision rate of 83.59% when the copied moved region undergoes rotation. In [8] Li et al. proposed a method by presenting rotation invariant uniform local binary pattern by utilizing square block matching technique to reduce the dimension of the feature vector. The prevalence of the proposed method was that it was robust to geometric transformations such as region rotation. In this paper, a novel method named as rotation invariant local binary pattern is used to detect the copy-move forgery. As the copied and moved part comes from the same image, so the duplicated regions may or may not be the forged regions. So, similarity criterion is utilized to detect the forged region. The forged region can be differentiated from the original region by calculating correlation and distance between them.

III. Proposed Method

The task of detecting copy move forgery is to find duplicated regions from the suspicious image. Also the replicated regions are unfamiliar both in size and shape, if we scrutinize every possible duo pixel by pixel, the computational intricacy will be very higher, and no one can abide that. The data flow of the presented technique is shown in figure 2:

Figure 1: Copy-move forgery detection steps



Step I

Input the gray scale suspicious image. If the input image is a colored image, then convert it into a gray scale image.

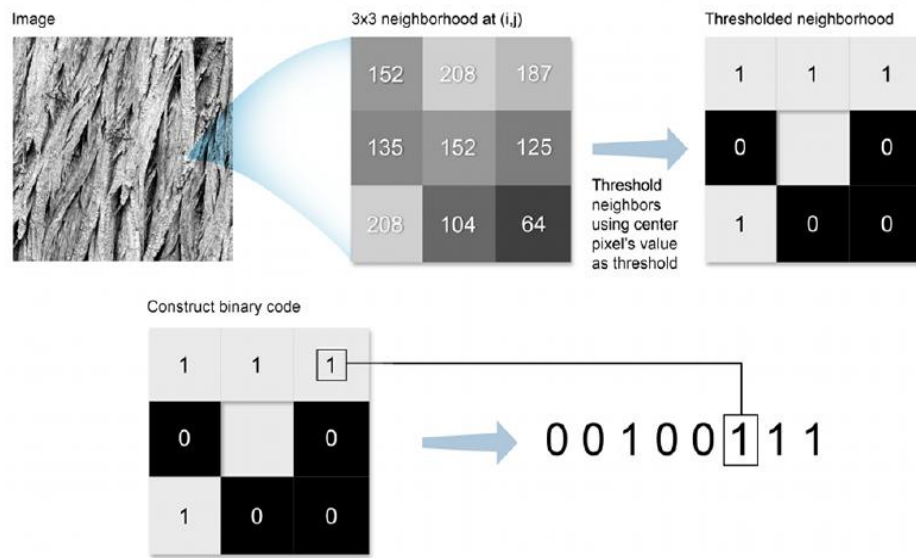
Step II

Divide the suspicious gray scale image into overlapping square chunks having block size of $B \times B$. At the end, these $B \times B$ block entries are stored in a matrix named as 'I'. The output matrix I has the size $(M-B+1) \times (N-B+1)$ rows and $B \times B$ columns, where M and N are the number of rows and columns of the input image respectively.

Step III

Feature extraction: Local binary pattern (LBP) is utilized for feature extraction. LBP is a kind of texture descriptor which quantifies the pattern of texture. It is gray scale invariant i.e it calculates differences between the intensity values.

Figure 2: Example of LBP operator [9]



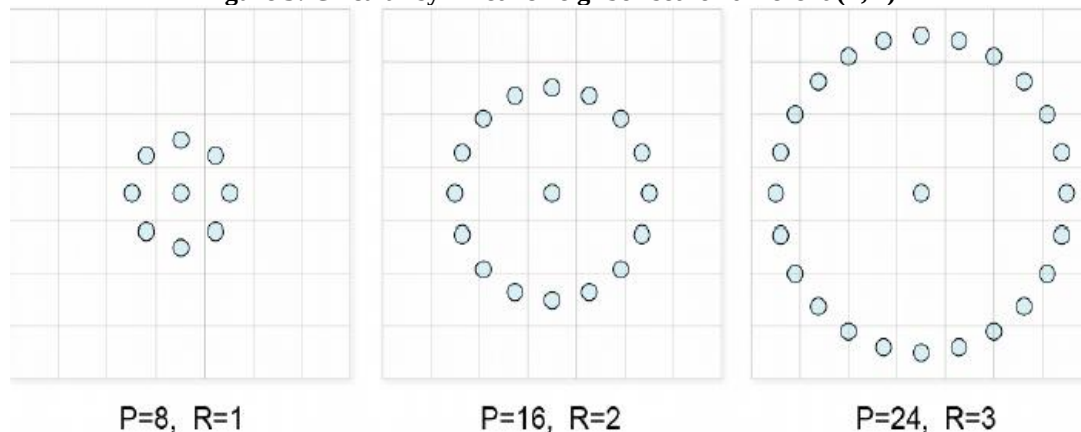
Circular LBP operator:

