Image Forensic For The Detection of Digital Image Copy Move Forgery

M. SHIREESHA [1], P. KEERTHI [2], M. NANDINI [3], V. PRASANTHI [4], DR. A. KISHORE REDDY [5]

[1]UG Scholar, Dept of ECE, Andhra Engineering College, Atmakur, AP, India.
[2]UG Scholar, Dept of ECE, Andhra Engineering College, Atmakur, AP, India.
[3]UG Scholar, Dept of ECE, Andhra Engineering College, Atmakur, AP, India.
[4]UG Scholar, Dept of ECE, Andhra Engineering College, Atmakur, AP, India.
[5]Professor, Dept of ECE, Andhra Engineering College, Atmakur, AP, India.

ABSTRACT

Forensic investigations, for example, frequently rely on images as part of their evidence. Investigations could be negatively affected by images that are not legitimate, even when they are meant to be actual images. Image forgery detection is crucial and sensitive in these applications. Methods that partition images into regular chunks and then determine the match between each block of the entire image are known as block-based. Despite the fact that it is computationally expensive, this approach is shown to be more accurate. These methods are different from those that compute the image's keypoints and look for a match between them. Using a copy move, the image will have the greatest number of corresponding regions with keypoint matches. Computationally, this is a more efficient way to do things, but accuracy suffers because of it Uses both keypoints and blocks to identify forgeries in the proposed approach. The amount of matching SIFT keypoints helps us discover important irregular blocks, and the similarity of these blocks is assessed as a result. An adaptive threshold is used on the number of keypoint matches to determine whether or not the image is forged, and it is wisely decided whether or not to go for block-based matching strategy for each block. We demonstrate that the suggested method has a higher detection rate without sacrificing the merits of keypoint-based forgery detection in terms of computing complexity.

1. INTRODUCTION

Adobe Photoshop and other readily available image-editing programmes have made digital picture tampering easy in this day and age. As picture editing software has advanced, it is now possible to alter images without affecting their quality or leaving any visible evidence. In disciplines including forensics, law enforcement, news photography, and medical imaging, photographs are now being used as supporting evidence and historical records. Tampered photographs have also surfaced in news reports and on social media in several occasions, such as the distorted images of an Iranian missile launch issued by Sepah News, the official media arm of Iran's Revolutionary Guard, on July 9, 2008.. It is a deliberate attempt to exaggerate the military capabilities of the country depicted in Fig. 1. It was only a day later that the same source provided another image shot from the same angle, but with different content, that the forgery was spotted. Image alteration affects everyone, even those in the scientific community. According to the Journal of Cell Biology, 20 percent of accepted publications feature incorrect figure modification. As a result, the detection and tampering of modified photographs have attracted a great deal of attention The following is the structure of this document: Copy-Move Forgery Detection approaches based on blocks and keypoints are the subject of Section II, which summarises current developments in the field. Section III covers the study approach for the proposed CMFD strategy, focusing on SURF and Oriented FAST and rotated BRIEF (ORB) as the feature extraction methods and 2 Nearest Neighbor (2NN) and Hierarchical Agglomerative Clustering (HAC) as the feature matching method. Our suggested CMFD technique is presented in Section IV, along with a review of our contributions and accomplishments. Finally, we summarise our findings and discuss possible next projects.

2. LITERATURE SURVEY

Images are divided into overlapping regular shaped blocks via block-based algorithms, as described in the introduction. In blocks that follow each other, a significant chunk of one block is reproduced in the following block. Block-level features are compared among the blocks once they have been separated. The structure for block-based algorithms is the same, but the feature and metric used for block matching is different. The quantized discrete cosine transform was utilised as a block feature by Fridrich et al. Principal component analysis is used by Popescu and Farid to minimise the dimensions of image blocks (PCA). A combination of

RGB colour components and information about orientation is used by Luo et al. Singular value decomposition (SVD) and discrete wavelet transform are both used by Li et al. to construct a block feature from an SV vector (DWT). There were 24 blur invariant moments employed by Mahdian and Saic. Singular values of a reduced rank approximation are used by Kang and Wei. The Fourier Mellin transformation of the picture blocks is calculated by Bayram et al. If the block centre is the centre of an imaginary circle, the average intensity can be calculated. The average grey value is calculated by Lin et al. for each block and sub-block. The Zernike moments of each block are calculated by Ryu et al. Each block's information entropy is calculated by Bravo Solario and Nandi. These algorithms have low recall rates due to the regular block shapes and their inherent complexity, which means they cannot identify fraud when the forgery is combined with an image alteration.

