Study and Analysis of Copy-Move & Splicing Image Forgery Detection Techniques

Mohanad Fadhil Jwaid
Department of Information Technology
Maharashtra Institute of Technology.Pune
Mohanad٠٢jwaid@gmail.com

Prof. Trupti N. Baraskar
Department of Information Technology
Maharashtra Institute of Technology.Pune
Trupti.baraskar@mitpune.edu.in

***Abstract*— With use of advanced image processing software's and tools, it becomes very easy to perform the tampering on original digital images with different intensions. Such kind of image tampering or manipulation is collectively called as image forgery. The main two types are ١) copy-move forgery and ٢) image splicing forgery of image forgery. Copy-move tampering is most generally used by attackers in which object of another image is copy and paste in original image in nearly matching areas. Hence to identify such image threats, it is required to automatic computer vision based method which can classify whether input digital image is original or tampered. The image processing based methods are mainly three important phases like as image pre-processing, image features extraction and detection of forged area on image using features extracted. For copy-move forgery detection there are many methods introduced from last ١٥ years. This all methods are categorized in two main types is active and passive forgery detection methods. This paper scope is limited to study on passive forgery detection methods. In this paper, aim is to present the study on different old methods of image forgery detection using different approaches like DWT (Discrete Wavelet Transform), SIFT, LBP (Local Binary Pattern) etc. The outcome of this paper is to find the current research challenges based on study of different methods of image forgery detection through the comparative study of all recent methods studied.**

***Keywords*— Image forgery, Tampering, Copy-Move Forgery, DWT, LBP, Detection Accuracy**

I. INTRODUCTION

In digital image processing, image forgery is nothing but the procedure of counterfeiting image visual content also tampering using the various different image analyses or editing tools. Hence image originality and authenticity becomes major threat in many real time applications like banking, news, legal processing documents, crime investigation, scientific processes etc. [١]. Therefore, such image forgery may have resulted into major security threat as any end user can tamer or modify the visual contents of original image without keeping any visibly known traces. There are different types of image forgery like as image splicing, copy-move etc.

Image cloning forgery which is called as copy-move forgery is only one most risk full method of image forgery, as user can able to change entire meaning of visual content of original image by copying some region from same or another image and pasted it on image part which is not required or to locate false information on original image by pasting it on original image part [٢]. Basically, images with regions like gravel, grass, foliage, fabric etc. are best suitable to perform copy-move forgery due to fact that copied regions are possibly blend with original image background and hence end users visually cannot able to maintain any suspicious artifacts by eyes.

Additionally, as copying is done from the same image, its color palette, noise factors, flexible range, and other image characteristics are become compatible with other regions of original digital image and hence not easily identifiable with help of techniques those are finding the incompatibilities during the statistical analysis over various image regions of image. Cropping or resizing is additionally used for make impact of forgery tough to locate. Figure ١ is point to the example of copy-move forgery [٣]. In figure ١, it is showing that the original authenticated image of three complete cars and copy move forgery image with four complete cars on road. Car is covered with the region of foliage region of original image.

Still this category of forgery by visually is possible to track as copied and original regions of foliage are having suspicious similarity. Another example in figure ٢ shows copy-move forgery which is difficult to track visually. This image is harder to track forgery part by third party, hence this kind of images we have to use with forgery detection methods. The visual contents of image are not revealing any suspicious presence in image [٤].

