A Comparative study of copy-move forgery detection methods

Ritu Agarwal¹,³, Om Prakash Verma¹,²

¹Delhi Technological University
²opverma.dce@gmail.com
³ritu.jeea@gmail.com

Abstract. Images hold a major influential power, as evidence or as a medium to convey messages. An image is worth a thousand words and is used extensively in this era for digital communications. Hence, their tampering can cause major losses, which is why their manipulations techniques have grown sophisticated over time. Copy-move forgery is a technique, wherein an area of an image is replicated to another area of the image. The paper reviews state of the art copy-move forgery detection (CMFD) methods listing the approach and limitations of various techniques with the help of a table for better readability.

1. Introduction
Image Tampering detection methods can be divided into two categories, namely active techniques and passive techniques. Active techniques for CMFD rely on the meta-information of the image, e.g. Digital Watermarking[1] and Digital signature[2]. Digital watermarking is used to affirm the authenticity and/or originality of digital multimedia[1]. These techniques can check the integrity of digital images. On the other hand, passive techniques, also called blind techniques, do not have any pre-embedded information such as digital signature or watermark and therefore analyze the content or structure of the images. Further, passive forgery techniques can be of two types, Splicing and Copy move forgery. Splicing refers to the tampering of the images in such a way that splices of some other image are placed onto the target image. In copy-move forgery, the source and target image are the same and several properties like color and texture of the spliced portion is same as the image itself. Hence, it becomes even more difficult to detect this kind of forgery. Techniques such as transformation, compression, and addition of noise are used to make detection of a forged image even more difficult. This paper deals with state-of-the-art, CMFD techniques namely, block-based and keypoint-based. Section 1 states and describes various image forgery techniques and methods that are used to handle them. Section 2 covers the basic steps involved in CMFD techniques. Section 3 and 4 discuss the keypoint and block-based methods, respectively, for CMFD. A table has been included highlighting the benefits and limitations of the most common and effective techniques which have been continuously used.
Figure 1. Classification of Image Forgery Techniques

In block-based CMFD techniques, the image is partitioned into several overlapping blocks. These blocks are matched against each other and compared to check if any block matches the other. If any two blocks match, then that region is identified as tampered. In keypoint-based method no such blocks are formed, rather the detection takes place using keypoints present in the image. These keypoints are high entropy regions found in the image.

2. Common CMFD steps

Figure 2. CMFD Process

2.1. Preprocessing:
This step is used to enhance the efficiency of CMFD techniques. Preprocessing involves transforming the original image to a form suitable for further processing. Some common transformation techniques involve conversion of RGB (red, green, blue) to grayscale[3][4], or to HSV[5], or to YCrCb[6], or to local binary pattern (LBP)[7], applying median filter[5]. To reduce the dimension of the image, methods such as principle component analysis (PCA), and Discrete Wavelet Transform (DCT)[8] are used. Advanced preprocessing also includes image segmentation and block division[9]. Superpixels may be extracted by algorithms like Simple Linear Iterative Clustering (SLIC). These superpixels are a means to identify image texture and give a rough indication of the forged regions. Morphological filtering, median filtering etc. are used to remove minor objects which are redundant for the target image.

2.2. Feature Extraction:
The feature extraction process is different in the case of block-based and key point-based methods. Feature are obtained through block-based methods are extracted from the blocks of an image. The feature descriptors obtained from the authentic image and the manipulated image are quite similar. The image can be divided into blocks using different techniques such as, overlapping square image blocks[10], non-overlapping square image blocks[11] etc and many such techniques are listed in the literature.

In case of keypoint-based method, the interest points are detected. Interest points have higher discriminative power and are bound to be unique. Various methods used for keypoint detection in CMFD includes Harris Corner detector[12]. This method relies on variation of intensity between interest points and local neighborhood. Other is discrete cosine transform (DCT) [13]. However, for the overlapping blocks DCT coefficients are calculated and further positioned into a vector. Other methods used which are explained later in the paper.

2.3. Feature Matching
After receiving the extracted features, matching between image patches takes place, to find the potential suspicious areas. If two blocks have similar features, it indicates the presence of duplicated regions. This technique is based on similarity between blocks. Another method is searching, where matches between original and CMF areas are found. Various other matching procedures like Euclidean distance, sorting, nearest neighbor[14] etc. are also employed.

2.4. Localisation and post processing
The regions detected after matching the features might be distributed or spread across the region, therefore morphological operations and filtering[15] are used for post-processing etc. Multiple duplicated regions problem is solved by clustering algorithms [16]. Localization involves how the results would be visualized.

