"A Review on Splicing Image Forgery Detection Techniques"

ChitwanBhalla Surbhi Gupta

M.Tech Scholar Associate Professor

RayatBahra University, Mohali, Punjab, India RayatBahra University, Mohali, Punjab, India

chitwan2993@gmail.com9988665390royal_surbhi@yahoo.com

Abstract-Images now-a-days are often used as an authenticated proof for any crime and if these images does not remain genuine, it will create a problem. This leads to the problem of Image Forgery. Image Forgery is defined as adding or removing important features from an image without leaving any obvious traces of tampering.Further, it can either be intrusive (active) or non-intrusive (blind or passive). In active approach, the digital image requires some kind of pre-processing such as watermark embedded or signatures are generated at the time of creating the image. Passive image forensics is usually a great challenge in image processing techniques. It includes the concept of Copy-Move Forgery, Retouching and Image Splicing. In this paper, more of the research work is done on Image Splicing Techniques and Copy-Move Forgery. It includes the basic survey of various forgery detection techniques and the ways to cure the problem.

Index Terms- Image Forensics, Forgery Detection, Copy-Move Forgery, Image Splicing.

I. INTRODUCTION

Digital images are present everywhere on magazine covers, in newspapers, in courtrooms as evidences, and all over the Internet signifying one of the major ways for communication. Nowadays, we are living in a digital age where digital imaging has developed to become the widespread technology. It plays a significant role in human life. Digital images are being used as a means of pictorial information in daily newspapers and magazines as evidence in courts of law, and in the medical diagnose field.

Moreover, with the spread of low-cost user friendly editing tools the art of tampering, content is no more restricted to experts. As a result, the modification (manipulation) of images for malicious purposes is now more common than ever. Based on the above reasons, it is important to develop a credible method to detect whether a digital image is tempered, so-called digital image forgery. The image forgeries can hide or add an important object in an original image to misguide the court of law. Image forensics have an important role where the authenticity of images is important in our daily and social life.

Techniques For detecting Image Forgery:

The authenticity of digital images security is a very serious problem and it has grown some time ago. Many techniques have been developed for verification of the authenticity of digital images. These techniques can be described as intrusive (active) and non-intrusive (blind or passive). The active techniques can be classified into two categories.

- **Active Approach**

In this active approach, the digital image requires some kind of pre-processing such as watermark embedded or signatures are generated at the time of creating the image. However, in practice this would limit their application.

Types-

1) **Watermark**-Watermarking is such a method of active tampering detection, as a security structure is embedded into the image, but most present imaging devices do not contain any watermarking or signature module and that are similar to the application of active protection.

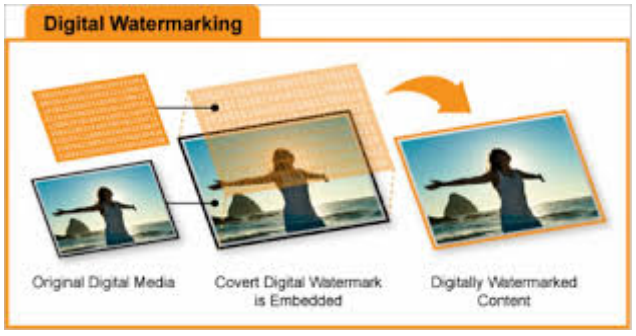

Fig. 1 Watermarked image

Fig. 1 shows a watermarked image that shows conversion from original digital media to digital watermarked content.

2) **Signature**-Signature is such a method of active tempering detection, in which signature is embedded into the image as a security means. Now-a-days biometric acceptance is much into demand for signature verification.

- **Passive Approach**

Passive image forensics is usually a great challenge in image processing techniques. There is not a particular method that can treat all these cases, but many methods each can detect a special forgery in its own way. The stream of passive tampering detection deals with analyzing the raw image based on various statistics and semantics of image content to localize tampering of image. Neither construct is embedded in the image and nor associated with it for security, as like active approaches and hence this method is also known as raw image analysis.

Types-

1) **Copy-Move Forgery**- Copy-Move is a special type of image manipulation technique in which a part of the image itself is copied and pasted into another part of the same image.

#

2) **Retouching-** Retouching is defined as hanging the image on a whole. For example by adding onto brightness, creating noise, creating clarity onto the base image etc.

3) **Image Splicing-** Image-splicing is defined as a paste-up produced by sticking together photographic images.

