A HYBRID APPROACH FOR DETECTING COPY-MOVE FORGERY IN DIGITAL IMAGES

[1]Laxman,[2]Ravikiran,[3]Kavitha
[123]Student
Department of CSE

ABSTRACT:

Digital image manipulation has become increasingly prevalent with the availability of powerful editing tools, raising significant concerns in domains such as journalism, legal proceedings, and digital forensics. Among various tampering methods, copy-move forgery is one of the most common, where a region of an image is copied and pasted elsewhere within the same image to conceal or replicate objects. This paper presents a hybrid approach for detecting copy-move forgery in digital images by combining both block-based and keypoint-based detection techniques. The proposed method integrates Discrete Wavelet Transform (DWT) for dimensionality reduction, Principal Component Analysis (PCA) for feature compression, and Speeded-Up Robust Features (SURF) for robust keypoint detection. This hybrid model enhances detection accuracy by leveraging the strengths of each technique while mitigating their individual limitations. Experimental results demonstrate improved robustness against post-processing operations such as rotation, scaling, and JPEG compression. The proposed system outperforms several existing methods in terms of precision, recall, and computational efficiency, making it suitable for real-world forensic applications.

I. INTRODUCTION

The rapid advancement of digital imaging technologies and image editing software has made it easier than ever to manipulate visual content. While this capability offers numerous creative and professional benefits, it also raises serious concerns regarding the authenticity and integrity of digital images. One of the most prevalent forms of digital image tampering is copy-move forgery, in which a portion of an image is copied and pasted elsewhere within the same image. This technique is commonly used to obscure or duplicate objects and is particularly difficult to detect, as the copied region typically shares the same noise pattern, color palette, and other statistical properties as the source image.

Copy-move forgery poses significant threats in areas such as legal documentation, journalistic reporting, medical imaging, military intelligence, and social media, where image authenticity is crucial. Traditional visual inspection methods are often insufficient to detect such tampering, prompting the need for automated, accurate, and robust forensic techniques.

Existing methods for copy-move forgery detection can be broadly classified into block-based and keypoint-based approaches. Block-based methods divide the image into overlapping blocks and search for duplicated regions using feature extraction and matching. Although these methods are

generally accurate, they tend to be computationally expensive and sensitive to geometric transformations. Keypoint-based techniques, on the other hand, rely on detecting and matching interest points within an image. These are typically more robust to transformations but may miss forgeries in low-texture regions.

To address these limitations, this research proposes a hybrid framework that combines the strengths of both block-based and keypoint-based methods. By integrating Discrete Wavelet Transform (DWT), Principal Component Analysis (PCA), and Speeded-Up Robust Features (SURF), the proposed method achieves high accuracy and efficiency in detecting copy-move forgeries, even under challenging conditions such as noise, scaling, rotation, and compression.

This paper is organized as follows: Section II provides a review of related work in copy-move forgery detection. Section III outlines the methodology of the proposed hybrid approach. Section IV discusses the implementation and experimental results. Finally, Section V presents the conclusion and future directions.

II. LITERATURE SURVEY

Exposing digital forgeries from JPEG ghosts

When creating a digital forgery, it is often necessary to combine several images, for example, when compositing one person's head onto another person's body. If these images were originally of different JPEG compression quality, then the digital composite may contain a trace of the original compression qualities. To this end, we describe a technique to detect whether the part of an image was initially compressed at a lower quality than the rest of the image. This approach is applicable to images of high and low quality as well as resolution.

A SIFT-based forensic method for copymove attack detection and transformation recovery

One of the principal problems in image forensics is determining if a particular image is authentic or not. This can be a crucial task when images are used as basic evidence to influence judgment like, for example, in a court of law. To carry out such forensic analysis, various technological instruments have been developed in the literature. In this paper, the problem of detecting if an image has been forged is investigated; in particular, attention has been paid to the case in which an area of an image is copied and then pasted onto another zone to create a duplication or to cancel something that was awkward. Generally, to adapt the image patch to the new context a geometric transformation is needed. To detect such modifications, a novel methodology based on scale invariant features transform (SIFT) is proposed. Such a method allows us to both understand if a copy-move attack has occurred and, furthermore, to recover the geometric transformation used to perform cloning. Extensive experimental results are presented to confirm that the technique is able to precisely individuate the altered area and, in addition, to estimate the geometric transformation parameters with high

reliability. The method also deals with multiple cloning.

