Study of Various Techniques Applied for Digital Image Forgery

Er. Abhijeet Ganpat Khadke[1] Prof. S. W. Ahmad[2] Prof. P. B. Lohiya[3]
[1]Student [2,3]Assistant Professor
[1,2,3]Department of Computer Science and Engineering
[1,2,3]Prof. Ram Meghe Institute of Technology & Research Badnera, Amravati, Maharashtra 444701, India

Abstract— Forensic consultant believes that no other criminal can do his activities without leaving evidence at the scene of crime. However it is hard to trace criminal proofs especially in case of digital image forgeries. Nowadays, image content alteration is a serious issue in digital image forensics. Due to numerous ways of image alteration, image splicing is a common way of image forgery. A spliced image is usually created by copying some portion or image and pasting portions of the image onto the same or another image. Much research in Image Forgery Detection has concentrated on the detection and localization of specific methods of forgery using methods like image pattern matching, comparing image histogram, patch-matching, anomaly detection, and examining residual-based local descriptors. The pixel-based picture imitation or identification intends to confirm the legitimacy of advanced pictures with no earlier learning of the first picture. There are numerous techniques for altering a picture, for example, joining or copy, move, re-examining, re-building, color enhanced etc. Copy-move falsification is a standout amongst the most prevalent altering ancient rarities in computerized pictures. This paper mainly focuses on study on various techniques used in digital image forgery.

Keywords: Image Forensics, Image Splicing, Copy-Move Forgery, Re-Sampling, Passive Techniques

I. INTRODUCTION

In the early days all information limited to original user only. But increasing era of online social platform, everyone need to share it. At the same time image forgeries, alterations, copy and move, resize, rescaling increased widely in the digital world. Images are used everywhere: in courtrooms as per evidence of a crime, Or by car insurance agencies to evaluate damage after an accident, in the proof images in magazines to sell products or brands.

Acquiring to digital image as official document has become an accepted mode and the scope of low cost technology in which the image could be easily manipulated are two most denoting impression towards image forgery detection. Even though there are many technologies to identify the digital image forgery, their implementation is limited by the conditions imposed by many systems. Naturally, as latest trend is digital imagery grows, so, too, does the use of photo editing software's like Adobe Photoshop windows software or the Linux based software GNU Image Manipulation Program (GIMP).

This software's are capable of easily modifying an image. It is also capable of removing red-eye in a family portrait to completely removing people or objects. Removing unwanted object is typically done by copying some content that already exists in the image over the pixels that contain the object. The process is called Copy-Move. To add in content from one image over another in a process called Splicing. With available of some free access to tools used in various operating system like GIMP and an internet full of free resources, the use and abuse of photo editing software has exploded.

Locate and identify manipulation of images takes place after it determined to be forged. With these Copy-Move forgeries, matching patches of pixel that are copied can be found within the image and highlighted. This Splicing and localization can be done by detecting and highlighting a break in a boundary between the host image's content and the foreign spliced content.

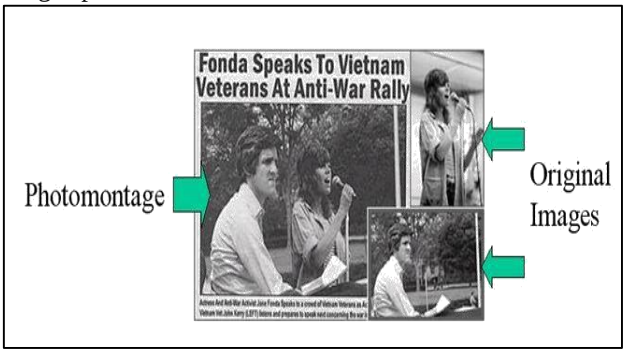

Fig. 1: Example of image forgery John Forbes Kerry with Jane Fonda

In general image forgery is the manipulation of digital images either in terms of destroying or inserting some information in the images. An example of such forged image is shown in Figure1. An American diplomat John Forbes Kerry with Jane Fonda, a Hollywood actress speaking to a crowd at an anti-Vietnam peace rally [1]. This manipulation of images is going on from the past and even accepted in areas like the forensic investigation,

