

Copy-Move Image Forgery Detection Tool

Ramandeep Kaur¹, Amandeep Verma²

Punjabi University Regional Centre for IT & Management, Mohali

Abstract: Digital images are extensively used as communication medium. Forgeries in digital image have grown to be a severe concern, owing to easy and liberated accessibility of puissant image processing tools. The literature addresses the stated issue extensively and presents solutions to them. The proposed elucidations have some commonalities in their methodologies. Nearly all of them are at variance either in feature extraction or in similarity measure used for forgery detection. A tool is missing in the literature that is capable to detect forgery on the choice of feature or similarity measure (the other steps of forgery detection remains same as these are extracted commonalities), and even perform the comparisons. In this paper, a GUI tool is proposed and designed to detect the Copy-Move forgery in digital images. This tool localizes image areas that are identical or extremely similar. Firstly, the tool decomposes the input image into number of overlapping chunks. It is followed by desired feature extraction. Further, duplicated regions are identified using the chosen similarity criterion. This approach allows the flexibility in selection of feature and similarity measure.

Keywords: Image processing, digital image forensics, digital tampering, feature extraction, similarity measure

I. Introduction

With the advent of high resolution digital cameras and puissant image processing tools such as Adobe Photoshop makes it facile to engender, alter and manipulate digital images [1]. As a result, digitally manipulated forgeries are arduous to distinguish from authentic photographs. Image forgery detection system is needed in many fields for forfeiting copyright and averting forgery of images with malignant intentions. In this sense, image tampering detection is one of the principal goals in image forensics. Existing Digital Image Forgery Detection Techniques are grouped into Intrusive (active) and Non-Intrusive (passive) approach [2]. In active approach, the digital image requires preferential treatment of image such as watermark embedding and signature generation at the time of digitization in order to protect it against forgery. Unlike active approach methods, passive approach does not require any watermark or signature.

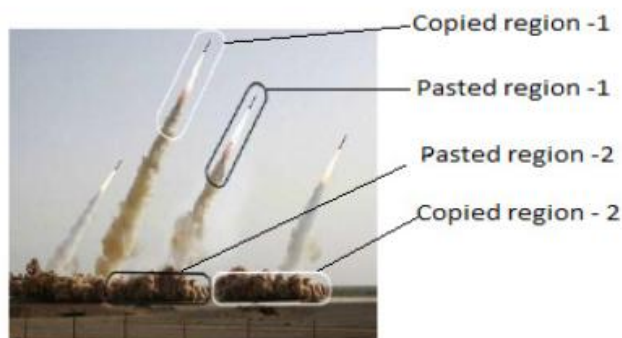
Now, Passive Digital Image Forensics is an incipient task in image processing. There are various types of tampering, however, concealing some objects from universal images is a prevalent form of digital image tampering, kenneled as Copy-Move Forgery (CMF). In Copy Move Image Forgery, a part of the image is copied and pasted in order to conceal extraneous portion of the image. As the replicated part emanate from the same image, its paramount properties like texture, noise and color palette will be compatible with the rest of the image and thus will be more arduous to distinguish and detect such type of falsification [3]. An example of Copy-Move forgery is exposed in figure 1.

Figure 1: Copy-Move forgery example [4] [5]





a) Original image



b) Forged image

We focus on the detection of malicious manipulation with digital image. In this paper, we introduce an efficient GUI tool which is proficient of detecting forgery on the cull of feature or similarity measure. Primarily, the tool crumbles the image into various overlapping chunks. It is followed by desired feature extraction. Further, duplicated regions are identified utilizing the culled kindred/similarity criterion, highlighting the source image if an astronomically immense number of matches are found. This approach sanctions the flexibility in culled of feature and other measures.

The rest of the paper is organized as follows: Related Work is discussed in Section 2. In Section 3, the proposed Copy-Move forgery tool is described in detail. In Section 4, we show some experimental results and in Section 5, we make a conclusion for this paper.

II. Literature Review

The literature reports many ways to counterfeit digital images. To ameliorate the robustness of matching precision and recede computational intricacy, many researchers have been done to utilize block matching methods.

