DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4146

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Review Paper on Copy Move Forgery Detection Techniques

Navdeep Kaur
Department of Computer Engineering, Punjabi University, Patiala
Patiala, Punjab

Abstract: Digital images are easy to manipulate and edit due to availability of powerful image processing and editing software. Nowadays, it is possible to add or remove important features from an image without leaving any obvious traces of tampering. As digital cameras and video cameras replace their analog counterparts, the need for authenticating digital images, validating their content and detecting forgeries will only increase. This paper reviews the detection techniques for copy move forgery tampering attacks. The copy-move attack in which a part of the image is copied and pasted somewhere else in the image with the intent to cover an important image feature is discussed in particular. It is done for hiding some image object, or adding more details resulting in atleast some part being cloned.

I. INTRODUCTION

The popularization of digital cameras and the internet have made it easy for anyone to capture and share pictures. As there are various image editing software tools such as Adobe Photoshop that allows anyone to alter images or to create or alter images for malicious purposes[1]. Image Forensics is a term that is often used to indicate the analysis of the authenticity of an image file, evaluate the presence of forgeries, and determine the device which has produced the picture. Digital image forensics is a research field which aims at validating the authenticity of images by recovering information about their history. Various methods have been developed to tackle with tampering and forgery in order to ensure the authenticity of images[2].

Digital image forensics can be divided into two approaches: active approach and passive approach. In the active approach, a digital watermark or signature verifies the integrity and authenticity of digital images. A watermark or signature is inserted into the image while it is acquired, and any malicious tampering of the image can be detected through analysis of the value of a digital watermark or signature. However, a major disadvantage is that the digital capture devices do not contain the module to insert watermarks or signatures. To overcome this problem, passive approaches which do not need any prior information about image to detect traces of tampering[3].

One of the main goals of Image Forensics techniques is to understand what kind of tampering has been applied. Images can be doctored in several ways: photo-compositing, re-touching, enhancing are only some examples of typical image alterations[4]. We particularly study copy-move tampering that is one of the most common image manipulations. The purpose of copy move forgery is to copy a part of an image, basically for the purpose of to hide an object, by copy-pasting a set of pixels from an area to another area of the same picture, and it is often very difficult to detect with the naked eye[4]. The classification of image forgery detection techniques is shown in the figure.

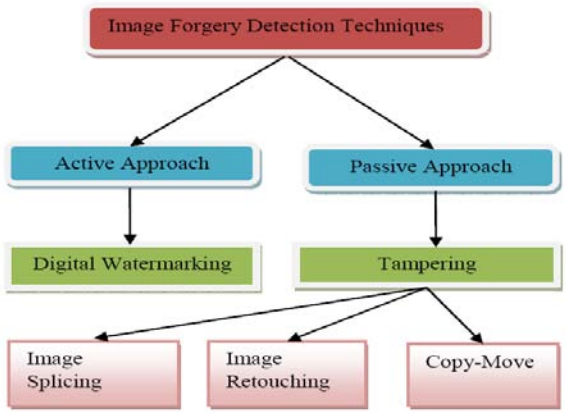

Figure 1: Classification of Image forgery Techniques

II. RELATED WORK

The literature has been concerned with copy-move forgery detection where additional operations are applied. Rotation, resizing, horizontal/vertical flipping, edge blurring and white Gaussian noise insertion are the main transformations used to give realism to manipulated images, thus expanding visual and computing efforts to check the image's authenticity.

Fridrich et al. [5] presented a method in which copy-move regions in digital images are detected. The method extracts the DCT Coefficients and then sort with lexicographically scheme. By doing so, the complexities of the comparisions are reduced. Finally, the method detects the tampered regions based on the approximate block matching. Cao et al. [6] proposed a DCT-based approach, the various attacks in the image such blurring and noise adding, so the main purpose of this DCT-based approach is to reduce the size of the feature vector and add robustness against attacks. Davarzani et al. [7] extracted feature vectors for each overlapping image block using multi-resolution local binary patterns operators (MLBP) and then sorted by lexicographical order for texture and intensity-based approach. To reduce the block matching time, the k-d tree is utilized, and to eliminate false detections, random sample consensus (RANSAC) algorithms are utilized. In [8], invariant key-points based approach, Amerini et al. used scale invariant features transform (SIFT). Using this