Information Technology, medical Imaging, Journalism, Intelligence service etc.[2] Nowadays organizations interested in paperless work and e-government services resulting a huge amount of data stored in digital format and this gives rise to many challenges to secure authentic data. Unfortunately, the various collections of data like documents, files, voice data, and image data are all vulnerable to manipulation and doctoring. This gives rises to an interest among the research community in developing image forensics techniques towards identifying the trust of digital images. Over the past decade, the image forensics emerged to help in restoring the lost trust to digital images [3].

Unfortunately, the various collections of data like documents, files, voice data, and image data are all vulnerable to manipulation and doctoring. This gives rises to an interest among the research community in developing image forensics techniques towards identifying the trust of digital images. Over the past decade, the image forensics emerged to help in restoring the lost trust to digital images.

II. LITERATURE SURVEY

Copy Move picture fabrication is the generally utilized strategy to alter the computerized image. Copy-Move phony

is performed with the goal to make an item "vanish" from the picture by covering it with a little square replicated from another part of the same picture. Since the replicated portions originate from the same picture, the shading palette, clamor segments, shading and alternate properties will be same with whatever remains of the picture, in this manner it is extremely troublesome for a human eye to detect [22].

A copy move extortion is definitely not hard to make. The duplicated substance of picture which is used to perform misrepresentation is called scrap. As the source and the target territories are from a similar picture, the image features like bustle, shading, and illumination condition, etc will be same for the fabricated region and whatever is left of the image. A smart forger may moreover do some post-taking care of on the duplicated region like rotate, scaling, darkening, confusion extension before the area is stuck.

In Passive approach technique overcome some drawback and is widely used for forgery detection in digital images. As in most of the images are available today are without any watermark or digital signature. In passive approach different image forgeries are resampling, copy-move or duplication portion, splicing and retouching.

Another method of detecting forgery is by using noise variance estimation at image blocks to point out the suspicious regions. Popescu and Farid [24] proposed noise inconsistencies detection method which depended on estimation of clamor fluctuations of covering obstructs in which the general picture is tiled into squares. In this strategy, white Gaussian commotion and non-Gaussian uncorrupted picture is accepted. Primary disadvantage of this technique is that the kurtosis of the first picture is thought to be realized which isn't valid by and by.

III. METHODOLOGY

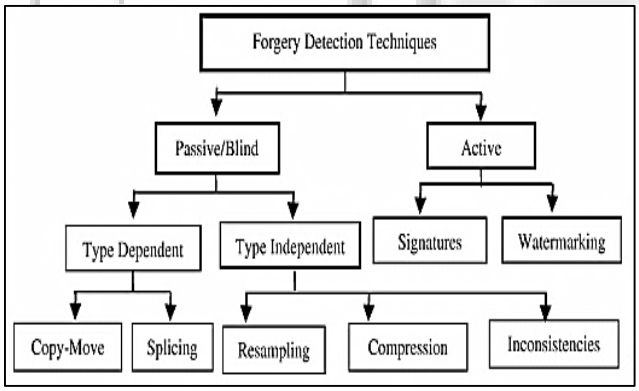

Fig. 2: Classification of image forgery detection

A. Passive/Blind Forgery

In literature, researchers classified Image Forgery in following ways [4]. Copy-Move or region duplication forgery is the most common image alteration technique used because of its simplicity and effectiveness. In this type, part of the original image is copied or moved to a destined location for pasting in order to hide certain details as well as duplicate parts of an image as given in figure3. Sometimes Textured regions are used as ideal parts for copy-move forgery, But due to some color adjustment areas has similar color and noise variations to that of an image which is unperceivable to human eye looking for inconsistencies in image statistical properties.

