Techniques of Copy Move Forgery Image Detection - Review

Ms. M. H. Kore[1] Dr. R. J. Shelke[2]
[1]PG Student [2]Assistant Professor
[1,2]Department of Electronics Engineering
[1,2]Walchand Institute of Technology, Solapur, India

Abstract— Copy Move forgery is common type of image forgery. A part of image is replaced (copied and pasted in the same image) with another part from the same image. The purpose behind this kind of forgery is may be to create duplication or to hide some particular detail of the image. Using some image editing tools someone can easily tamper the image. This results into loss of image authenticity or image integrity. This paper discusses on different methods used for detection of image forgery. A considerable number of different algorithms have been proposed focusing on different types of post processed copies. Here the aim is to discuss on different copy-move forgery detection algorithms.

Key words: Image Detection, Copy Move Forgery

I. Introduction

Since the invention of photography, images have been retouched and manipulated. Image data was manipulated in papers, fashion magazines, court room etc. Detection of image forgery is a challenging task due to various methods of tampering the image and a large number of distinct image capturing devices available. Most of the forgery detection techniques are categorized into two major categories: active and passive. Active methods, also known as non-blind/intrusive methods, require some information to be embedded in the original image. Due to this pre-requisite, active methods have limited scope. Some of the examples of these methods are watermarking and use of digital signature of the camera. Passive methods, also known as non-intrusive/blind methods, don't require any information to be embedded in the digital image. A digital image can be forged by applying various transformations like that of rotation, scaling, resizing, addition of noise, blurring, compression etc [4]. Copy-move attack is the common form of image tampering amoug the various types of image forgeries. A copy-move forgered image will contain some part of the image copied and pasted to another portion of the same image. This may be done by a forger to hide some object or truth or to enhance the visual effect of the image. With the use of any available image editing software like Adobe Photoshop a forger can easily tamper the image and can hide the tamper trace. This can cause loss of image integrity or authenticity. Mostly forger hides the tampering trace by making some geometric transformations such as rotation, scaling etc. in the image or by making some illumination adjustments. Some may hide the tampering by noise addition, lossy compression or blurring the image. These operations are done to make copy-move forgery detection harder. So there is a need for an effective copy-move forgery detection (CMFD) method.

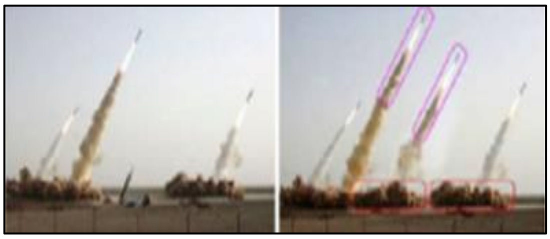
Fig. 1: (a) Original image (b) Forgery image.

II. Literature review

In the last few years researchers are putting their efforts in image forgery detection. The main methods to detect forgery are categorised in two types.

1) Block based: In this approach the image is divided into various blocks. These block division is done on the basis of Discrete Wavelet Transform, Discrete Cosine Transform, Zernike moment, and Fourier Mellin Transform.
2) Keypoint based: In this approach, all kind of geometric transformed manipulated images can be detected. Two of the techniques is to use SIFT (Speed Invariant Feature Transform) and SURF (Speed up Robust Feature).

Jessica Fridrich, David Soukal, Jan Lukas [5] used block based approach by using the Exhuastive search and the autocorrelation for copy move forgery detection. Exhaust search method is that first the input image is eroded followed by dilation. This approach is very much effective but computational cost is very high. Whereas in autocorrelation a strong mathematical support is used with the Fourier transform. Both the original and the tampered images will introduce some peaks. By checking these peaks, it is possible to and the cloned areas. A high pass filter is used along with this autocorrelation. Any kind of detection system should be tested using the image in both image level and pixel level. From image level, it is possible to conclude that whether the chosen algorithm can or can't detect the cloned regions. And with the pixel level testing the level of accuracy of the tampered regions is identified.

