Copy move Forgery Detection Approaches: A Survey

Rajeev Rajkumar, Thounaojam Angaleima Chanu, Ningthoujam Nejit Singh
Khwairakpam Robinson Singh[1],

Manipur Institute of Technology, Takyelpat, Imphal, Manipur University
Takyelpat, Imphal - 795004, Manipur. INDIA.
rajeev.bono@gmail.com
leimaathouna@gmail.com
nejit12@gmail.com
robsimkhwairakpam@gmail.com

Abstract: ***Copy-move forgery detection is one of the most popular image forgery technique in which a part of a digital image is copied and pasted to another part in the same image with the intension to make an object "disappear" from the image by covering it with a small block copied from another part of the same image. Hence, the main task of copy-move forgery detection is to detect image areas that are same or almost similar within an image. These method in general use two approaches namely key-point based and block based. This paper provides a review of copy move forgery detection on various techniques.***

Keywords: Copy move forgery, Lexicographical Sorting, Digital Image Forgery, Duplicated Region.

1. Introduction

A copy-move forgery is a specific type of image manipulation in which a part of its content has been copied and pasted within the same image as shown in Figure 2. Its main motivations are either to hide or to conceal unwanted portion of an image, or to emphasize particular object. A copy-move forgery is straight forward to create. Additionally, both source and the target regions stem from the same image, thus properties like the color temperature, illumination conditions and noise are expected to be well-matched between the tampered region and the image. Most techniques follow a common pipeline, as shown in Figure 1. Copy-move forgery detection methods are either key point-based methods [3, 11], or block-based methods [4, 7, 9, 10, 12, 18].Preprocessing of the images may be included before performing these methods. However, for instance, most of the methods operate on gray-scale images, and as such require that the color channels be first merged.

A feature vector is computed for every such region and similar feature vectors are subsequently matched. By contrast, key Point-based methods compute their features only on image regions with high entropy, without any image subdivision. Afterwards, the area which has same features within an image are then matched. Because of the differences in the computational cost and detected details between block-based and key point-based methods, this paper consider various methods. The rest of paper is organized as follows: In Section II, Review of algorithms are discussed. In Section III, proposed methods are discussed. Analysis of the result is done in Section IV and Section V describes the conclusion of the paper.

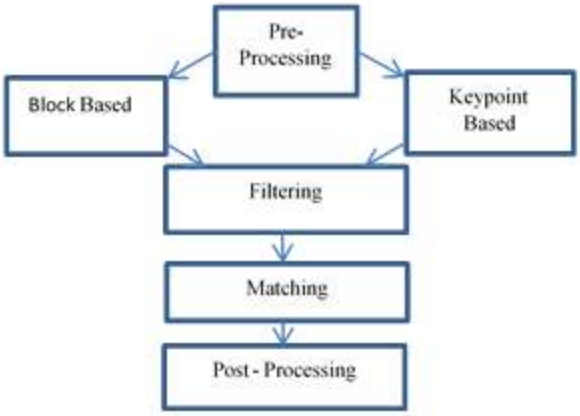

Figure1: Two different Processing methods for the detection of copy move forgeries.

(i) (ii)

Figure 2: (i) Original Image (ii) Forged Image

2. Steps involved in Copy move Forgery Detection

Copy move Forgery Detection consists of the following steps which are discussed below:

2.1 Preprocessing

It comprises of the conversion of RGB image to its gray format.

2.2. Block Based

It is a method for feature extraction. For block-based methods, a threshold which is based on the Same Affine Transformation Selection (SATS) [8] connected area in order to filter out spurious detection is used. Because SATS can gives the most reliable results. Examining a 13 different block-based features, which we considered the representative of the entire field, we can be classified into four different categories namely moment-based, dimensionality reduction-based, intensity-based, and frequency domain-based features (see Table I).

Moment-based: Within this class we evaluated 3 distinct approaches as given in TABLE I. Mahdian and Saic [20] proposed the use of 24 blur- invariant moments as features (Blur).

I. TABLE I:CATEGORIES OF FEATURES SETS FOR COPY-MOVE FORGERY DETECTION

CATEGORY	METHOD
Moments	BLUR HU ZERNIKE
Dimensionality Reduction	PCA SVD KPCA
Intensity	LUO BRAVO LIN CIRCLE
Frequency	DCT DWT FMT
Keypoint	SIFT SURF

Dimensionality reduction-based: The feature matching space was reduced via principal component analysis (PCA). Bashar *et al*. [4] proposed the Kernel-PCA (KPCA) variant of PCA. Kang *et al*. [13] computed the singular values of a reduced-rank approximation (SVD). A fourth approach using a combination of the discrete wavelet transform and Singular Value Decomposition [15] did not yield reliable results in our setup and was, thus, excluded from the evaluation.

Intensity-based: This method work with both gray scale image and color image. Additionally, Luo *et al* [21] used directional information of blocks (Luo) while Bravo-Solorio *et al*. [7] also consider the entropy of a block as a discriminating feature (Bravo). Lin *et al* [17] (Lin) computed the average gray-scale intensities of a block and its sub blocks. Wang *et al* [18], works on the mean intensities of circles along with different radii around the block center (Circle).