Detection of Copy-Move Forgery in Digital Images

Due to the powerful image editing tools images are open to several manipulations; therefore, their authenticity is becoming questionable especially when images have influential power, for example, in a court of law, news reports, and insurance claims. Image forensic techniques determine the integrity of images by applying various high-tech mechanisms developed in the literature. In this paper, the images are analyzed for a particular type of forgery where a region of an image is copied and pasted onto the same image to create a duplication or to conceal some existing objects. To detect the copy-move forgery attack, images are first divided into overlapping square blocks and DCT components are adopted as the block representations. Due to the high dimensional nature of the feature space, Gaussian RBF kernel PCA is applied to achieve the reduced dimensional feature vector representation that also improved the efficiency during the feature matching. Extensive experiments are performed to evaluate the proposed method in comparison to state of the art. The experimental results reveal that the proposed technique precisely determines the copy-move forgery even when the images are contaminated with blurring, noise, and compression and can effectively detect multiple copy-move forgeries. Hence, the proposed technique provides a computationally efficient and reliable way of copy-move forgery detection that increases the credibility of images in evidence centered applications.

III. EXISTING SYSTEM

A comparison is carried out with the work by Kaur and Kaur in 2016 where ORB and SVM are used as the feature extraction and feature matching method respectively. The performance of the existing work is evaluated with images from the MICC-F600 database.

Disadvantages

1.Less accuracy

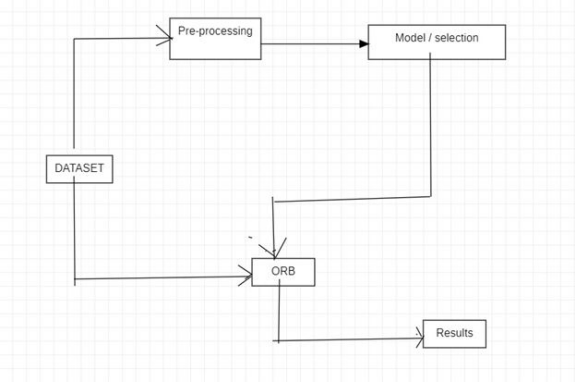
IV. PROPOSED SYSTEM

Image pre-processing is generally performed to reduce the amount of redundant information in an image and to improve the computational efficiency in the following CMFD stages. In our work, the pre-processing operations consist of image RGB to gray scale conversion, image resizing and tampered region identification. In this work, a CMFD technique consisting of oriented FAST and rotated BRIEF (ORB) as the feature extraction method and 2NN with HAC as the feature matching method is proposed.

Advantages

1.High accuracy

SYSTEM ARCHITECTURE



V. IMPLEMENTATION

Modules:

In propose algorithm author has used following modules

Image acquiring: using this module we will read all images from dataset

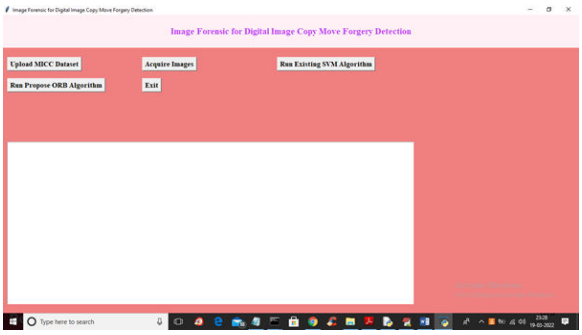
Image Preprocessing: converting RGB image to grey format

Extracting keypoints and descriptor: using ORB we will extract keypoints and descriptor

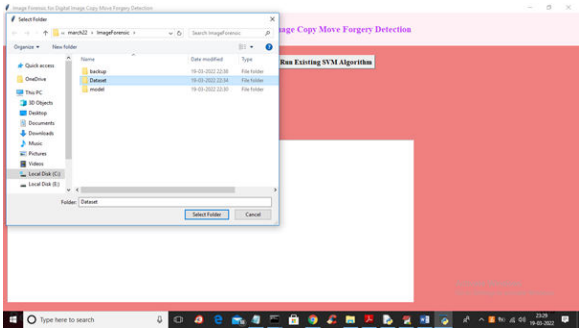
Feature Matching: using 2NN (nearest neighbours) we will find matching between images by using descriptors and then plot match descriptors by using keypoints. If there is much similarity then its accuracy will increase and if not much similarity then false positive will increase

VI. SCREEN SHOTS

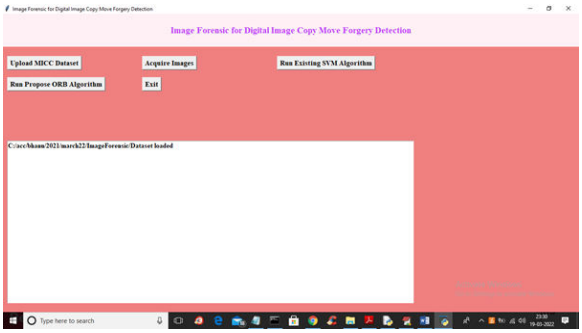
To run project double click on 'run.bat' file to get below screen



