Journal of Transactions in Systems Engineering
https://ijitis.org/index.php/JTSE
ISSN: 2806-2973
Volume 1, Issue 3
DOI: doi.org/10.15157/JTSE.2023.1.3.140-147
Received: 03.11.2023; Accepted: 29.12.2023

Spliced Image Forgery Detection Using Adaptive Over-Segmentation Combined With AKAZE, ORB, and SIFT Feature Descriptors

Aziz Makandar[1], Syeda Bibi Javeriya[1*], Shilpa Kaman[1*]

[1]Department of Computer Science, Karnataka State Akkamahadevi Women's University, Vijayapura, India
***syedajaveriya84@gmail.com; *shilpaksawu@gmail.com**

Abstract

The detection of digital image forgery is an essential component in the process of safeguarding the authenticity and integrity of visual data. Image forgery can be accomplished through a variety of tools. One of these techniques is called splicing, and it involves combining the contents of multiple images in order to create a composite image that has been forged. The identification of digital forgeries of this kind presents a significant challenge. One of the tried-and-true methods that is utilized in the process of forgery detection is called Adaptive Over Segmentation (AOS). Within the scope of this paper, we are integrating adaptive over-segmentation with effective feature extraction methods such as AKAZE, ORB, and SIFT. With the assistance of parameters like precision, recall, and F1 measures, the proposed method intends to enhance the outcomes in order to achieve the desired results.

Keywords*:* Forgery Detection, Image splicing, AKAZE, ORB, SIFT, Adaptive Over Segmentation.

INTRODUCTION

One of the rapidly expanding areas of research in digital forensics and computer vision is the identification of digital picture forgeries. Research in this area mainly focuses on the development of algorithms that can efficiently detect manipulated or tampered images [1]. Forgery detection becomes very crucial when these manipulated images are misused in unethical ways to violate laws. There are many forgery techniques. Copy-move, image splicing, retouching, morphing, etc. To produce a fake image, image splicing combines various parts of several real photographs into one. The resulting image may appear authentic, but it contains objects and information that are not present in the original image. Even without any post-processing, the tampering traces are invisible and hardly detectable [2, 3]. Figure 1 displays an illustration of a spliced counterfeit image.

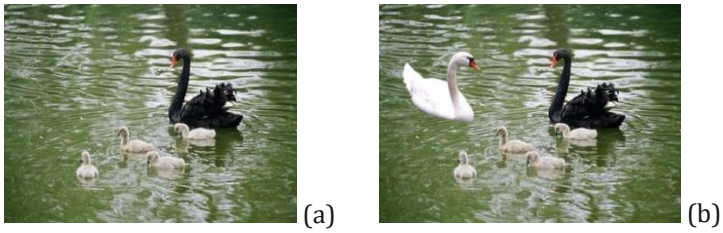

Figure 1. (a) Real Image (b) Spliced Image

There are many forgery detection techniques proposed in the literature, but they still face some challenges, and there is always scope for improvement in the results. Input images are divided into rectangular blocks with the help of discrete cosine transform (DCT) coefficients. These quantized blocks are used to detect tampered regions, as proposed by Fridrich et al.

[4]. The feature dimensionality reduction is achieved using principal component analysis (PCA), as proposed in [5] by Popescu and Farid. The RGB color components and orientation data were employed by Luo et al. [6] as block characteristics. The combination of discrete wavelet transforms (DWT) and singular value decomposition (SVD) is used to detect forgery by extracting features from images in Li et al. [7]. The 24 Blur-invariant moments were estimated by Mahdian and Saic [8] as features. Kang and Wei [9] propose a methodology that uses the singular value decomposition method for approximation in each block. The Fourier-Mellin Transform (FMT) was utilized by Bayram et al. [10] to acquire characteristics. Wang et al. [11, 12] proposed a technique to extract block features that uses the mean intensity values of circles with various radii around the block center. The block features employed by Lin et al. [13] consider the grey average values of every block and sub-blocks. Zernike moments were employed by Ryu et al. [14, 15] as block characteristics. Information entropy was employed by Bravo-Solorio and Nandi [16] as a block characteristic. All of these techniques detect forgery by dividing the image block-wise.