Frequency-based: The use of 256 coefficients of the discrete cosine transform as features (DCT) was proposed by Fridrich *et al*. [10] . Bashar *et al*. [4]. Proposed the coefficients of a discrete wavelet transform (DWT) using Haar–Wavelet as features. The use of the Fourier–Mellin Transform (FMT) for generating feature vectors was introduced by Bayram *et al*. [6].

Disadvantages of the existing methods are discussed below:

Discrete Wave transform (DWT): The performance relies on the location of copy-move regions. Discrete cosine transform (DCT): This can only be done for very small images because it is computationally costly.

Fourier-Mellin transform (FMT): The algorithms works for the case of only slight rotation.

Speeded up Robust features (SURF): The method fails to automatically locate the tampered region and its boundary.

Scale Invariant Features Transform (SIFT***):*** Choice on the number of clusters is to be made sensitively.

2.3 Key-point based Algorithms

The key point-based methods depends on the identification and the selection of high-entropy image region i.e. the “key points”. A feature vector is then extracted per key point. Consequently, fewer feature vectors are estimated, resulting to reduce the computational complexity. The lower number of feature vectors indicates that post processing, thresholds are used to lower the block-based methods. One drawback of key point method, is that the region which are copied are thinly covered by matched key points. If the regions of copied show little structure, it may take place that the region is totally missed. So we investigated two different version of key point-based form vector. Namely, they are known as SIFT and SURF.As they approach with different technique respectively. The form of extraction is practicable in standard libraries. However, particular differences of key point-based algorithms lie in the post-processing of the matched features, as stated in the previous section [3, 11].

2.4. Filtering

The main reason for applying a filtering scheme is to minimize the probability of false matches within an image. In general, a common noise suppression measure involves the removal of matches between the spatially close regions. A false forgery detection is mainly occurred due to the neighboring pixels which often have similar intensities. So, in order to filter out the weak matches, a number of distance criteria have been proposed.

2.5. Matching

A very high similarity between two feature descriptors depicts a high chance of duplicated regions. For the block-based methods most author propose the use of *lexicographic sorting* in identifying the similar feature vectors [4 ,7,9, 10,12,18].Every feature vector becomes a row in the matrix after performing lexicographic sorting, a matrix of feature vectors. After that, the matrix is sorted row-wised and then, the features which are similar are appeared in consecutive rows.

Many authors also use the Best-Bin-First search method derived from the kd-tree algorithm to get approximate nearest neighbors [11]. In particular, key point-based method often used this approach. Matching with a kd-tree yields a relatively efficient nearest neighbor search. Typically, the Euclidean distance is also used as a similarity measure. In prior work, it has been shown that the use of kd-tree matching leads to better results than lexicographic sorting, but the memory requirements are significantly higher. For these features, the performance gain over lexicographic sorting is minimal. The paper matched feature vectors by using the approximate nearest neighbor method of Muja *et al* [19]. It uses multiple randomized kd-trees for a fast neighbor search.

2.6. Post-Processing

The main aim of the post processing is to preserve matches that exhibit a similar behavior. Assume a set of matches that belongs to a copied region. These matches are expected to be spatially close to each other in both the source and the target blocks. Furthermore, matches that originate from the same copy-move action should exhibit similar amount of translation, scaling and rotation.

The most commonly used post-processing variants handle the outliers by imposing a minimum number of similar shift vectors between matches. A shift vector contains the translation in image coordinates between two matched feature vectors. For example, a number of blocks which are simply copied without any rotation or scaling then, the histogram of shift vectors exhibits a peak at the translation parameters of the copy operation. Mahdian and Saic *et al* [22] consider a pair of matched feature vectors are forged if: i) They are sufficiently similar, i.e. their Euclidean distance is below a threshold, and ii) The neighborhood around their spatial locations contains similar features. Many authors use morphological operations to connect matched pairs and remove outliers [16]. An area threshold can also be applied, so that the detected region has at least a minimum number of points to handle rotation and scaling, Pan and Lyu *et al* [23] proposed to use RANSAC. For a certain number of iterations, a random subset of the matches is selected, and the transformations of the matches are computed. The transformation which is satisfied by most matches i.e., which yields most inliers is chosen. Recently, Amerini *et al*. [3] proposed a scheme which first builds clusters from the location of detected features and then uses RANSAC to estimate the geometric transformation between the original area and its copy-moved version. Alternatively, the ***Same Affine Transformation Selection (SATS)*** [8] groups location of feature vectors to clusters. In general, an affine transformation is used to perform region growing, on the areas which can be mapped onto each other. If the features computed on three spatially close blocks matched to three feature vectors whose blocks are also spatially close, then these groups of blocks might be a part of copied region. Place table titles above the tables.

3. Discussion

It is worth noting that the problem with copy move forgery is the detection of duplicated image regions which is made by the software which is easily available in today's world. The other challenge is computational load which is excessive. The two algorithms which are discussed in the above, Key point based methods like SIFT is an effective method to detect the duplicated regions even if the image undergoes transformation like scaling and rotation. And in Block based methods, Zernike moment is effective in detecting the copy move blocks even for the flat regions. One drawback of Block based methods is that the techniques can't detect the region if the square block is rotated or scaled duplicated blocks.