Image splicing is a common type to create a tampered image where a region from one image is copied and pasted into another image which produces composite image called spliced image; cut and join two or more snaps of pictures. The complicated forgery may include some post-processing like blurring, JPEG compression, etc. that performs the forgery detection very hard.

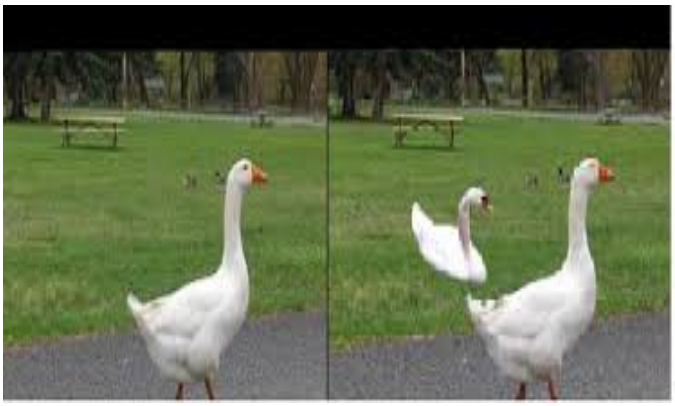

Fig. 2 Image Splicing

In Fig. 2, the left picture is the base image and the right one is the spliced image as in that case some cropped image is pasted over the base image and a new image is generated.

Image splicing is a common form of image forgery. Such alterations may leave no visual clues of tampering. Image splicing is to create a new image from two or more images, and it is far and wide used for image forgery. Image splicing detection is a main difficulty in image Forensics.

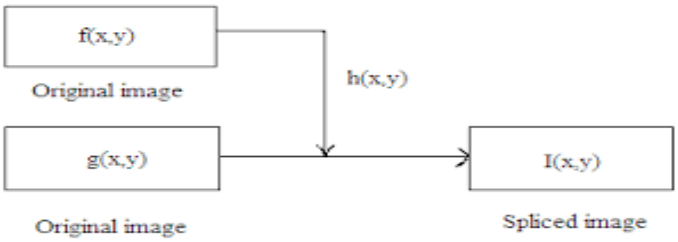

Fig. 3 Image Splicing

Fig 3 shows the basic pattern of Image Splicing. Two images are combined and a new image is generated out of that.

In Image Splicing, two images are combined to create one tampered image or it is a technique that involves a composite of two or more images, which are combined to create a fake image. Below shows an example of image splicing image forgery.

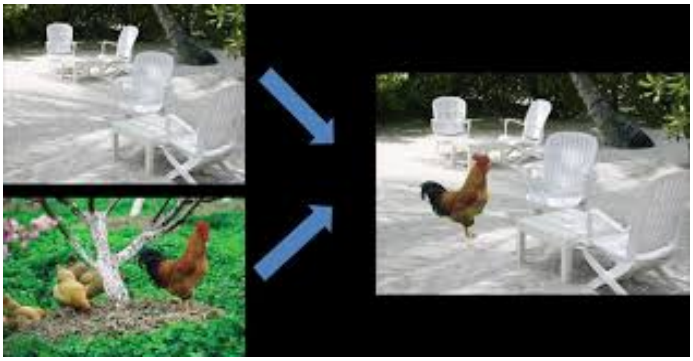

Fig. 4 Spliced Image

In Fig. 4, we can see that two images are combined and a new image is generated. One image is taken as the base image and out of the second image, some part is cropped and pasted over the base image.

II. LITERATURE SURVEY

It includes the basic survey of Research papers studied regarding the concept of Copy-Move forgery and Image Splicing.

Chennamma and Rangarajan (2010) [1] proposed an intrinsic camera parameter, namely lens radial distortion (Barrel and Pincushion) is used, for the detection of image splicing. In this paper, passive technique is proposed for detecting copy-paste forgery by quantitatively measuring lens radial distortion from different portions of the image using line-based calibration. Experiment shows that most consumer level digital cameras have small or large amount of lens radial distortion at different zoom levels. Experimental demonstrates how efficiently the lens radial distortion parameter may be used for the detection of image splicing and the experimental result shows that the method works well in case of real images. The primary contribution of our work is that the use of inherent lens distortion as a unique imprint on the images for the detection of image splicing.