3. Keypoint based methods
In keypoint-based methods, various methodologies to detect CMFD have been proposed. Image segmentation is done on an image followed by affine estimation. Keypoints are extracted and a kd tree is formed. For every region, k nearest neighbor search is performed to find similar keypoints. The region pairs that match substantially with each other are then subjected to affine estimation. The matching process receives this transform matrix as input[17] PCT is used to describe the interest points detected. Then an improved method of matching is applied to detect copy-move forged region which is adaptive matching using lexicographic sorting[18] KAZE and SIFT are also used for extracting feature points. N-best matched features found using improved matching algorithm. Filter out false matches using image segmentation technique[19] SIFT has proved to be a very effective technique for CMFD, but suffers from a disadvantage of higher computational complexity and cost. The higher time complexity has always been a hindrance to effective algorithm. Hence to reduce this time complexity, SIFT has been used to extract features along with FMC(Fuzzy C-means) clustering algorithm[20].
4. Block-based methods
Various block-based methods have also been proposed from time to time. One of the limitations of block-based methods is that a powerful technique might blur the edges of the forged patches. SWT[21] has been used to find the matches between the blocks as it is effective against edge blurring. SVD has been used to extract features in this work.[21] Enhancements of block-based methods have also been proposed. One of them is to make use of polar representation where blocks are converted from Cartesian to polar system. Such technique is effective for images even when they are being manipulated by noise, blurring, rotation, scaling etc.[3] Efforts have been made to counter the problem of false matches in CMFD techniques. Segmentation of image into superpixel patches is done using SLIC. Two stage localisation process has been proposed. In the first stage, superpixel features are extracted using Weber Local Descriptor (WLD). Second level of localisation is performed by extracting block features using Discrete Analytic Fourier Mellin Transform (DAFMT).[9] SWT has been used to divide the image into four subbands(vertical,diagonal,horizontal and approximation). The approximation sub band is further divided into overlapping blocks for extracting features. Dimensionality reduction is done using DCT for each overlapping block. this method also provides robustness against image manipulations.[6] To deal with the post processing operation of geometric distortions, feature is extracted using DRHFM, making copy move forgery even more accurate[22]

Table 1. Benefits and Limitations of copy move forgery techniques

| Name of the technique                  | Method                                                                 | Benefits                                                                                     | Limitations                                                                                           |
|----------------------------------------|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Block based using k-means clustering[23]| This method improves upon the matching technique. Usage of k-means clustering to group overlapping blocks. Then, the matching is done within each cluster, which in turn boosts the matching speed. | k-means clustering technique is used which speeds up the process. It reduces the processing time with LSH-based matching. | The accuracy varies with the datasets. The image downscaling during the pre-processing step results in removal of details of the copy-move region. |
| Stationary wavelet and discrete cosine transform[5]| Features are extracted using SWT. Approximation subband has been used as it carries the most information. Then DCT is applied over feature vectors to reduce the dimension | Feature representation becomes quite diverse, because of the combination of SWT and DCT | The post processing operations such as noise addition, scaling, rotation etc. have not yet been covered in this technique for efficient forgery detection. |
| Hybrid features[18]| Features are extracted through KAZE detector, and SIFT | This method is also effective for CMFD even when the matched points are less, few tempered regions |                                                                                                         |
| Algorithm                        | Relevant Features | Tampered Image | Might Be Missed Out |
|---------------------------------|-------------------|----------------|---------------------|
|                                 |                   |                | in this algorithm.  |
|                                 | Relevant features are kept for matching from the plethora of features obtained through both algorithms. Thereafter, matching of the features are performed for CMF detection. | Tampered image is distorted by factors like scaling, rotation, noise addition etc. | |
| **Feature extraction and adaptive matching**[24] | Firstly, segmentation of image into patches which are non-overlapping and irregular in shape takes place. Features are then extracted using SIFT. Finally, adaptive matching takes place to detect forged regions. | The proposed scheme performs very well for geometric transforms, such as scaling and rotation, JPEG compression and noise addition. The scheme works well for down-sampling and multiple forgeries. | Recall rates aren’t too good under various attacks. |
| **Modified SIFT with key-point distribution.**[25] | A method is proposed to disperse the key-points evenly throughout the image for extracting important feature from the whole image. Then meaningful information are taken through SIFT descriptor for efficient CMF detection from images. | The method works well even for small number of key-points in the texture less area. Improves invariance of mirror transformation & rotation. | Difficulty in forgery detection of areas which have undergone non-affine transformations. |
| **Deep neural network for CMFD**[26] | A two layer deep neural network called buster net is implemented for efficient CMF detection which is end-to-end trainable through out-of-domain datasets. | Fully trainable solution, optimized for the forgery mask reconstruction loss. Robust against incursions like affine transformation, JPEG compression, blurring. | Not very effective for pure texture images. Sometimes, the prediction is erroneous in case of similar regions. |
| **Bidirectional** | A detailed review is | Computational | For ideal conditions, |
| Method                                    | Description                                                                                                                                                                                                 | Complexity | Other Methods |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------------|
| Coherency Error Refinement[27]           | Given on the various techniques for CMF detection. Furthermore, an approach is presented in which false matches are removed and localization of the detected forgeries are visualized.                                      |            | Performing better |
| Hierarchical feature point matching[28]  | This technique first finds a reasonable number of keypoints for matching in an image. Then, keypoint matching is done via this novel hierarchical matching strategy.                                                  |            | Scaling factor of images covered is narrow (80%, 120%) |
| Fractional Quaternion Zernike Moments[29]| Fractional quaternion zernike moments are to be considered as a feature of the image. The matching algorithm used is modified version of PatchMatch.                                                       |            | Robustness of other features to various kind of operations is yet to be explored. |
| GLCM-based Rotation-invariant Feature[30]| Well-known SURF technique has been used in conjugation with GLCM based feature descriptor.                                                                                                                   |            | Robustness against brightness and rotation. This technique can also be in used in classification tasks e.g SVM, which is used to perform detection and localization of anomalies. |
| SWT and SIFT[31]                         | This technique majorly deals with being robust against various techniques such as brightness and rotation.                                                                                                    |            | Percentage of accuracy and false positives can be |
operations on images. It first uses stationary wavelet transform to decompose image into four parts and keypoints are finally extracted using SIFT. DWT and SIFT. improved upon

