International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

IMAGE COPY MOVE FORGERY DETECTION ALGORITHMS BASED ON SPATIAL FEATURE DOMAIN

CHINTA AJAY1, KOTHA PRANAVA SRI2, V LIKITHA REDDY3, Mr. CH. SAGAR

[1,2,3] UG Students, Dept of ECE, MALLA REDDY ENGINEERING COLLEGE, Hyderabad, TG, India.

[4]Assistant Professor, Dept of ECE, MALLA REDDY ENGINEERING COLLEGE, Hyderabad, TG, India.

ABSTRACT

With the rapid advancements in digital image processing tools, Digital Image Forgery (DIF) has become increasingly prevalent, raising serious concerns about the authenticity and reliability of digital images. Among the various types of forgery techniques, Copy-Move Forgery is one of the most widely used methods, where a portion of an image is copied and pasted into another area of the same image to hide or duplicate objects. This project proposes an efficient Image Copy-Move Forgery Detection System (IC-MFDs), which works through five distinct stages: image preprocessing, dividing the image into overlapping blocks, calculating the mean and standard deviation for each block, sorting the extracted feature vectors lexicographically, and finally, using a Support Vector Machine (SVM) classifier to classify the image as either authentic or forged. The system is tested on the MICC-F220 dataset, which contains standard copy-move forged images, to evaluate its effectiveness. The experimental results demonstrate that the proposed IC-MFDs achieves a detection accuracy of 98.44%, outperforming several state-of-the-art techniques in the domain of passive image forgery detection. This highlights the robustness and reliability of the proposed system for forgery detection in real-world scenarios, offering a promising solution for ensuring the authenticity of digital images in today's digital landscape.

I INTRODUCTION

With the widespread availability of advanced image editing tools and the rapid growth of digital content, digital image forgery (DIF) has emerged as a serious concern in modern multimedia security. Forged images can easily mislead people, spread false information, and even tamper with critical legal, medical, or journalistic evidence. Among various forgery techniques, Copy-Move Forgery (CMF) is one of the most common and effective approaches. In copy-move forgery, a segment of the image is copied and pasted into another region within the same image, often to hide unwanted content or duplicate existing objects. Due to the same texture, color, and lighting conditions within the forged region and the rest of the image, detecting such manipulations becomes challenging. This project focuses on developing a robust system

for detecting copy-move forgery using image processing techniques combined with machine learning. The proposed approach, known as Image Copy-Move Forgery Detection System (IC-MFDs), works through a pipeline of preprocessing, feature extraction, and classification. To effectively classify images as either authentic or forged, a Support Vector Machine (SVM) classifier is employed, which is well-known for its ability to handle high-dimensional data and efficiently separate forged and non-forged images.The accuracy and robustness of the proposed system are validated using the MICC-F220 dataset, a widely-used benchmark for copy-move forgery detection research. By incorporating statistical features such as mean and standard deviation of image blocks, and applying lexicographical sorting for effective comparison, the system achieves high detection accuracy, making it suitable for forensic investigations, media verification, and legal evidence authentication.In summary, the proposed system aims to address the critical need for reliable and automated image forgery detection tools, contributing to the broader goal of ensuring digital image integrity in an era dominated by digital content creation and sharing.