The photos' keypoints are located using keypoint-based approaches. Determine the degree to which each keypoint in the image bears a resemblance to any of the other key points. If the similarity between two keypoint regions exceeds a predetermined level, the keypoint area in question is assumed to be forged. There are two approaches that can be used to discover the most essential parts of an image, one of which is the Scale Invariant Feature Transform (SIFT). SIFT is used to determine the SIFT-key vector's points and find the SIFT-similarity. vector's Use SURF to locate the most important points. The forging region may not exactly match the keypoint region that was matched. Some regions of an image may have more than one fake occurring at the same time, which means that forgery detection will not be possible in those regions. When compared to block-based approaches, the detection accuracy of this algorithm will be lower. Because it avoids exhaustive searching and has a high recall rate for photos with altered copy move image patches, the complexity is clearly reduced.

Image forgery can also be detected using a combination of block-based and keypoint-based approaches. Block-based and feature key point-based approaches are used in these algorithms to achieve the best of both worlds. The image is divided into non-overlapping units using such an approach. Key points for each block should be computed. Afterwards, compare the blocks by comparing their main points. The forged region is detected based on a predefined similarity criterion. Image blocks are created by using adaptive over-segmentation and the SIFT technique to discover feature key points.

When the copy-move occurred in the same picture block and the number of image key points is less, the detection accuracy will be lower. An upgraded variant of existing block-based and feature key point approaches is proposed for increased accuracy without much complexity. Images are segmented into non-overlapping irregular blocks using the adaptive over-segmentation algorithm described by Pun et al. Find the SIFT key points for each block and count the number of key points that match. A copy move is identified and the image is found to be forged if the number of key point matches for two blocks exceeds a precomputed threshold. Additional procedures may be necessary if there are no key point matches, in which case the image can be considered unchanged. Block-based technique is applied to a regular area around matching key points rather than to the entire image in order to reduce computational complexity.

3. PROPOSED SYSTEM

Five primary phases are included in the standard workflow: picture acquisition, pre-processing and feature extraction and matching.

In the first place, the acquisition of images:
Images from the MICCF600 and MICC-F2000 datasets are used to test the proposed CMFD approach in our proposed work. All of the photographs in both datasets have been altered in some way, either by translation or rotation, symmetric or asymmetric scales, or a combination of the three. The MICC-F2000 database includes a number of geometrical attacks, as shown in Table I. For each assault, we have, SX, and SY to indicate the distinct scaling factors in x and y axis, as well as for the degree of rotation.

B. Pre-processing of images Images are typically pre-processed to reduce the quantity of redundant information and increase computing efficiency in the subsequent CMFD phases. Pre-processing in our work includes image RGB to grayscale conversion, image scaling, and the identification of tampered regions in the image

CMFD with Oriented FAST and Rotated BRIEF Orientation (ORB) ORB (Oriented FAST and Rotated BRIEF) [11] is a binary descriptor for feature extraction that makes use of oFAST keypoints and rBRIEF features. In a standard binary descriptor, the sampling pattern, orientation compensation, and sampling pairs are the three most important parts of the algorithm. No precise sample pattern is used in the ORB technique. For orientation compensation and sampling pairs, oFAST moments and rBRIEF learning pairs are used. One way to gather orientation information for an interest point is to use an intensity centroid that Rublee et al. [11] introduced with ORB. ORB is a descriptor that can produce uncorrelated feature vectors, which means that each element of the feature vector has distinct information. The significant variance of ORB's descriptors suggests that the features respond differently to different inputs, enhancing its discriminative power even further. First, focus on the FAST essential points. FAST detector is used by the ORB algorithm to locate interesting areas inside a picture. In real-time systems, FAST is the method of choice for locating interest spots. It is a feature of rapid segment testing. It is necessary to compare the brightness of the central pixel's neighbours on a fixed-radius circle in order to generate FAST keypoints.

Using Harris corner measure, the top N interest points are ranked after detecting a collection of interest points. The cheap processing cost of FAST does not make it scalability or rotation invariant. As a result, a scale pyramid of the image is used to produce FAST features at each level in order to ensure scale invariance.