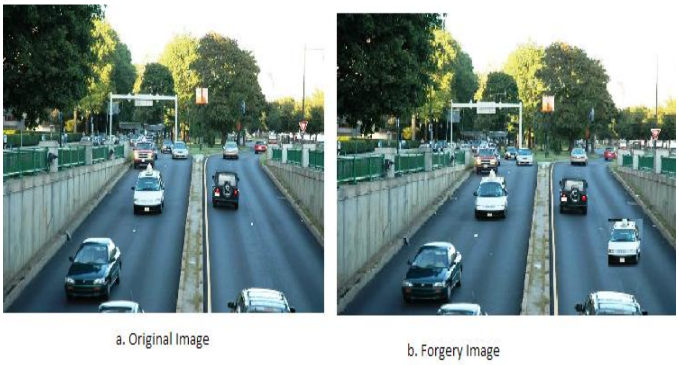
a. Original Image
b. Forgery Image

Figure ١: Example of Car Copy-Move Forgery

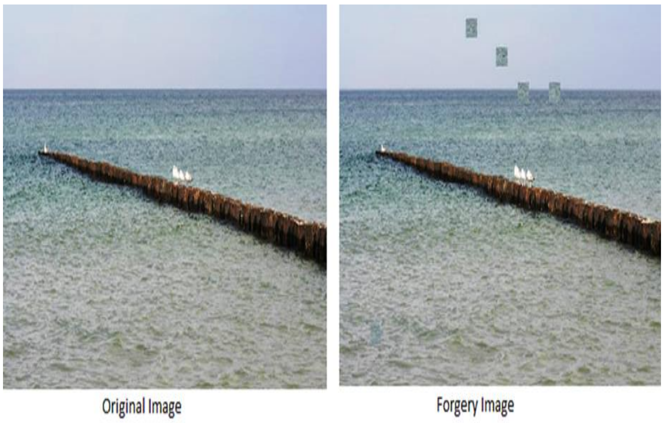

Figure ٢: Complex Example of Copy-Move Forgery

Similarly figure ٣ is showing the splicing forgery image example.

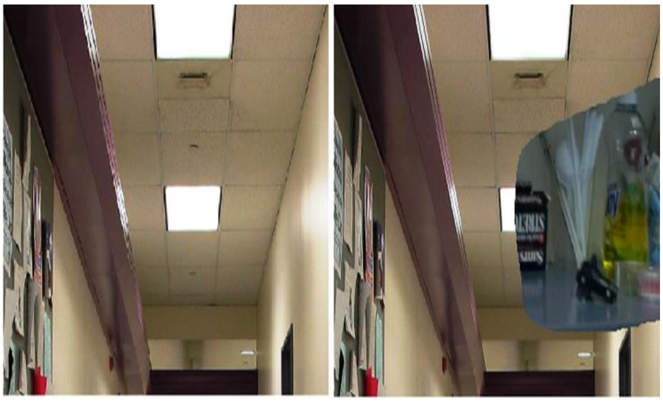

Figure ٣: Splicing Forgery Image Example (Original and Forged)

Number of automated techniques introduced so far by number of researchers for detect the image forgery. Basically copy-move forgery resulted into the correlation among original image region and forged image region. Such correlation factor is utilized for accurate identification of such category of forgery [٥] [٦]. The detected regions of forgery many not accurately located due to saving the image in lossy JPEG format also use of different resizing, retouch image processing tools. Therefore, below listed are basic requirements for copy-move forgery detection:

- Algorithm for forgery detection must do the approximate matching of small regions of image.
- Algorithm must work speedy with more accuracy and less errors.
- Forged region of image must be represented in form of connected component rather than small pixels.

With the consideration of above mentioned forgery detection requirements, recently different methods presented for accurate copy-move forgery detection. Basically for detection of copy-move forgery, searching of block by block similarities is done with value to spatial variation and internal noise pattern. Images are captured through different cameras hence different type of background noises introduced into image [٧] [٨]. The noise based forgery detection methods introduced in which forged region identification is done by finding region which is having lack of noise pattern. But the restriction of these methods is that number of images collected from the same camera is not fixed and varying. Another algorithm which is based on key point methodology introduced. This approach is depending on detection and selection of image parts with high entropy [٩].

