# FORENSIC TECHNIQUES FOR IDENTIFYING COPY-MOVE MANIPULATIONS IN DIGITAL IMAGES

**BHASKAR RAO KASIREDDI,** Assistant Professor, Department of CSE, Avanthi's Research & Technological Academy, Bhogapuram,Vizianagaram, Email- bhaskarkasireddi@gmail.com

**SAILAJA BODDU**, Assistant Professor. Department of CSE, Avanthi's Research & Technological Academy, Bhogapuram,Vizianagaram, Email-sailaja.chris@gmail.com

**GAYATRI YANDRAPU,** Assistant Professor. Department of CSE, Avanthi's Research & Technological Academy, Bhogapuram,Vizianagaram, Email- gayatriyandrapu2@gmail.com

**PILLA JAGADAMBA ALEKHYA ,** Assistant Professor. Department of CSE, Avanthi's Research & Technological Academy, Bhogapuram,Vizianagaram, Email-alekhyapj@gmail.com

**LAVANYA YEDLA**, Assistant Professor. Department of CSE, Avanthi's Research & Technological Academy, Vizianagaram, Email-lavanyayd@gmail.com

**ABSTRACT:**

The development of picture editing software over the past several years has led to the establishment of a topic of active research in the field of digital image fraud detection. Passive forgery detection, or Copy Move Forgery Detection (CMFD), is the focus of this work. Using the copy move approach, it is applied to photographs that have been altered. The proposed feature extraction method for a CMFD technique that uses 2 Nearest Neighbor (2NN) with Hierarchical Agglomerative Clustering (HAC) as the feature matching method is Oriented Features from Accelerated Segment Test and rotated Binary Robust Independent Elementary Features (Oriented FAST and rotated BRIEF). It is suggested that this method be used for CMFD. The suggested CMFD method was tested on pictures that were subjected to different geometrical attacks at different times. The suggested approach for evaluations, which utilizes images from the MICC-F600 and MICC-F2000 databases, can achieve an overall accuracy rate of 84.33% and 82.79%, respectively. When applied to photos that had been manipulated in a number of ways, such as rotated, magnified, or object translated, the True Positive Rate for forgery detection was above 91%.

## I. INTRODUCTION

Nowadays, with the widespread availability of image altering programs like Adobe Photoshop, tampering with digital images has become simple. With the development of picture editing software, it is now possible to alter images without causing noticeable alterations or deteriorating their quality. Images are now used as historical records and supporting evidence in a variety of sectors, including forensic investigation, law enforcement, journalistic photography, and medical imaging. This is concerning.

Furthermore, modified photographs have frequently been published in the press or on social media. One example is the July 9,

2008, broadcast of manipulated images of an Iranian missile launch by Sepah press, the Iranian Revolutionary Guard's official media outlet. Fig. 1's manipulated image is intended to inflate the nation's military prowess. The counterfeit was discovered a day later when the same source published a second image with different content that was taken from the same perspective at nearly the same time. The scientific community is not immune to picture manipulation either. 20% of accepted submissions in the Journal of Cell Biology, according to Farid et al., contain improper figure manipulation. Image tampering and detection have therefore attracted a lot of attention since modified images might be used maliciously to falsify their meaning.

## II. LITERATURE SURVEY

Identifying digital fakes from JPEG ghosts

It is frequently required to merge many photos while producing a digital fraud, such as when compositing the head of one person onto the torso of another. The digital composite might have remnants of the original JPEG compression quality if these pictures had differing compression settings at first. We therefore outline a method for determining if a portion of an image was originally compressed at a lesser quality than the remainder of the image. This method works with both high- and low-quality and high-resolution photos.

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

Determining the authenticity of a given image is one of the main issues in image forensics. In situations where photos are utilized as fundamental evidence to sway judgment, such as in a court of law, this can be an extremely important task. The literature has produced a number of technology tools to perform such forensic analysis. This study examines the issue of determining whether a picture has been forged; specifically, it looks at situations where a portion of an image is duplicated and then pasted into another region to make a duplicate or to erase an uncomfortable element. The picture patch usually requires a geometric adjustment to fit the new context. A unique methodology based on the scale invariant features transform (SIFT) is proposed to detect such alterations. This technique enables us to determine whether a copy-move attack has taken place and, moreover, to retrieve the geometric transformation that was utilized to carry out the cloning process. Numerous experimental findings are provided to demonstrate the method's capacity to accurately identify the changed region and, additionally, to very reliably estimate the geometric transformation parameters. The technique also addresses multiple cloning.

Finding Copy-Move Forgeries in Digital Pictures

Image forensic techniques use a variety of high-tech mechanisms developed in the literature to determine the integrity of images. Because of the powerful image editing tools, images are susceptible to various manipulations, making their authenticity questionable, especially when images have influential power, such as in news reports, insurance claims, and court cases. In order to make a duplicate or hide some existing items, a portion of an image is

copied and pasted onto another image. This sort of forgeries is examined in this work. DCT components are used as the block representations after images are initially split into overlapping square blocks in order to identify the copy-move forgery attempt. Given the high dimensionality of the feature space, a lower dimensional feature vector representation is obtained by using the Gaussian RBF kernel PCA, which also increases feature matching efficiency. The suggested approach is evaluated against the state of the art through extensive experiments. According to the experimental results, the suggested method can successfully identify multiple copy-move forgeries and accurately identify the forgery even when the photos are tainted by noise, blurring, and compression. In order to improve the trustworthiness of photographs in evidence-based applications, the suggested strategy offers a computationally effective and trustworthy method of copy-move forgery detection.