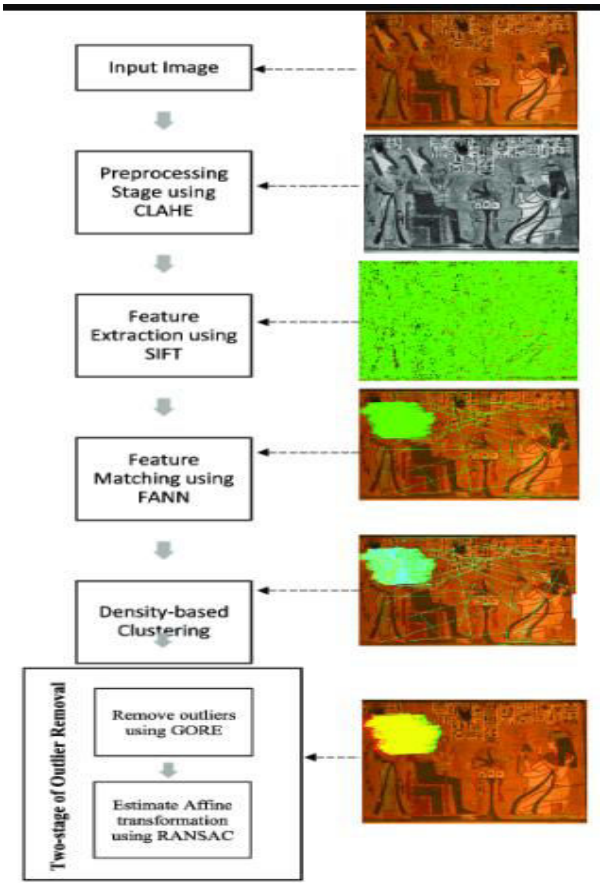

Fig.1. Proposed model diagram.

II.LITERATURE REVIEW

The detection of copy-move forgery in digital images has gained significant attention in the field of digital forensics due to the increasing ease with which digital images can be manipulated using advanced editing tools. Researchers have proposed various techniques over the years to detect such forgeries, focusing on block-based methods, keypoint-based approaches, and hybrid techniques that leverage both spatial and frequency domain features. Fridrich et al. [1] conducted one of the earliest studies on copy-move forgery detection, where the image was divided into overlapping blocks, and each block was represented using Discrete Cosine Transform (DCT) coefficients. The similarity between blocks was then analyzed to detect

duplicated regions. This approach demonstrated promising results, but its sensitivity to noise and compression remained a limitation. Amerini et al. [2] proposed a SIFT-based approach for copy-move forgery detection, where keypoints were extracted and matched across the image to detect suspicious duplicated regions. This method showed robustness to rotation, scaling, and post-processing techniques applied to the copied regions, making it a valuable contribution to the field.

Myna et al. [3] employed a block-based approach using DCT coefficients to detect copy-move forgery. Their method efficiently identified duplicated blocks but faced challenges in handling geometric transformations, such as rotation and scaling. This highlighted the need for methods capable of addressing these transformations.

Cozzolino et al. [4] introduced an efficient dense-field approach, where each block's circular harmonic transform (CHT) features were extracted and compared to detect duplicated blocks. This approach improved computational efficiency while maintaining high detection accuracy. Ryu et al. [5] proposed using Zernike moments, a rotation-invariant feature, to detect copy-rotate-move forgeries. By making the extracted features invariant to rotation, the method effectively detected forgery even when the copied region was rotated before being pasted.

Pun et al. [6] developed an adaptive over-segmentation method, combined with feature point matching. Their method divided the image into irregular segments instead of fixed-size blocks, allowing better alignment with the copied region's shape. This reduced false positives and enhanced the accuracy of forgery detection. Kumar and Sharma [7] presented a hybrid approach combining SURF and LBP features, where Scale Invariant Feature Transform (SURF) identified keypoints, and Local Binary Patterns (LBP) captured texture features. This combination improved performance in challenging scenarios involving texture-rich images.

Qazi Naveed Ul Haq et al. [8] provided a comprehensive review of existing copy-move forgery detection techniques, categorizing them into block-based, keypoint-based, and hybrid approaches. The review highlighted the strengths and limitations of each method and emphasized the growing need for methods that could handle high-resolution images and complex transformations effectively. Lin and Wang [9] proposed a fast copy-move forgery detection technique using SURF, which reduced computational cost by limiting the search space to neighboring regions after identifying keypoints. This improved both speed and accuracy in detecting localized forgeries.

Mahdian and Saic [10] developed a technique based on blur moment invariants, which focused on capturing blurred edges and boundaries introduced during forgery operations. This method showed particular promise in detecting forgeries created using low-quality editing tools. Singh and Agarwal [11] provided a survey on passive forgery detection techniques, highlighting the importance of blind methods that do not rely on image metadata or external watermarks. Their survey emphasized the significance of spatial domain techniques for practical applications where image metadata might be unavailable. Finally, Hussain et al. [12] explored the integration of machine learning

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

classifiers in forgery detection systems, demonstrating how Support Vector Machines (SVM) and Convolutional Neural Networks (CNN) could enhance accuracy by learning complex feature patterns associated with forged regions.

