IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 4, April 2018

A Review on different Copy Move Forgery Detection Methods

Sreemol R[1]

M.Tech in Computer Science and Engineering, CSE, Rajiv Gandhi Institute of Technology, Kottayam, India[1]

Abstract: Nowadays, images have an important impact on our society and play a crucial role in most people's lives. However, due to the availability of low-cost, high-performance computers and many powerful editing software packages, digital images have become easy to manipulate and edit even for nonprofessional users. Misuse of such digital forgeries has become a serious problem in various fields. Without a doubt, image authenticity is necessary in many social areas. So, the detection of a forged image received significant attention among the application of image analysis in digital forensic science. In this paper, a survey on different copy move forgery detection scheme is done.

Keywords: Dimensionality, Forgery, Image, Keypoint, Moment

I. INTRODUCTION

Detection of a forged image received significant attention among the application of image analysis in digital forensic science. Image forgery detection is driven by the need of authenticity and to maintain integrity of the images. And in most of the cases copy- move image forgery is used to tamper the digital image, in which a part of the image is copied and pasted somewhere else in the image. This is usually performed with the intention to make an object disappear from the image by covering it with a segment copied from another part of the image. Textured areas, such as grass, foliage, gravel, or fabric with irregular patterns, are ideal for this purpose because the copied areas will likely blend with the background and the human eye cannot easily discern any suspicious artifacts. Because the copied parts come from the same image, its noise component, color palette, dynamic range, and most other important properties will be compatible with the rest of the image and thus will not be detectable using methods that look for incompatibilities in statistical measures in different parts of the image. To make the forgery even harder to detect, one can use the feathered crop or the retouch tool to further mask any traces of the copied-and-moved segments.

II. LITERATURE REVIEW

Copy-Move forgery is performed with the intention of either making an object hidden from the image by covering it with a small block of background, copied from another part of the same image or creates additional copy of an object already existing in the image by copying it to the desired location. Since the copied segments are part of the same image, the color palette, noise, components, dynamic range and the other properties will be consistent with the rest of the image, and thus making it is very difficult for a naked human eye to detect the forgery. Copy-move forgery detection can be either block-based or key-point based methods. In block based methods, the image is divided into overlapping/non-overlapping blocks and feature vector is computed for each blocks. Similar feature vectors are identified and matched to find forged regions. In key-point based methods, image is scanned for keypoints and feature vector is calculated for every keypoints. The image is not sub-divided into blocks, the feature vectors are matched to find duplicated regions.

A. Block Based Methods

Several techniques to detect copy-move forgery are based on block based method. The main idea of these techniques is that rather than trying to identify the entire forged region, the image is divided into small overlapping or non-overlapping blocks. The blocks are compared against each other in order to see which blocks are matched. The regions of the image covered by the matching blocks are the copied and forged regions. These techniques can classify as- Moment-based Techniques, Dimensionality – Reduction based methods, Intensity- based and Frequency-based.

1) Moment-Based Techniques:

Mahdian and Saic [1] used blur moment invariants to represent image regions because they cannot be affected by blur degradation and additive noise. Their method begins with tilting of images by blocks of a particular size. They represented each block with blur invariants. The feature vector for each block is of length 72. These are normalized further to improve the duplication detection abilities of the algorithm. They applied principal component transformation (PCT) to reduce the dimension of feature vector. For blocks similarity analysis, they used k-d tree representation. Using a certain threshold value, they found similar blocks. Once the similar blocks are found, they must be verified. They

DOI 10.17148/IJARCCE.2018.7468

verified this by finding the neighborhood of similar blocks which are also identical. Two similar blocks with non-identical neighborhood are considered as false positive. By using this method, they successfully detected copy-move forgery for images which have blurred duplicated region. They could also detect duplicated regions with changed contrast values. Blur moment technique [1] has high ability to detect copy move forgery in an image even with the presence of blur, noise or contrast changes in the copied areas. The method even works well with lossy JPEG format data. But computation time of the algorithm is comparatively high.

Wang, Liu, Zhang, Dai and Wang [2] conducted a study on copy-move forgery detection by using Hu moments. They developed the algorithm to be more efficient and also robust to various post processing techniques such as blurring, lossy JPEG compression. They reduced the dimensions of the image by using Gaussian pyramid. They divided the image into several fixed sized blocks which 9 are overlapping. They applied Hu moments to the blocks and calculated the Eigen values. They sorted these vectors lexicographically and an area threshold is selected to reduce false detections. They performed finding matching blocks by using mathematical morphological techniques. Their method is successful in detecting copy-move forgery even when post-processing is done.

