Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

A Survey Paper on Copy-Move Forgery Detection in Digital Images

Navpreet Kaur Gill
Assistant Professor
Deptt. Of CSE, Khalsa College
Mahilpur, India

***Abstract*— With the rapid growth of digital photography over the past few years, digital image forgery with the help of image editing tools to alter the original image has become an easy practice. Images can be used as an authenticated proof for any crime, hindering the genuineness of the image has become a serious problem at present. Techniques based on the Active methods are a limit to the scope of authentication to only those images captured from specific cameras. Passive Techniques for image forensics work on the principle that there may be no visual clue in the forged image but altering the image will definitely change the statistics of the image. The aim of such techniques is to authenticate the image without any knowledge of the prior information.**

Keywords*—- *Image Forensics, Copy-move forgery detectioncomponent, Block Based Techniques, Keypoint Based Techniques

I. INTRODUCTION

In the present era, digital multimedia content has turned out to be effortlessly accessible and available to general public. Excellent portable cameras and other handy gadgets permit anybody to capture the images of high quality. Web permits clients to process any type of digital media within seconds all over the globe. These conditions allow administrative, legal and news media associations to depend on digital interactive multimedia content [4].

Among prior procedures, the advanced watermarking method has been a method which provides good security. But the limitation of the technique is the requirement of an explicit watermark or computerized signature must be embedded into the original image by a trusted source before any tampering happens. This is essentially not achievable in present situations, in light of the fact that the person who takes the digital images can modify it before embedding the watermark. Moreover, encryption techniques cannot help in this kind of forgeries because they can deny the accessibility of an unauthorized person but they cannot prohibit the owner of the digital content from manipulation before encryption.

With expanding utilization of digital multimedia content like pictures and video, the techniques for detecting the digital image forgery has also increased parellely. In the blink of an eye, many advanced image manipulation software has been launched in the market which grants the forgers to manipulate the image in any desirable way that is visually not perceivable. There is a requirement for methods equipped for confirming multimedia media content in the fields where legitimate issues are vital. In light of such requests, scientists and legal examiners have begun creating advanced scientific strategies that are equipped for distinguishing digital image forgeries by analyzing statistics and quality of images. These image forgery detection strategies work by identifying left out clues embedded by altering operations in digital multimedia content[5].

Fig. 1: Example of Copy-Move Forgery

II COPY-COVER FORGERY DETECTION METHODS

Copy-cover forgery became the most important issue in the image forgery. Copy-cover forgery is the most important issue in the image forgery. As depicted in Fig. 2 copy-cover forgery detection is primarily categorized into following classes:

1.1 Brute force Methods

Brute force method is based on exhaustive search and auto correlation technique. In exhaustive search, image is used to examine matching segment with circularly shifted versions. As it makes such large number of comparisons, its computational unpredictability is high. Autocorrelation determine location change.

2.2 Block Based Techniques

Block based techniques came into existence because of different downsides of exhaustive search. These techniques work by dividing the image into small blocks and after that features are calculated and listed in a feature matrix. Comparison has been made to detect similar blocks. These techniques are robust against blurring, Noise addition and JPEG compression but cannot deal with geometric transformations. Block based approach use the algorithms such as Discrete Wavelet Transform (DWT), Principle Component Analysis [2] (PCA), Singular Value Decomposition (SVD) [3] and Discrete Cosine Transform[4] (DCT).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

2.3 Key-Point Based Techniques

Keypoint based techniques overcome the shortcomings of block based techniques. These techniques show robustness in case of scale invariants and scan the whole image at once to extract the keypoints. After that sort the keypoints lexicographically to find the similar features. Key-point based approach use the algorithms such as SIFT and SURF [5].

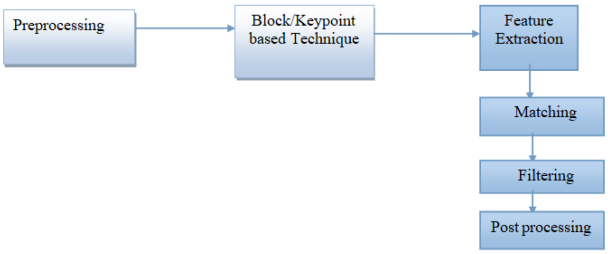

Fig. 2: Generalized Schema for Forgery Detection

III RELATED WORK

H.Farid et al. [1] discussed a framework for image forgery detection. Major focus of this paper is Passive image forgery detection techniques along with the disadvantages of Active techniques like digital watermarking in which pre-embedded information is required. Different image forgery detection techniques are examined which are:-

1) Pixel-based strategies
2) Format-based strategies
3) Camera-based strategies
4) Physically based systems
5) Geometric-based systems.