But this may have resulted into problem while detecting forged part of image. Block by block features similarity is measured in methods based on spatial variation. In this methods, to separate the features of each block either DCT (discrete cosine transform) or pixel intensity variation methods used. In some cases, SIFT (Scale Invariant Feature Transformation) method is also used. Later DWT (discrete wavelet transforms) used in some methods, SVD (singular value decomposition) used in some methods for reducing the features dimension. Some recent methods presented with combination of using above methods such as DCT+DWT+SVD, DWT+SVD, DCT+SVD etc. However, there is still area of improvement in this domain with goal of achieving better detection accuracy within less time [١٠].

In this paper, first recent methods are discussed with their methodology used and benefits of using them, this method are based on two types of image forgery such as copy-move and splicing. The comparative study among the studied methods is done regarding advantages, disadvantages and techniques used. The accuracy analysis of these methods is done for find out the current research problems and research gap to overcome incoming future. In section II, recent forgery detection methods have been studied year wise. In section III, the comparative study among all literature survey methods is done in tabular and graphical forms. In section IV, the current research problems have been discussed. Finally, in section V, the conclusion and future work presented.

II. STUDY ON METHODS

In this section, various techniques of image forgery detection are consider and analyzed. Basically we present study on copy-move and splicing forgery detection techniques.

Fahime Hakimi et. al (٢٠١٥)

In [٥], author presenting novel technique for the image splicing forgery detection is based on three methods such as SVM (Support Vector Machine) classifier, LBP, and PCA (Principal Component Analysis). In this technique author first converted input RGB image into YCbCr color channel, and then chrominance component is formulated into the non-overlapping blocks. Secondly Local Binary Pattern (LBP) operator is performed, & the wavelet transform is utilized into the all blocks. Finally, Principal Component Analysis (PCA) is applying for all blocks & the results are fed to the Support Vector Machine (SVM) classifier as features. The practical evaluation of this method was done using two research datasets such as CASIA and Columbia. Below figure ٤ is showing the system architecture of this method.

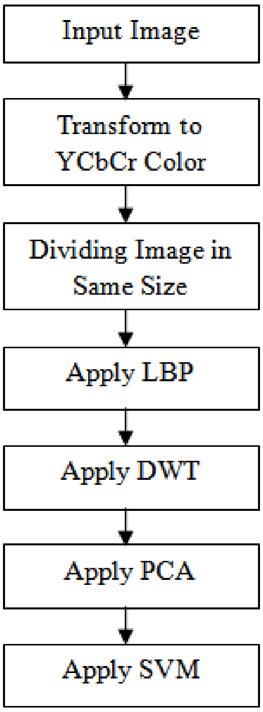

Figure ٤: Proposed Approach of Splicing Detection from [٥]

Diaa M. Uliyan et.al (٢٠١٥)

In [٦], author introduced approach to copy-move forgery detection using Hessian and Center Symmetric Local Binary Pattern (LBP) method. This method was named as Hessian features and a center-symmetric local binary pattern (CSLBP). This approach presented by author composed of four steps: (١) detecting the object based on normalized cut segmentation, (٢) localizing the local interest keys of every object construct on the Hessian method, (٣) extracting CSLBP features, and (٤) getting dummy regions into the image forgeries. At first author segmenting the input image construct on the color palette. Then forgery regions are selected based on the least frequently used method. Centroids and Hessian characteristics are separated for each segment. In experimental study of this approach was done using MICC-F٢٢٠ research dataset.

Amani Alahmadi et.al (٢٠١٦)

In [٧], author introduced a novel passive image forgery detection method is planned basis on Local Binary Pattern (LBP) and Discrete Cosine Transform (DCT) to detect copy-move & the splicing forgeries. Here first, from the chrominance element of the input image, discriminative localized features are separated by attempting the ٢D DCT into the LBP space. Then, support vector machine (SVM) is use for detection. This was learning basis on the passive technique that showing copy move & image splicing forgeries. This is most recent method which works on both category of image forgery detection. The experimental study and evaluation of this method was done using CASIA TIDE v١,٠ and Columbia research datasets.