| PCET moments and morphological operators[5] | Morphological operations have been can remove redundant objects. PCET moments are used as features. Features vectors are then subjected to Euclidean distance and correlation coefficient in order to search for similar objects. | Highly robust against post processing operations. Less time complexity. | Not being applied to color images yet |

5. Conclusion
This paper mainly deals with a specific kind of image tampering technique which is copy-move forgery. The basic steps of CMFD techniques have been explored in detail. At every step, methods and techniques proposed in the recent times are referenced state of art techniques are discussed, by dividing them into block-based and key-point based methods. Both have their own benefits and limitations. Block-based offers good accuracy but are computational time expensive. On the other hand, keypoint based techniques overcome this disadvantage, but they are not that effective in certain cases such as when dealing with uniform areas. The most common methods which have been used for a long time now for CMFD have been discussed in the table.

References
[1] A. K. Singh, “Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images,” Multimed. Tools Appl., 2016.
[2] D. M. Uliyan, “Detection of Scaled Region Duplication Image Forgery using Color based Segmentation with LSB Signature,” no. September, 2017.
[3] S. M. Fadl and N. A. Semary, “Robust Copy-Move Forgery Revealing in Digital Images Using Polar Coordinate System,” Neurocomputing, 2017.
[4] X. Pan and S. Lyu, “Region Duplication Detection Using Image Feature Matching,” vol. 5, no. 4, pp. 857–867, 2010.
[5] K. M. Hosny, H. M. Hamza, and N. A. Lashin, “Copy-move forgery detection of duplicated objects using accurate PCET moments and morphological operators,” Imaging Sci. J., vol. 0, no. 0, pp. 1–16, 2018.
[6] T. Mahmood, Z. Mehmoood, M. Shah, and T. Saba, “A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform,” J. Vis. Commun. Image Represent., vol. 53, no. September 2017, pp. 202–214, 2018.
[7] A. Kuznetsov and V. Myasnikov, “A new copy-move forgery detection algorithm using image preprocessing procedure,” Procedia Eng., vol. 201, pp. 436–444, 2017.
[8] A. Hilal, “Copy-Move Forgery Detection using Principal Component Analysis and Discrete Cosine Transform,” pp. 1–4, 2017.

[9] C. Pun and J. Chung, “A Two-stage Localization for Copy-Move Forgery Detection,” Inf. Sci. (Ny.), 2018.