## III. EXISTING SYSTEM

A comparison is made with the work of Kaur and Kaur (2016), in which the feature extraction and matching methods are ORB and SVM, respectively. The MICC-F600 database's photos are used to assess the performance of the current task.

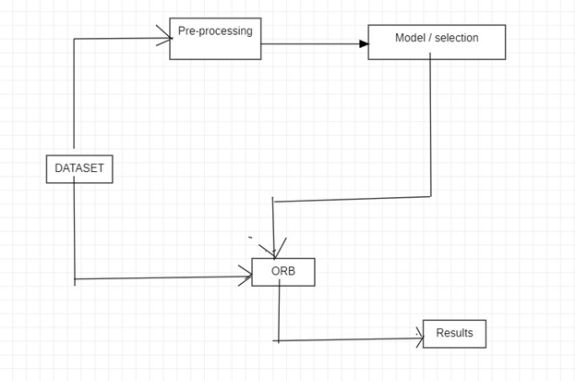
Negative aspects

1. A decrease in precision

## IV. PROPOSED SYSTEM

Reducing superfluous information in a picture and increasing computational efficiency in the subsequent CMFD phases are the two main goals of image pre-processing. Image scaling, tampered region recognition, and RGB to grayscale conversion are the pre-processing steps in our work. An approach to CMFD is shown in this study, which uses oriented FAST and rotating BRIEF (ORB) for feature extraction and 2NN with HAC for feature matching.

## SYSTEM ARCHITECTURE




## V. IMPLEMENTATION

Modules: The author has utilized the following modules in the suggested algorithm.

Getting images: This module will be used to read every image from the dataset.

Pictures Getting ready: RGB to greyscale picture conversion

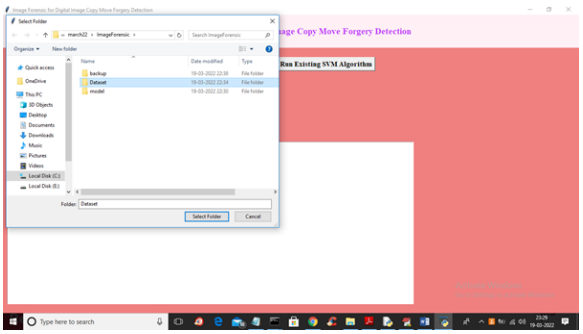
The process of extracting important points and descriptors will be carried out utilizing ORB.

Feature Matching: descriptors will be used to find picture matching using 2NN (nearest neighbors), and keypoints will be used to plot the descriptors that match. Its accuracy will rise if there is a lot of similarity, and false positives will rise if there is none.

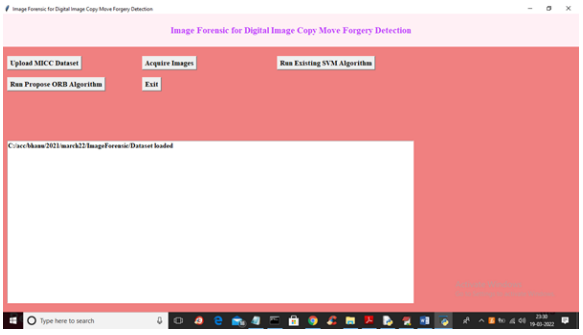
## VI. SCREEN SHOTS

To launch the project, double-click the "run.bat" file to see the screen below.

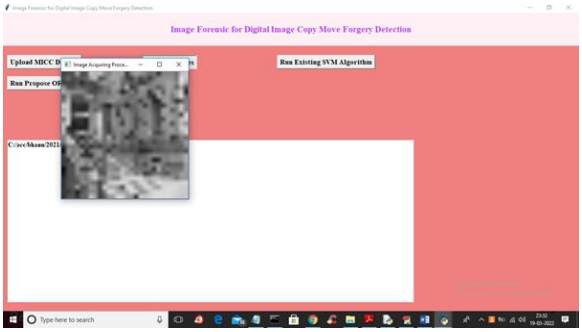

To upload photos and obtain the screen below, click the "Upload MICC Dataset" button in the above screen.



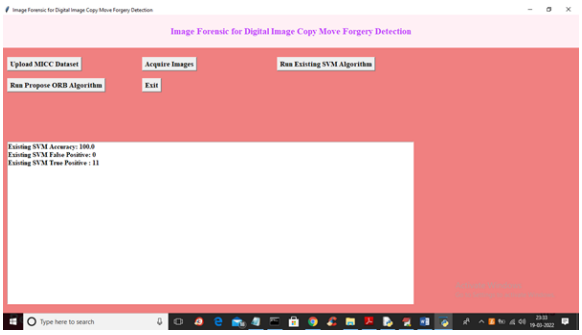

To load the dataset and view the screen below, choose and upload the "Dataset" folder in the above page, then click the "Open" button.



