IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Review of Common Image Forgery Methods and Techniques to Detect Image Forgery

Ariba Khanam[#1], Narendra Chaurasiya[*2]
M.Tech Scholar[#1], Assistant Professor[*2]
Buddha Institute of Technology, Gorakhpur

Abstract— **Image Forgery is one of the common issues in today's world. The existence of software tools for image modification has led to the easy modification of the original images some times for genuine purposes and other times with a bad intention. It is very difficult to identify the original images and forged images using naked eyes. In this paper, some of the most prominent techniques of forgery and tampering have been discussed. Along with it the paper also gives a detailed account of the work done by the researchers in the past decade in the fields of image forensics and forgery detection.**

Keywords— **Image forgery, forensics, copy-move, splicing, retouching, brightness modification.**

I. INTRODUCTION

The rapid advancement of photographic, video recording and telecommunication technologies broadens the possibilities of traditional methods of repairing videos, images, and modern data formats, necessitating the continuous updating of specialized knowledge in the field of digital photography research. Many photographic software programs, such as CorelDraw, Photoshop, Neo-Imaging, and others, can easily modify or tamper with digital content, undermining people's traditional belief that "seeing is believing." Documents or their images, photographs, videos, and scanned copies of the digital nature of creation are increasingly being presented as material evidence in pre-trial and court proceedings. Given the ease with which digital images can be created, modified, and distributed, the issue of their authenticity is logically raised during an investigation or in court. Composited, morphed, retouched, enhanced, computer-generated, painted, and rebroadcast images are the most common types of forged images. Most forged images use the basic operations of copy-paste, rotation, rescaling, stretching, zooming, contrast enhancement, and histogram equalization.

With cases increasing on an annual basis, developing and deploying effective approaches to detect the authenticity of digital images has emerged as a new field of forensic science in recent years. Image forensics is typically concerned with the following issues [1]:

(1) Determine the image's origin: determine whether the image is generated by a specific imaging device or by a computer. Determine the device's reference parameters, such as imaging equipment types, time, location, and so on, if the image is obtained by the device.

(2) Confirm the image's authenticity: determine whether the image is the result of second imaging or has been tampered with using photographic software. Determine the tampered region and operations if the image has been tampered with.

(3) Determine whether the image contains any hidden information. Determine whether the image contains steganography or a digital watermark, and if so, what they are.

A number of researchers have suggested frameworks to cater to these issues. Methods to detect and authenticate the images have been suggested. All forensic methodologies are classified into two types: active forensics and passive forensics [2]. Active forensics refers to forensic techniques that use previously embedded relevant information to authenticate a digital image, such as a digital watermark or signature. Active forensics does, in fact, restore the human credibility of digital images due to its high detection efficiency. Active forensics, on the other hand, has the limitation of not being widely used because the embedding mechanism must be available. Furthermore, active forensics is confronted with additional questions/problems, such as what happens when multiple people merge their media or how to embed

robust information that can be retrieved regardless of the media modification an active attacker can perform. As a result, the emphasis of the digital image forensic investigation is on passive forensics, with no prior information embedded [3].

In this paper a review on various types of prominent image forgery and tampering techniques has been discussed along with the work done to date in the past decade by researchers in the area of image forgery detection and image forensics has been discussed.

II. MOST COMMON IMAGE FORGERY TECHNIQUES

The authenticity of digital images is at stake in digital image forgery. The introduction of powerful computer graphics editing software such as GIMP, Corel Paint, and Adobe Photoshop has simplified the process of creating fake images. Numerous cases of digital image forgery have been reported. All of these cases can be divided into three major groups based on the process involved in creating the fake image. The groups are Image Retouching, Copy-Move Attack, Image Splicing and Morphing.

a) Copy Move Forgery

One of the most common image tampering techniques is copy-move; it is also difficult to detect because the copied image is taken from the same image. In Copy-Move image forgery, a portion of an image is copied and pasted to another portion of the same image. It simply entails pasting image blocks into the same image and concealing important information or objects. This technique involves copying a section of an image and superimposing it on another section of the same image. Figure 1 depicts a copy-move forgery example.

(a) The original images (b) The copy-move forged images

Figure 1: Copy Move Forgery on Images

b) Splicing

Splicing is another common manipulation technique that duplicates one or more objects from a first image and copies them into a second image. Because the new forged image is composed of disparate elements from two or more original real images, this tempering technique is also known as a composite forgery. Unlike copy-move tempering, the spliced object is from a different image. The detection of splicing is a difficult problem in which the composite regions are investigated using a variety of methods. Acute differences between combined areas and their backgrounds provide useful traces for detecting splicing in the image being examined.