4. Conclusion

Copy move forgery detection is discussed in this paper. It gives an idea to others the important steps involved in copy move forgery detection system. Its two different techniques are also discussed, that is Keypoint based and block based methods which is still an active area of research, and its applications are also many. The outcome of this work is to detect authentic image from pirated images.

References

[1] J. Redi, W. Taktak, and J.-L. Dugelay, "Digital image forensics: A booklet for beginners," Multimedia Tools Application., vol. 51, no. 1, pp.133–162, Jan. 2011.

[2] H. Farid, "A survey of image forgery detection," *Signal Process. Mag.*, vol. 26, no. 2, pp. 16–25, Mar. 2009.

[3] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection

and trans- formation recovery," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.
[4] M. Bashar, K. Noda, N. Ohnishi, and K. Mori, "Exploring duplicated regions in natural images," IEEE Trans. Image Process., accepted for publication.
[5] S. Bayram, I. Avcıbaş, B. Sankur, and N. Memon, "Image manipula- tion detection with binary similarity measures," in Proc. Eur. Signal Processing Conf., Antalya, Turkey, Sep. 2005.
[6] S. Bayram, H. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, pp. 1053–1056,Apr. 2009.
[7] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions af- fected by reflection, rotation and scaling," in Proc. Int. Conf. Acoustics, Speech and Signal Processing, pp. 1880–1883, May 2011.
[8] V. Christlein, C. Riess, and E. Angelopoulou, "On rotation invariance in copy-move forgery detection," in Proc. IEEE Workshop on Informa- tion Forensics and Security, Seattle, WA, pp. 129–134, Dec. 2010.
[9] B. Dybala, B. Jennings, and D. Letscher, "Detecting filtered cloning in digital images," in Proc. Workshop on Multimedia & Security, pp. 43–50,Sep.2007.
[10] J. Fridrich, D. Soukal, and J. Lukáš, "Detection of copy-move forgery in digital images," in Proc. Digital Forensic Research Workshop, Cleveland, OH, Aug. 2003.
[11] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in Proc. Pacific-Asia Workshop on Computational Intelligence and Industrial Application, vol. 2, pp. 272–276, Dec. 2008.
[12] S. Ju, J. Zhou, and K. He, "An authentication method for copy areas of images," in Proc. Int. Conf. Image and Graphics, pp.303–306,Aug. 2007.
[13] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in Proc. Int. Conf. Computer Science and Software Engineering, vol. 3, pp.926–930, 2008 .
[14] Y. Ke, R. Sukthankar, and L. Huston, "An efficient parts-based near- duplicate and sub-image retrieval system," in Proc. ACM Int. Conf. Multimedia, pp. 869–876, Oct. 2004.
[15] 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 Proc. IEEE Int. Conf. Multimedia and Expo, pp.1750–1753, Jul. 2007.
[16] A. Langille and M. Gong, "An efficient match-based duplication detection algorithm," in Proc. Canadian Conf. Computer and Robot Vision, pp. 64–71, Jun. 2006.
[17] C.-Y. Lin, M. Wu, J. Bloom, I. Cox, M. Miller, and Y. Lui, "Rotation, scale, and translation resilient watermarking for images," IEEE Trans. Image Process., vol. 10, no. 5, pp. 767–782, May 2001.
[18] H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection",WSEAS Trans. Signal Process., vol. 5, no. 5, pp. 188–197, 2009.
[19] M. Muja and D. G. Lowe, "Fast approximate nearest neighbors with automatic algorithm configuration," in Proc. Int. Conf. Computer VisionTheory and Applications, pp. 331–340, Feb. 2009.
[20] B. Mahdian and S. Saic, "Detection of copy-move forgery using amethod based on blur moment invariants," Forensic Sci. Int., vol. 171,no. 2, pp. 180–189, Dec. 2007.
[21] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital images," in Proc. Int. Conf. Pattern Recognition, vol. 4, pp. 746–749,Aug. 2006.
[22] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," Forensic Sci. Int., vol. 171,no. 2, pp. 180–189, Dec. 2007.
[23] X. Pan and S. Lyu, "Region duplication detection using image feature matching," IEEE Trans. Inf. Forensics Security, vol. 5, no. 4, pp. 857–867, Dec. 2010.

Author Profile

Rajeev Rajkumar, is working as an Assistant Professor at Manipur Institute of Technology, Imphal (India).

Thounaojam Angaleima Chanu completed her B.E from MIT, Imphal.

Ningthoujam Nejit Singh received his B.E in Computer Science & Engineering Department from MIT, Imphal. He is pursuing M.Tech in the Department of Computer Science & Engineering at NIT, Manipur (India). His research interests include Image Processing, Cryptography, and Artificial Neural Networks.

Khwairakpam Robinson Singh is pursuing M.Tech in the Department of Computer Science & Engineering at NIT, Manipur (India).