approach, the duplicated region which altered the size or angle is detected using the geometric transformations before it is pasted. Chi-Man Pun et al.[9] Proposed a scheme which combines two forgery detection methods that are block based and keypoint based methods. There can be various challenging conditions like JPEG Compression, geometric transforms, down sampling. By using this scheme, much better detection results can be achieved. Lynch et al. [10] proposed an efficient expanding block algorithm, which primarily use direct block comparison based on block features for detecting the duplicated region. Ardizzone and Mazzola[11] presented a method to detect duplicated areas in a digital image. This method analyzes a digital image in the bit-plane domain. Block of bits are encoded, using the ASCII code, into strings of characters, in order to find identical sequences in each bit plane. Detected candidate areas in a plane are processed in the following planes. Output of the last processed plane indicates tampered areas. This Method proves to reach very high accuracy without spending much execution time. Babak et. al.[12] proposed a method to detect to detect copy–move forgery in an image with the high ability even with the presence of blur, noise or contrast changes in the copied areas. The method even works well with lossy JPEG format data. L. Juan et. al.[13] evaluated two feature detection methods for image registration. SIFT has detected more number of features compared to SURF but it is suffered with speed. The performance of SURF is good and fast as the same as SIFT. Preeti Yadav et. all[14] introduced an improved algorithm by proposed an algorithm based on Discrete Wavelet Transform (DWT) for detecting copy move forgery. Reduce the dimension of the features. Best performance for detection of small size copy-move forgery and can also detect multiple copy-move forgery. Lower computational complexity. M. Buvana Ranjani et. al.[15] Introduces a row reduction and a column reduction algorithm with the support of DCT. This paper identified the affective part of the original image by converting the tampered image and the original one as a matrix. The computational Complexity is also improved.

III. COPY-MOVE FORGERY

Copy-move forgery is that process in which one region of the image is copied and pasted to another location within the same image. By copy-move attack, an object is disappear from the image because that object is covered with a segment that is copied from another region of the image. The copied

Figure 2: Forged Image

Original Image

areas can be textured areas like gravel, grass, leaves, or fabric because it will likely mix with the background and the human eye cannot easily discern any suspicious artifacts. The copied regions picked from the same image because the most important properties of the image such as color palette, range would be appropriate with the rest of the image[5]. Some algorithms for detection of copy move are:

A. Exhaustive search

This is the simplest (in principle) and most obvious approach. In this method, the image and its circularly shifted version are overlaid looking for closely matching image segments[5]. Here, the image is first divided into uniform blocks of fixed size (say B pixels), so that the blocks serve as the units of forgery detection. Initially, each pixel of both the circularly shifted image and the original image, are matched with one another and if their absolute difference is greater than or equal to a predefined threshold *t*, the entire block of size B pixels (containing the test pixel) is checked for duplication[16].

Figure 3: Test image "Lenna" and its circular shift.

B. Autocorrelation

Autocorrelation of a signal is defined as the degree of similarity between the signal and a lagged version of itself. Over successive time intervals[16]. The autocorrelation of image A of size M×N is defined as:

$$r_{k,l} = \sum_{k=0}^{M-1} \sum_{0}^{N-1} x_{i,j} x_{i+k,j+l}, 0 \leq i < M, 0 \leq j < N, \forall i,j \quad (1)$$

The original and the duplicated segments will introduce peaks in the autocorrelation for the shifts that corresponds to the copy-moved segments. If the autocorrelation is a spike, it says that the image has no elements that are correlated, that is every element is unique. Lobes, away from (0,0), suggest repetition. The distance away from (0,0) is the periodicity of the repetition[17].

C. Exact Block Matching

In exact block matching based copy-move forgery detection algorithm, the test image is divided into overlapping square blocks of size b×b pixels (say). The square block is slid by one pixel at a time, from left to right and top to bottom. For each block position, the pixel values of the block are extracted in column wise order into a row of a 2-D matrix A with b2 columns and (Mb+ 1)×(N-b+1) rows, where M×N is the size of the image in pixels[17].

D. Robust match

The idea for the robust match detection is similar to the exact match except we do not order and match the pixel representation of the blocks but their robust representation that consists of quantized DCT coefficients. The quantization steps are calculated from a user-specified parameter *Q*. This parameter is equivalent to the quality factor in JPEG compression, i.e., the Q factor determines the quantization steps for DCT transform coefficients. Because higher values of the Q-factor lead to finer quantization, the blocks must match more closely in order to be identified as similar. Lower values of the Q-factor produce more matching blocks, possibly some false matches.

