WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Copy move forgery Detection

Gowthaman

UG Student, Rathinam college of arts and science, India

ABSTRACT

Scrutiny of digital images refers increasingly vital in our everyday lives, with Copy-Move Forgery Detection (CMFD) being a crucial area of focus in academia. While keypoint-based methods, especially those relying on SIFT, have shown promise in CMFD, they often struggle to detect enough matches in smooth regions where tampering occurs. To address this limitation, we propose using entropy images to accurately locate keypoints, significantly boosting their numbers. Additionally, we introduce an entropy level clustering technique to manage the heightened complexity of matching due to irregular grayscale distributions in keypoints. Our experiments validate that our approach strikes a favorable balance between accuracy and computational efficiency.

Index Terms— Image forensics, CMFD, SIFT, entropy level clustering

INTRODUCTION

As technology advances, the prevalence and sophistication of digital image forgeries have increased while the costs associated with such manipulations have decreased. This trend has led to a growing challenge in verifying the authenticity of images, which was not as prevalent decades ago. However, not all types of image manipulations are of equal concern. In practical applications, there is a particular focus on forgeries that alter the semantic meaning of an image, such as copy-move and splicing. These types of manipulations have garnered significant attention in the academic community due to their potential to deceive viewers.

Digital image forgery detection techniques can broadly be categorized into two types: active and passive methods. Active techniques, like digital watermarking and signatures, involve embedding prior information into the image to detect tampering. However, these methods can potentially degrade the overall quality of the image. On the other hand, passive techniques solely rely on analyzing the content of the image itself without introducing any alterations to the original data, making them more versatile and widely applicable.

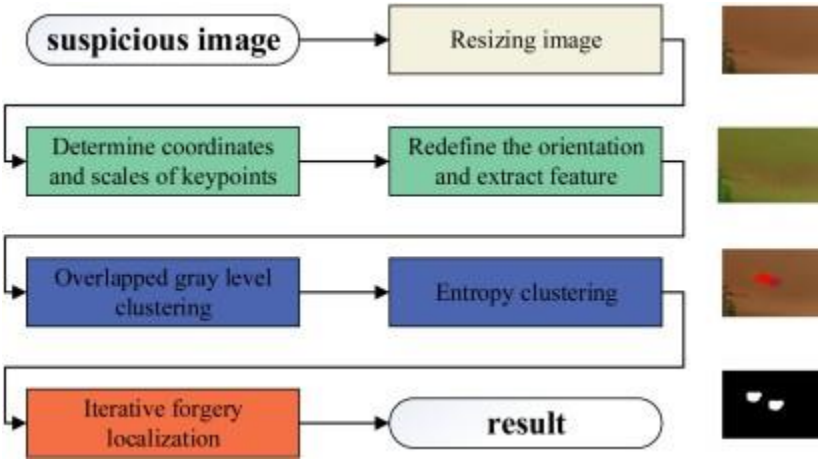
Among the various types of image manipulations, copy-move forgery presents a unique challenge due to its inherent similarity. Detecting such forgeries typically involves keypoint-based, block-based, or deep learning-based algorithms. While deep learning approaches have shown promise, they often struggle with high-resolution images and lack interpretability compared to conventional methods. Keypoint- based algorithms aim to distribute keypoints evenly across the image, typically relying on grayscale images for detection. However, conventional algorithms may struggle in regions with low texture, affecting their effectiveness in detecting forgeries.

To address these challenges, this paper proposes a novel Copy-Move Forgery Detection (CMFD) algorithm. The proposed algorithm introduces entropy images to enhance keypoint detection accuracy by redefining orientation and feature extraction in grayscale images, leveraging SIFT features.

Additionally, an entropy level clustering algorithm is developed to handle the increased complexity resulting from non-ideal grayscale distributions of keypoints.