[10] B. Ustubioglu et al., “Improved copy-move forgery detection based on the CLDs and colour moments Improved copy-move forgery detection based on the CLDs and colour moments,” vol. 2199, no. April, 2016.

[11] J. Zhang, “A New Approach for Detecting Copy-Move Forgery in Digital Images,” pp. 362–366, 2008.

[12] N. Monz, “An Analysis and Implementation of the Harris Corner Detector An Analysis and Implementation of the Harris Corner Detector Introduction,” no. October, 2018.

[13] S. Kumar, “Detecting Copy move Forgery using DCT,” no. May, pp. 1–5, 2014.

[14] A. S. Neighborhood, A. For, D. Duplicated, R. In, I. Forgeries, and B. On, “A SORTED NEIGHBORHOOD APPROACH FOR DETECTING DUPLICATED REGIONS IN Guohui Li, Qiong Wu, Dan Tu, Shao / ie Sunl,,” pp. 1750–1753, 2007.

[15] H. Lin, C. Wang, and Y. Kao, “Fast Copy-Move Forgery Detection,” no. May 2009, 2014.

[16] G. Jin and X. Wan, “An improved method for SIFT-based copy–move forgery detection using non-maximum value suppression and optimized J-Linkage,” Signal Process. Image Commun., vol. 57, pp. 113–125, 2017.

[17] J. Li, X. Li, B. Yang, X. Sun, and S. Member, “Segmentation-based Image copy-move Forgery Detection Scheme,” vol. 6013, no. c, pp. 1–12, 2015.

[18] M. Zandi, A. Mahmoudi-aznaveh, and A. Talebpour, “Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector,” vol. 6013, no. c, 2016.

[19] F. Yang, J. Li, W. Lu, and J. Weng, “Copy-move forgery detection based on hybrid features,” Eng. Appl. Artif. Intell., vol. 59, no. October 2016, pp. 73–83, 2017.

[20] H. A. Alberry, A. Hegazy, and G. Salama, “A Fast SIFT Based Method for Copy Move Forgery Detection,” Futur. Comput. Informatics J., 2018.

[21] R. Dixit, R. Naskar, and S. Mishra, “Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD,” vol. 11, pp. 301–309, 2017.

[22] J. Zhong, Y. Gan, and J. Young, “A new block-based method for copy move forgery detection under image geometric transforms,” Multimed. Tools Appl., 2016.

[23] O. M. A. Bee and E. Khoo, “Enhanced block-based copy-move forgery detection using k-means clustering,” Multidim. Syst. Signal Process., 2018.

[24] X. Bi, C. Pun, and X. Yuan, “Multi-scale feature extraction and adaptive matching for copy-move forgery detection,” Multimed. Tools Appl., 2016.

[25] B. Yang, X. Sun, and H. Guo, “A copy-move forgery detection method based on CMFD-SIFT,” Multimed. Tools Appl., no. 1800, 2017.

[26] Y. Wu, W. Abd-Almageed, and P. Natarajan, “Image copy-move forgery detection via an end-to-end deep neural network,” Proc. - 2018 IEEE Winter Conf. Appl. Comput. Vision, WACV 2018, vol. 2018-Janua, no. d, pp. 1907–1915, 2018.

[27] X. Bi and C. M. Pun, “Fast copy-move forgery detection using local bidirectional coherence error refinement,” Pattern Recognit., vol. 81, pp. 161–175, 2018.

[28] Y. Li and J. Zhou, “Fast and Effective Image Copy-Move Forgery Detection via Hierarchical Feature Point Matching,” IEEE Trans. Inf. Forensics Secur., vol. 14, no. 5, pp. 1307–1322, 2019.

[29] B. Chen, M. Yu, Q. Su, H. J. Shim, and Y. Q. Shi, “Fractional quaternion zernike moments for robust color image copy-move forgery detection,” IEEE Access, vol. 6, pp. 56637–56646, 2018.

[30] S. Teerakanok and T. Uehara, “Copy-move Forgery Detection Using GLCM-Based Rotation-Invariant Feature: A Preliminary Research,” Proc. - Int. Comput. Softw. Appl. Conf., vol. 2, pp. 365–369, 2018.
[31] T. Das, R. Hasan, M. R. Azam, and J. Uddin, “A Robust Method for Detecting Copy-Move Image Forgery Using Stationary Wavelet Transform and Scale Invariant Feature Transform,” Int. Conf. Comput. Commun. Chem. Mater. Electron. Eng. IC4ME2 2018, pp. 1–4, 2018.