Mohamadian and Pouyan [3] described new method of detecting copy-move forgeries by using SIFT algorithm along with Zernike moments. They used SIFT algorithm to perform normal copy move forgery detections. But SIFT cannot be used to detect flat copied regions. To account for this, they used Zernike moments. Their method used the SIFT algorithm, which has only one disadvantage of not able to detect flat copy-move forgeries. They overcame this disadvantage by using Zernike moments.

2) Dimensionality – Reduction Based Techniques:

In PCA dimensionality reduction based technique author proposed [4], a technique and used PCA (Principal Component Analysis) for forgery image. This approach is same like DCT method and improved in capturing discriminating features. In this method the image transformed into gray scale and separated into many parts, which are represented into vectors. These parts or blocks are organized it lexicographically earlier matching and used PCA to represent the dissimilar blocks in a substitute mode. It is proficient for detection even minor variations because of noise or lossy compression. However the proposed technique is for grey scale images and also processes every color channel in color images and PCA is for detection the counterfeits. The proposed method is better for detecting copy-move forgeries and gives less number of false positives.

Ting and Rang-ding [5] proposed a copy-move forgery detection method using Singular Value Decomposition (SVD). Their developed algorithm is computationally less complex and is robust to post-processing techniques. They used the correlation between the copied and pasted regions and searched for identical regions. In the first step, they divided the image into several small overlapping blocks. Then, they applied SVD to every block and extracted unique singular values feature vector for each block. Using these vectors, they found the matching blocks by transforming each block features into k-d tree. They used a threshold value to increase the robustness and eliminate pseudo-matching. A natural image will not have identical regions with coherent orientation. So, the obtained matched blocks are an evidence for copy-move forgery. They used lines to connect two identical blocks in a figure which clearly shows the tampered regions. They downloaded images from internet and used their algorithm to detect forgeries. They chose an empirical value of threshold. Their algorithm successfully detected copy- move forgeries even when post-processing is done on the images. However, it fails to detect that out of two matched blocks which block is copied and which block is pasted. Their algorithm is not robust against JPEG compression.

A method proposed by Bashar, Noda, Ohnishi and Mori [6], uses Discrete Wavelet Transform (DWT) and Kernel Principal Component Analysis (KPCA) for copy-move forgery detection. They used these methods because of their robust block-matching feature. They divided the image into several small-sized blocks. They calculated KPCA-based vectors and DWT vectors for every block. Then they placed these vectors in a matrix and sorted it lexicographically. They used the sorted blocks to find the similar points and calculated their offset frequencies. To avoid false detections, they placed a threshold value for offset-frequency.

They developed a new algorithm to detect flip and rotation type of forgeries using labeling technique and geometric transformation. This algorithm showed promising improvements compared to conventional PCA-approach. It also detects forgeries which have an additive noise and lossy JPEG conversation. The method can detect Flip and Rotation duplications well. The detection of Flip forgery by this method is quite efficient because only two iterations corresponding to the HF and VF is necessary to come up with the final result. This method has no limitations of detecting the degree of rotation of the duplicated regions unlike other methods. One limitation is however the computational efficacy because the current method needs a maximum of 360 iterations using 1 degree precision for detecting Rotation forgery. A pre-processing step for an approximate computation of rotation can significantly reduce the search space of the proposed method.

Zimba and Xingming [7] proposed a new method of copy-move forgery detection. Their method begins with conversion of color image into grayscale image. Then, they applied DWT to entire image. This gives sub-bands, out of

DOI 10.17148/IJARCCE.2018.7468

which low frequency sub-band is enough to perform detection process. They divided the image into several overlapping blocks. They performed Principal Component Analysis Eigen Value Decomposition (PCA- EVD) on the blocks. They placed these feature vectors are placed into the matrix and sorted the entries lexicographically. This method of sorting makes the matching less complex. They calculated the normalized shift vector and then offset frequency. This offset frequency is subjected to morphological processing to give final results. They made this method more efficient than conventional PCA method by reducing the image size in the beginning of the process. Their algorithm can detect duplications involving rotation of varying degrees. They included morphological operations to avoid false detections. The only disadvantage is that the duplicated region should be bigger than the block size, otherwise it cannot be detected. Also, their method fails to detect forgeries involving scaling, rotation and heavy compression.