The detection techniques based on key points were offered as an alternative to block-wise methods, where key points are retrieved and matched over the entire image to withstand some image modifications while recognizing duplicated parts. As proposed in [17–19], the host images were initially transformed using the Scale-Invariant Feature Transform (SIFT) [20] to extract the feature points, and these feature points were matched to detect forgery. These techniques can find the important points that match, but they often struggle to find the counterfeit regions. In [1], a novel copy-move forgery detection method is put forth that combines key point-based and standard block-based forgery detection techniques to identify forgery regions with greater accuracy. This method uses adaptive over-segmentation and feature point matching.

METHODS

In our study, we conducted experiments using the CASIA dataset, which is a widely used benchmark dataset in the field of image forensics. The CASIA dataset provides a diverse collection of images, including various types of image manipulations and forgeries, making it suitable for evaluating the performance of forgery detection techniques. Our experiments involved analyzing a subset of 50 spliced images of size 384 x 256 pixels from the CASIA dataset. The following figure 2 represents the flowchart of the proposed work on spliced images.

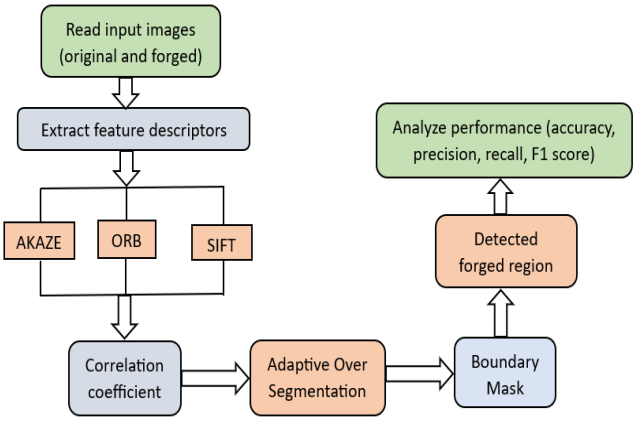

Figure 2. Workflow for the detection of spliced image forgery

Combining adaptive over-segmentation with AKAZE, ORB, and SIFT: Adaptive over-segmentation is used to divide the image into a set of small regions. Feature points are extracted from each region using AKAZE, ORB, and SIFT. These feature points are then matched between the different regions to identify regions that are likely to be spliced. The regions that are likely to be spliced are then further analyzed to confirm the presence of forgery. The step-by-step process used in the proposed forgery detection approach is given below.

- Read the input images in 384x256 resolution, including original and forged images.
- Apply the discrete wavelet transform (DWT) to the original image to obtain wavelet coefficients. Calculate wavelet coefficients for low-frequency and high-frequency energy. Determine the percentage of low-frequency coefficients in the image. Decide the region size 'S' for superpixel segmentation based on the percentage of low-frequency.
- Perform super-pixel segmentation, i.e., simple linear iterative clustering (SLIC), on the real image using the chosen region size 'S'. Count the number of segments in the original image.
- Repeat these previous steps for the forged image.
- Match the SIFT/ORB/AKAZE features between the original and forged images. Sort the matches based on the distance between the features. Draw the top 100 matched features and their lines on the original and forged images.
- Calculate the correlation coefficient between the real and forged images using the matched key points.
- Convert both images to grayscale. Compute the absolute difference between the grayscale images. Set a threshold to identify differing pixels.
- Create a binary mask where differing pixels above the threshold are set to white (255) and the rest to black (0). Convert the binary mask to a color mask for visualization.
- Evaluate performance by calculating pixel-level accuracy as well as the values of recall, precision, and F1 score, then comparing the results of the forged mask to the ground truth image.

Adaptive Over-Segmentation

Adaptive over-segmentation (AOS) is a technique that divides an image into a set of regions, each representing a coherent and visually meaningful part of the image. This approach allows for the identification of potential spliced regions by analyzing the inconsistencies in the appearance and texture of different segments.