H.Farid et al. [2] introduced another methodology that could recognize local tampering dissimilar to other methodologies which might just identify crop and recompression; this methodology could identify altering performed on low-quality images and doesnot need discrete cosine transform(DCT) quantization from an original image(as estimating those quantization starting with just the underlying DCT coefficients may be computationally not simpler and generally subject to bear with percentage estimation error) and that is computationally simpler [-and doesnot require an extensive database about images to train a support vector machine(SVM). This methodology meets expectations by assuming that original image might have been initially compressed at different value than tampered image-this methodology is called JPEG Ghost. This methodology works well with image splicing and there is no need to crop the image to identify blocking inconsistencies.

F.Zach et al. [3] introduced a technique for computerizing the recognition of the JPEG ghosts. However the proposed automation needs vast image dataset training of classifier.

M.Kaur et al. [4] introduces image tampering detection techniques based on JPEG artifacts. Tampering detection is performed in low-quality images when a part of a JPEG image is spliced on the other image which is of higher quality .This technique doesnot require an estimation of the DCT quantization of the original image and there is no need of support vector machine(SVM).

Schaefer et al. [5] introduced UCID after analyzing various parameters of images like color moments and color coherence vectors etc. UCID dataset is the dataset in which images are saved in their uncompressed state. Hence it is a benchmark database for the evaluation of compressed domain image retrieval techniques and this dataset can also be used for the testing and comparison of image compression techniques.

T. Bianchi et al. [6] proposed a novel strategy in which NA-JPEG layering is distinguished by preparation of classifier based on compression characteristics. In this approach, firstly DCT coefficients are find with the help of image characteristics. After that threshold detector is applied which is capable of estimating the quantization level and from that quantization level, forged image will get detected if it is double compressed. Subsequently it has capability to detect forged image at pixel level.

T. Bianchi et al. [7] introduced double JPEG compressions which can be aligned (A-DJPG) or nonaligned (NADJPG). Without necessity of manually selecting the suspected region, the approach utilizes Factual model characterizing the artifacts that will possibly appear as A-DJPG or NA-DJPG. Although this is a good technique for image forgery detection but determining the correct location of the forgery is still the hot research area.

T. Bianchi et al. [8] presented an algorithm which will separate forged area from original area in JPEG images. It works under the principle that the non-aligned JPEG compression will result in case of the tampering in the JPEG images. This is a pure automated technique ad there is no need to manually select the forged areas. From above literature we have derived that there is no proper technique that can locate the exact location of the forgery. The authors are claiming that this method is even successful for the localization of the forged area. There is no need of prior information to detect the exact location of the forgery. The proposed algorithm works on the concept of probability and the output of this algorithm is the probability for each 8*8 block to be tampered.

F.Zhao et al. [9] recommended a novel approach that utilizes the moment characteristics of the mode based DCT histogram's function and support vector machine(SVM) as the classifier. The moment features as well as well as Mode based Fist Digit Features (MBFDF) are combined together to increase the accuracy. The algorithm can detect the forged region with the accuracy of upto 95 percent.

J.Lukas et al. [10] exhibited a technique for estimation of essential quantization table from a double compressed JPEG image by recognizing forged highlights that came to notice in DCT histograms of individual coefficients because of double compression blocking.

J.Mian et al. [11] presented various different file formats that can be used for the image forgery detection.

F.Zach et al. [12] has introduced Copy-move forgery detection with the help of classification of JPEG ghosts. This technique is a fully automated technique in which image inconsistencies of different areas of image will be detected. Camera response function has been estimated for the test

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

image which is segmented further. To authenticate the image various features are computed.

L.Vrizlynn et al. [13] presented an improved double compression detection technique for image forgery detection in JPEG images.

R.M.Ashraf et al. [14] proposed a fast copy-move forgery detection method using patch based descriptors. The image is divided into the blocks and Speeded up Robust Features (SURF) algorithm has been applied to every block for extracting SURF feature points. The features of the different blocks are matched and the matching features are known as Labelled Feature Points (LFP).

H.Lin et al. [15] proposed a new method based on some descriptors and a SVM classifier is optimized on training set. Although this method gave the best results but detection of duplicated areas in small region is nearly impossible as they contribute very less to the descriptors.

