IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124175

IMAGE FORGERY DETECTION USING SUPERPIXEL SEGMENTATION

Aishwarya K M[1], Annapoorna E S[2], Aparna N V[3], Arpitha M S[4], Darshan K V [5]

Student, Electronics and Communication, Jawaharlal Nehru New College of Engineering, Shivamogga, India[1-4]

Assistant Professor, Electronics and Communication, Jawaharlal Nehru New College of Engineering, Shivamogga, India[5]

Abstract: Super pixel segmentation is an effective technique for detecting copy-move forgery, which is a type of image manipulation where a portion of an image is copied and pasted onto another area of the same image. This technique works by grouping neighboring pixels with similar properties into perceptually meaningful units called super pixels.

These super pixels are used to identify regions of an image that have been manipulated by identifying identical clusters of pixels. Various techniques can be combined with super pixel segmentation to improve the accuracy of the detection process, such as feature extraction and machine learning algorithms. The use of super pixel segmentation for copy-move forgery detection simplifies the image analysis process, making it easier to detect duplicate regions in the image. As image manipulation becomes increasingly prevalent, the development of new and innovative techniques like super pixel segmentation will become increasingly important for ensuring the integrity of digital images.

Index Terms - Super pixel segmentation, copy-move forgery, image manipulation, identical clusters of pixels, feature extraction, machine learning, accuracy, detection process, image analysis, digital images.

I. INTRODUCTION

Copy-move forgery is a common type of image tampering that involves copying a portion of an image and pasting it onto another area of the same image, often in an attempt to conceal or duplicate certain elements. This technique is commonly used to manipulate images for deceptive purposes, such as altering evidence or creating fake news. To detect copy-move forgery, researchers have developed various algorithms that analyze the image's content and identify similarities between different regions. One such algorithm is super pixel segmentation, which can be used to group pixels together into perceptually meaningful units. This technique has been shown to be effective in detecting copy-move forgery and is commonly used in many image processing applications.

Super pixel segmentation works by dividing the image into clusters of pixels, with each cluster representing a super pixel. These super pixels are generated by grouping neighboring pixels with similar characteristics, such as color or texture. This grouping process reduces the complexity of the image and simplifies subsequent analysis, making it easier to identify regions of the image that have been manipulated. In copy-move forgery detection, super pixel segmentation can be used to identify regions that have been copied and pasted in the image. When a portion of the image is copied and pasted, it creates a duplicate region that appears identical to the original region. By dividing the image into super pixels, it becomes easier to identify these identical clusters of pixels, allowing the algorithm to detect copy-move forgery.

The super pixel segmentation algorithm can be combined with other image processing techniques to improve the accuracy of the detection process. For example, feature extraction techniques can be used to extract distinctive features from each super pixel, which can be compared with features from other super pixels to identify similarities.

In addition, machine learning algorithms can be trained to recognize patterns and identify regions that have been manipulated. Overall, using super pixel segmentation for copy-move forgery detection has become an effective tool for detecting image tampering. This technique simplifies the image analysis process, making it easier to detect duplicate regions in the image. As image manipulation continues to become more prevalent, the development of new and innovative techniques like super pixel segmentation will become increasingly important for ensuring the integrity of digital images.

II. METHODOLOGY

Figure 1 shows the framework of cloning detection using adaptive over segmentation and feature point matching.