SURF

Speeded-Up Robust Features (SURF) is a feature detection and description algorithm used in computer vision and image processing. It is designed to identify distinctive points, or key points, in an image that can be used for various computer vision tasks, including image matching, object recognition, and image stitching. The SURF algorithm is an improvement over the SIFT (Scale-Invariant Feature Transform) algorithm. It has been studied by researchers [21,22] and it is known for its computational efficiency, making it suitable for real-time applications. In the context of image forgery detection, SURF features can be used to identify distinctive patterns or textures within an image. By comparing these features across different regions of an image, inconsistencies or anomalies may be detected, indicating potential forgery or manipulation.

AKAZE

AKAZE (Accelerated-KAZE) is a feature matching technique used in computer vision and image processing tasks. It enhances the KAZE algorithm by introducing improvements in efficiency and robustness. AKAZE is particularly well-suited for image matching and recognition tasks involving substantial transformations such as changes in viewpoint, scale, or rotation. It detects and describes local features or keypoints in an image and handles nonlinear intensity variations and challenging lighting conditions. AKAZE's computational efficiency is achieved through the use of binary descriptors and its ability to handle images at multiple scales. Overall, AKAZE is a powerful and efficient technique for various computer vision applications.

ORB

ORB (Oriented FAST and Rotated BRIEF) is a feature matching technique in computer vision that combines the efficiency of the FAST corner detector with the robustness of the BRIEF descriptor. It is designed for fast and real-time applications, providing a good balance between speed and performance. ORB detects keypoints using the FAST corner detector and computes binary descriptors using BRIEF, allowing for fast matching using Hamming distance. It also incorporates an orientation assignment step for improved robustness to image rotations. ORB is commonly used in resource-constrained devices and applications requiring real-time processing, such as mobile robotics and augmented reality [23].

SIFT

One of the most widely used feature matching techniques in computer vision is the scale-invariant feature transform (SIFT). It detects and describes local features or key points in images that are invariant to changes in scale, rotation, and affine transformations. SIFT is robust to various image transformations and provides accurate matching of key points. It is widely applied in object recognition, image stitching, and 3D reconstruction tasks. SIFT detects stable key points using a difference of Gaussians approach and computes distinctive descriptors based on local image gradients. Its scale invariance and robustness to occlusions and lighting changes make it a versatile tool in computer vision applications [24, 25].

RESULTS AND DISCUSSION

Here we have calculated the performance measure between the predicted forgery image and the ground truth image. Metrics used for performance analysis are

Precision: The algorithm's positive predictions are accurate to a certain degree, which is measured by precision. In other words, it is the proportion to find positivity in the predictions by considering true positives and both true and false positives.

$$Precision = \frac{TP}{TP + FP} \qquad (1)$$

Recall: The algorithm's capacity to detect all positive cases is measured by recall; it is also referred to as sensitivity or true positive rate. It measures the positive instances correctly identified. It also considers false negative values along with true positives.

$$Recall = \frac{TP}{TP + FN} \qquad (2)$$

F1 Score: It is calculated as the harmonic mean of recall and precision values. The value of F1score ranges from 0 to 1, and prediction values near 1 mean the model is performing really well.