BLOCK DIAGRAM:

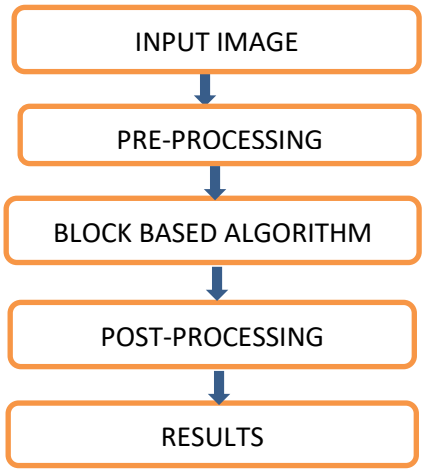

Fig 1: Block Diagram

It is proposed that the grayscale image be converted into a number of super pixels using the SLIC algorithm. The recall rate will be improved by SLIC's division of images into relevant super pixels. In order to detect forgery, SIFT keypoints are identified for each block and utilised as the primary check. Euclidean distance is used to match the critical points. There are a number of matching keypoints between the blocks that will be utilised to identify the fabricated regions. We can classify a picture as "Forged," "Not-Forged," or "Forgery Suspected" based on the key points and thresholds that match. There is a possibility of forgery if the number of matches is more than 0 but less than the threshold. Instead of applying the block based method to the entire image, focus on the region surrounding the matched keypoints while working with this type of image. When all else fails, use Pun et almorphological .'s procedures to estimate the faked area. The following subsections cover each of these steps in greater detail. A. The Preparation of the Materials The image is divided into meaningful chunks in the pre-processing step. Traditionally, photos are segmented into overlapping blocks of the same size and identical structure in block-based forgery detection systems. If the block size is small, this strategy will yield better results, but the complexity of the programme will grow. It has been suggested that an adaptive over segmentation method might be used to reduce the complexity without sacrificing much accuracy. With the simple linear iterative clustering technique (SLIC), pictures are divided into blocks. Using the K-means clustering approach, this algorithm will break down the image into meaningful groups. An picture will be clustered into k groups via SLIC. After that, split the photos into relevant regions by combining

similar superpixels. This will improve the accuracy of the forgery area and reduce the amount of work required. Cluster size can be determined based on the image's texture. The segment size might be large for a smooth textured image or tiny for a detailed textured image. The texture of an image is used to determine the cluster's starting size. Pun et alenergy .'s distribution of the image is used to calculate the starting size of SLIC. It is determined if an image's low-frequency energy distribution is more than 50% of the frequency energy, then Eq.1 is used, else Eq.2 is used, where H x W denotes the image's height and width. It is important to keep in mind that smooth images have larger blocks, while detailed images have smaller blocks, according to the equations Eq.1 and 2. This is the initial size of the object (1) In the beginning, the sizeinitial is equal to the sum of the dimensions of H and W divided by 0.01. (2) B. Detection of Keypoints Images will be divided into meaningful superpixels through the process of segmentation. Blocks and critical points are specified for each superpixel, which represents a block. According to Christlein et al., SIFT is an excellent feature detector that is invariant to geometric transformations such as scale, translation, and rotation as well as brightness and illumination. Key spots will be identified utilising SIFT technique as part of our proposed method. Instead of focusing on the image as a whole, we'll focus on each individual block and use that to identify the block's feature. Normalized SIFT descriptor describes essential points in terms of location, scale and orientation in a 128-dimensional space.