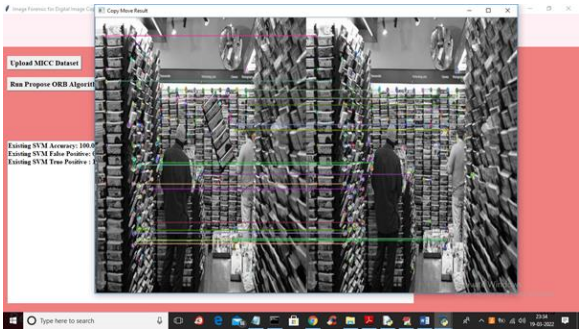

Click the "Acquire Images" button to read and preprocess all of the images after the dataset has loaded in the screen above.

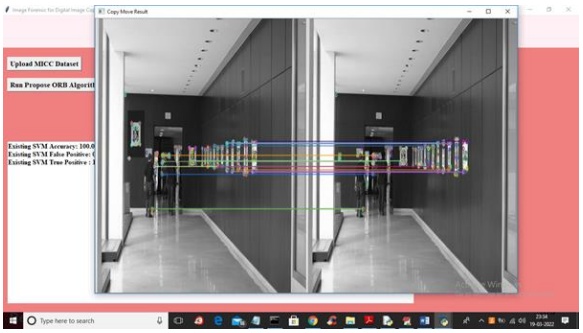



Images are loaded and preprocessed by turning their color to grey, as shown in the screen above. I'm only showing one image for illustration purposes. Click "Run Existing SVM Algorithm" to train SVM and obtain the output below.

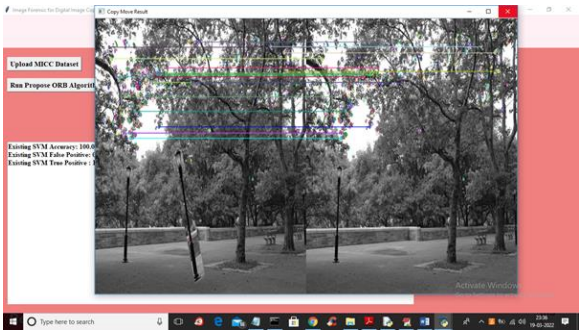


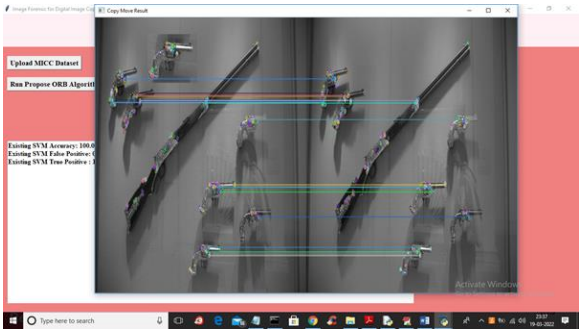

Click the "Run Propose ORB Algorithm" button to obtain the output below. In the SVM screen above, we obtained 100% accuracy and 0% False Positive Rate.

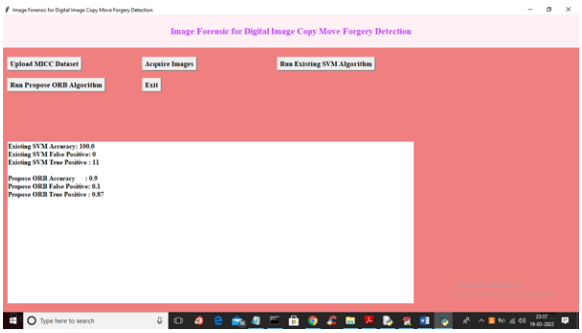




In the screens above, we can observe that the proposed ORB is analyzing each image and then identifying/classifying those that are FORGE. The forge portion of the image is displayed with connecting lines, where the original image is in the first part and the forgery image is in the second. The application will then display all of the detected FORGE images; you must close each image as you receive the output until you obtain the proposed algorithm accuracy, as shown in the screen below.








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

In the screen above, we obtained 90% accuracy; however, the false positive rate (FPR) was 0.1 and the SVM gave it Our goal in this research was to identify methods for ensuring that copy-move forgeries in digital photographs are detected. Reducing the feature length dimension and identifying the forged items in the suspected image were the primary considerations of this work. In order to extract features that take into account the similar things present in the forged image, we have utilized DCT and kernel PCA. This method also functions without a digital signature or watermark and doesn't require any previous information to be included in the image. According to the findings, the suggested method not only successfully identifies numerous copy-move forgeries and accurately pinpoints the forged regions, but it also exhibits good resilience to postprocessing techniques including compression, AWGN, and Gaussian blurring. Furthermore, the suggested technique's detection performance is comparatively good in terms of average TPR and FPR when compared to the current standard copy-move forgery systems [11–14].

**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. Tewfik, "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.