S. Ryu et al. [16] conducted a study on copy-move forgery detection by using Zernike moments. This method works well for all type of geometric transformations like JPEG Compression, Gaussian noise, blurring and rotation up to 30 degrees.

Z. Wang et al. [17] proposed a method by using Hu moments for forgery detection. Dimension will be reduced in this method by using Gaussian pyramid and the image is divided into overlapping blocks. Apply Hu moments to each block and calculate eigenvalues. Sort these vectors using lexicographical sorting and false detections can be reduced by selecting an area threshold. Mathematical morphological techniques are used for matching purpose.This method works well even when the post-processing is performed on the image.

B. Mahdian et al. [18] utilize blur moment invariants to represent the forged image. Firstly tilt the image with blocks of a particular size and represent them with blur invariants.Then apply the PCT (Principal Component Transformation) to reduce the dimensions of each feature vector. K-d tree is used for matching purpose. Further, verify the similar blocks found by finding the neighborhood of similar blocks. This method works well in case of duplicated regions with changed contrast and blurring. The disadvantage of this algorithm is that it has high computational complexity.

B. Ustubioglu et al. [19] presented the method which decreases the false negative rate. Firstly image is divided into the non-overlapping blocks. After that obtain the LBP values for every block and apply the DCT on every block. This method decreases the computational cost and gives the more accurate results than the existing DCT method.

J. Zheng et al. [20] presented a new method based on ORB (Oriented FAST and Rotated BRIEF) on the basis of visual descriptor BRIEF (Binary Robust Independent Elementary Features) and FAST (Features from Accelerated Segment Test) key-point detector. This method is the alternative for other keypoint based techniques like SIFT and SURF for the detection of duplicated regions. The advantage of this method is that its matching time is less than the other keypoint based techniques. Less storage space is required by this method and it can also handle all type of geometric transformations like scaling and rotation etc.

C. Haipeng et al. [21] proposed a method based on scale space and ORB (Oriented FAST and rotated BRIEF). Detection of forgery in high-resolution images is very time-consuming with this method. But the main advantage of this method is that it lowers the false matches and can handle the different geometric transformations.

D. Lin et al. [22] proposed a technique which combines the features of Discrete cosine transform (DCT) with Speeded Up Robust Features (SURF).This method will tell the exact position of the forgery and works well with the JPEG format. It can also detect forgery at multiple positions. This method does not work well in case of flat regions

G. Zhang et al. [23] proposed a technique which combines the features of Fourier Mellin Transform (FMT) with Speeded Up Robust Features (SURF). The block-based technique is used to determine the forgery in case of flat regions while the keypoint based technique is used for forgery detection in non-flat regions.

P. Mishra et al. [24] proposed a technique based on speeded up robust features (SURF) and hierarchical agglomerative clustering (HAC). A keypoint based method named SURF is used for determining Keypoints from the image. Based on detected keypoints, forgery decision is taken. Hierarchical agglomerative clustering is used to remove the false positives.

M. F. Hashmi et al. [25] proposed different algorithms on the basis of Speeded-Up Robust Feature (SURF) for the detection of forged regions. Firstly it combines the Discrete Wavelet Transform (DWT) and SURF and then combines Dyadic Wavelet Transform (DyWT) and SURF. After that results are compared with SURF in terms of precision and computational complexity. Shift invariance of DyWT is robust for forgery detection.

E. Ardizzone et al. [26] proposed a technique in which features are extracted using SIFT and further matching operation is performed on the clusters of keypoints as this will increase the accuracy and also decreases the false matching rates.

I. Amerini et al. [27] proposed the improvement on Sift Algorithm for better accuracy. This method works well for both image splicing and copy-move forgery detection.Multiple cloning can be handled with the help of this method. This method works well in case of non-flat regions but fails in case of flat regions.

B. Su et al. [28] proposed a method based on LPP (Locality Preserving Projection) with the combination of SIFT features. Dimension reduction property of the locality preserving projection method will reduce the computational complexity and also capable of dealing with the geometric transformations like scaling, rotation, and JPEG compression etc.

M. Jaberi et al. [29] proposed a method based on key-point feature extraction technique named Mirror Invariant Feature Transform (MIFT) to detect the forged regions in the image. MIFT has all the properties of SIFT features with robustness against mirror reflection transformations. With the help of new method, False Positive Rate (FPR) and False Negative Rate (FNR) can be reduced.

K. Li et al. [30] proposed a technique by combining the features of PCA, SIFT and k-nearest neighbor for detection of

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

copy-move forgery. Accuracy can be increased and computational complexity can be reduced over existing SIFT techniques. It can handle geometric transformations in the forged region. The existing method can be improved so that it can localize the forged region more precisely.