Chi-Man Pun et. al (٢٠١٥)

In [٨], another technique for copy-move forgery detection recently introduce in this article by author. This was novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching introduced. This method integrated both block-based and keypoints-based forgery detection methods. First, Adaptive Over-Segmentation algorithm was proposed to segments the host image into non-overlapping & the certain blocks automatically. After that, the next points are separated from each block as block features, and the block functions which are matched with second to locate the labeled function points; this procedure can almost point the suspected forgery regions. In addition to this, author did work on accuracy forgery regions localization by introduced the algorithm of Forgery Region Extraction which exchange the feature points with small super pixels as the feature blocks & after that merges the near blocks that have similar local color features into the feature blocks which is for generating the merged regions; and then it used the morphological operation to the integrate regions to produce the detected forgery regions. For experimental study, author used MICC dataset.

Khosro Bahrami et.al (٢٠١٥)

In [٩], author presented different technique for image splicing detection using block based approach. This method was introduced to reduce the problem of blur type inconsistencies in splicing forgery images. The novel framework for blurred image splicing localization depends on partial blur type inconsistency was designed by author of this paper. In this framework, then the block depends on image deviations, the local blur type detection feature are separated from the estimated local blur kernels. The image blocks have been formulated into the out of focus blur based on this feature to produce invariant blur type regions. After then fine splicing localization is utilized to enhance the accuracy of regions boundary. Basically in this technique, the blur type differences of the regions were utilized to trace the inconsistency for the splicing localization. Author itself created the tampering dataset for the evaluation purpose

Mohsen Zandi et.al (٢٠١٦)

In [١٠], this is another recent technique proposed for efficient copy-move forgery detection on research public dataset images. Author presented this method for interest point detection is presented which was specialized for copy-move forgery detection. In this approach, distribution of separated feature points reflects the local information content. It is worth considered that the exploited key point’s extractors in copy-move forgery detection are mostly proposed for object recognition. Additionally, author used new filtering scheme in order to preserve the correct matches among a great number of potential matches with a low computational cost. Finally, author performed an iterative improvement strategy depend on the new interest point detector which greatly enhances the pixel-based accuracy. The practical evaluation was conducted using two public research datasets such as SBU-CM١٦١ and IMD (Image Manipulation Dataset).

Anselmo Ferreira et.al (٢٠١٦)

In [١١], author introduced technique for copy-move forgery detection with aim of solving three existing problems. At first author overcome the issue of missing probability estimations caused by the lack of training data, using generative models to best assumption missing entries & extracting noise from the existing probabilities in the representation space adopted. Secondly, author utilized the expert knowledge to the adopted BKS representation for more robust to some common operations into the image tampering which is lead to confusion in the classification of individual classifiers. Finally, this article overcomes the issue of individual pixel classification, present in most copy-move detection approaches by incorporating the post-processing step to the detection BKS-based technique, which classifies a pixel depends on the outcomes of its neighborhood. Author did their practical analysis on CPH dataset.

E. Ardizzone et.al (٢٠١٥)

In [١٢], the approach for copy-move forgery detection using the key points matching triangles was proposed. It is most novel hybrid approach introduced by author, this was very novel hybrid approach proposed by author, which weigh triangles rather than blocks, or single points. Interest points were separated from the image and objects are modeled as a group connected triangles construct onto these points. Triangles were compare using their shapes (inner angles), their content (color information), and the local feature vectors separated on the vertices of the triangles. The goal of this method was to be robust to different geometric transformations. For key points extraction author used three different Methods such as SIFT, SURF and Harris. This method was evaluated with different datasets named as D٠, D١, and D٢.

