FORENSIC IMAGING FOR COPY MOVE FORGERY DETECTION IN DIGITAL PHOTOGRAPHS

Dr. K.C Ravi Kumar[1], Jahnavi.G[2], Sayma Tamkeen[3], M.Tarunika[4]

Article History: Received: 13.02.2023 **Revised:** 28.03.2023 **Accepted:** 15.05.2023

Abstract

Currently, digital images are very significant because they are the primary information carriers. However, the simplicity of image manipulation makes their authenticity vulnerable. Different methods could be used to forge images, but the copy-move forgery, in which a portion of an image is duplicated and moved to another location within the same image, is the most popular. A fundamental flaw in the SVM method was that it was unable to classify the original and altered images separately. To get around this, the ORB algorithm is used as a feature extraction approach on photos that have been subjected to various geometric attacks in order to find the fabricated portions of the image**.** The recommended method, when evaluated with images from the different databases, has a higher accuracy rate thanks to procedures like preprocessing and feature matching to detect fabricated regions.

Keywords: Tampering, forgery, Copy Move Forgery, Photoshop, Authenticity.

[1]Professor, Department of CSE, Sridevi Women's Engineering college, Hyderabad, Telangana, India.
[2,3,4]UG Student, Department of CSE, Sridevi Women's Engineering college, Hyderabad, Telangana, India

Email: [1]kcravikumar1971@gmail.com, [2]gjahnavi24@gmail.com, [3]saymatamkeen26@gmail.com, [4]mahankalitarunika15@gmail.com

DOI: 10.31838/ecb/2023.12.s3.334

1. SCOPE

Overall, the scope of copy move forgery detection is vast, and it can be applied in any area where digital images are used, and where the authenticity and integrity of these images are essential. Copy move forgery detection can be used in forensic analysis to detect tampering in digital images used as evidence in criminal cases. In the field copy move forgery detection can be used to verify the authenticity of images used in news reporting and to prevent the spread of fake news**.** Copy move forgery detection can also be used in digital watermarking to detect and prevent the unauthorized copying of images. It can be used in security and surveillance systems to detect tampering in images captured by security cameras.

2. INTRODUCTION

Digital picture manipulation is now a breeze thanks to readily accessible photo editing like Adobe Photoshop. The image editing software has progressed to the point that images may be manipulated without suffering quality loss or leaving blatant fingerprints. This is concerning since photographs are increasingly used as evidence and documentation in many disciplines, including forensics, law enforcement, journalism, medicine, and the legal system. Another issue is the prevalence of doctored photos in the media. In 2017, a political party in India was accused of using copy move forgery to inflate size of the crowd at a political rally. It was found that several images of crowd have been duplicated a pasted in different areas to make it appear as a larger crowd than it was. Image manipulation is a problem in the scientific community as well. Image tampering detection has received a great deal of interest since manipulated images can be used to purposefully distort their meaning. For example, in figure 1, we can see that there exists one large rifle and six other smaller guns. In figure 2 there exists seven smaller guns and one large rifle. Here one of the smaller gun is copied and moved to another region of the same image. On the basis of the compatibilities of the segments included in an image, we focus on detecting forgeries.

Figure 1 Original Image

Figure 2 Tampered Image

3. RELATED WORK

"JPEG ghosts: exposing digital frauds,"

Several photos are commonly composited together to create a digital counterfeit, such as when a person's head is placed on the body of another. If the source photos had varying degrees of JPEG compression, that difference may have been preserved in the final digital composite. As such, we detail a method for determining whether a specific region of a picture was originally constricted at a lesser quality than the remaining part of the image.

Images of varying resolutions and quality levels may both benefit from this method

"A SIFT-based forensic technique"

Most often used to make fake pictures is the copy-move forgery technique. The photos might have been doctored to hide anything or alter their meaning. So, it is crucial to check the pictures to make sure they are real. Copy-move forgery detection can be categorised into two basic categories as block-based and key-point-based techniques. Although most block-based approaches have a common architecture, they vary in how they use feature extraction. The block-based approaches have great accuracy for recognizing the forged sections but a very high computing complexity. In this study, we examine one alternative to the block method, which we call the "keypoint approach."

"Copy-Move Forgery Detection in Digital Pictures,"

Powerful picture processing and editing software makes it simple to modify and edit digital photos. Modifying a picture by super imposing or erasing elements is now a common practice without any blatant signs of manipulation. Authenticating digital photographs, confirming their information, and identifying forgeries will become more important as cameras and videos gradually replace their predecessors. This research focuses on methods for identifying instances of fraudulent picture alteration (digital forgeries). Here, we concentrate on identifying a subclass of digital forgeries called the copy-move assault, in which a component of the image is copied from another location with the goal of concealing an important aspect of the original. If the cloned portion is improved to blend it with the backdrop and the forged picture is stored in a lossless format, this approach may still be able to identify the forged component.

4. METHODOLOGY

Several stages are required to identify forged parts in an image using ORB detector.

Data Gathering: The first step is gathering of the images needed. MICC image dataset is used which consists of original and tampered images.

Image Acquiring and Pre-processing: Action of retrieving and reading an image

from a source for further process is called image acquiring. Pre-processing is performed by converting the image from RGB (Red, Green, Blue) format to grayscale format. RGB is a coloured pixel image which consists of primary colour components. Conversion to grayscale format eliminates the complexity while image processing for applying the algorithm.