4. RESULTS AND DISCUSSION

Fig 2: input image

Fig 3: block processing image

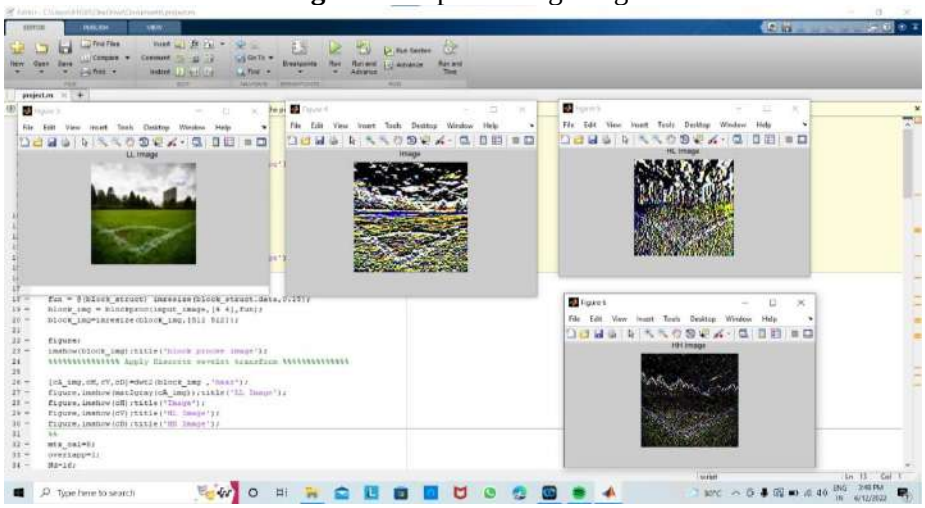

Fig 4: DWT outputs

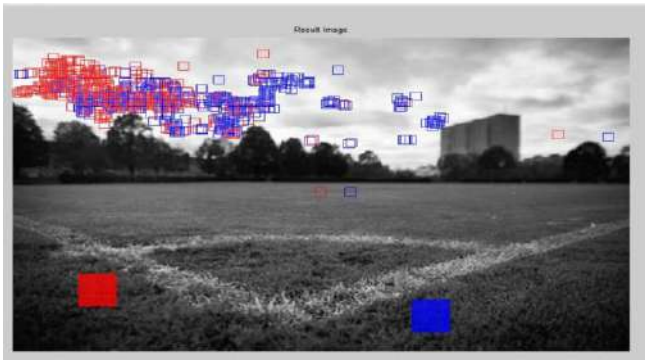

FIG 5: OUTPUT IMAGE

5. CONCLUSION

It has been demonstrated that a block-based detection strategy can achieve high detection accuracy without sacrificing the computational advantages and high-recall rates of Keypoint detection methods. Comparing the precision, recall, and F-Measure reported in with those of other methods demonstrates the method's superiority. As a result, the forgery detection process relied on a Keypoint detection strategy, and the block-based approach was only used when suspicious candidate regions were found during primary screening. A few exceptions to this rule were when the copied component and the target location were both located inside one block. These problems might be alleviated if an improved adaptive block segmentation approach could be found. By developing a false proof copy move forgery detection tool, we want to eventually help law enforcement authorities accept photos as evidence for their cases of criminal activity..

REFERENCES

[1] A Jessica Fridrich, B David Soukal, and A Jan Luka´s.ˇ "Detection of copy-move forgery in digital images". In: in Proceedings of Digital Forensic Research Workshop. 2003.
[2] Alin C Popescu and Hany Farid. Exposing digital forgeries by detecting duplicated image regions. Tech. rep. 2004.
[3] Weiqi Luo, Jiwu Huang, and Guoping Qiu. "Robust Detection of Region-Duplication Forgery in Digital Image". In: 18th International Conference on Pattern Recognition (ICPR'06). Vol. 4. 2006, pp. 746–749.
[4] G. Li et al. "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries Based on DWT and SVD". In: 2007 IEEE International Conference on Multimedia and Expo. 2007, pp. 1750–1753.
[5] Babak Mahdian and Stanislav Saic. "Detection of copy–move forgery using a method based on blur moment invariants". In: Forensic Science International 171.2 (2007), pp. 180–189. ISSN: 0379-0738. DOI: https : / / doi . org / 10 . 1016 / j . forsciint . 2006 . 11 . 002. URL: http : / / www. sciencedirect . com / science / article / pii/S0379073806006748.
[6] X. Kang and S. Wei. "Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics". In: 2008 International Conference on Computer Science and Software Engineering. Vol. 3. 2008, pp. 926–930.
[7] S. Bayram, H. Taha Sencar, and N. Memon. "An efficient and robust method for detecting copy-move forgery". In: 2009 IEEE International Conference on Acoustics, Speech and Signal Processing. 2009, pp. 1053–1056.
[8] J. Wang et al. "Detection of Image Region Duplication Forgery Using Model with Circle Block". In: 2009 International Conference on Multimedia Information Networking and Security. Vol. 1. 2009, pp. 25–29.
[9] Junwen Wang et al. "Fast and robust forensics for image region-duplication forgery". In: Acta Automatica Sinica 35.12 (2009), pp. 1488–1495.
[10] Hwei-Jen Lin, Chun-Wei Wang, Yang-Ta Kao, et al. "Fast copy-move forgery detection". In: WSEAS Transactions on Signal Processing 5.5 (2009), pp. 188–197.
[11] Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee. "Detection of copy-rotate-move forgery using Zernike moments". In: International workshop on information hiding. Springer. 2010, pp. 51–65.