Jian Li, Xiaolong et.al (٢٠١٤)

In [١٣], another new method designed for copy-move tampering detection. With technique, input forgery image first segmented into non-overlapped blocks. Then the one image is transferred to partial matching among the obtained blocks, which was a problem having been deeply studied in the computer graph research domain by author. After that author proposed EM algorithm as new solution for the problem which has been proved to be an extension of the classic registration method iterative closest point (ICP). This method designed in two phases such as: first stage was designed to find the suspicious matches, and a transform matrix between them is roughly estimated. Then in the second stage author confirmed the existence of copy move forgery by means of refining the transform matrix. This is nothing but the two stages matching based forgery detection method. The practical study conducted on MICC-F٦٠٠ dataset.

III. COMPARATIVE ANALYSIS

The methods studied above are compared regarding advantages, disadvantages, techniques and accuracy performance. Table ١ has display the comparative study among these methods. And figure ٥ is display the accuracy comparison.

TABLE ١: COMPARATIVE STUDY OF IMAGE FORGERY DETECTION METHODS

Paper Title	**Key Techniques and Methods**	**Advantages**	**Disadvantages**	**Forgery Type**
Image Splicing Forgery Detection using Local Binary Pattern and Discrete Wavelet Transform	LBP, DWT, SVM, YCbCr and PCA	Evaluated on Two Different Datasets and having good efficiency	Processing Time is not evaluated.	Splicing
Copy Move Image Forgery Detection Using Hessian and Center Symmetric Local Binary Pattern	Hessian features, center-symmetric local binary pattern,		Less accuracy and processing time is not counted	Copy-Move
Passive Detection of Image Forgery using DCT and Local Binary Pattern	Discrete Cosine Transform, LBP, SVM.	Robust and simple method	Processing time is not calculated and very complex method	Splicing and Copy-Move
Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching	Adaptive over segmentation, SIFT, Block based.	Working on both Splicing and Copy-Move Forgery Images.	Processing time is not evaluated.	Copy-Move
Blurred Image Splicing Localization by Exposing Blur Type irregularity	Maximum a posteriori (MAP), LDA, binary classifier.	Having good Accuracy	Processing time is not calculated and conflicts resulted sometimes while	Splicing

			classification process.	
Iterative Copy-Move Forgery Detection depends on a New Interest Point Detector	Polar Cosine Transform, Adaptive matching, RANSAC.	Evaluated and compared in terms of precision, recall and accuracy rates.	This is complex method and processing time is not evaluated.	Copy-Move
Behavior information Space-Based Fusion for Copy-Move Forgery Detection	Multiscale BKS, Random Forest, SVM.	Probably it is first method of considering the Blur Type irregularity.	No complementarily of the underlying classifiers.	Copy-Move
Copy-Move Forger Detection by comparing Triangles of Keypoints	SIFT SURF, Harris, And Triangles Matching.	Showing good accuracy and precision, recall rates are evaluated.	No evaluation of complexity or processing time. Less accuracy.	Copy-Move

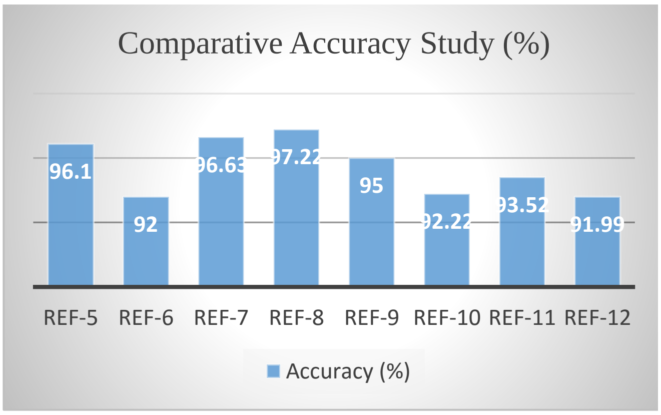

Figure ٥: Accuracy Analysis of Studied Methods

IV. RESEARCH PROBLEMS

After studying the recent methods and comparing their performances, in this section the current limitations and research challenges are highlighted for future work. Working on image forgery detection is very essential now days, hence its must that method should be efficient and robust in all aspects. Recently many researchers did work to deliver the best solution to detect forgery in images, but we had below observations through our study:

- Most of existing methods are not consider and evaluated the processing time and complexity parameters.
- The methods with best accuracy are having very complex procedure for forgery detection.
- Some methods are designed and evaluated by considering on accuracy metrics while precision, recall and complexity are equally important for evaluation purpose.