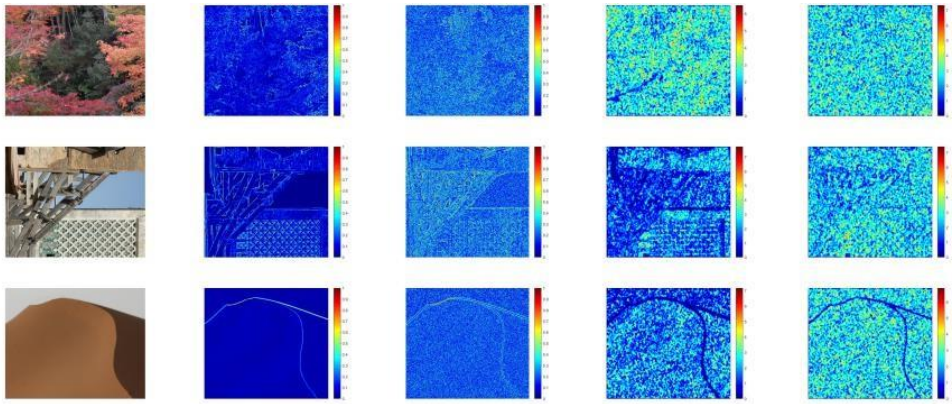
In summary, this paper presents a comprehensive approach to tackle copy-move forgery detection, aiming to improve accuracy and efficiency in identifying manipulated regions within images. The subsequent sections detail the proposed methodology and present experimental results to validate the effectiveness of the approach.

The proposed algorithm, depicted in Figure 1, comprises three main stages. The third stage, as described in existing literature [1], involves post-processing techniques that leverage dominant orientation and scale information extracted from matched keypoints. We will detail this post-processing stage later in this section.



In the pre-processing stage, we leverage entropy images to better quantify the texture complexity within specific areas of the image. This approach results in a denser distribution of keypoints compared to traditional grayscale images. To illustrate this, we utilize three different types of images from the GRIP dataset: one with high texture, one with smooth and complex textures, and one with smooth texture.
Figure 2 (a) showcases the selected images, while Figures 2 (b) and (c) display the results of standard deviation filtering for the grayscale and entropy images, respectively. To enhance visual clarity, we normalize the results to the range [0, 1] and represent them using pseudocolored images. Notably, Figure 2 (c) demonstrates a more suitable distribution of standard deviation.

In literature [1], a method extracts patches with minimum variance to ensure the generation of four keypoints per patch on the GRIP dataset. While this method is commendable, it doesn't guarantee the presence of four correct matches within copy-move patches after matching. To address this issue, we propose a strategy aimed at ensuring the presence of four keypoints within each patch.
Given that commonly used block sizes for extracting invariant moment features range from 8×8 to 32×32, we opt for the smallest size. Our objective is to generate a minimum of four keypoints within each 8×8 region. We believe that this strategy will improve the effectiveness of our Copy-Move Forgery Detection (CMFD) algorithm.



(a) RGB image: This represents the original input image in its color form.
(b) Standard deviation of grayscale image: This visualizes the variability or texture complexity within the grayscale version of the image.
(c) Standard deviation of entropy image: This illustrates the variability or texture complexity within the entropy-transformed image, which provides a more effective quantification of texture complexity compared to grayscale images.
(d) Average density distribution of keypoints in grayscale images: This shows how keypoints are distributed across the grayscale image on average, providing insights into where keypoints are concentrated or sparse.
(e) Average density distribution of keypoints in entropy images: This demonstrates how keypoints are distributed across the entropy-transformed image, highlighting areas with high texture complexity where keypoints are likely to be densely populated.

These visualizations provide valuable insights into the texture characteristics of the images and the distribution of keypoints, which are crucial for subsequent stages of the proposed algorithm.

In simpler terms, "step1" represents the size of each interval, while "step2" indicates how much these intervals overlap (with the condition that step1 is larger than step2). The number of gray level groups, denoted as Nu, is calculated using the formula:
Nu = (255 - step1) / (step1 - step2) + 1
This formula determines how many groups of gray levels are needed based on the size of the intervals, the amount of overlap between intervals, and the total range of gray levels (from 0 to 255). The aim is to ensure that each group covers a specific range of gray levels while taking into account the overlap with adjacent groups. Essentially, this calculation helps organize the gray levels into distinct groups for further analysis or processing.