TABLE1 COMPARISION TABLE

Author	Year of Publication	Title	Description
1. B.L. Shiva Kumar [18]	2010	Detecting copy move forgery in digital images: A survey and analysis of current methods	(a) Manipulated images with noise, manipulated images with compression, and manipulated images with rotation are discussed in this paper. (b) Region duplication detection without scaling and rotation and region duplication detection with scaling and rotation are also discussed.
2. Davide Cozzolino et. all[19]	2015	Efficient Dense-field copy-move forgery detection	(a) propose an algorithm towards fast and accurate copy-move detection. (b) To compute efficiently a high-quality approximate nearest neighbor field for the whole image, patchmatch algorithm is used. (c) the overall complexity by implementing also a fast post-processing procedure based on dense linear fitting is reduced. (d) a good robustness to various type of geometrical distortions is achieved.
3. Bayram et. al [20]	2009	An Efficient and Robust Method for	(a) proposed to employ Fourier-Mellin Transform (FMT) and Counting Bloom

		Detecting Copy-Move Forgery	Filters(CBF) to describe and sort image blocks, respectively. (b) In spite of increasing efficiency, the use of CBF decreases the effectiveness of the method, since CBF deals only with very similar blocks. (c) The method was able to identify clonings under JPEG compression (quality factors greater than 70%), resizing (up to 5%) and rotation (up to 10).
4. Mohammad Farukh Hashmi et. all[21]	2014	Copy move image forgery detection using efficient and robust method combining Un-decimated Wavelet Transform and Scale invariant Feature Transform.	(a) This paper introduces a hybrid method. Dyadic Wavelet Transform (DyWT) and Scale Invariant Transform (SIFT) are combined for copy move forgery detection. (b) There is no down sampling is done in DyWT. Efficiency is much higher.
5. Prema.C et. all.[22]	2013	A keypoint based copy-move forgery detection.	(a) This paper proposed K-D (K-Dimensional) Tree algorithm. (b) This Tree obtains the matching patterns and it is much faster as compared to other algorithms. (c) It consists of various transformations from which the duplicated region can be identified by estimating the transform between matched SIFT Keypoints. (d) This algorithm finds the forged region more effectively.
6. Chen-Ming Hsu et. all[23]	2015	An efficient detection algorithm for copy-move forgery	(a)Proposed a method to detect forged regions based on the histogram of the Gabor magnitude. (b) Also a robust method against compression, rotation, blurring etc.
7. Tarman Garg et. al.[24]	2017	A Review on Various Techniques of Image Forgery Detection	(a) concluded that every method has its own strengths and limitations. (b) some are effective for blurred, noise, or cropped regions and some are good for the rotated and scaled parts of the image. (c). less computational complexity is provided by some methods while some are complex but effective.
8. Mona F. et. al[25]	2017	An Improved SIFT-PCA-Based Copy-Move Image Forgery Detection Method	(a) introduced SIFT+PCA along with DBSCAN Clustering. (b) detection accuracy is higher of SIFT with PCA that DWT with SIFT alone or together with PCA. (c) Very good performance (97%).

IV. CONCLUSION

This paper reviews various copy-move forgery detection techniques. A number of image forgery detection techniques have been proposed such as Exhaustive Search, Autocorrelation, Exact Match, and robust Match. Exhaustive search technique is one of the most primitive techniques of copy-move forgery detection, where the copied-moved regions are tried to be detected by circular shifting and overlaying the image with itself. The logic behind the detection based on autocorrelation is that the original and copied segments will introduce peaks in the autocorrelation for the shifts that correspond to the copied-moved segments. The exact match algorithm identifies those segments in the image that match exactly. Even though the applicability of this tool is limited, it may still be useful for forensic analysis. The idea for the robust match detection is similar to the exact match except we do not order and match the pixel representation of the blocks but their robust representation that consists of quantized DCT coefficients. The proposed Paper would help the users select an appropriate forgery detection algorithm.

REFERENCES

[1] V. Schetinger, M. Iuliani, A. Piva, and M. M. Oliveira, "Digital Image Forensics vs. Image Composition: An Indirect Arms Race," pp. 1–13, 2016.

[2] J. C. Lee, C. P. Chang, and W. K. Chen, "Detection of copy-move image forgery using histogram of orientated gradients," Inf. Sci. (Ny)., vol. 321, pp. 250–262, 2015.