3) Intensity- Based Techniques:

A study proposed by Luo, Huang and Qiu [8] describes the method of copy-move forgery detection based on intensities. They divided into several overlapping blocks. Then they divided the blocks into two equal parts and four directions. Then a block characteristic vector is computed for all the blocks using Additive White Gaussian Noise (AWGN) operation and they are lexicographically sorted. Every pair of similar block feature vectors need not represent a duplicated region of image. So, a method has to be developed to determine which pairs actually represent duplicated region. For this, they used shift vector method. They set a particular value of shift vector and two blocks are considered equal only when the shift vector of that pair exceeds it. The highest occurring shift vector is found and the pairs are discarded whose shift vectors are much different from this value. Then they employed some method to ensure whether forgery is actually done or not. Their algorithm has lower computational complexity and robust to post-processing operations. It holds well only when the forged regions are larger than the block size. However, the algorithm fails when the images are highly distorted and have large smooth regions.

In [9] W.Luo, J.Huang, and G.Qiu describe an efficient and robust algorithm for detecting and localizing this type of malicious tampering. Also presented experimental results which show that the method is robust and can successfully detect this type of tampering for images that have been subjected to various forms of post region duplication image processing, including blurring, noise contamination, severe lossy compression, and a mixture of these processing operations. They proposes algorithm first divides an image into small overlapped blocks and it then compares the similarity of these blocks and finally identifies possible duplicated regions. W. Luo, J. Huang, and G. Qiu proposed a novel algorithm to detect tampered images automatically and effectively. Compared with others, this algorithm has lower computational complexity and is more robust against various post region duplication image processing operations.

Bravo-Solorio and Nandi [10] conducted a study on copy- move detection technique to find forgeries involving reflection, rotation and scaling. They tiled the image as block of pixels by sliding pixel by pixel with a window of particular size in a raster-scan order. They calculated feature vectors which are color-dependent. By this, they reduced the number of searches thereby increasing the efficiency. They calculated four features out of which three features are independently computed as red, green and blue components. The fourth feature is calculated as the entropy of luminance channel. They used this fourth feature to discard blocks with insufficient textural information. These features are listed lexicographically and then matching is performed. Their method produces lot of matches; hence they used refinement to reduce them. They used one-dimensional (1-D) descriptors to reduce memory usage. These 1-D descriptors are invariant to rotation and reflection. This method is efficient than many other methods in terms of computation and detecting tampered regions with post-processing.

B. Key-point Based Methods:

A study by Huang, Guo and Zhang [11], describes a method of detecting copy-move forgery by taking the advantage of correlation between the original image region and the pasted region. They introduced SIFT (Scale Invariant Feature Transform) algorithm for precise detection and to make the technique robust against post image processing. They first calculated the SIFT keypoints. They matched these with one another to find forgeries. If any identical SIFT points are found, then the image has copy move forgeries. Matching process was done for each keypoint by identifying its nearest neighbor. They set a threshold value, which is the ratio of closest to second- closest neighbors. This increases the robustness of the method. They faced difficulties in implementing for high scale images. Hence, they used BBF (Best-Bin-First) search method, which is derived from k-d algorithm, for matching. This method identifies the most similar vectors with maximum probability and minimum computation. They took one tampered image and repeated the detection method for different threshold values. They found out that the accuracy of detection is dependent on it. An optimum threshold value has to be chosen. They tested the robustness of the method by successfully detecting forgeries in a tampered image with post-processing. Their method is successful in using SIFT algorithm to detect the copy- move forgery and is robust post-processing done on the images. However, their method is not efficient when the tampered region is small and SNR value is low.

Bo, Junwen, Guangjie and Yuewei [12], conducted a study on copy-move forgery detection by using SURF (Speeded up Robust Features) algorithm, which is developed by Herbert Bay et al. It involves keypoint detection and description.

DOI 10.17148/IJARCCE.2018.7468

They used Hessian matrix for detecting the keypoints and Haar wavelets for assigning the orientation. They estimated dominant orientation and described the orientation of the interest point descriptor. By extracting square regions around these interest points, they constructed SURF descriptors which are aligned to the dominant orientation. By weighting the responses with Haar wavelets, they increased the robustness to localization errors and geometric deformations. They chose Haar wavelets because they are invariant to the illumination bias. The SURF descriptors are then used for matching. They used a threshold to increase the robustness and avoid false detections. They chose an empirical value of threshold and tested their algorithm on different images and they were successful. Further, they performed post processing like scaling, rotation and blurring on the forged images. They used the algorithm to test and were successful in showing its robustness for post processing. Their method is successful in locating the tampered regions even when post processing is done on the images. It is robust and speed in detecting. However, they couldn’t find the exact boundaries of the tampered region.