While overlapped gray level clustering can be effective, its efficacy diminishes when keypoints' grayscale values are concentrated within a narrow range. In Fig. 3 (a), the grayscale distribution of keypoints from a suspicious image reveals that their values predominantly fall within the range of [150, 200], with approximately 70% of keypoints clustered within this interval based on our analysis. This concentration of keypoints within a narrow range significantly hampers the efficiency of clustering for matching purposes.
To address this challenge, we propose the entropy level clustering algorithm. As depicted in Fig. 3 (b), even when the grayscale distribution is suboptimal, the entropy distribution displays a more favorable pattern. Therefore, we can intelligently partition the two- dimensional plane of grayscale and entropy values to mitigate the issues caused by the concentration of keypoints within a narrow grayscale range. This approach allows us to effectively manage the clustering of keypoints for matching, even in cases where the grayscale distribution is not ideal.

CONCLUSION

Detecting copy-move forgery in digital images relies on advanced techniques like DCT- based CMFD. Future research should focus on refining algorithms to handle modern image complexities and evolving tampering strategies. Our proposed method achieves an accuracy of 92.2 with reduced execution time (64.02). Copy-move forgery detection is essential for various applications like criminal investigations and copyright disputes.
Advanced algorithms analyze image content to identify duplicated regions, but challenges remain, including handling diverse manipulations and complex image content. Continued research aims to enhance the reliability of detection techniques.

REFERENCES:

[1] Li, Y., & Zhou, J. (2018). Fast and effective image copy-move forgery detection via hierarchical feature point matching. IEEE Transactions on Information Forensics and Security, 14(5), 1307–1322.
[2] Silva, E., Carvalho, T., Ferreira, A., & Rocha, A. (2015). Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. Journal of Visual Communication and Image Representation, 29, 16–32.
[3] Niu, P., Wang, C., Chen, W., Yang, H., & Wang, X. (2021). Fast and effective keypoint- based image copy-move forgery detection using complex-valued moment invariants. Journal of Visual Communication and Image Representation, 77, 103068.
[4] Niyishaka, P., & Bhagvati, C. (2020). Copy-move forgery detection using image blobs and brisk feature. Multimedia Tools and Applications, 79(35-36), 26045–26059.
[5] Lyu, Q., Luo, J., Liu, K., Yin, X., Liu, J., & Lu, W. (2021). Copy move forgery detection based on double matching. Journal of Visual Communication and Image Representation, 76, 103057.
[6] Cozzolino, D., Poggi, G., & Verdoliva, L. (2015). Efficient dense-field copy–move forgery detection. IEEE Transactions on Information Forensics and Security, 10(11), 2284–2297.
[7] Ryu, S.-J., Kirchner, M., Lee, M.-J., & Lee, H.-K. (2013). Rotation invariant localization of duplicated image regions based on Zernike moments. IEEE Transactions on Information Forensics and Security, 8(8), 1355–1370.
[8] He, Y., Li, Y., Chen, C., & Li, X. (2023). Image copy-move forgery detection via deep cross- scale patchmatch. In 2023 IEEE International Conference on Multimedia and Expo (ICME) (pp. 2327–2332). IEEE.
[9] Wu, Y., Abd-Almageed, W., & Natarajan, P. (2018). Busternet: Detecting copy-move image forgery with source/target localization. In Proceedings of the European conference on computer vision (ECCV) (pp. 168–184).
[10] Chen, B., Tan, W., Coatrieux, G., Zheng, Y., & Shi, Y.-Q. (2020). A serial image copy-move forgery localization scheme with source/target distinction. IEEE Transactions on Multimedia, 23, 3506–3517.
[11] Islam, A., Long, C., Basharat, A., & Hoogs, A. (2020). Doa-gan: Dual-order attentive generative adversarial network for image copy-move forgery detection and localization. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 4676–4685).
[12] Zhong, J.-L., Yang, J.-X., Gan, Y.-F., Huang, L., & Zeng, H. (2022). Coarse-to-fine spatial- channel-boundary attention network for image copy-move forgery detection. Soft Computing, 26(21), 11461–11478.