[3] C. C. Chen, H. Wang, and C. S. Lin, "An efficiency enhanced cluster expanding block algorithm for copy-move forgery detection," Multimed. Tools Appl., pp. 1–20, 2016.

[4] E. Ardizzone, A. Bruno, and G. Mazzola, "Copy-Move Forgery Detection by Matching Triangles of Keypoints," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 10, pp. 2084–2094, 2015.

[5] J. Fridrich, D. Soukal, and J. Lukáš, "Detection of Copy-Move Forgery in Digital Images," Int. J., vol. 3, no. 2, pp. 652–663, 2003.

[6] Y. Cao, T. Gao, L. Fan, and Q. Yang, "A robust detection algorithm for copy-move forgery in digital images," Forensic Sci. Int., vol. 214, no. 1–3, pp. 33–43, 2012.

[7] R. Davarzani, K. Yaghmaie, S. Mozaffari, and M. Tapak, "Copy-move forgery detection using multiresolution local binary patterns," Forensic Sci. Int., vol. 231, no. 1–3, pp. 61–72, 2013.

[8] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Secur., vol. 6, no. 3 PART 2, pp. 1099–1110, 2011.

[9] Chi-Man Pun, Xiao-Chen Yuan, and Xiu-Li Bi, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 8, pp. 1705–1716, 2015.

[10] G. Lynch, F. Y. Shih, and H. Y. M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection," Inf. Sci. (Ny)., vol. 239, pp. 253–265, 2013.

[11] E. Ardizzone and G. Mazzola, "Detection of duplicated regions in tampered digital images by bit-plane analysis," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5716 LNCS, pp. 893–901, 2009.

[12] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," Forensic Sci. Int., vol. 171, no. 2–3, pp. 180–189, 2007.

[13] L. Juan and O. Gwun, "A comparison of sift, pca-sift and surf," Int. J. Image Process., vol. 3, no. 4, pp. 143–152, 2009.

[14] P. Yadav and Y. Rathore, "Detection of Copy-Move Forgery of Images Using Discrete Wavelet Transform," Int. J. Comput. Sci. Eng., vol. 4, no. 4, pp. 565–570, 2012.

[15] M. B. Ranjani, "Image Duplication Copy Move Forgery Detection Using Discrete Cosine Transforms Method Matrix Sorting – Row Wise Matrix Sorting – Colum Wise," vol. 11, no. 4, pp. 2671–2674, 2016.

[16] J. Wadhwa, T. Ahemad, R. Naskar, and R. Dixit, "On parameterization of block based copy-move forgery detection techniques," Proc. 2015 Conf. Res. Adapt. Converg. Syst. - RACS, pp. 125–130, 2015.

[17] W. Jing and Z. Hongbin, "Exposing Digital Forgeries by Detecting Traces of Image Splicing," vol. 2, no. 2, pp. 758–767, 2006.

[18] B. L. Shivakumar and S. S. Baboo, "Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods," Glob. J. Comput. Sci. Technol., vol. 10, no. 7, pp. 61–65, 2011.

[19] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient Dense-Field Copy-Move Forgery Detection," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 11, pp. 2284–2297, 2015.

[20] H. T. S. and N. M. Bayram, Sevinc, "an Efficient and Robust Method for Detecting Copy-Move Forgery," Image (Rochester, N.Y.), pp. 1053–1056, 2009.

[21] M. F. Hashmi, V. Anand, and A. G. Keskar, "Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform," AASRI Procedia, vol. 9, no. December, pp. 84–91, 2014.

[22] C. Prema and P. G. J, "A Keypoint Based Copy-Move Forgery Detection," Int. J. Adv. Inf. Sci. Technol., vol. 12, no. 12, pp. 175–180, 2013.

[23] C. M. Hsu, J. C. Lee, and W. K. Chen, "An efficient detection algorithm for copy-move forgery," Proc. - 2015 10th Asia Jt. Conf. Inf. Secur. AsiaJCIS 2015, pp. 33–36, 2015.

[24] T. Garg and H. Saini, "A Review on Various Techniques of Image Forgery Detection," vol. 4, no. 4, pp. 490–493, 2017.

[25] M. F. M. Mursi, M. M. Salama, and M. H. Habeb, "An Improved SIFT-PCA-Based Copy-Move Image Forgery Detection Method," vol. 6, no. 3, pp. 23–28, 2017.