W. Luo, J. Huang, and G. Qiu [7] suggested an algorithm for detection of copy move forget that first divides the image into overlapping blocks and then it compares each block to find similarities among them so as to identify copy move forgery. It is based on DCT (Discrete Cosine Transform), which is used for describing blocks. In this DCT method, matching blocks of the forgered image can be find out by comparing the coefficients of individual patches. If two patches have same coefficient then there exists possibility of copy move image forgery. This method uses dictionary sort which is used for decreasing the complexities involved for finding the similarities among the matching block.

Mohammad Farukh Hashmi etal[4] developed an algorithm of image-tamper detection based on the Discrete

Wavelet Transform i.e. DWT. DWT is used for dimension reduction, which in turn increases the accuracy of results. First DWT is applied on a given image to decompose it into four parts LL, LH, HL, and HH. Since LL part contains most of the information, SIFT is applied on LL part only to extract the key features and find descriptor vector of these key features and then find similarities between various descriptor vectors to conclude that the given image is forged. This method allows us to detect whether image forgery has occurred or not and also localizes the forgery i.e. it tells us visually where the copy-move forgery has occurred.The result parameter is Accuracy. The database used is MICC F220.

Reshma Raj, Niya Joseph [1] proposed a new approach which can efficiently identify the copy move forged areas. For achieving the copied image area they first segment the image that is the test image is segmented into different independent patches. These patches are evaluated based on their matching and then the copied images are identified. For patch matching a two level of matching is carried out. In the first stage, suspicious pairs of matches is obtained and affine transform matrix is roughly estimated. In-order to confirm the existence of copy move forgery a second level of patch matching with respect to Expectation Maximization algorithm is used. In this way the copy move forged areas are identified. The database used is MICC F600. The result parameter are Recall and precision.

Jian Li, Xiaolong Li, Bin Yang [2] proposed a scheme to detect the copy-move forgery in an image, mainly by extracting the key-points for comparison. The main difference to the traditional methods is that the proposed scheme first segments the test image into semantically independent patches prior to key-point extraction. As a result, the copy-move regions can be detected by matching between these patches. The matching process consists of two stages. In the first stage, they find the suspicious pairs of patches that may contain copy-move forgery regions, and they roughly estimate an affine transform matrix. In the second stage, an EM-based algorithm is designed to refine the estimated matrix and to confirm the existence of copy-move forgery. Experimental results prove the good performance of the proposed scheme via comparing it with the state-of-the-art schemes on the public database. The database used are MICC F600. The detection error is measured using Recall and Precision.

From the above discussion, it can be compared that, the keypoint extraction based approach is better than the block based one. For feature extraction keypoint approach is best suited because of their low computational time and good performance. This approach also has advantage that is very sensitive to low contrast regions and repetitive image content [1]. This motivate the researchers to use keypoint approach for the detection of copy move forgery. The methodology is designed to develop algorithm using keypoint approach.

III. METHODOLOGY

Suggested method for detection of copy move forgery image is based on keypoint extraction approach. It uses SURF (Speeded UP Robust Feature) algorithm for Feature extraction. Figure 2 shows overview of the method our proposed that we are proposing for copy move forgery detection. It shows sequence of steps that should be followed for the CMF detection. The method involves main four steps.

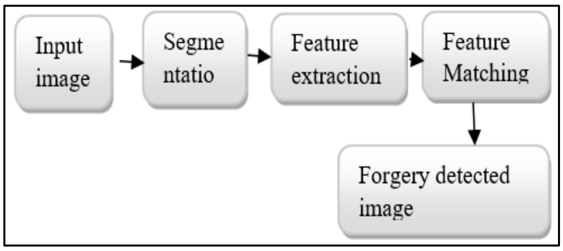

Fig. 2: Overview of CMFD

A. Input Images

The forgerd images to be used for copy move image forgery detection are easily available on the internet.

B. Pre-Processing

The input images available are mostly colour images therefor are converted into grayscale images for further processing.