J. Li et al. [31] proposed a method based on SIFT features and Zernike moments to detect Forgery in both flat as well as non-flat areas. SIFT will detect the forgery in the whole image firstly. In case it is not capable to detect the forgery in some regions then Zernike moments will be applied in those areas to determine the forgery.

M. Hashmi et al. [32] proposed a method based on DWT with SIFT for detection of image forgery to take the advantage of both methods. Dimension reduction property of DWT is used to reduce the computational time and accuracy is increased with the help of SIFT. However, the existing method can be improved by replacing the DWT with the help of Dyadic Wavelet Transform (DyWT) to make use of the shift invariant.

V. Anand et al. [33] proposed a new technique by combining DyWT and SIFT for copy-move forgery detection. This method is more efficient than the other existing methods as True Positive Rate can be increased with the help of this method and robustness of this method can be seen in case of geometric transformations.

K. Sudhakar et al. [34] proposed a method by combining features of SIFT and Chan-Vese's level set approach for forgery detection. The speed of this method beats all other existing methods.

IV CONCLUSION

Digital image forgery is a growing field of research. Although limitations are there in the existing methods, still it promises the improvement in detection methods. Two major issues that are performance and robustness against malicious operations must be addressed to give the platform for a good research.

The major concern of this field is that the method should achieve better performance than existing methods in terms of true-positive rate and false alarms. The clear understanding of performance affecting factors is also necessary. Refinement in the existing methods can be performed by clearly designing the test-cases and with the use of benchmark datasets.

The other challenge is the robustness of existing methods to various malicious operations. Every method should be designed only after considering these possibilities. This can be achieved only after consulting with image forensic experts and after receiving feedback from them to implement the changes. Another future scope is that till date there is no unified algorithm for image forgery detection which can identify every type of forgery.

REFERENCES

[1] M. K. Johnson and H. Farid ,"Exposing Digital Forgeries by Detecting Duplicated Image Regions", *ACM Multimedia and Security Workshop*, New York, NY, 2005.

[2] H. Farid , " Exposing Digital Forgeries from JPEG Ghosts",*IEEE Transactions on Information Forensics and Security*, 154-160, 2009.

[3] F. Zach ,"Automated Image Forgery Detection through Classification of JPEG Ghosts " , *Springer Berlin Heidelberg*, 0302-9743, 2012.

[4] M. Kaur, "Image Tamper Detection based on JPEG Artifacts ", *International Journal of Application or Innovation in Engineering and Management*,2014.

[5] F. Schaefer, G. Stich , Michal,"UCID: an uncompressed colour image database", *Proceedings of the SPIE*, Volume 53,pp. 472480,2003.

[6] T. Bianchi, A. Piva, "Analysis of Non-Aligned Double JPEG Artifacts for the Localization of Image Forensics",*IEEE international workshop on WIFS,pp.1-6*,2011.

[7] T. Bianchi, A. Piva, "Detection of Non-Aligned double JPEG compression with estimation of Primary compression parameters ", *IEEE international conference on ICIP*, pp.1929-1932, 2011.

[8] T. Bianchi, A. Piva, "Image forgery Localization via Block- Grained Analysis of JPEG Artifacts", *IEEE Transaction on Information Forensics and Security*, Vol.7, No.3, pp.1003-1017,*2012*.

[9] F. Zhao, Z.Yu, S.H.Li, "Detecting Double compressed JPEG images by using moment features of mode based DCT", *IEEE international conference on multimedia technology(ICMT)*, pp.1-4, 2010.

[10] J.Lukas and J.Fridrich, "Estimation of primary quantization matrix in double Compressed JPEG images ", i*n Proceedings of Digital Forensic Research Workshop, Cleveland, OH*, Aug.2003.

[11] J. Mian, "Compressed Image File Formats: JPEG, PNG, GIF, XBM, BMP ",*1/e Addison Wesley Longman,Massachusetts*,1999.

[12] F. Zach, C. Rises, E. Angelopoulos,"Automated Image Forgery Detection through classification of JPEG ghosts", *Pattern recognition lab joint 34thh DAGM and 36th OAGM Symposium*,pp.185-194, Aug 2012.

[13] L. Vrizlynn, L. Thing, "An improved double compression detection method for JPEG image forensics", *IEEE International Symposium on Multimedia*, pp.290-297, 2012.