A study by Zheng, Haoa and Zhub [13] reveals a new method for keypoints matching based on the position relationship of the keypoints. Keypoints in tampered region and original region should be consistent and they should be distributed evenly over the entire image. This ensures that large similar textures, like sky, also produce considerable number of keypoints. Their algorithm is built to scan and discard the keypoints for the first time. This ensures that noise has no impact on them. They scanned the keypoints again and found the features for all keypoints. They developed new algorithm to find the features and stored these features into a matrix. Their algorithm differs from SIFT in the way of determining features. By noticing the consistent keypoints in the matrix, their algorithm detected copy-move forgery in the image. Their algorithm finds a pair of consistent keypoints and marks them as candidate keypoints only when they satisfy certain conditions. They also set a threshold value to reduce the number of false detections. They noted that the computational time is very less and also there are very less number of false detections on a large similar texture like sky. Their algorithm is advantageous in this kind of detections but cannot detect tampering involving post-processing like rotation and scaling.

CONCLUSION

Blur Moment Method has high ability to detect copy move forgery even with the presence of blur, noise or contrast changes in the copied areas. Also, it works well with lossy JPEG format data. But it needs High computational time of the algorithm. In the case of Zernike moments, flat regions of forgeries are detected and it provides shoulder surfing resilience. But, calculating Zernike moment coefficients is complex. PCA is an efficient method and it has low false positives. But it has low efficiency for low quality of image, low SNR and small blocks. SVD can detect duplication even post-processing is done. It is robust and computationally less complex. But it cannot detect copy paste regions and the performance to resist JPEG compression is weaker than other post processing. SIFT has good recall rates. But, it is slow and didn’t work well with blur. SURF has less computational time. But, Accuracy of detection result is less for large images.

REFERENCES

[1]. Mahdian and S. Saic, “Detection of copy move forgery using a method based on blur moment invariants”, Forensic Sci. Int., vol. 171, nos. 23, pp. 180189, 2007.
[2]. J. W. Wang, G. J. Liu, Z. Zhang, Y. W. Dai, and Z. Q. Wang, “Fast and robust forensics for image region-duplication forgery”, Acta Automat. Sinica, vol. 35, no. 12, pp. 14881495, 2009
[3]. Mohamadian, Z., & Pouyan, A. A. “Detection of Duplication Forgery in Digital Images in Uniform and Non-uniform Regions”. Paper presented at the UKSim, 2013.
[4]. Alin C. Popescu and Hany Farid. “Exposing Digital Forgeries in Color Filter Array Interpolated Images”, IEEE Transactions On Signal Processing, Vol. 53, No. 10, Oct 2005.
[5]. Ting, Z., & Rang-ding, W. (2009). “Copy-move forgery detection based on SVD in digital image”, Paper presented at the Image and Signal Processing, 2009.
[6]. Bashar, M., Noda, K., Ohnishi, N., & Mori, K, “Exploring duplicated regions in natural images”, IEEE Transactions on Image Processing,(99), 1, 2010.
[7]. Zimba, M., & Xingming, S, “DWT-PCA(EVD) Based Copy-move Image Forgery Detection”, International Journal of Digital Content Technology and its Applications, 2011.
[8]. Luo,W., Huang, J., & Qiu, G, “Robust detection of region-duplication forgery in digital image”, Paper presented at the Pattern Recognition ICPR , 2006.
[9]. Wang, J., Liu, G., Li, H., Dai, Y., & Wang, Z, “Detection of image region duplication forgery using model with circle block”, Paper presented at the Multimedia Information Networking and Security, 2009.
[10]. S. Bravo-Solorio and A. K. Nandi, “Exposing duplicated regions affected by reflection, rotation and scaling”, in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), May 2011.
[11]. Lin, H.-J., Wang, C.-W., & Kao, Y.-T, “Fast copy-move forgery detection”. WSEAS Transactions on Signal Processing, 2009.
[12]. Bo, X., Junwen, W., Guangjie, L., & Yuewei, D, “Image copy-move forgery detection based on SURF”. International Conference on Multimedia Information Networking and Security (MINES), 2010.
[13]. Zheng, J., Haoa W., & Zhub,W, “Detection of Copy-move Forgery Based on Keypoints Positional Relationship”. Journal of Information and Computational Science, 2012.

DOI 10.17148/IJARCCE.2018.7468