Fridrich *et al.* [6], 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 similar or not. Similarly, Kulkarni *et al.* [7], probed the homogeneous blocks in an image by utilizing discrete wavelet transform [DWT]. Further duplicated regions were analyzed by using phase correlation. Sridevi *et al.* [4], proposed a copy-move forgery detection algorithm using block matching technique, which first divided the image into overlapping blocks followed by feature extraction. Correlation was used in order to distinguish between the forged region and the original ones.

Currently many researchers consider detecting copy-move forgery utilizing image rotation and scaling invariant such as Zernike moments, scale invariant feature transform [8]. This scheme was also resilient to distortion and achieved a precision rate of 83.59% when the copied region bear rotation but virtually had high computational cost. Mahdian *et al.* [9], detects the blurred copy-move forgery utilizing blur invariant moments. As they were invariant, these schemes were robust against noise contamination, blur degradation and contrast changes. In [10], Li *et al.* proposed a method by introducing rotation invariant uniform local binary pattern to reduce the dimension of the feature vector. The advantage of the proposed method was that it was robust to geometric transformations also, such as region rotation.

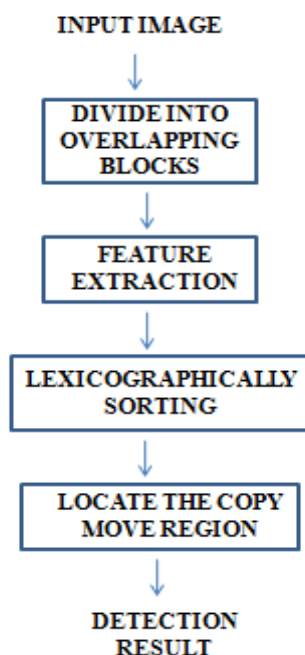
The proposed illustrations have some commonalities in their methodologies. To this end, a tool is lacking in the literature that is proficient to detect forgery on the cull of features or kindred similarity measures and even perform the comparison.

III. Design

The task of detecting copy move forgery is to find astronomically immense kindred regions in an image. As 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, no one can abide that. In order to take an efficacious detection a bit sound features must be extracted from the blocks which can not only represents the whole blocks, but also reduces the dimensions of the feature vector.

The data flow of the proposed tool is shown in the figure 2.

Figure 2: Forgery detection steps



In consonance with the above colloquy, we built a prevalent framework for CMFD methods. Figure 2 depicts the structure consisting of following four steps: 1) image block-division, 2) feature extraction, 3) lexicographic sorting and 4) Block matching.

First, Input the gray scale image chosen by the user. Tile the input gray scale image into many overlapping blocks (square or circular). Slide the $B \times B$ block throughout the entire image from the upper left corner of the image. The block entries are stored in a matrix I . The size of the matrix I is $(M-B+1) \times (N-B+1)$ rows and $B \times B$ columns, where M and N are the number of rows and columns of the chosen image respectively [11]. Further, features are extracted by making use of block matching technique ([12], [8], [13]). It is followed by lexicographic sorting([14], [4]). In the sorted list, the similar rows are proximate to each other. In the last step, replicated regions are identified using the similarity criterion ([9], [10]).

The proposed tool is veteran to discover forgery on the choice of features and similarity measures. The other steps of forgery detection remains same as these are extracted commonalities. The main distinguishment between the sundry methods lies in the feature extraction.

Feature is a piece of erudition which is pertinent for solving the computational task cognate to a certain application [15]. Bayram et al. applied Fourier-Mellen-Transform (FMT) to each block [16].Fridrich et al. [6] proposed the use of 256 coefficients of the DCT as features. For demonstrative purpose the present study use following features:

- Intensity: it is the simplest one. The intensity features are captured from the input image by utilization of overlapping chunks [4].
- Blur Moments: these schemes are robust against noise contamination, blur degradation and contrast changes. Along with this, PCA is utilized to reduce the feature dimensions [9].
- Zernike Moments: these are also resilient to distortion and achieve a precision rate of 83.59%, when copied region bear rotation [8].
- Local binary pattern: it is robust to geometric transformation, such as region rotation [10].