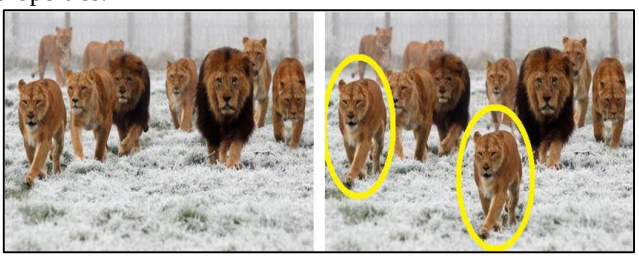

Fig. 3: Copy-Move Forgery Example

Image splicing involves replacing of image fragments from one or more different images into another image in order to produce a fake image as shown in figure2. This is one of the simple and commonly used tampering techniques. When splicing is performed carefully, the borders between the spliced regions can visually be imperceptible. However, splicing disturbs the higher order Fourier statistics such as the bi-spectrum.

Fig. 4: Splicing Image Forgery (Fake Face Mapping)

Image Re-sampling involves in creating a high quality forged image by applying some transformations like rotation, scaling, stretching, skewing, flipping etc in order to produce a convincing composite between two objects of different dimensions as shown in figure5. This process requires resample the original image onto a new by introducing specific periodic correlations between neighboring pixels.

Fig. 5: Re-Sampling Image Forgery

Typically, splicing detection involves the use of handcrafted filters and features within a neural network or other machine learning system.

B. Active Forgery Technique

1) Watermarking:

Watermarking is used for image forgery detection. Watermark must embed at the season of making the picture. Installing a watermark in the picture/video is proportionate to marking a particular computerized maker distinguishing proof (mark) on the substance of pictures/recordings. Once the picture/video is controlled, this watermark will be

devastated such that the authenticator can look at it to confirm the innovation of contents. The watermarking comprises of concealing an imprint or a message in a photo keeping in mind the end goal to secure its copyright at the season of picture obtaining and to check the legitimacy this message is separated from the picture and confirmed with the first watermarks. In the event the picture is not controlled these watermarks will stay same else they won't coordinate the first watermarks. Thus this strategy depends on the source of data beforehand. Some camera sources don't insert watermarks into picture consequently this technique is not that helpful and more often than does not function admirably with lossy compression.

Fig. 6: Watermark and original image

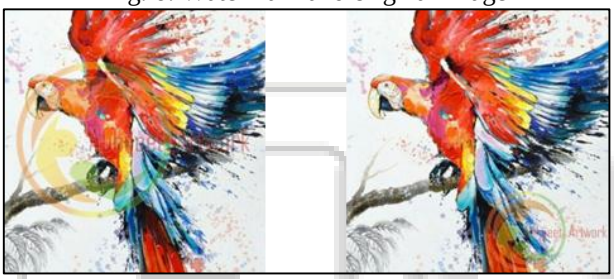

Fig. 7: Watermark embed on middle and corner

2) Digital Signature:

Advanced marker is some kind of cryptographic is a scientific plan for exhibiting the validness of computerized document. It creates a substance based computerized signature which incorporates the essential data of substance and selective maker recognizable proof. The mark is produced by a maker particular private key such that it cannot be manufactured. In this manner, a authenticator can check a got picture/video by inspecting whether its substance coordinate the data passed on in the mark.