CONCLUSION AND FUTURE WORK

In this paper, introduction to image forgery is presented and explained at first, and then importance of detecting image forgeries on digital images is given. The different categories of image forgery and different types of methods explained. Basically this paper is aimed to present the study on all recent ٢٠١٤ to ٢٠١٦ digital image forgery methods either on copy-move or splicing based with comparative analysis. Section II and III, presented the complete study on all recent techniques and compare them accuracy wise. Finally, the research limitations and problems have been pointed out in section IV. For future work, we suggest to work on addressing the current research problems.

REFERENCES

[١] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in in Proceedings of Digital Forensic Research Workshop, ٢٠٠٣.

[٢] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR٢٠٠٤-٥١٥, ٢٠٠٤.

[٣] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," Ieee Transactions on Information Forensics and Security, vol. ٧, pp. ١٨٤١-١٨٥٤, Dec ٢٠١٢

[٤] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Susstrunk, "SLIC superpixels compared to state-of-the-art superpixel methods," IEEE Trans Pattern Anal Mach Intell, vol. ٣٤, pp. ٢٢٧٤-٨٢, Nov ٢٠١٢.

[٥] Fahime Hakimi, Mahdi Hariri, Farhad GharehBaghi, "Image Splicing Forgery Detection using Local Binary Pattern and Discrete Wavelet Transform", ٢nd international conference on KBEI, IEEE, ٢٠١٥.

[٦] Diaa M. Uliyan, Hamid A. Jalab, Ainuddin W. Abdul Wahab, "Copy Move Image Forgery Detection Using Hessian and Center Symmetric Local Binary Pattern", ٢٠١٥ IEEE conference on ICOS, ٢٠١٥.

[٧] Amani Alahmadi, Muhammad Hussain, Hatim Aboalsamh, Ghulam Muhammad, George Bebis, Hassan Mathkour, "Passive Detection of Image Forgery using DCT and Local Binary Pattern", Signal Image and Video Processing · April ٢٠١٦.

[٨] Chi-Man Pun, Xiao-Chen Yuan, Xiu-Li Bi, "Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching", IEEE Transactions on Information Forensics and Security, ٢٠١٥.

[٩] Khosro Bahrami, Alex C. Kot, Li, and Haoliang Li, "Blurred Image Splicing Localization by Exposing Blur Type Inconsistency', IEEE Transactions on Information Forensics and Security, ٢٠١٥.

[١٠] Mohsen Zandi, Ahmad Mahmoudi-Aznaveh, and Alireza Talebpour, "Iterative Copy-Move Forgery Detection based on a New Interest Point Detector", IEEE Transactions on Information Forensics and Security, ٢٠١٦.

[١١] Anselmo Ferreira, Siovani C. Felipussi, Carlos Alfaro, "Behavior Knowledge Space-Based Fusion for Copy-Move Forgery Detection", TRANSACTIONS ON IMAGE PROCESSING, ٢٠١٦.

[١٢] E. Ardizzone, A. Bruno, and G. Mazzola, “Copy-Move Forgery Detection by Matching Triangles of Keypoints”, IEEE Transactions on Information Forensics and Security, ٢٠١٥.

[١٣] Jian Li, Xiaolong Li, Bin Yang, and Xingming Sun, “Segmentation-based Image Copy-move Forgery Detection Scheme”, IEEE Transactions on Information Forensics and Security, ٢٠١٤.