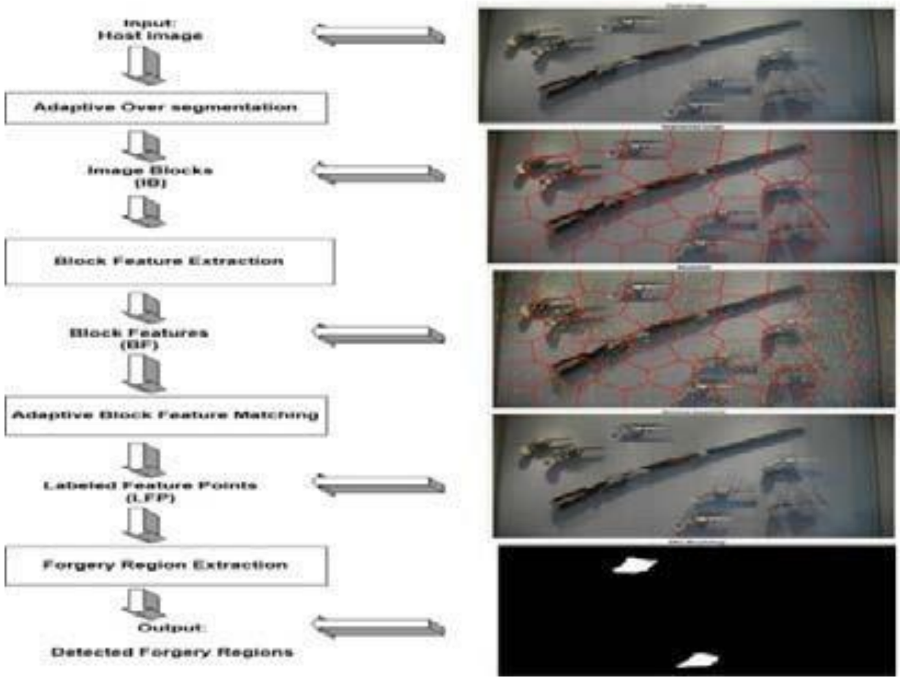

Figure 1: Framework of cloning detection using adaptive over segmentation and feature point matching.

In first stage, image is divided into non- overlapping irregular and regular blocks using adaptive over segmentation algorithm which are called as image blocks (IB). Further, SIFT and SURF is used for extracting feature points from each segment which are referred as block features (BF) [18]. Using feature matching algorithm, BF are compared with other features which helps in determining the Labeled Feature Points (LFP), which are indication to suspected tampered regions. In last stage, detection of tampered region is done by using forgery region extraction algorithm.

2.1 Adaptive Over Segmentation Algorithm

The Discrete Wavelet Transform (DWT) algorithm is widely used for image processing, including image segmentation. However, conventional DWT algorithms suffer from over-segmentation issues, where small regions are excessively segmented, leading to high computational complexity and reduced segmentation accuracy. To address this issue, an adaptive over-segmentation approach has been proposed for the DWT algorithm. This approach adjusts the segmentation parameters based on the characteristics of the image, such as texture and edge information. This allows the algorithm to better adapt to the specific features of the image, reducing over-segmentation and improving segmentation accuracy. The adaptive over-segmentation approach has been shown to outperform conventional DWT algorithms in terms of segmentation accuracy and computational efficiency. This approach has been applied in various image processing applications, such as medical imaging and remote sensing. Overall, the DWT algorithm with adaptive over-segmentation is a promising technique for image segmentation that can improve the accuracy and efficiency of the segmentation process.

2.2 Entropy Rate Super Pixel Segmentation

ERS (Entropy Rate Super Pixel Segmentation) is a super pixel segmentation algorithm that has been shown to be effective in detecting copy-move forgeries in images. The algorithm works by dividing an image into small, perceptually meaningful super pixels based on the concept of entropy rate. The resulting super pixels can then be used to identify regions of the image that may have been manipulated. In CMIFD, the ERS super pixel segmentation algorithm can be used to extract features from an image that are robust to copy-move forgeries. The algorithm works by first computing the entropy rate of the image and then using this information to group neighboring pixels into super pixels. The resulting super pixels are more likely to correspond to meaningful objects in the image and are less likely to be affected by small changes in the image caused by copy-move forgeries.

DOI: 10.17148/IJARCCE.2023.124175

Once the image has been segmented into super pixels, various features can be extracted from each super pixel to identify potential forgeries. These features can include color histograms, texture descriptors, and edge information. By using superpixels as the basis for feature extraction, the resulting features are more robust to copy-move forgeries and can be used to accurately identify manipulated regions of the image. In summary, the ERS super pixel segmentation algorithm is an effective technique for detecting copy-move forgeries in images. By segmenting the image into perceptually meaningful super pixels, the resulting features are more robust to copy-move forgeries and can be used to accurately identify manipulated regions of the image.