(i) Authentic images (ii) Spliced image

Figure 2: Image Splicing

c) Image Retouching

Image retouching is regarded as the least dangerous form of digital image forgery. Image retouching does not significantly alter an image; rather, it enhances or decreases specific aspects of an image. Before combining two images, retouching may require one of them to be rotated, scaled, or stretched. It is a very common type of image change that can be seen in many commercials. In image retouching, "cloning" a portion of an image is also common. Because there is no significant change in the various parts of the image, detection is extremely difficult. Despite the fact that such enhancement is unethical, it can be said that almost all magazine covers would use this technique to enhance certain aspects of an image in order to make it more appealing.

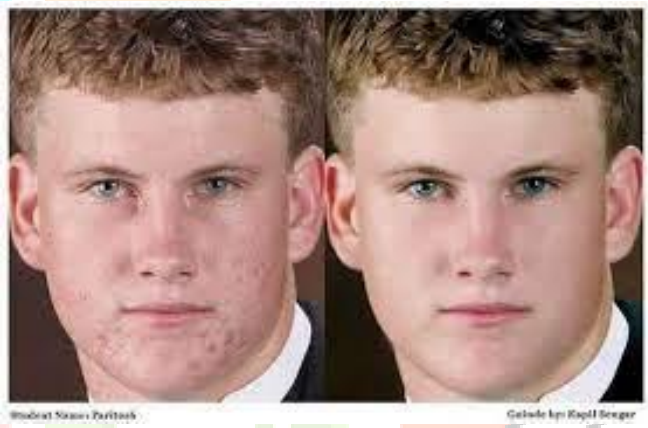

Figure 3: Image Retouching Forgery

d) Brightness/Intensity Modification:

Gamma correction is a common image acquisition technique that modifies an image's brightness to improve its display on a screen. However, from a forensic standpoint, one can frequently emphasise a portion of an image in order to change the semantic purpose by adjusting the brightness or illumination within the image. Brightness modification is rarely considered a forgery on its own, but it is a common operation used in conjunction with other types of forgeries. Another common example of brightness modification is in the context of copy-move or splicing forgery, where the brightness of the altered region must be adjusted to remain consistent with the original image in order to improve visual realism. As a result, brightness tempering can be used as an auxiliary forensic tool to provide vital information. Figure 4 depicts an example of image forgery involving brightness modification.

Figure 4: Brightness Modification Image Forgery

III. RELATED WORK

Tu K. Huynh et al.[4] gave an overview of Image Forgery Detection methods for images affected from Copy-Move and splicing. The algorithms were classified based on whether they transformed the input images before feature extraction in the copy-move forgery. Image of camera features is used to categorize detection techniques for spliced images.

The process of increasing detection rates, reducing complexity, and constructing a large database to test has concluded.

Amerini et al. [5] proposed a system for evaluating the effectiveness of attacking methods based on perceptual image quality, as well as a new version of a Scale Invariant Feature Transform(SIFT) based removal method using metrics of perpetually. The authors explain the criteria for selecting quality metrics, and then they present a comparison with other methods of Counter-forensics and their SIFT-based copy-move detection via key point classification, both in terms of keypoint removal and final perceptual quality. According to the authors, the method has the least impact on the visual quality of any method presented thus far while removing a significant number of key points.

Nandini Singhal et al.[6] reviewed techniques for detecting pixel-based forgery. The author discussed two methods: copy-move or duplicacy detection and fast-copy move detection. They have explained that copying and pasting contents from one image into another is the copy-move or cloning. Its main disadvantage is that it cannot detect very small areas. As presented the detection of duplicated regions become easy and fast

Mohammad Farukh Hashmi et al. [7] presented an image forgery detection method. According to the author, an original image has a homogeneity in its nonspectral representation, which on applying any kind of morphing gets lost. Thus they proposed various transform domain techniques like Discrete Cosine Transform, Local Binary pattern transform, curvelet method, and Gabor transform.

Bin Yang et al. [8] demonstrated a method for detecting copy-move forgery based on features. A modified Scale Invariant Feature Transform (SIFT) detector is used to detect key points. A key-point distribution strategy was developed to spread the key points across the image. Finally, the enhanced SIFT descriptor pinpointed the critical points for detecting copy-move forgery. It provides detailed experimental results in order to validate the efficacy.