Chadha et al. (2011) [2]face Recognition method using Discrete Cosine Transform (DCT) for Local and Global Features involves recognizing the corresponding face image from the database. The face image obtained from the user is cropped such that only the frontal face image is extracted, eliminating the background. The image is restricted to a size of 128 × 128 pixels. All images in the database are gray level images. DCT is applied to the entire image. This gives DCT coefficients, which are global features. Local features such as eyes, nose and mouth are also extracted and DCT is applied to these features. Depending upon the recognition rate obtained for each feature, they are given weightage and then combined. Both local and global features are used for comparison.

Alahmadi et al. (2013) [3] proposed the authenticity of a digital image suffers from severe threats due to the rise of powerful digital image editing tools that easily alter the image contents without leaving any visible traces of such changes.A novel passive splicing image forgery detection scheme based on Local Binary Pattern (LBP) and Discrete Cosine Transform (DCT) is proposed. First, the chrominance component of the input image is divided into overlapping blocks. Then, for each block, LBP is calculated and transformed into frequency domain using 2D DCT. Finally, standard deviations are calculated of respective frequency coefficients of all blocks and they are used as features. For classification, a support vector machine (SVM) is used. Experimental results on benchmark splicing image forgery databases show that the detection

#

accuracy of the proposed method is up to 97%, which is the best accuracy so far.

Gupta et at. (2013) [4] proposed Copy-move forgery technique. Robust method is used to detect the duplicated region in the digital image. Some tests are conducted on the algorithm against sample images from the internet. The result of the test is very encouraging since we got improvements in the detection rate and the detection time of the copy-move attack detection algorithm that we used. We are happy that the project is able to meet the outlined objectives proved that the use of DCT is better than using PCA for detecting copy-move attacks in highly textured images.

Jaberi et al. (2013) [5] proposedthe problem of copy–move image forgery detection. Our emphasis was on detecting and extracting duplicated regions with higher accuracy and robustness. The proposed methodologyemploys a new set of key point-based features, called MIFT, for finding similar regions in an image. To estimate the affine transformation between similar regions more accurately, we have proposedan iterative scheme which refines the affine transformationparameter by finding more key point matches incrementally.To reduce false positives and negatives when extracting theduplicated region, dense MIFTfeatures in conjunction with hysteresis thresholding andmorphological operations is proposed. Comprehensiveexperiments are done using a large dataset of real images toevaluate the proposed approach. In particular, investigation is done to detect theeffect of different transformations in creating the image forgery on detection accuracy. Among all transformationconsidered, blurring and deformation affect detectionresults most. Obviously, blurring affects the accuracy ofmatching key point-based features while deformation cannotbe modeled well by the affine transformation model beingused here for bringing similar regions into correspondence. Comparisons with competitive methods indicate that theproposed methodology can extract duplicated regions moreaccurately. It should be mentioned that like similar methodsemploying key point-based features for matching, the proposedapproach will not work well if the duplicated regioncorresponds to a flat surface where no interest points can bedetected.

Sushama and Rasse (2014) [6] proposed advanced image processing tools and computer graphics techniques make it straightforward to edit or modify digital images. Image splicing is a common type of image tampering operation. The image integrity verification as well as identifying the areas of tampering on images without need to any expert support or manual process or prior knowledge original image contents is now days becoming the challenging research problem. This paper is focused on authenticity of images and is based on concept of using illumination color estimation. Recently new method introduced for efficient forgery detection particular for faces in images. The illuminant color is estimated using the physics based method as well as

statistical edge method which make the use of inverse intensity-chromaticity color space. The estimate of illuminant color is extracted independently from the different mini regions. For the classification used the Support Vector Machine (SVM) approach. In this paper our main goal is to take review of different methods for digital image forgeries detection.

Zhu et al. (2014) [7] proposedan efficient forensic method based on the scaled ORB for detecting copy-move forgery in digital images was proposed. The proposed method not only detects duplicated regionsbut also determines the geometric transformations and postprocessingapplied to the forged regions. In addition, when locating the duplicated regions of which SIFT and SURF cannot detect, the proposed algorithm also performs well. However, the method is still time-consuming for forgery detection of high resolution images.