It describes a circular neighborhood around each pixel. The texture T, in a local neighborhood of gray scale image having P gray levels can be defined as:

$$T = t(g_c, g_0, \dots, g_{P-1})$$

where g_c is the gray value of the centre pixel, $g_p (p = 0, 1, \dots, P-1)$ corresponds to the values of its neighbors[8]. Following figure 4 shows the three examples of circular symmetric neighbor sets for different configurations of (P,R).

Figure 3: Circular symmetric neighbor set for different (P,R)



After that a $B \times B$ block is moved smoothly over the resulting image and image is scanned from the upper left corner to the lower right corner. Further feature vector is calculated by applying the local binary pattern operator. These values are stored as one row in a matrix I. The output matrix I has the size $(M-B+1) \times (N-B+1)$ rows and $B \times B$ columns, where M and N are the number of rows and columns of the input image respectively.

STEP IV

Lexicographically sorting: This type of sorting is applied on the rows of the matrix. In the organized list, homogeneous rows are proximate to each other.

Step V

The main conception of this step is that a duplicated region consists of many neighboring duplicated blocks. If we find two homogeneous blocks in the analyzed space and if their neighborhoods are additionally kindred to each other, there is a high possibility that they are duplicated. The method finds all homogeneous blocks for each one (homogeneous to the most proximate neighbors search) and analyses their neighborhood.

The similarity measure correlation is employed here. Keep only those blocks whose correlation is greater than threshold T_s . That is,

$$\text{Corr}(B_i, B_j) > T_s$$

If the above condition is satisfied, then there is a higher possibility that these blocks are copy moved. Here, T_s is the minimum required similarity threshold.

Step VI

Matching block detection: After two blocks with the required homogeneous attribute have been found, a verification step commences. In the verification step, homogeneous blocks with different neighbors will be eliminated. For analyzing the blocks neighborhood, the neighboring blocks with a maximal Euclidean distance of 14 pixels from the analyzed block (distance from their upper left corners). If 95% of these neighboring blocks gratify the homogeneous attribute condition, the analyzed block is labeled as duplicated. More formally, if block 1 with coordinates (i, j) and block 2 with coordinates (k, l) are labeled as copy moved if

$$\text{Dis}(B_i, B_j) > T_D$$

Note that the threshold T_s and T_D plays a very paramount role. It expresses the degree of reliability with which blocks i and j correspond with each other. It is conspicuous that the cull of chosen threshold directly affects the precision of results of the method.

IV. Experimental Results

In experiment, the test images are amassed from the Internet, and the replica-move forgery is performed utilizing Photoshop. Here, the block size chosen is 8x8, similarity criterion $T_s = 0.8$ and matching threshold $T_D = 14$.

Figure 4: Forgery detection result (a) original image (b) tampered image (c) detection result

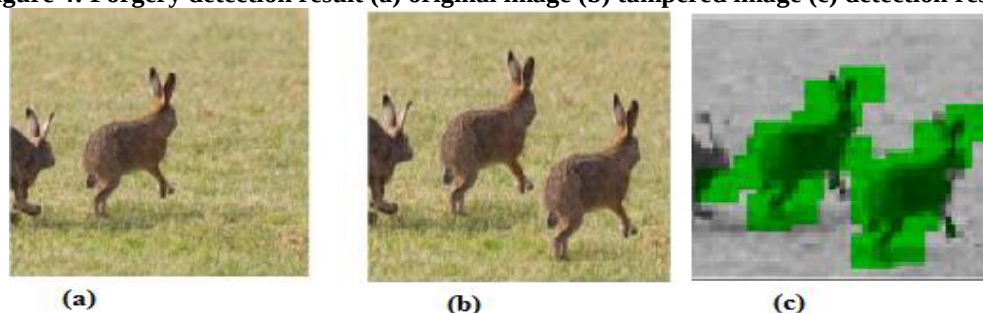


Figure 5: Forgery detection result (a) original image (b) tampered image (c) detection result