[14] R. M. Ashraf and V. K. Viswam," A Fast Copy-Move Forgery Detection Scheme Using Patch-Based Descriptors ", *International Journal of Advanced Research in Computer Science and Software Engineering*, pp. 255-260,2016.

[15] H .Lin, C .Wang and Y. Kao, "An efficient method for copy-move forgery detection", *International conference on applied computer and applied computational science*, pp.250-253,2009.

[16] S. Ryu, M. Lee, H. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in Proc.International Workshop Information Hiding, Springer , pp. 51–65, 2010.

[17] Z.Wang," A passive image authentication scheme for detecting region-duplication forgery with rotation",Journal of Network and Computer Applications, Vol. 34 , pp. 1557-1565, 2011.

[18] B.Mahdian , S. Saic," Detection of copy-move forgery using a method based on blur moment invariants", *Forensic Science International, an international journal dedicated to the applications of medicine and science in the administration of justice*, Vol.171 ,pp. 181-189,2007.

[19] B.Ustubioglu, G.Ulutas, M.Ulutas, V.Nabiyev, and A.Ustubioglu, "LBP-DCT Based Copy-Move Forgery Detection Algorithm," *Springer International Publishing Switzerland*, pp. 127-136, 2016.

[20] J. Zheng and L. Chang, "Detection of Region-duplication Forgery in Image Based on KeyPoints Binary Descriptors", *Journal of Information & Computational Science*, vol. 11, pp. 3959-3966, 2014.

[21] Z.Ye, S.Xuanjing and C.Haipeng, "Copy-Move Forgery Detection Based on Scaled ORB", *Proceedings of Multimedia Tools and Applications*, vol. 75, pp. 1-13, 2015.

[22] D. Lin and W.Tszan, "An Integrated Technique for Splicing and Copy-move Forgery Image Detection", *4thInternational Conference on Image and Signal Processing (CISP)*, pp. 1086 – 1090, 2011.

[23] G.Zhang and W. Hang, "SURF based Detection of Copy-Move Forgery in Flat Region", *International Journal of Advancements in Computing Technology (IJACT)*, vol. 4, 2012.

[24] P. Mishra, N. Mishra, S.Sharma, "Region Duplication Forgery Detection Technique Based on SURF and HAC", *The Scientific World Journal*, 2013.

[25] M.F.Hashmi, V.Anand, A.G. Keskar, "A Copy move Image Forgery Detection Based on Speeded-up Robust Feature Transform and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

Wavelet Transforms", *International Conference on Computer and Communication Technology (ICCCT),* pp. 147 – 152, 2014.

[26] E. Ardizzone, A. Bruno and G. Mazzola , "Detecting Multiple Copies in Tampered Image", *in Proceedings of IEEE 17th International Conference on Image Processing*, pp. 2117-2120, 2010.

[27] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, "A SIFT-based Forensic Method for Copy-Move Attack Detection and Transformation Recovery," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099-1110, 2011.

[28] B. Su and K. Zhu, "Detection of Copy Forgery in Digital Images Based on LPP-SIFT", *International Conference on Industrial Control and Electronics Engineering*, pp. 1773 – 1776, 2012

[29] M. Jaberi, B. George, H. Muhammad and M. Ghulam, "Improving the Detection and Localization of Duplicated Regions in Copy-Move Image Forgery", *18th International Conference on Digital Signal Processing (DSP),* pp. 1-6, 2013.

[30] K. Li, L. Hexin, Y. Bo, M. Qi and L. Shangdong, "Detection of Image Forgery Based on Improved PCA-SIFT", *in Proceedings of Computer Engineering and Networking*, vol. 277, pp 679-686, 2014.

[31] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme", IEEE Transactions on Information Forensics and Security, 10(3), 507–518, 2015.

[32] M. Hashmi, H. Aaditya, and K. Avinash, "Copy-Move Forgery Detection using DWT and SIFT Features", *International Conference on Intelligent Systems Design and Applications (ISDA),* pp. 188 – 193, 2013.

[33] V. Anand, H.Mohammad and K. Avinash, "A Copy-Move Forgery Detection to Overcome Sustained Attacks Using Dyadic Wavelet Transform and SIFT Methods", *in Proceedings of Intelligent Information and Database Systems, Springer*, vol. 8397, pp. 530–542, 2014.

[34] K. Sudhakar, V. M. Sandeep and S. Kulkarni, "Speeding-up SIFT-based Copy-Move Forgery Detection Using Level Set Approach*", International Conference on Advances in Electronics, Computers and Communications (ICAECC),* pp. 1-6, 2014.