Chun-Su Park and Joon Yeon Choeh[9] proposed a fast method for detecting forgery by employing a variety of geometric transformations such as region rotation, resizing, deformation, and reflection. SIFT detects copy-move forgery by extracting key points and descriptors. The proposed CMFD method is theoretically sound and outperforms existing SIFT-based algorithms. The processing time for this method is relatively short.

A Sobel filter-attached enhanced regional convolutional neural network (R-CNN) mask was presented by Xinyi Wang et al.[10]. The Sobel filter is used as an additional function to allow predicted masks to find gradients that are similar to the real mask. The network as a whole can detect two types of image tampering: copy-move and image tampering.

Payal Srivastava et al. [11] proposed an image integrity verification SURF algorithm. The suggested method works for four randomly selected image blocks. The SURF function is used to locate copy-move forgery within images. The data was manipulated by the image blocks, and the matched points were detected by the proposed SURF, according to testing with CASIA images. The authors discovered that the respective blocks of both images with pixel differences of over 40000 are fabricated images after analyzing various images.

Kunj Bihari Meena and Vipin Tyagi[12] demonstrated a new technique that combined two. The image is divided into texture and smooth regions in the current proposal. To extract key points from these texture regions, the SIFT algorithm was used. Furthermore, due to its rotation and scale-invariant properties, the proposed method used a block based on the smooth region via the Fourier Mellin Transformation (FMT), which is an excellent choice for detecting forged objects. Finally, the patch match algorithm was used to match the key point using generalized 2 Nearest-Neighbor and the FMT algorithm.

IV. CONCLUSIONS

With the advancement of digital imaging technology and the availability of low-cost image editing tools, image tempering has become common. A number of image forgery techniques exist like copy-move, splicing, retouching, and brightness modification. It is critical to improve and expand current research in the field of digital image forensics in order to re-establish trust in digital images. The various types of digital image tampering and forgery methods have been discussed in this work along with contributions in this field by other researchers.

REFERENCES

[1] Cheng Yan, "Research on forensic identification of forged images," Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC), 2013, pp. 1152-1155, doi: 10.1109/MEC.2013.6885238.

[2] Liu, Y., Wang, H., Chen, Y. et al. A passive forensic scheme for copy-move forgery based on superpixel segmentation and K-means clustering. Multimed Tools Appl 79, 477–500 (2020).

[3] Singh, R.D., Aggarwal, N. Video content authentication techniques: a comprehensive survey. Multimedia Systems 24, 211–240 (2018). https://doi.org/10.1007/s00530-017-0538-9

[4] Tu K. Huynh, Thuong Le-Tien, KhoaV.Huynh, SyC.Nguyen, "A Survey on Image Forgery Detection Techniques", The 2015 IEEE RIVF International Conference on Computing & Communication Technologies Research, Innovation, and Vision for Future (RIVF), p. 71-76, 2015

[5] I Amerini, F. Battisti, R. Caldelli, M. Carli, A. Costanzo, "Exploiting Perceptual Quality Issues In Countering SIFT-Based Forensic Methods",

[6] Nandini Singhal, Savita Gandhani, "Analysis of Copy-move Forgery Image Forensics: A Review", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.8, No.7, pp.265-272, 2015.

[7] Mohammad FarukhHashmi, Avinash G. Keskar, "Image Forgery Authentication and Classification using Hybridization of HMM and SVM Classifier", International Journal of Security and Its Applications Vol. 9, No. 4, pp. 125-140, 2015.

[8] Bin Yang, Xingming Sun, Honglei Guo, Zhihua Xia, and Xianyi Chen, 2017, A copy-move forgery detection method based on CMFD-SIFT, Springer Science+Business Media New York 2017

[9] Chun-Su Park, Joon Yeon Choeh, 2017, Fast and robust copy-move forgery detection based on scalespace representation, Springer Science+Business Media, LLC 2017.

[10] Xinyi Wang, He Wang, Shaozhang Niu and Jiwei Zhang, 2019, Detection and localization of image forgeries using improved mask regional convolutional neural network, Mathematical Biosciences, and Engineering.

[11] Xinyi Wang, He Wang, Shaozhang Niu and Jiwei Zhang, 2019, Detection and localization of image forgeries using improved mask regional convolutional neural network, Mathematical Biosciences, and Engineering.

[12] Kunj Bihari Meena and Vipin Tyagi, A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale-invariant feature Transforms, Multimedia Tools and Applications, 2020, DOI: https://doi.org/10.1007/s11042-019-08343-0.