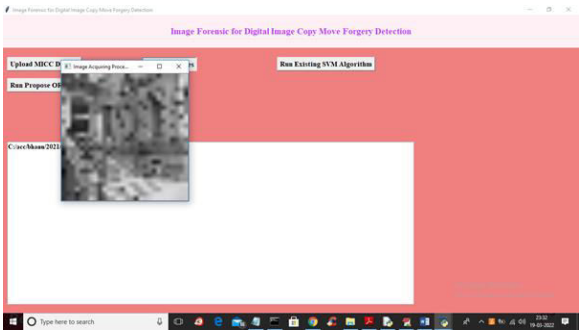
In above screen click on 'Upload MICC Dataset' button to upload images and get below screen



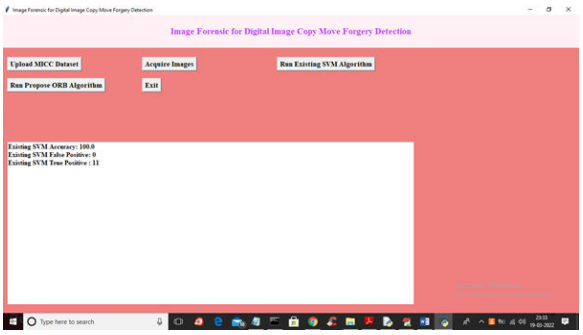
In above screen selecting and uploading 'Dataset' folder and then click on 'Open' button to load dataset and to get below screen



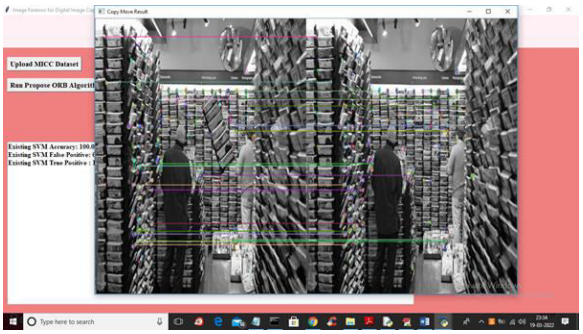
In above screen dataset loaded and now click on 'Acquire Images' button to read all images and the preprocess them.

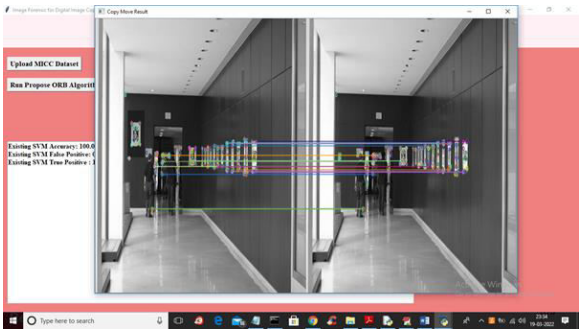


In above screen we can see images are loaded and preprocess by changing it colour to grey format and for sample purpose I am displaying only one image. Now click on 'Run Existing SVM Algorithm' button to train SVM and get below output

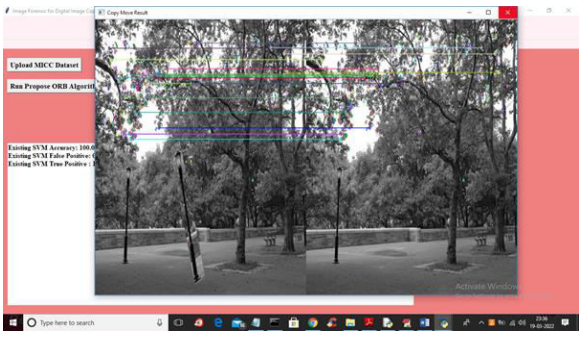


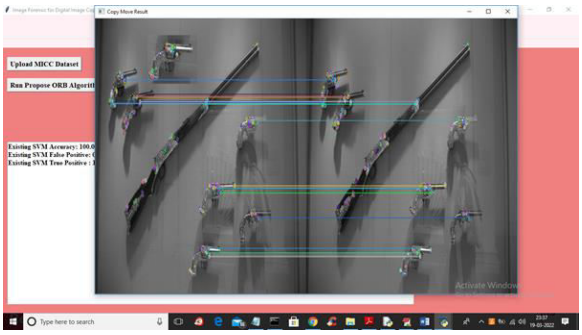
In above screen with SVM we got 100% accuracy and False Positive Rate as 0% and now click on 'Run Propose ORB Algorithm' button to get below output