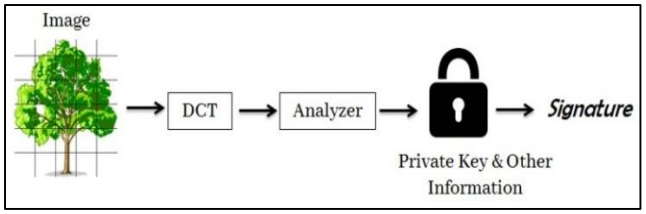

Fig. 8: Image encryption with private key

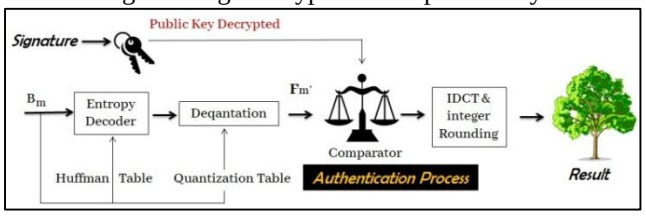

Fig. 9: Signature Generator and Image Authentication Process

C. Splicing Image Forgery Detection Color Pattern

Image splicing is a technique in which crops and pastes regions of the image from the same or different image. This is a fundamental step used in digital photomontage, which is very popular in digital image content editing. It is also referred as paste-up produced by sticking the images together using available digital software tools such as Photoshop. The spliced image used in many ways such as news reports, photography contest, key proof in the academic papers, and so on, which could bring certain negative influences.

As the digital images become more vulnerable to malicious tampering compared to their non-digital counterparts naturally it becomes an important and challenging research area in order to determine the authenticity of an image and detecting tampered parts of an image. The following are various techniques found in the literature and we classify them as illumination color estimation, inconsistency in image noise levels, statistical properties inherent in the source image (camera characteristics) and other feature based methods.

1) Illumination Color Estimation

In identifying the authenticity of a digital image illumination inconsistencies are potentially effective for splicing detection among other telltale signs. This is due to proper adjustment of the illumination conditions is hard to achieve while creating a forged image.

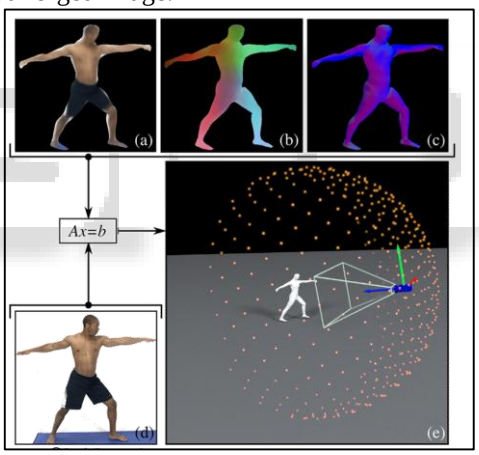

Fig. 10: Surface color on the body model and 3D Image

In [12] developed a physics based on illuminant color model for detecting the difference in the local image regions. The authors used illumination map based on distance measure to estimate the results thereby employing in forensic analysis. This technique requires user intervention.[13] Used inconsistencies of the illuminant color in the object region in order to detect the region splicing forgeries based on local illumination estimation. They proposed to combine five low-level statistics-based algorithms to estimate illuminant of each horizontal and each vertical band. For further development,[14] presented a new technique to detect forged images of people using the illuminant color. They evaluated illuminant shading utilizing a measurable dim edge strategy and a material science based technique which abuses the reverse power chromaticity shading space. HOGedge calculation is utilized to consolidate surface and edge based prompts and utilized AI late combination. Accordingly decrease client mediation to negligible.

2) Forgeries based on inconsistency in image noise levels - Noise that exists in images can be used to improve accuracy in detecting spliced image regions. It is evident that each image obtained by a digital camera prone to contain certain type of noise which may happen during to process of photons comes into the sensor until the camera output the image.

In [15] a blind forgery detection method based on local noise inconsistencies to detect small regions corrupted by local noise is proposed. The method uses the high pass diagonal wavelet coefficients at the highest resolution with non-overlapping blocks. The image segmented on the basis of homogeneity condition into several homogenous sub-regions using simple region merging algorithm in order to detect spliced forgery. The methods work well on the image where there is homogeneous noise level but fail when the authenticated image contains the same.