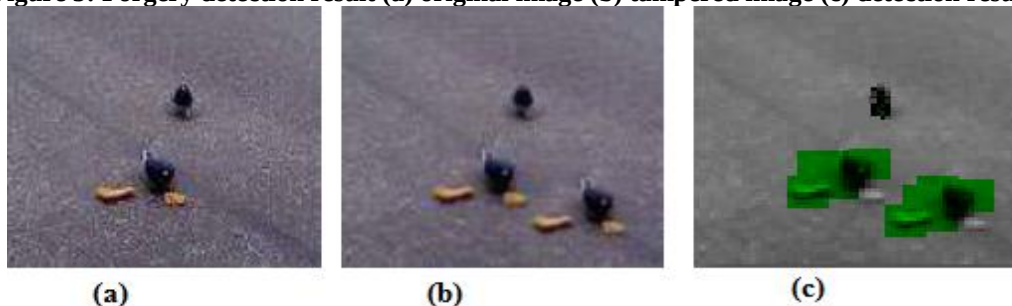
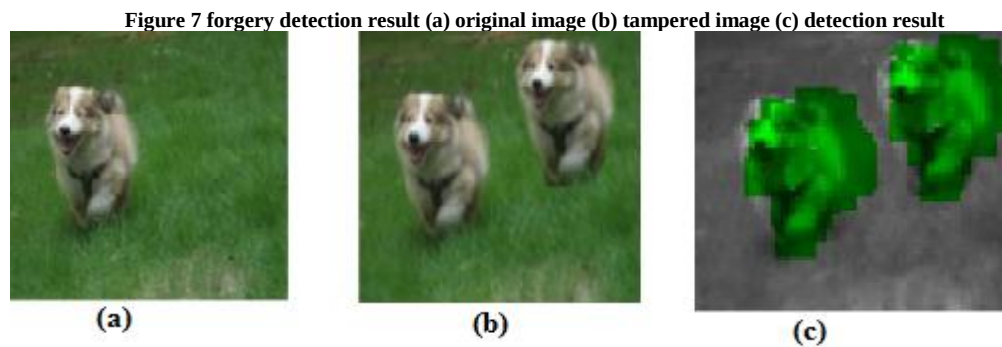


Figure 6: Forgery detection result (a) original image (b) tampered image (c) detection result





V. Conclusion

Copy-move forgery is a very prevalent way to tamper an image. Many researchers have proposed sundry schemes to detect the tampered images. However, sometimes the facsimiled regions are rotated or flipped afore being pasted. This paper presents a local binary pattern method to detect this kind of forgery. The main aid of this paper is that given scheme is robust not only to the traditional signal processing operations, but additionally to the rotation and flipping. A deficiency of the presented scheme is that when the region is rotated by general angles, it is arduous to detect the forgeries. The future work is to examine the invariant block features and congruous cull of the dimension of the features to make the method robust to desultory region rotations.

References

- [1] C.Mala, S.Sandeep and M.Sridevi, "Copy – Move Image Forgery Detection in a Parallel Environment", Computer Science & Information Technology, vol. 2, 2012, pp. 19-29.
- [2] R.Kaur and A. Verma “ Copy-Move Image Forgery Detection Tool”, International Journal of Emerging Technologies in Computational and Applied Sciences, vol. 5, no.5, 2013, pp. 527-534
- [3] D. Soukal, J. Lukas and J. Fridrich, "Detection of Copy-Move Forgery in Digital Images", Digital Forensic Research Workshop, USA, Cleveland, OH, 2003, pp.55-61.
- [4] B.L. Shivakumar and S.Santhosh Baboo, "Detection of Region Duplication Forgery in Digital Images Using SURF", International Journal of Computer Science, vol. 8, no. 1, Jul. 2011, pp. 199-205.
- [5] S. Khan and A. Kulkarni, "Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform", International Journal of Computer Applications, vol. 6, no. 6, 2010 , pp. 31-36.
- [6] B. Mahdian and S. Saic, "Detection of Copy-Move Forgery Using a Method Based on Blur Moment Invariants", Forensic Science International, vol. 171, 2007, pp. 180-189.
- [7] S. Ryu, M. Lee and H. Lee, "Detection of Coy-Rotate-Forgery Using Zernike Moments", Proc. of the 12th International Conference on Information Hiding, vol. 6387, 2010, pp. 51-65.
- [8] L. Li, S. Li and H. Zhu, "An Efficient Scheme for Detecting Copy-Move Forged Images by Local Binary Patterns", Journal of Information hiding and Multimedia Signal Processing, vol. 4, Jan. 2013, pp. 46-56.
- [9] V.Arola, N. Kurvinen and Eero Siniluhta, "Local Binary Pattern", Machine Vision and Digital Image Analysis, November 9th, 2011.