C. Segmentation

The main aim of the segmentation is to extract useful information from the image. Many researchers have implemented different segmentation methods. In this the appropriate method of segmentation is to be used.

D. Feature Extraction

SURF (Speed up Robust Feature) is used as the technique for keypoint extraction. SURF is a robust local feature descriptor that extracts the features of the image. Surf is used to detect blob features. It is robust and scale invariant feature.

E. Feature Matching

After the feature extraction using surf, these features are matched to find duplication by using nearest neighbour method. If the distance is below a particular threshold, such pairs can be removed, otherwise copy-move forgery can be detected.

The Precision and Recall are the parameters used for the analysis.

IV. CONCLUSION

Copy move forgery images detection by various techniques with two approaches, block based and keypoint based. Methodology discuss using keypoint approach as it is very sensitive to low contrast. SURF algorithm is used for feature extraction and matching. The Precision and Recall are the parameters to be used for the analysis.

ACKNOWLEDGMENT

We express our deepest gratitude towards our Head of Department Dr S.R.Gengaje and PG Coordinator Professor A.S.Gundale for providing us technical suggestions.

REFERENCES

[1] Reshma Raj, Niya Joseph, “Key point extraction using SURF algorithm for CMFD” Science Direct Procedia Computer science93, 6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India

[2] Jian Li, Xiaolong Li, Bin Yang, and Xingming Sun, “Segmentation-Based Image Copy Move Forgery Detection Scheme”,IEEE Trans.Inf. Forensics Security, Vol. 10, No. 3, March 2015

[3] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, “An evaluation of popular copy-move forgery detection approaches,” IEEE Trans. Inf. Forensics Security vol 7, DEC 2012

[4] A. J. Fridrich, B. D. Soukal, and A. J. Lukas, “Detection of copy-move forgery in digital images”,in Proc. Digit. Forensic Res. Work-shop,20034)

[5] Mohammad Farukh Hashmi, Aaditya R. Hambarde, Avinash G. Keskar, “Copy Move Forgery Detection using DWT and SIFT Features”.

[6] Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra,“A SIFT-based forensic method for copymove attack detection and transformation recovery”,IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 10991110, Sep. 2011.

[7] W. Luo, J. Huang, and G. Qiu, “Robust detection of region-duplication forgery in digital image” in Proc 18th Int. Conf. Pattern Recognition (ICPR), vol. 4, 2006.

[8] S.-J. Ryu, M. Kirchner, M.-J. Lee, and H.-K. Lee, “Rotation invariant localization of duplicated image regions based on Zernike mo-ments”, IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 13551370, Aug. 2013.

[9] Bhavya Bhanu M P, Dr. Arun Kumar M. N., “Copy Move Forgery Detection Using Segmentation.” 11th International Conference on Intelligent Systems and Control (ISCO) 2017.

[10] P. Kakar and N. Sudha,“Exposing postprocessed copypaste forgeries through transform-invariant features”,IEEE Trans. Inf. Forensics Security,vol. 7, no. 3, pp. 10181028, Jun. 2012

[11] D. G. Lowe, “Distinctive image features from scale-invariant keypoints” Int. J. Comput. Vis.,vol. 60, no. 2, pp. 91110, Nov. 2004

[12] S. Bayram, H. T. Sencar, and N. Memon,“An efficient and robust method for detecting copy-move forgery”,in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Washington, DC, USA, Apr. 2009, pp. 10531056.

[13] Sudhakar. K, Sandeep V.M, Subhash Kulkarni,“Speeding-up SIFT based Copy Move Forgery Detection Using Level Set Approach”,2014 International Conference on Advances in Electronics, Computers and Communications.

[14] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei,“Image copy-move forgery detection based on SURF”,in Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES), Nov. 2010.

[15] Ramesh Chand Pandey, Sanjay Kumar Singh, K. K. Shukla and Rishabh Agrawal,“Fast and Robust Passive Copy-Move Forgery Detection Using SURF and SIFT Image Features”.