As an improvement in [16] authors proposed an effective method based. First, the image is divided into non-overlapping blocks and clustering applied to make them clean and tampered blocks. The detected suspicious regions are further segmented to refine noise estimation and finally applied classification to obtain the final result. To improve the results further the author estimate local noise variances by segmenting the image into regions with significantly different noise variances. Simple k-means clustering algorithm applied and then post-processing steps on detected regions to refine the result. In [17] an automated technique is proposed to detect spliced forgery in raw images. They used the relative consistency of noise parameters by looking at image inconsistencies from quad-tree decomposition to detect the potential sliced images. An efficient technique is proposed in [18] to detect region splicing. The technique is based on observed projection kurtosis concentration phenomenon. The noise statistics estimation is an optimization problem with a closed-form solution. All these techniques based on noise discrepancies in a single scale. Taking the advantage of multi-scales as an indicator for detecting spliced image forgery [19] proposed a technique where the image segmented into super-pixels of multiple scales and then noise level function applied on each individual scale. Those segments which are not constrained by the noise level function are further processed by Optimal Parameter Combination Searching algorithm in order to mark the spliced regions.

IV. Conclusion

Above review, present a summary and study of various image forgery techniques these all above techniques is mostly use over internet and social media. These forged images are produced from various sources of images. Sometimes due to low quality of image it's very easy to find modified portion of image. With the help of pixel-based calculation and based techniques we classify it into further illumination color estimation, pattern matching, statistical characteristics of the image, some noise inconsistency and finally presented other feature based methods. There may be several techniques found in the literature survey but, every technology has some limitations. This Image forensics is a grown research field in IT industry.

References

[1] K L Fonda, Kerry, And P Fakery, "The Washington Post," P- A21, Feb. 2004.
[2] M A Qureshi, M Deriche, "A Review On Copy Move Image Forgery Detection Techniques", 11th IEEE International Multi-Conference On Systems, Signals & Devices (SSD), 2014.
[3] Farid, "Image Forgery Detection A Survey," IEEE Signal Processing Magazine, Vol. 26, No. 2, Pp. 16-25, Mar 2009.
[4] G K Birajdar, V H Mankar, "Digital Image Forgery Detection Using Passive Techniques: A Survey", Digital Investigation (10) 2013 @Elsevier.
[5] Aa Alahmadi, M Hussain ; Hatim A ; Ghulam M ; George B, "Splicing Image Forgery Detection Based On DCT And Local Binary Pattern", Global Conference On Signal And Information Processing (Globalsip), 2013 IEEE.
[6] Saurabh A, Satish Ch," Image Forgery Detection Using Multi-Scale Entropy Filter And Local Phase Quantization", Internation Journal Of Image, Graphics And Signal Processing, 2015.
[7] Y Zhang, Ch Zhao, Yiming Pi, Shenghong Li1, Shilin W", Image-Splicing Forgery Detection Based On Local Binary Patterns Of DCT Coefficients", Security And Communication Networks, Published Online In Wiley Online Library, 2013.
[8] Ce Li1,2(&), Qiang Ma1, Limei Xiao1, Ming Li1, And Aihua Zhang1," Image Splicing Detection Based On Markov Features InQDCT Domain", LNCS, Springer, 2015.
[9] P.Kakar, N. Sudha, And W. Ser, "Exposing Digital Image Forgeries By Detecting Discrepancies In Motion Blur," IEEE Trans. Multimedia, Vol. 13, No. 3, Pp. 443–452, Jun. 2011.
[10] Zhang Z, Wang G, Bian Y, Yu Z,"A Novel Model For Splicing Detection", In IEEE 5th International Conference On Bio-Inspired Computing: Theories And Applications (Bic-Ta), 2010.
[11] TuK.Huynh, KhoaV.Huynh, Thuong Le-Tien, SyC.Nguyen, "A Survey on Image Forgery Detection Techniques", International Conference on Computing & Communication Technologies Research, Innovation, and Vision for Future (RIVF),2015.B. Su, S. Lu, And C. L. Tan, "Blurred Image Region Detection And Classification," In Proc. 19th Acm Int. Conf. Multimedia, 2011, Pp. 1397–1400.
[12] C. RiessAnd E. Angelopoulou, "Scene Illumination As An Indicator Of Image Manipulation," Inf. Hiding, Vol. 6387, Pp. 66–80, 2010.
[13] Yu Fan, Philippe Carré, Christine Fernandez-Maloigne" Image Splicing Detection With Local Illumination Estimation", ICIP 2015.
[14] C. RiessAnd E. Angelopoulou, "Exposing Digital Image Forgeries By Illumination Color Classification", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 7, July 2013.
[15] Xunyu Pan, Xing Zhang, SiweiLyu, "Exposing Image Forgery With Blind Noise Estimation", Thirteenth