Classification using SVM: It is used for classifying the images, but failed to identify which one is original and which one is forged.

Forgery Detection: Forged parts in the images are detected using ORB. It extracts the important features of an image and coverts it into a binary vector format. Later feature matching is performed in order to detect the forged parts of image. Finally, the accuracy of SVM and ORB is compared.

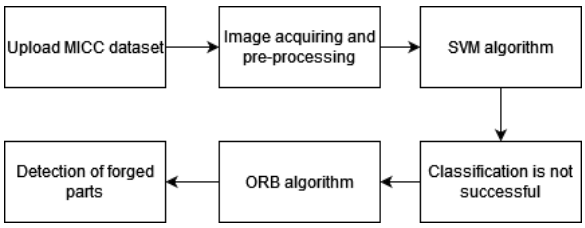

Figure 3 System Architecture

5. RESULTS

Although several methods including support vector machine [SVM] have been developed to detect this kind of picture fraud, their great accuracy with a 0% False prediction rate indicates that they cannot distinguish between genuine and forged images. Copy Move Forgery Discovery (CMFD) is a cutting-edge concept for analysing images that uses cutting-edge algorithms like Oriented FAST and rotated BRIEF to showcase extraction method as well as feature matching to solve this problem. Figure 3 displays the forged parts of the image while comparing the original with the tampered image. Figure 4 displays the comparison of the accuracy, FPR, TPR that SVM and ORB has produced at the end. The suggested method works well for object translation as well as various degrees of rotation and enlargement.

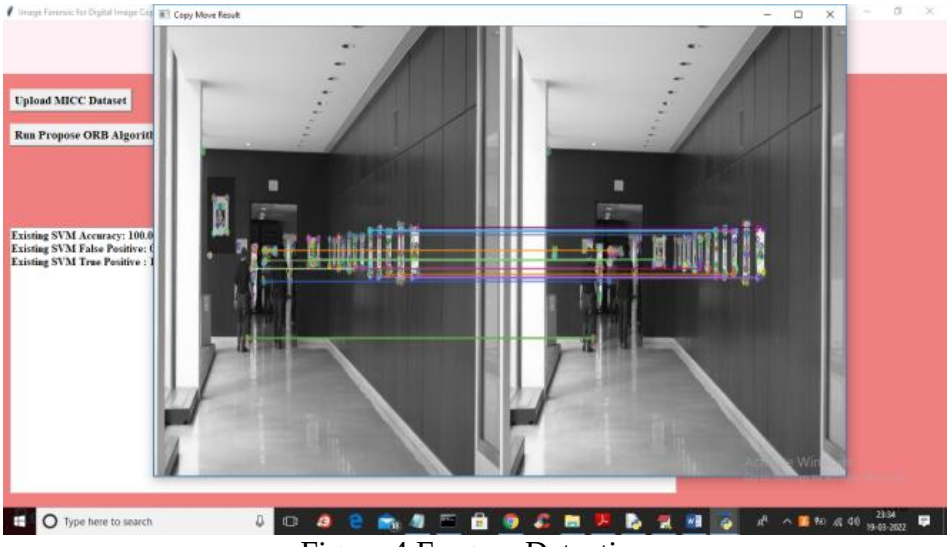

Figure 4 Forgery Detection

Figure 5 Accuracy Comparison

6. CONCLUSION

This paper proposes a CMFD approach that uses Oriented FAST and rotated BRIEF (ORB) for the extraction. Images corrupted in a variety of geometrical ways are used to test the efficacy of the suggested CMFD method. The use of the ORB algorithm as the CMFD helps people to more accurately identify manipulated photos. This might be a huge benefit for a variety of professions, including law and medicine. Therefore, by developing a new method to identify various crimes related to forgery, it aids in the resolution of many issues. Evaluations performed using pictures yielded overall accuracy rates, TPR and FPR rates. These values are taken into consideration to judge how accurately the classification and detection is taken place.

7. REFERENCES

[1] H. Farid, "Exposing digital forgeries from JPEG ghosts," IEEE Trans. Inf. Forensics Secur., vol. 4, no. 1, pp. 154–160, 2009.

[2] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copymove attack detection and transformation recovery," IEEE Trans. Inf. Forensics Secur., vol. 6, no. 3 Part 2, pp. 1099–1110, 2011.

[3] J. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images," Int. J., vol. 3, no. 2, pp. 652–663, 2003.

[4] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth Coll. Tech. Rep. TR2004-515, no. 2000, pp. 1–11, 2004.

[5] H. He, X. Huang, and K. Jun, "Exposing copy-move forgeries based on a dimension-reduced SIFT method," Information Technology Journal, vol. 12, no. 14. pp. 2975–2979, 2013.

[6] M. F. Hashmi, V. Anand, and A. G. Keskar, "A copymove image forgery detection based on speeded up robust feature transform and wavelet transforms," Proc. - 5th IEEE Int. Conf. Comput. Commun. Technol. ICCCT 2014, pp. 147–152, 2015.

[7] M. Calonder, V. Lepetit, C. Strecha, and P. Fua, "BRIEF: Binary robust independent elementary features," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6314 LNCS, no. PART 4, pp. 778–792, 2010.

[8] P. Mishra, N. Mishra, S. Sharma, and R. Patel, "Based on SURF and HAC," vol. 2013, no. July 2008, 2013.