International Journal of Psychosocial Rehabilitation, Vol. 23, Issue 04, 2019
ISSN: 1475-7192

DETECTING DIGITAL IMAGE COPY-MOVE FORGERY WITH IMAGE FORENSICS

[1]Guguloth Laxman,[2]Sanga Ravikiran,[3]Valasa Kavitha,[4]Shaik Mahamood

ABSTRACT

Over the last several years, the growth of photo editing software has resulted in the emergence of a subject of active research in the field of digital image fraud detection. Copy Move Forgery Detection (CMFD), also known as passive forgery detection, is the subject of this study. It is used to photographs that have been manipulated via the use of the copy move technique. Oriented Features from Accelerated Segment Test and rotated Binary Robust Independent Elementary Features (Oriented FAST and rotated BRIEF) are proposed as the feature extraction method for a CMFD technique that uses 2 Nearest Neighbor (2NN) with Hierarchical Agglomerative Clustering (HAC) as the feature matching method. This technique is proposed as a CMFD technique. The proposed CMFD approach was evaluated using images that were exposed to a variety of geometrical assaults at various points in time. Using the proposed method for assessments, which makes use of photographs from the MICC-F600 and MICC-F2000 databases, it is possible to attain an overall accuracy rate of 84.33% and 82.79% respectively. The True Positive Rate for forgery detection was more than 91% when applied to photographs that had been altered in a variety of ways, including using different degrees of rotation, magnification, and object translation.

INTRODUCTION

In this day and age, digital image tampering has been made easy with widely available image editing softwares, such as Adobe Photoshop. The advancement of image editing softwares has reached a level such that image tampering can be done without degrading its quality or leaving obvious traces. This is alarming as images are now being presented as supporting evidence and historical records in various fields, such as in forensic investigation, law enforcement, journalistic photography and medical images.

Moreover, in many instances, tampered images have appeared in the news or social media, such as the manipulated images of Iranian missile test released on July 9, 2008 by Sepah News, the official media arm of Iran's Revolutionary Guard. The tampered image, shown in Fig. 1 is aimed at exaggerating the country's military capabilities. The forgery is detected a day later when the same source released another image taken from the same angle at almost the same time, but with different content. The scientific community is also not spared from image tampering. Farid et al. stated that 20% of accepted manuscripts of the Journal of Cell Biology contains inappropriate figure manipulation. Hence, image tampering and detection have garnered substantial attention as manipulated images can be used to misrepresent their meaning with malicious intent.

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,

[123]Assistant Professor, Department of CSE, Abdul Kalam Institute of Technological Sciences, Kothagudem, Telangana

[4]Student, Department of CSE, Abdul Kalam Institute of Technological Sciences, Kothagudem, Telangana

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.

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

PROPOSED SYSTEM

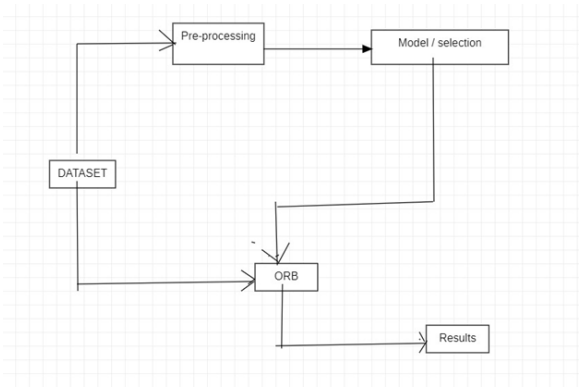
Image pre-processing is generally performed to reduce the amount of redundant information in an image and to improve the computational efficiency in the following CMFD stages. In our work, the pre-processing operations consist of image RGB to gray scale conversion, image resizing and tampered region 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



IMPLEMENTATION

Modules:

In propose algorithm author has used following modules

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

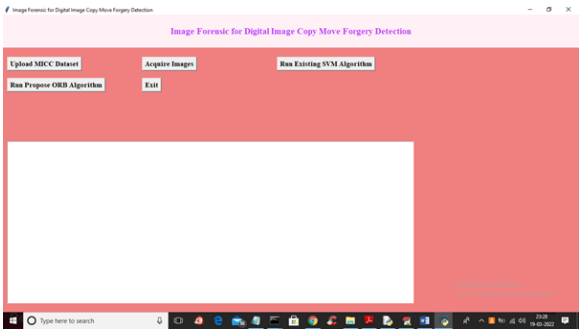
Image Preprocessing: converting RGB image to grey format

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

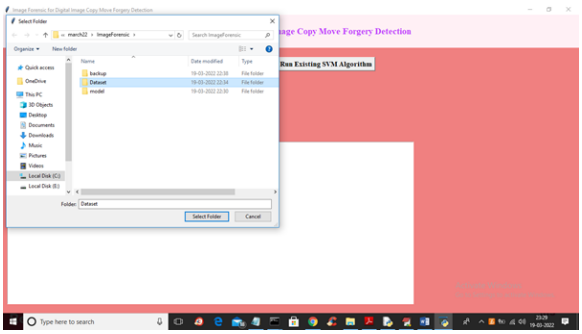
Feature Matching: using 2NN (nearest neighbours) we will find matching between images by using descriptors and then plot match descriptors by using keypoints. If there is much similarity then its accuracy will increase and if not much similarity then false positive will increase

V. SCREEN SHOTS

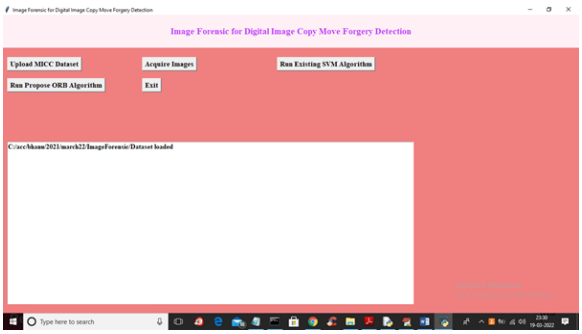
To run project double click on ‘run.bat’ file to get below screen



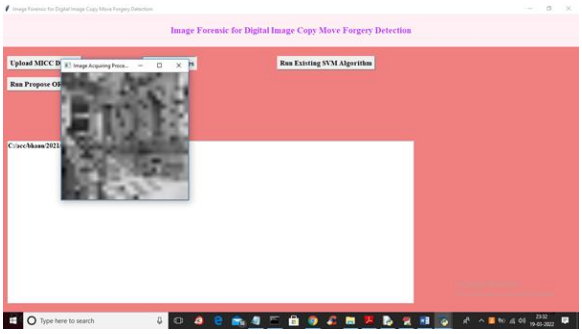
In above screen click on 'Upload MICC Dataset' button to upload images and get below screen



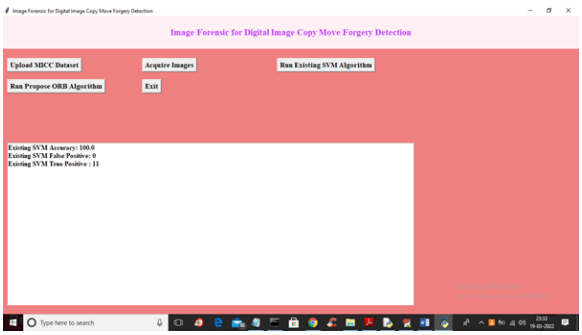
In above screen selecting and uploading 'Dataset' folder and then click on 'Open' button to load dataset and to get below screen



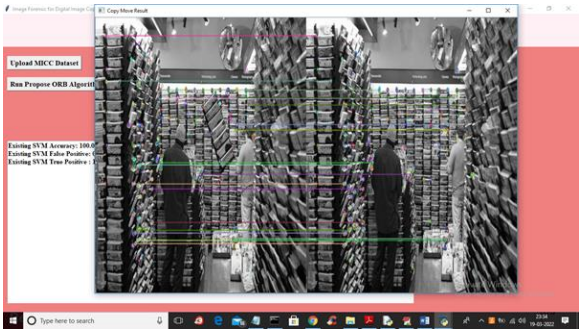
In above screen dataset loaded and now click on 'Acquire Images' button to read all images and the preprocess them.