Similarity measure quantification must be culled to decide how close an image to another. Chu et al. [17] discussed various similarity measures for comparing the images. Lin et al. utilized shift vector as similarity measure in [12] in order to identify the duplicate regions. Phase correlation was employed in [7] for template matching. Selection of felicitous similarity measure becomes even more consequential when matching involves flaw. Similarity measures available in the implement are:

- Correlation: It is widely utilized for analyzing images. Two images are absolutely identical if correlation is 1. It is defined as:

$$r = \frac{\sum_i (x_i - x_m)(y_i - y_m)}{\sqrt{\sum_i (x_i - x_m)^2} \sqrt{\sum_i (y_i - y_m)^2}}$$

Where, x_i the intensity of the i th pixel in image1 is, y_i is the intensity of the i th pixel in image2, x_m is the mean intensity of image1 and y is the mean intensity of image2.

- **Euclidean distance:** Extract sound features and calculate Euclidean distance between the feature sets. If the computed distance is minimal, more homogeneous are the images and vice-versa.

$$d = \sqrt{\sum_j (x_j - y_j)^2}$$

Also, similar measurement called the city block distance [17], is computed by:

$$d = \sum_j |x_j - y_j|$$

Where x_j and y_j are the feature vector of image1 and image2 respectively.

- **Root mean square error:** To acquire a quantification of how homogeneous two images are, calculate the root-mean-square (RMS) value of the distinguishment between the images. If the images are precisely identical, this value is zero.

$$rms = \sqrt{\sum (D.^2)/N}$$

Where, $D = \text{image1} - \text{image2}$, N is the total number of elements in image1 (or image 2).

- **Peak-Signal-to-Noise Ratio:** It is an approximation to human judgment of restoration quality. The images are identical when MSE is zero. It is defined as:

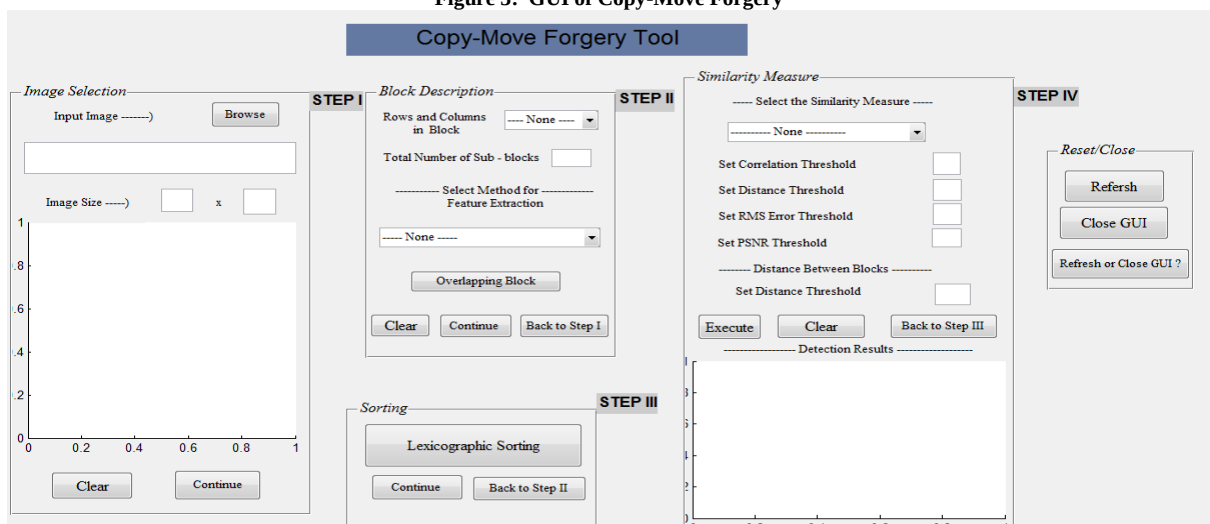
$$psnr = 10 \cdot \log_{10} \left(\frac{255}{MSE} \right)$$

Where, MSE is the mean square error.