$$F1\ Score = \frac{2 * (Precision * Recall)}{(Precision + Recall)} \qquad (3)$$

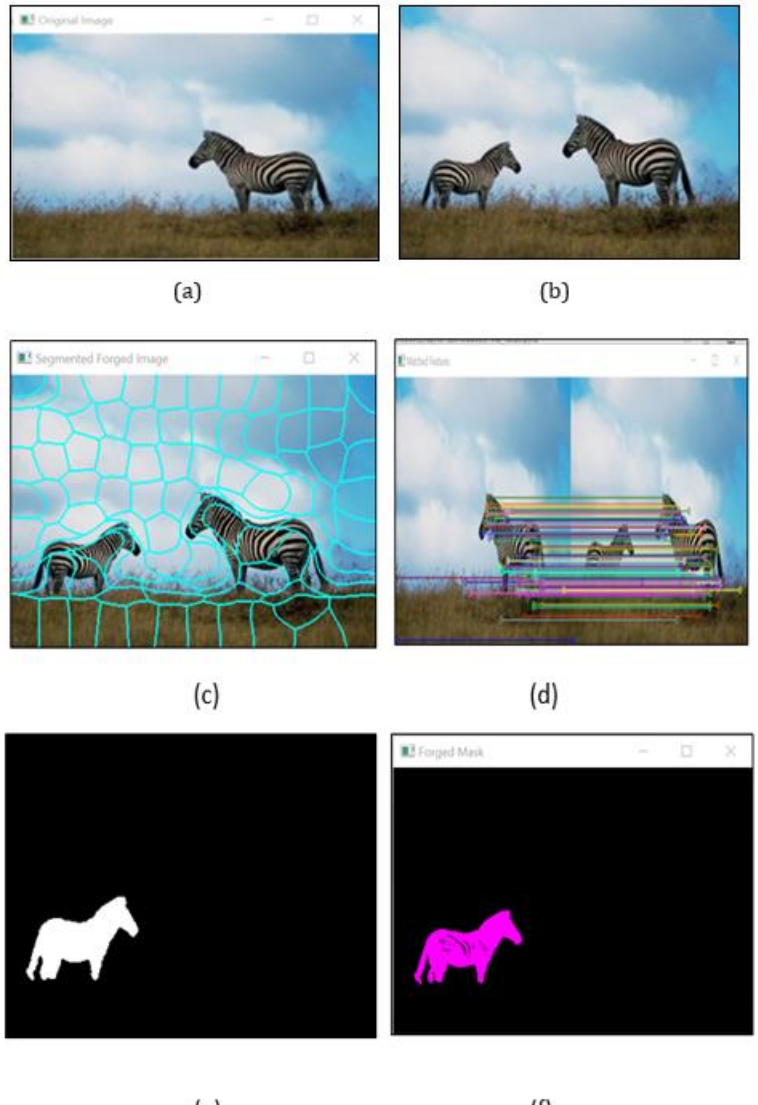

Figure 3. Resultant images (a) Real image (b) Spliced image (c) Segmented image (d) Feature matching (e) Ground truth of forged image (f) Forged mask detected

Table 1 shows the comparative results of different forgery detection techniques on spliced images at the pixel level. Feature descriptors ORB, AKAZE [26], and SIFT give good results when combined with adaptive over-segmentation compared to the individual results of SURF and SIFT on spliced image forgery detection, as represented in the following table. Adaptive Over Segmentation [27] with ORB and SIFT achieves accurate results with higher values of precision, recall, and F1 scores, as shown in the table.

Table 1. Spliced image forgery detection results at pixel level

Methods	Precision (%)	Recall (%)	F1 score (%)
SURF [21,22]	68.13	76.43	69.54
SIFT [18,19]	60.80	71.48	63.10
AOS+AKAZE	77.65	84.48	80.10
AOS+ORB	94.45	89.78	92.06

Results are displayed in the following figure 3. It shows input original and forged images followed by segmented images, which is the result of adaptive over-segmentation. Feature matching with SIFT between original and forged images is shown in (d), and the spliced mask detected is shown in (f).

CONCLUSION

Through the utilization of adaptive over-segmentation in conjunction with robust feature descriptors such as ORB, AKAZE, and SIFT, we are able to effectively recognize forged regions within the spliced frames. In order to conduct a comparative analysis, three feature extraction algorithms were applied to a variety of spliced images. Performance parameters such as accuracy, precision, recall, and F1 score were utilized at the pixel level to facilitate the analysis. As a whole, the findings indicate that the combination of SIFT descriptors and adaptive over-segmentation yields superior outcomes in comparison to AKAZE and ORB. When compared to previous works on forgery detection that make use of adaptive over-segmentation, it also performs significantly better. In order to address a wide range of image manipulation techniques, the approach can be further extended.

CONFLICT OF INTERESTS

The authors confirm that there is no conflict of interests associated with this publication.