Fadl et al. (2014) [8]proposed a fast and efficient method for CM forgery detection whether without modification and with rotation modify, by using Fast K-means and block frames features. It works in the absence of digital watermarking and does not need any prior information about the tested image. Compare with previous works, the proposed algorithm works fast and more effectively. The experiment results show that the proposed method has the ability to detect CM and CRM forgery in an image faster than other systems by about 75%. In future, work can be done on Copy-Rotate-Move with any angle, and detect CM with scale modification.

Zhang et al. (2014)[9]proposed the method for image tampered detectionbased on SIFT and bi-coherence features through a novel perspective: forgery motive. According to the content of original source region and the duplicated one,copy-move forgery motive is classifiedinto three types. For a given image, it is detected that weather it is a tempered one and a reliable detection can be obtained by bi-coherence phase histogram, simultaneously, the original source region and duplicated one can be distinguished for a deeper analysis. Future work will be mainly dedicated to two issues: 1) how to achieve more correctly matched key points and less mismatched ones, 2) how to improve the bi-coherence phase feature performance to decrease the FPR and increase the TPR and TCR. In particular, the bi-coherence feature can’t be affected by the content of duplicated regions.

Liu et al. (2014) [10]proposed a common copy-move forgery, in which one or more parts of an image are copied and pasted elsewhere in the same image to add or conceal other parts. However, the satisfactory matching results can’t be acquired by applying the standard SIFT-based algorithm when detecting

#

multiple copied regions. To solve this problem, an efficient and robust method based on SIFT is proposed, which combines BFSN clustering and CFA features. BFSN clustering algorithm can avoid the mutual interference between key points extracted from different copies effectively. The original regions and the tampered regions can be distinguished, according to the inconsistency revealed by CFA features. Experiments havebeen performed to demonstrate the efficiency of the proposed method.

Kaur et al. (2015) [11] proposed all the existing image splicing techniques and their relative forgery detection methods. Because the spliced images are produced by different images so the common idea of the techniques in spliced image detection is the inconsistency of features in images. Most of algorithms are proposed to find the discrepancies in image. These discrepancies may be caused by Re-Sampling, Blur, Image features or Camera features. It tells an overview of the existing splicing image forgery detection techniques. The attempt to presents this papers cover all the splicing types of image based and camera based techniques.

Kaur and Kaur (2015) [12] proposed pixel-based image forgery detection that aims to verify the authenticity of digital images without any prior knowledge of the original image. There are many ways for tampering an image such as splicing or copy-move, re-sampling an image addition and removal of any object from the image. Copy-move forgery is one of the most popular tampering artifacts in digital images. The paper presents different technique to detect copy move forgery using block based method.

Hsu et al. (2015) [13]proposed that copy-move is a common method for image forgery. It works without any digital watermarks or signature information. The paper proposes an effective method for detecting duplicated regions based on the histogram of Gabor magnitude. The experimental results demonstrate that the proposed algorithm could not only detect multiple copy-move forgery instances, but is also robust against actions aimed at concealing forgery, including slight image rotation, JPEG compression, blurring, brightness adjustment. Furthermore,the computational complexity involved is low. This study, therefore, makes a valuable contribution to the field of multimedia forensics styles.

Kaur and Kaur (2015) [14] proposed new method for image forgery detection method based on SPT and LBP. Experiments revealed that the LAB channels are better suited for image forgery detection than the luminance channel or gray scale for further processing then SPT is used for detecting the rotational part of forged image so that it can detect even 360 degree rotation and LBP is for highlights the texture more accurately. Classification is done to detect the forged part and then check the accuracy of detecting image by using sensitivity and specificity values. The best accuracy of the proposed method is 96.78 % which is more than the previous methods. This method also

detect the Splicing Forgery method is 96.78 % which is more than the previous methods. This method also detects the Splicing Forgery.