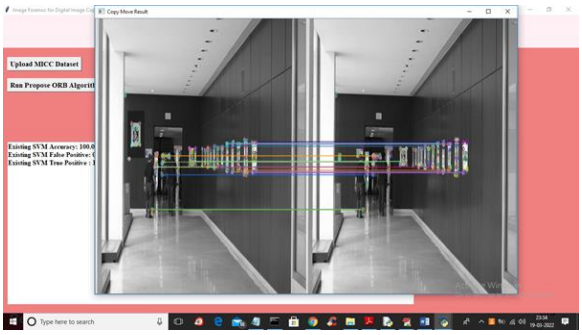


In above screen we can see images are loaded and preprocess by changing it colour to grey format and for sample purpose I am displaying only one image. Now click on 'Run Existing SVM Algorithm' button to train SVM and get below output

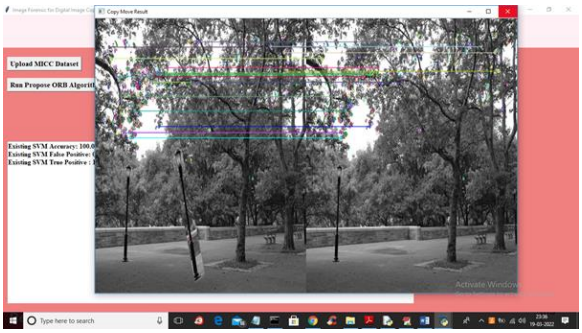


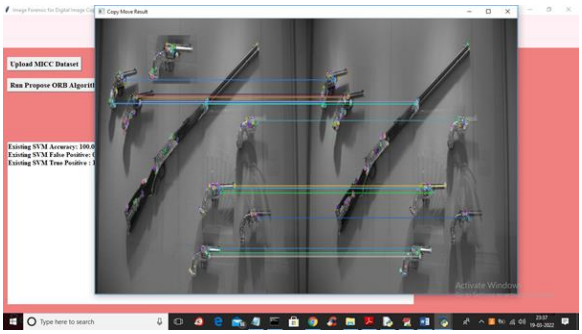
In above screen with SVM we got 100% accuracy and False Positive Rate as 0% and now click on 'Run Propose ORB Algorithm' button to get below output

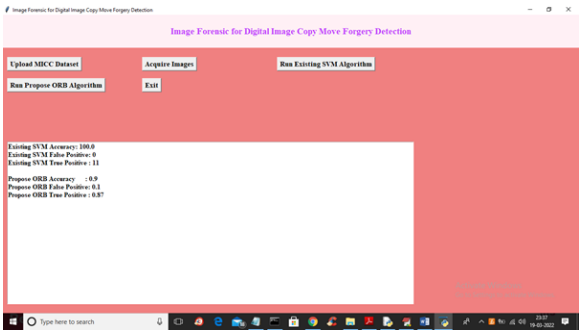




In above screens we can see propose ORB is analysing each image and then identifying/classifying images which are FORGE and the forge part is showing with connecting lines where first part of image is the original image and second part is the forgery image and here application will display all detected 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.

CONCLUSION

In this paper, we focused on finding the ways through which we can assure the detection of copy-move forgery in digital images. The main consideration of this paper was to reduce the dimension of the feature length and find the forged objects in the suspected image. Therefore, we have applied DCT and kernel PCA for feature extraction which considers the identical objects found in the forged image. Furthermore, this technique does not require any prior information embedded into the image and works in the absence of digital signature or digital watermark. From the results, a conclusion can be drawn which is that the proposed technique not only effectively detects multiple copy-move forgeries and precisely locates the forged areas but also has nice robustness to postprocessing operations such as Gaussian blurring, AWGN, and compression. Moreover, comparing the detection performance of the proposed technique with existing standard copy-move forgery systems [11–14], the results of our technique are reasonably good in terms of average TPR and FPR.

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.