Acm Multimedia Workshop On Multimedia And Security, 2012.
[16] Thibaut Julliand, Vincent Nozick And Hugues Talbot," Automated Image Splicing Detection From Noise Estimation In Raw Images", 6th International Conference On Imaging For Crime Prevention And Detection (ICDP-15).
[17] SiweiLyu ,Xunyu Pan And Xing Zhang, "Exposing Region Splicing Forgeries With Blind Local Noise Estimation", Springer, Int J Comput Vis,2014.
[18] Chi-Man Pun, Bo Liu, Xiao-Chen Yuan, "Multi-scale noise estimation for image splicing forgery detection", Journal Of Visual Communication Image Representation, Elsevier, 2016.
[19] Yu-Feng Hsu And Shih-Fu Chang," Image Splicing Detection Using Camera Response Function Consistency And Automatic Segmentation", 2007 IEEE International Conference On Multimedia And Expo.
[20] MS. Rupali Wankhade, Dr. G.R. Bamnote And Ms. S.W. Ahmad "Data Hiding in Video Stream by Efficient Data Embedding" , International Research Journal of Engineering and Technology (IRJET) Volume: 05 Issue: 12 | Dec 2018.
[21] Ankit Naik And S.W. Ahmad "Data Mining Technology for Efficient Network Security Management" International Journal of Computer Science Trends and Technology (IJCST) – Volume 3 Issue 3, May-June 2015 .
[22] Rohini. A. Maind, Alka Khade, D.K.Chitre: "Image Copy Move Forgery Detection using Block Representing Method" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4, Issue-2, May 2014.
[23] Amaninder Kaur, Sheenam Malhotra "Passive Image Forensic Method to Detect Resampling Forgery in Digital Images" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. VII (May – Jun. 2015).
[24] C. Popescu, "Statistical Tools for Digital Image Forensics", Proceedings of the 6th International Workshop on Information Hiding & LNCS, 2004, pp. 128-147.
[25] Yu-Feng Hsu And Shih-Fu Chang," Image Splicing Detection Using Camera Response Function Consistency And Automatic Segmentation", 2007 IEEE International Conference On Multimedia And Expo.
[26] T.-T. Ng and S.-F. Chang, "A model for image splicing," in Proc. IEEE Int.
[27] Conf. Image Processing, Singapore, 2004, vol. 2, pp. 1169–1172.
[28] P. Nillius and J.-O. Eklundh, "Automatic estimation of the projected light source direction," in Proc. IEEE Conf. Computer Vision and Pattern Recognition, 2001, pp. 1076–1083.
[29] S. Ye, Q. Sun, and E. C. Chang, "Detecting digital image forgeries by measuring inconsistencies of blocking artifact," in Proc. IEEE Int. Conf. Multimedia and Expo, Beijing, China, 2007, pp. 12–15.
[30] Mahdian and S. Saic, "Detection of copy move forgery using a method based on blur movement invariants," Forensic Sci. Int., vol. 171, pp. 180–189, 2007.