III. COMPARISON TABLE

Author/year	Methodology	Parameters	Accuracy Achieved/ Description
Chennamma and Rangarajan (2010) [1]	Lens Radial Distortion	Intrinsic Camera	96%
Chadha et al. (2011) [2]	DCT	Feature Extraction	94.5%
Alahmadi et al. (2013) [3]	LBP,DCT	Standard Deviation	97.7%
Gupta et at. (2013) [4]	DCT,PCA	Detection rate, Detection Time	97%
Jaberi et al. (2013) [5]	SIFT,MIFT	Feature Extraction	Comparison b/w SIFT and MIFT
Sushama and Rasse (2014) [7]	Illumination Color Estimation	Digital Image Forgery	Statistical generalized gray world and physics-based inverse-intensity chromaticity space estimates
Zhu et al. (2014) [8]	SIFT,SURF	ORB Features	Comparison done between SIFT and SURF
Fadl et al. (2014) [9]	K- means Clustering	Feature Extraction	94%
Zhang et al. (2014)[10]	3PCC	SIFT Feature, bi-coherence Features	Comparison b/w TCR and TPR
Liu et al. (2014) [11]	SIFT	BFSN,CFA	BFSN clustering and CFA features are combined
Kaur et al. (2015) [12]	Image Feature Technique, Camera Based Technique	Image Splicing	Image Feature and Camera characteristics based techniques
Kaur and Kaur (2015) [13]	Passive Technique: Copy-Move Forgery	Block based Approach, Key Based Approach	Description of image forgeries
Hsu et al. (2015) [14]	Feature extraction	Gabor magnitude	96.1%
Kaur and Kaur (2015) [15]	SPT,LBP	Forgery Detection	96.7%

IV. CONCLUSION

Image Forgery is one of the techniques used to detect the authenticity of tempered images and to work on the various possible options to reduce the level of errors. In Active approach, Watermarking is a method of active tampering detection, as a security structure

#

embedded into the image. Signature is second method of active tempering detection, in which signature is embedded into the image as a security means. In case of Passive approach, the first one is copy-move, which is a special type of image manipulation technique in which a part of the image itself is copied and pasted into another part of the same image. The second one is Re-touching that is defined as hanging the image on a whole.For example by adding onto brightness, creating noise etc. The last is image-splicing which is defined as a paste-up produced by sticking together photographic images.

V. REFERENCES

[1]H. R. Chennamma and L. Rangarajan, "Image Splicing Detection using Inherent Lens Radial Distortion", International Journal of Computer Science Issues, Volume 7, November 2010.

[2]A. R. Chadha, P. P. Vaidya and M. M. Roja, "Face Recognition using Discrete Cosine Transform for Global and Local Features", International Conference on Recent Advancements in Electrical, Electronics and Control Engineering, IEEE Xplore, 2011.

[3] A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammadand G. Bebis, "Splicing Image Forgery Detection Based on DCT and LBP", college of Computer and Information Sciences, King Saud University Riyadh 11543, Saudi Arabia, 2013 IEEE.

[4] A. Gupta, N. Saxena andS. K. Vasistha, "Detecting Copy-Move Forgery using DCT", International Journal of Scientific and Research Publications, Volume 3, May 2013.

[5]M. Jaberi, G. Bebis, M. Hussain and G. Muhammad, "Accurate and robust localization of duplicated region in copy–move image forgery", Springer-Verlag Berlin Heidelberg 2013.

[6] S.G.Rasse,"Review of Detection of Digital Image Splicing Forgeries with Illumination Color Estimation", International Journal of Emerging Research in Management and Technology, Volume 3, March 2014.

[7] Y. Zhu, X. Shen and H. Chen, "Copy-move forgery detection based on scaled ORB", Springer Science and Business Media New York 2015.

[8]S. M. Fad, N. A. Semary and M. M. Hadhoud, "Copy-Rotate-Move Forgery Detection Based on Spatial Domain", Menofia, Egypt, 2014 IEEE.

[9] J. Zhang, Q. Ruan,Y. Jin, "Combined Sift and Bi-Coherence Features to Detect Image Forgery", China, 2014 IEEE.

[10] L. Liu, R. Ni, Y. Zhao and S. Li, "Improved SIFT-based Copy-move Detection Using BFSN Clustering and CFA Features", China,2014 IEEE.

[11]J. Kaur, S. Kundra andH. Kundra, "Review on Splicing Image Forgery Detection Techniques", International Journal of Advances in Computer Science and Communication Engineering (IJACSCE) Volume 3, August 2015.

[12]H. Kaur andK. Kaur, "A Brief Survey of Different Techniques for Detecting Copy- Move Forgery",InternationalJournal of Advanced Research in Computer Science and Software Engineering Volume 5, 2015.

[13]C. M. Hsua,J. C. Leeb, and W. K.Chena,"An Efficient detection algorithm for Copy-Move Forgery", Taiwan,2015 IEEE.

[14]H. Kaur andK. Kaur, "Image Forgery Detection using Steerable Pyramid Transform and Lab Color Space", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, August 2015.

#