REFERENCES

[1] Pun, Chi-Man & Yuan, Xiaochen & Bi, Xiu-Li. (2015). Image Forgery Detection Using Adaptive Over-Segmentation and Feature Points Matching. IEEE Transactions on Information Forensics and Security. 10. 1-1. 10.1109/TIFS.2015.2423261.

[2] D. Vaishnavi and T. Subashini, “Recognizing image splicing forgeries using histogram features,” in 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC). IEEE, 2016, pp. 1–4.

[3] H. Benhamza, A. Djeffal and A. Cheddad, "Image forgery detection review," 2021 International Conference on Information Systems and Advanced Technologies (ICISAT), Tebessa, Algeria, 2021, pp. 1-7, doi: 10.1109/ICISAT54145.2021.9678207.

[4] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in in Proceedings of Digital Forensic Research Workshop, 2003.

[5] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.

[6] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in Pattern Recognition, 2006. ICPR 2006. 18th International Conference on, 2006, pp. 746-749.

[7] 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 Multimedia and Expo, 2007 IEEE International Conference on, 2007, pp. 1750-1753.

[8] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," Forensic science international, vol. 171, pp. 180-189, 2007.

[9] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in Computer Science and Software Engineering, 2008 International Conference on, 2008, pp. 926-930.
[10] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, 2009, pp. 1053-1056.
[11] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, "Detection of image region duplication forgery using model with circle block," in Multimedia Information Networking and Security, 2009. MINES'09. International Conference on, 2009, pp. 25-29.
[12] J. Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, "Fast and robust forensics for image region-duplication forgery," Acta Automatica Sinica, vol. 35, pp. 1488-1495, 2009.
[13] H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection," WSEAS Transactions on Signal Processing, vol. 5, pp. 188-197, 2009.
[14] S. Ryu, M. Lee, and H. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in Information Hiding, 2010, pp. 51-65.
[15] S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments," Ieee Transactions on Information Forensics and Security, vol. 8, pp. 1355-1370, Aug 2013.
[16] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling," in Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on, 2011, pp. 1880-1883.
[17] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on, 2008, pp. 272-276.
[18] 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, Dec 2010.
[19] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, 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.
[20] D. G. Lowe, "Object recognition from local scale-invariant features," in Computer vision, 1999. The proceedings of the seventh IEEE international conference on, 1999, pp. 1150-1157.
[21] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in Multimedia Information Networking and Security (MINES), 2010 International Conference on, 2010, pp. 889-892.
[22] B. Shivakumar and L. D. S. S. Baboo, "Detection of region duplication forgery in digital images using SURF," IJCSI International Journal of Computer Science Issues, vol. 8, 2011.
[23] E. Rublee, V. Rabaud, K. Konolige and G. Bradski, "ORB: An efficient alternative to SIFT or SURF," international Conference on Computer Vision, Barcelona, Spain, 2011, pp. 2564-2571, doi: 10.1109/ICCV.2011.6126544.
[24] Lowe, David G., "Object recognition from local scale-invariant features" . Proceedings of the International Conference on Computer Vision, 1999, Vol. 2. pp. 1150-1157. doi:10.1109/ICCV.1999.790410.
[25] Lowe, David G., "Distinctive Image Features from Scale-Invariant Keypoints". International Journal of Computer Vision, 2004, 60 (2): 91–110. CiteSeerX 10.1.1.73.2924.
[26] Alcantarilla, P.F., Bartoli, A., Davison, A.J., KAZE Features. In: Fitzgibbon, A., Lazebnik, S., Perona, P., Sato, Y., Schmid, C. (eds) Computer Vision – ECCV 2012. ECCV 2012. Lecture Notes in Computer Science, vol 7577. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-33783-3_16.
[27] S. Zahra, M. Sadim, "Image Forgery Detection with Modified Adaptive Over Segmentation Technique and Noise Attacks", International Journal of Computer Science and Mobile Computing, Vol. 9, Issue. 7, July 2020, pg.33 – 42, ISSN 2320–088X.