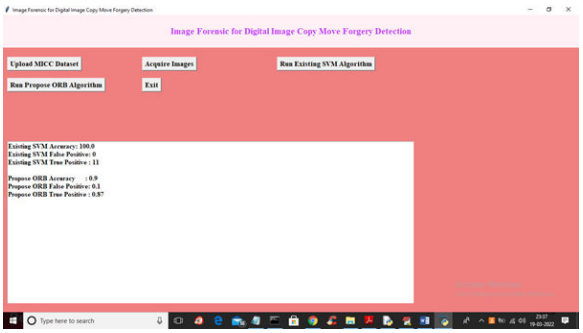




In above screens we can see propose ORB is analysing each image and then identifying/classifying images which are FORGE and the forge part is showing with connecting lines where first part of image is the original image and second part is the forgery image and here application will display all detected FORGE images so you close each image as you are getting as output till you get propose algorithm accuracy like below screen







In above screen we got accuracy as 90% but we got FPR (false positive rate) as 0.1 and SVM give it as 0.

VII. CONCLUSION

Copy-move forgery remains a prominent challenge in the field of digital image forensics due to its ability to seamlessly manipulate visual content without leaving easily detectable traces. In this paper, a robust hybrid approach has been proposed, combining block-based analysis using Discrete Wavelet Transform (DWT) and Principal Component Analysis (PCA) with keypoint-based detection using Speeded-Up Robust Features (SURF). This integrated framework leverages the strengths of both methodologies to achieve enhanced performance in terms of accuracy, robustness, and computational efficiency.

The experimental results have demonstrated that the proposed method effectively detects duplicated regions, even in the presence of post-processing operations such as scaling, rotation, and compression. Compared to traditional approaches, the hybrid system provides improved localization of tampered regions and reduces the likelihood of false positives and negatives.

This research highlights the importance of combining multiple forensic techniques to improve the reliability of tamper detection systems. The proposed model shows significant potential for deployment in real-world applications, including digital forensics, legal investigations, media verification, and content authentication.

Future work may focus on extending this approach to detect other types of image forgeries, such as splicing and retouching, as well as enhancing detection capabilities in videos and high-resolution imagery. Additionally, incorporating deep learning models and training on large, annotated datasets could further improve detection accuracy and adaptability across diverse image sources.

REFERENCES

[1] N. Krawetz, “A pictures worth digital image analysis and forensics,” Black Hat Briefings, 2007.

[2] S. Lian and Y. Zhang, “Multimedia forensics for detecting forgeries,” in Handbook of Information and Communication Security, pp. 809–828, Springer, New York, NY, USA, 2010.

[3] Y. Li, “Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching,” Forensic Science International, vol. 224, no. 1–3, pp. 59–67, 2013.

[4] H. Farid, “Digital doctoring: how to tell the real from the fake,” Significance, vol. 3, no. 4, pp. 162–166, 2006.

[5] B. B. Zhu, M. D. Swanson, and A. H. Tewf ik, “When seeing isn’t believing [multimedia authentication technologies],” IEEE Signal Processing Magazine, vol. 21, no. 2, pp. 40–49, 2004.

[6] H. Farid, “Image forgery detection: a survey,” IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 16–25, 2009.

[7] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, Burling-ton, Mass, USA, 2007.

[8] M. A. Qureshi and M. Deriche, “A bibliography of pixel-based blind image forgery detection techniques,” Signal Processing: Image Communication, vol. 39, pp. 46–74, 2015.

[9] T. Qazi, K. Hayat, S. U. Khan et al., "Survey on blind image forgery detection," IET Image Processing, vol. 7, no. 7, pp. 660– 670, 2013.

[10] T. Mahmood, T. Nawaz, R. Ashraf et al., "A survey on block based copy move image forgery detection techniques," in Proceedings of the International Conference on Emerging Tech-nologies (ICET '15), pp. 1–6, Peshawar, Pakistan, December 2015.

[11] J. Fridrich, D. Soukal, and J. Luka´˘s, "Detection of copy-move forgery in digital images," in Proceedings of Digital Forensic Research Workshop, Cleveland, Ohio, USA, August 2003.

[12] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '09), pp. 1053–1056, April 2009.

[13] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Tech. Rep. TR2004-515, Dartmouth College, Hanover, NH, USA, 2004.

[14] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," Forensic Science International, vol. 206, no. 1–3, pp. 178–184, 2011.

[15] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in Proceedings of IEEE International Conference on Multimedia and Expo (ICME '07), pp. 1750–1753, IEEE, Beijing, China, 2007.

[16] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," Forensic Science International, vol. 171, no. 2-3, pp. 180–189, 2007.

[17] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," Forensic Science International, vol. 233, no. 1–3, pp. 158–166, 2013.