2.3 Block Feature Extraction Algorithm

The Scale-Invariant Feature Transform (SIFT) is a popular feature extraction technique in image processing that is used for various applications, including Copy-Move Image Forgery Detection (CMIFD). SIFT is a powerful algorithm that can extract key points and features from images that are invariant to scale, rotation, and illumination changes. The algorithm first identifies key points in the image that are invariant to changes in scale, rotation, and illumination. These key points are then used to extract local features that describe the image content. To apply SIFT to CMIFD, the first step is to divide the image into small patches or blocks. Then, the SIFT algorithm is applied to each block to extract local features. These features are represented as feature vectors, which can be used to compare different parts of the image to detect any potential copy-move forgeries. By using SIFT, the algorithm is able to identify key points and features that are invariant to changes in scale, rotation, and illumination, which makes it robust against different types of forgeries.

The SIFT algorithm has been used in various applications, including object recognition, image retrieval, and CMIFD. In the context of CMIFD, SIFT has been shown to be effective in detecting copy-move forgeries, even when the forgeries are rotated, scaled, or have different lighting conditions. By using SIFT, the algorithm is able to extract local features that are unique to each block of the image, which makes it more effective in detecting forgeries compared to other traditional methods. In summary, SIFT is a powerful feature extraction technique that is invariant to changes in scale, rotation, and illumination, which makes it a useful tool for CMIFD. By using SIFT to extract local features from image blocks, the algorithm is able to detect potential copy-move forgeries in an image. This technique has applications in various domains, including digital forensics, security, and multimedia data analysis.

2.4 Block feature matching Algorithm

Block feature matching is an important algorithm used in Copy-Move Image Forgery Detection (CMIFD) to identify potential forgery regions in an image. The algorithm works by comparing feature vectors extracted from different blocks of the image and identifying those that are similar. In general, the block feature matching algorithm involves the following steps:

1. Divide the image into small patches or blocks.
2. Extract feature vectors from each block using a feature extraction algorithm such as SIFT or SURF.
3. Compute a distance metric between the feature vectors of different blocks. Euclidean distance or cosine similarity are commonly used metrics.
4. Identify pairs of blocks that have feature vectors with a distance below a certain threshold. These blocks are considered to be potential copies of each other and could indicate the presence of a copy-move forgery in the image.

To improve the performance of the block feature matching algorithm, various techniques can be used, such as block normalization and geometric verification. Block normalization involves normalizing the feature vectors of each block to reduce the effect of differences in illumination and contrast. Geometric verification involves analyzing the spatial relationship between the matched blocks to verify that they have been copied and pasted from each other. Block feature matching is a commonly used technique in CMIFD and has been shown to be effective in detecting copy-move forgeries in images. However, it is not perfect and can suffer from false positives and false negatives, especially when dealing with complex forgeries. Therefore, it is important to use multiple algorithms and techniques in combination to improve the accuracy of the detection process.

2.5 Forgery region extraction algorithm

Step 1: Load Local Feature Point and perform ERS method.
ERS method divides the input image into small super pixels. To generate SR, LFP are replaced by corresponding super pixel blocks.
Step-2: Measure the color feature of SR (suspected Region) and its neighbor super pixels and merge the neighbor blocks. The color features of neighboring super pixels to SR which are called as neighbor blocks are measured. When SR and

DOI: 10.17148/IJARCCE.2023.124175

neighbor blocks are having similar color feature, merge the neighbor blocks with SR which generates MR(Merged Region).

Step 3: Apply morphological operation to MR to locate forgery regions. Close morphological operation uses structuring element as a circle whose radius depends on image size. This operation helps in filling the gaps in the MR and shape of the forged region is kept as it is.

III. RESULTS AND DISCUSSIONS

In this section, experiments are conducted on MICC-F220 dataset to check the performance of forgery detection methods. The image dataset MICC-F220 is used to test the methods. This dataset consists of 220 images, in that 110 are tampered and 110 are originals.

Precision and recall rate are used for performance evaluation. Precision is defined as the ratio of number of correctly identified forged images to totally identified forged images. Recall is also called as true positive rate which is defined as the ratio of number of correctly identified forged images to total forged images in database. In general, the important measures considered for the calculation of precision and recall rate are:

1. True Positive (TP): represents the number of correctly identified forged images.
2. False Negative (FN): represents number of wrong detections of forged images.
3. False Positive (FP): represents the number of wrong detections of original images.
4. True Negative (TN): represents the number of correctly detected original images.

