A Review on Image Forgery and Detection Methods

Amandeep Kaur[1], Isha Vatts[2]
[1]*M.Tech (Scholar),* [2]*Assistant Professor*
Department of Computer Science Engineering, Chandigarh Engineering College, Landran - Punjab

Abstract: Images now-a-days are often used as an authenticated proof for any crime & 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 eliminating significant features from an image without leaving any obvious traces of tampering. Further, it can either be intrusive (active) or non-intrusive (sightless or passive). In active method, 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 generally a great challenge in image processing procedures. It includes the concept of Copy-Move Forgery, Retouching & Image Splicing. In this paper, more of the research work is done on Image Splicing Techniques & Copy-Move Forgery. It includes the basic survey of various forgery detection techniques & the ways to cure the problem.

Keywords: Image Forensics, Forgery Detection, Copy-Move Forgery, Image Splicing.

I. INTRODUCTION

Digital Image forensics is an emerging branch of image processing, which is aimed at obtaining quantitative evidence on the origin & truthfulness of a digital image[1][4] .One of the principal tasks of image forensics is image tampering detection. Tampering means to interfere with something in order to cause injury or make unauthorized alterations. Pictures are treated as proofs in various scenarios & thus image tampering is defined as intentional manipulation of images for malicious purposes [2]. Image tampering dates its source to the first twentieth century when it was used for political propaganda. image tampering is not a rare phenomenon & as a result the last decade marked tremendous improvements in the field of image forensics methods. Image forensics techniques can be classified under two different approaches, Active approaches & Passive/Blind methods [3]. Active approaches were used conventionally by employing data hiding (watermarking) or digital signatures. Passive approaches or blind forensic approaches use image statistics or content of the image to verify its genuineness [4].Now days, digital images are widely used all over the world. Exchanging soft copy of various documents is a normal practice in these days. So there is a probability of forgery while exchanging such kind of documents. Image Forgery is the process of making illegal changes of image information. Forgery may occur in applications which uses digital image as user can change it by using editing tools presented in market.

II. RELATED WORK

Ye Zhu et.al (2016) [5] present Copy-move forgery (CMF) is measured easier to detect than general forgery devices, but detecting it in the presence of multiple similar but genuine scene objects (SGOs) is non-trivial. Author study the efficiency of human visual perception for copy-move image forgery detection (CMFD) linking SGOs, & compare the same with machine performance. Via an eye tracking study performed with 16 users where pairs of images (one real & the other tampered) were displayed in either parallel or serial fashion, author make the following observations: (1) Forgery detection is quicker & more accurate when images are spatially aligned & presented serially, so that the tampering is conspicuous. (2) Eye fixations focus on corresponding regions of the real & tampered images, with fewer & more localized fixations noted during serial judgment. (3) A gap is noted among CMFD performance of humans & machines, with each being more sensitive to different tampering factors. Qingzhong Liu et.al (2016) [6] describe effectively exposes inpainting forgery under post recompression attacks; especially, it noticeably improves the detection accuracy while the recompression quality is lower than the original JPEG image quality, & thus bridges a gap in image forgery detection. Haodong Li, et.al (2017) [7] present first select & improve two existing forensic approaches, i.e., statistical feature based detector & copy-move forgery detector, & then adjust their results to obtain tampering possibility maps. After investigating the properties of possibility maps & comparing various fusion schemes, author finally propose a simple yet very effective strategy to integrate the tampering possibility maps to obtain the final localization results. Ira Tuba et.al (2016) [8] present an algorithm for digital image forgery detection that deals with the situation when some object, together with its shadow, is copied & pasted to some other location in the same or different image. Algorithm is based on the property that shadows do not change the texture of the underlaying surface.

Areas of application

• Authentication of pictures captured from CCD (charge coupled device) cameras.

• Authentication of info available in an image

• Authenticity of evidences • Fingerprint recognition

• Document authentication

III. TECHNIQUES FOR DETECTING IMAGE FORGERY

The authenticity of digital images security is a very serious problem & it has grown some time ago. Many techniques have been developed for verification of the authenticity of digital pictures. These procedures can be described as intrusive (active) & nonintrusive (blind or passive). The active techniques can be classified into two categories [9].

• 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 making the image. Yet, 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 maximum present imaging devices do not comprise any watermarking or signature module & that are similar to the application of active protection.

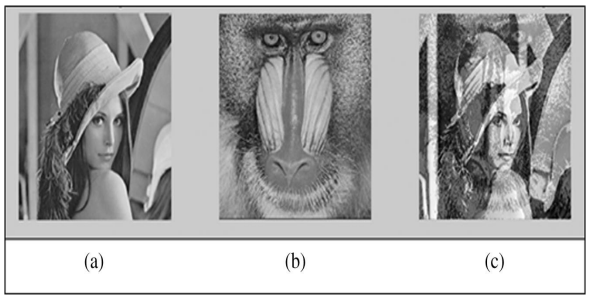

Fig.1: Watermarked image [13]

Fig. 1 shows a watermarked image that shows change from actual digital media to digital watermarked content [10].

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

• Passive Approach

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

Types-

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

2) Retouching- Retouching is defined as hanging the image on a entire. For example by adding onto brightness, making 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 [11].