IV. Implementation

In this paper, the implement fixates on the feature extraction and the kindred attribute measures. The main distinguishment between the sundry methods lies in the feature extraction. It localizes image areas that are identical or extremely similar. The GUI for copy-move forgery is shown in figure 3.

Figure 3: GUI of Copy-Move Forgery



The above tool has the four sections namely: 1) Image selection, 2) image block description and feature extraction, 3) lexicographic sorting and 4) similarity measures.

Firstly, the tool decomposes the input suspicious image of dimension $M \times N$ into number of overlapping chunks of $B \times B$ pixels in dimension, by sliding the chunk over the entire image from the upper left corner to the bottom of the image, in a raster scan order. Square block-matching technique is utilized to represent each block. Totally we could get N_{blocks} , where:

$$N_{\text{blocks}} = (M-B+1) \times (N-B+1)$$

Next we apply the desired feature extraction to each sub-block. These features are stored as one row in a matrix. The resultant matrix will have $(M-B+1) \times (N-B+1)$ rows and $B \times B$ columns. This step is followed by nominal lexicographic sorting. If two consecutive rows of the sorted matrix are encountered, garner the location of the matching chunks in a separate list. That is, the similar rows will be proximate to each other in the sorted list.

Further, as the copied part belongs to the same image, sharing the properties like noise turbulence, texture and color palette, it is arduous to discriminate the forged region from the original region. Selection of felicitous similarity measure becomes even more consequential when matching involves flaw. Similarity measures are employed to detect the duplicate regions, accordingly the identical regions can be facilely pinpointed.

V. Results

In the experiment, images are taken from the cyber world. This approach allows the flexibility in selection of feature and similarity measure. The similarity (T_s) and distance (T_D) threshold is user-defined parameter determines the minimum distance between the forged regions.

The experimental results based on **features** are:

- Intensity :

Parameter were set to $B=8$ (block size), $T_s = 5$ and $T_D = 69$ with Euclidean Distance.



a) Original Image



b) Forged Image



c) Result

- Blur Moment Invariant:

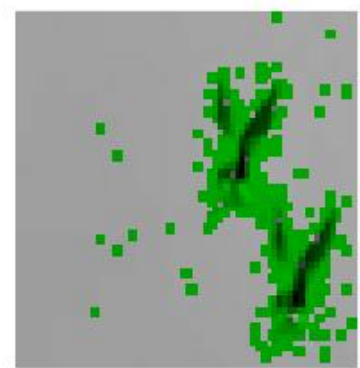
Parameter were set to $B=2$ (block size), $T_s = 15$ and $T_D = 5$ with Euclidean Distance.



a) Original Image



b) Forged Image



c) Result

- Zernike Moments:

Parameter were set to $B=8$ (block size), $T_S = 25$ and $T_D = 33.5$ with PSNR.



a) Original Image



b) forged Image



c) Result

- Local Binary Pattern:

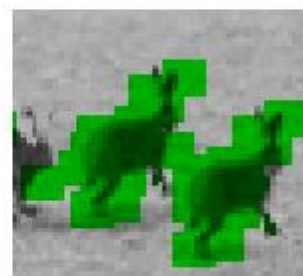
Parameter were set to $B=8$ (block size), $T_S = 0.8$ and $T_D = 5$ with correlation.



a) Original Image



b) Forged Image



c) Result

The experimental results based on **Similarity Measures:**

- Euclidean distance:

Parameter were set to $B=2$ (block size), $T_S = 15$ and $T_D = 5$.



a) Original Image



b) Forged Image



c) Result

- Root-Mean-Square Error:

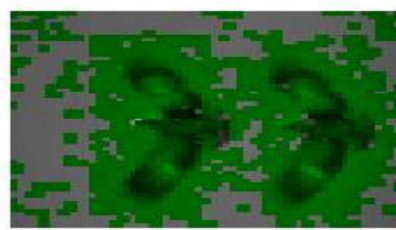
Parameter were set to $B=2$ (block size), $T_S = 20$ and $T_D = 20$.



a) Original image



b) Forged Image



c) Result

- Correlation:

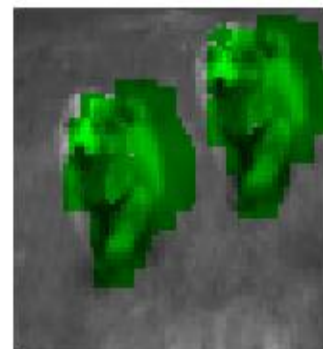
Parameter were set to B=8 (block size), $T_S = 0.87$ and $T_D = 21$.



a) Original Image



b) Forged Image



c) Result

- Peak-Signal-to-Noise ratio:

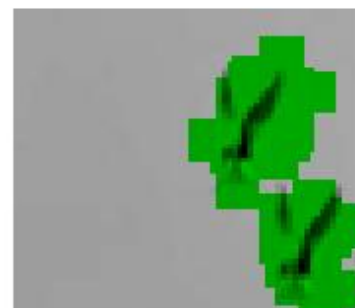
Parameter were set to B=8 (block size), $T_S = 12$ and $T_D = 17.8$.



a) Original Image



b) Forged Image



c) Result

VI. Conclusion

Copy-move forgery is prevalent way to forge a digital image. Many researchers have exploited various techniques to recognize the copy-move forgery. We proposed a Copy-Move forgery detection implement, which detects the replicated regions with various sizes on the cull of features and similarity attribute measures. It works in consummate absence of digital watermarks or signatures.

As the each listed feature and similarity measure have different impact on the result of detection. So, with this tool it is possible to use the feature and similarity measure depending upon the requirement of detection e.g. robust against compression, robust against geometric transformations, robust against noise contamination etc. Experimental results fortified that the proposed implement was felicitous to detect and localize the copy-move region even when the region had been manipulated intentionally. To this end, the proposed implement sanctions the flexibility in cull of feature and similarity measure. Thus, we hope that our implement can be very utilizable in many areas of forensic science.

References

- [1] Y. Cao, T. Gao, L. Fan and Q. Yang, "A Robust Detection Algorithm for Copy-Move Forgery in Digital Images", *Forensic Science International*, vol.214, Jan. 2012, pp. 33-43.
- [2] M. Hussain, K. Khawaji, G. Bebis and G. Muhammad, "Passive Copy Move Image Forgery Detection Using Undecimated Dyadic Wavelet Transform", *Digital Investigation*, vol. 9, 2012, pp. 49-57.
- [3] S. Santhosh Baboo and B.L. Shivakumar, "Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods", *Global Journal of Computer Science and Technology*, vol. 10, Sept. 2010, pp. 61-65.

- [4] 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.
- [5] Y. Rathore and P. Yadav, "Detection of Copy-Move Forgery of Images Using Discrete Wavelet Transform", International Journal on Computer Science and Engineering, 2012, pp. 565-570.
- [6] 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.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] 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.
- [11] H. Yao, T. Qiao, Z. Tang, Y. Zhao and H. Mao, "Detecting Copy-Move Forgery Using Non-Negative Matrix Factorization", Proc. of the Third International Conference on Multimedia Information Networking and Security, Shanghai, 4-6 Nov. 2011, pp. 591-594.
- [12] C. Wang, Y. Kao and H. Lin, "Fast Copy-Move Forgery Detection", Transactions on Signal Processing, vol. 5, no. 5, 2009, pp. 188-197.
- [13] 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.
- [14] Christlein, V. Riess, C. Angelopoulou and Elli, "A Study on Features for the Detection of Copy-Move Forgeries", Proc. of Information Security Solutions Europe, Berlin, Germany, 2010.
- [15] H. Sencar, N. Memon and S. Bayram, "An Efficient and Robust Method for Detecting Copy-Move Forgery", Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing , 2012, pp. 1053-1056.
- [16] C. Chen and H. Chu, "Similarity Measurement Between Images", Proc. of the 29th Annual International Conference on Computer Software and Applications, vol. 2, 26-28 Jul. 2005, pp. 41-42.
- [17] E. K. Yen and R G. Johnston, " The Ineffectiveness of the Correlation Coefficients for Image Comparisons", Journal of Physical Security, vol. 2, no. 1, 2007, pp. 1-13.