Precision and Recall can be calculated using equation Precision = TP/ (TP + FP)
Recall = TP/ (TP + FN)
Along with precision and recall, F1 measure is used to measure the forgery detection results which can be computed using equation
F1 = 2× (precision × recall) / (precision + recall)
By considering these parameters, accuracy of the methods can be evaluated using equation.
Accuracy = (TP + TN) / (TP + TN + FP + FN)
The achieved Precision is 90%, recall is 81.81, F1 measure is 85.7099 and accuracy is 86.36.

IV. CONCLUSION

Copy-Move Image Forgery Detection (CMIFD) is a challenging task in the field of image processing, as it involves identifying regions in an image that have been copied and pasted within the same image. Super pixel segmentation is a powerful technique that can be used to address this problem by dividing an image into small, perceptually meaningful regions called super pixels. These super pixels can be used to extract features from the image that are more robust to copy-move forgeries and can be used to accurately identify manipulated regions of the image. In recent years, several super pixel segmentation algorithms have been developed for CMIFD, including ERS (Entropy Rate Super pixel Segmentation) and SLIC (Simple Linear Iterative Clustering). These algorithms have been shown to be effective in detecting copy-move forgeries in images and have been used in combination with other techniques such as feature extraction and matching algorithms to improve the accuracy of the detection process.

One of the advantages of using super pixel segmentation for CMIFD is that it simplifies the image analysis process by dividing the image into regions that correspond to perceptually meaningful objects. This makes it easier to extract features from the image and to identify potential forgeries. Additionally, by using super pixels as the basis for feature extraction, the resulting features are more robust to copy-move forgeries and can be used to accurately identify manipulated regions of the image. Despite the benefits of using super pixel segmentation for CMIFD, there are still several challenges that need to be addressed. For example, some super pixel segmentation algorithms may not work well for complex images or forgeries that involve only slight modifications to the image. Additionally, the accuracy of the detection process may be affected by the choice of feature extraction and matching algorithms.

In conclusion, super pixel segmentation is an effective technique for detecting copy-move forgeries in images. By segmenting the image into perceptually meaningful regions, super pixel segmentation can simplify the image analysis process and extract features that are more robust to copy-move forgeries. With the continued development of new and innovative super pixel segmentation algorithms, it is expected that CMIFD will become even more accurate and effective in the future.

DOI: 10.17148/IJARCCE.2023.124175

V. ACKNOWLEDGMENT

First, we acknowledge for the provision of the required infrastructure by my esteemed institute **J N N College of Engineering, Shivamogga** and **Department of Electronics and Communication Engineering**. we would like to thank our head of the department **Dr. S V Sathyanarayana.,** who stood as a guiding spirit and lending guidance to achieve the aim with added zeal. My special thanks to **Prof. Darshan K V** my project guide for providing all the inputs and corrections needed for the preparation of this paper.

REFERENCES

[1] H. Farid, "image forgery detection", IEEE signal processing magazine, 2009.
[2] B. D. S. A. J. Fridrich and A. J. Luk, "Detection of copy-move forgery in digital images," Digital Forensic Research Workshop, 2003.
[3] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," IEEE Transomed. Image., 2004.
[4] J. H. W. Luo and G. Qiu, "Robust detection of region-duplication forgery in digital image," 18th International Conference. 746-749, 2006.
[5] X. Y. Pan and S. Lyu, "Region duplication detection using image feature matching," Ieee Transactions on Information Forensics and Security, vol. 5, pp. 857-867, 2010.
[6] L. G. X. Bo, W. Junwen and D. Yuewei, "Image copy-move forgery detection based on surf," Multimedia Information Networking and Security (MINES), International Conference on, pp. 889-892, 2010.
[7] R. C. A. D. B. I. Amerini, L. Ballan and G. Serra, "A sift-based forensic method for copy-move attack detection and transformation recovery," Information Forensics and Security, IEEE Transactions on, vol. 6, pp. 1099-1110, 2011.
[8] P. Kakar and N. Sudha, "Exposing postprocessed copy-paste forgeries through transform-invariant features," Information Forensics and Security, IEEE Transactions on, vol. 7, pp. 1018-1028, 2012.
[9] X.-C. Y. C.-M. Pun and X.-L. Bi, "Image forgery detection using adaptive over segmentation and feature point matching," IEEE Transaction on Information Forensics and Security, 1705- 1716, 2015.
[10] H R Arpita, "Image Forgery Detection Using Adaptive Over segmentation and Feature Point Matching", Master's thesis, Visvesvaraya Technological University, 2019.