Image splicing is a common type to create a tampered image where a region from one image is copied & pasted into another image which produces composite image called spliced image; cut & 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.

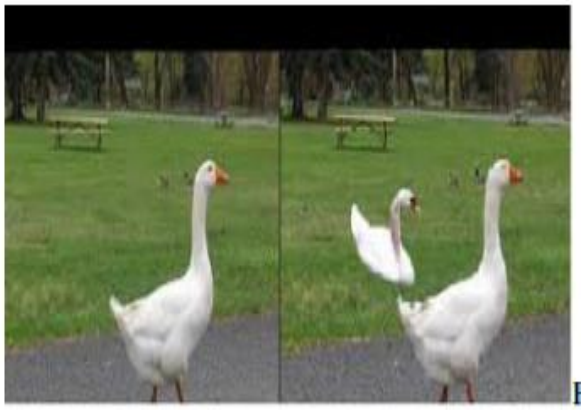

Fig.2: Image Splicing [14]

In Fig. 2, the left image is the base image & the right one is the spliced image as in that case some cropped image is pasted over the base image & 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, & it is far &

wide used for image forgery. Image splicing detection is a main difficulty in image Forensics.

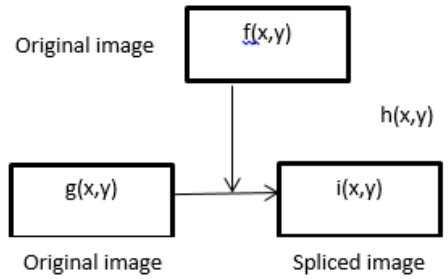

Fig.3: Image Splicing [14]

Fig 3 shows the basic pattern of Image Splicing. Two images are combined & 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 mutual to create a fake picture. Below shows an example of image splicing image forgery.

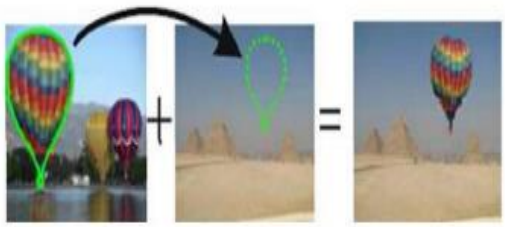

Fig.4: Spliced Images [13]

In Fig. 4, we can see that two images are combined & a new image is generated [12]. One image is taken as the base image & out of the second image, some part is cropped & pasted over the base image.

IV. CONCLUSION

Image Forgery is one of the techniques used to detect the authenticity of tempered images & 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 & 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]. E. Lin, C. Podilchuk, E. Delp, "Detection of image alterations using semi-fragile watermarks," Proc. SPIE, Security and Watermarking of Multimedia Content II, vol. 3971, 2000, pp. 152–163.

[2]. Gajanan K. Birajdar, Vijay H. Mankar, "Digital image forgery detection using passive techniques: A survey," Digital Investigation, vol. 10, no.3, 2013, pp. 226-245.

[3]. S. Kumar, P. Das, and S. Mukherjee, "Copy-Move Forgery Detection in Digital Images: Progress and Challenges," International Journal on computer Science and Engineering, vol. 3, no. 2, 2011, pp. 652-663.

[4]. J. Fridrich, D. Soukalm, J. Luka ´s ˇ, "Detection of copymove forgery in digital images," Digital Forensic Research Workshop, Cleveland, OH, 2003, pp. 19–23.

[5]. Zhu, Ye, Ramanathan Subramanian, Tian-Tsong Ng, Stefan Winkler, and Rama Ratnam. "COMPARISON OF HUMAN AND MACHINE PERFORMANCE FOR COPY-MOVE IMAGE FORGERY DETECTION INVOLVING SIMILAR BUT GENUINE OBJECTS."

[6]. Liu, Qingzhong, Andrew H. Sung, Bing Zhou, and Mengyu Qiao. "Exposing Inpainting Forgery in JPEG Images under Recompression Attacks." In Machine Learning and Applications (ICMLA), 2016 15th IEEE International Conference on, pp. 164-169. IEEE, 2016.

[7]. Li, Haodong, Weiqi Luo, and Jiwu Huang. "Image Forgery Localization via Integrating Tampering Possibility Maps." IEEE Transactions on Information Forensics and Security (2017).

[8]. Tuba, Ira, Eva Tuba, and Marko Beko. "Digital image forgery detection based on shadow texture features." In Telecommunications Forum (TELFOR), 2016 24th, pp. 1-4. IEEE, 2016.

[9]. 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.

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

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

[12]. J. Zhang, Q. Ruan,Y. Jin, "Combined Sift and BiCoherence Features to Detect Image Forgery", China, 2014 IEEE.

[13]. Nampoothiri, V. Parameswaran, and N. Sugitha. "Digital image forgery—A threaten to digital forensics." In Circuit, Power and Computing Technologies (ICCPCT), 2016 International Conference on, pp. 1-6. IEEE, 2016.

[14]. Gupta, ChitwanBhalla Surbhi. "A Review on Splicing Image Forgery Detection Techniques." IRACST-International Journal of Computer Science and Information Technology & Security (IJCSITS) 6, no. 2 (2016).