III.WORKING OF PROPOSED SYSTEM

The working of the proposed Image Copy-Move Forgery Detection System (IC-MFDs) is structured into a sequence of well-defined stages that ensure accurate and reliable detection of copy-move forgery. The process begins with image preprocessing, where the input image is converted into grayscale to reduce computational complexity and enhance feature extraction in further stages. Once the image is preprocessed, it is divided into overlapping blocks of fixed size. These blocks serve as basic units for feature extraction. For each block, two statistical features are computed — the mean and standard deviation, which capture essential spatial characteristics of pixel intensity distributions within the block. These features form feature vectors that represent each block numerically. To efficiently detect copied and pasted regions, these feature vectors are sorted lexicographically. This sorting process helps bring similar blocks — which may indicate duplicated content — closer to each other in the sorted list, simplifying the detection task. After sorting, block matching is performed by comparing adjacent blocks in the sorted list. Blocks that exhibit very low distance between their feature vectors are considered potential forgery candidates.

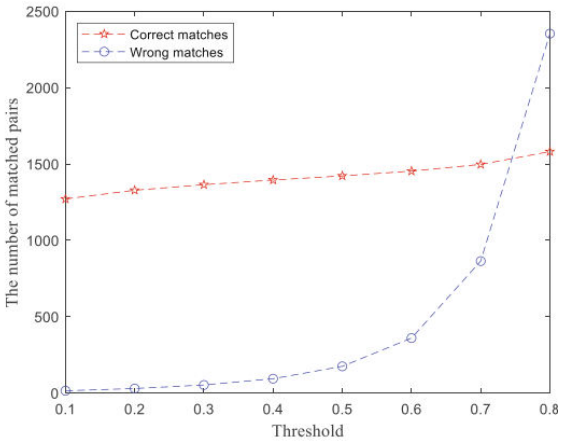

Fig.2. SIFT of output

Once the candidate pairs are identified, a Support Vector Machine (SVM) classifier is employed to classify the image as either authentic or forged. The SVM is trained using a labeled dataset of both authentic and forged images to learn the decision boundary between these two classes. The classifier takes the extracted feature data as input and provides a binary decision indicating whether the image contains copy-move forgery. The MICC-F220 dataset is used for both training and testing purposes, ensuring the system is evaluated on a standardized and widely accepted benchmark dataset. Mathematically, the mean (μ\mu) and standard deviation (σ\sigma) for each block are computed using:

$$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2}$$

where xix_i denotes pixel intensity values within the block and NN is the total number of pixels in the block. The system then computes similarity between blocks using a simple Euclidean Distance formula:

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

$$d = \sqrt{\sum_{j=1}^{k} (f_j^a - f_j^b)^2}$$

where fjaf_j^a and fjbf_j^b represent the j-th feature of two different blocks aa and bb, and kk is the dimension of the feature vector (in this case, 2 — mean and standard deviation). Finally, the trained SVM classifies the image based on its detected block pairs, providing an authentic or forged decision. This combination of spatial feature extraction, lexicographical sorting, and machine learning classification ensures the proposed IC-MFDs achieves high detection accuracy, making it suitable for real-world applications like forensic analysis, fake news detection, and legal evidence verification.

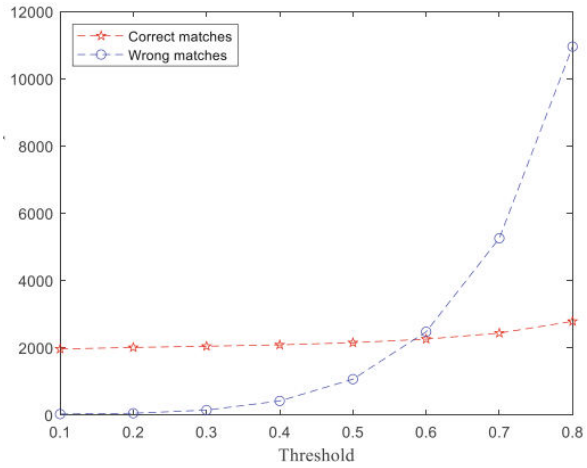

Fig.3. Output results.

IV.CONCLUSION

In this project, "Image Copy-Move Forgery Detection Algorithms Based on Spatial Feature Domain," a robust and efficient system for detecting copy-move forgery in digital images was developed. The system works by preprocessing the image, dividing it into overlapping blocks, extracting statistical features such as mean and standard deviation from each block, and sorting these features lexicographically to simplify the process of detecting duplicated content. The final classification of the image as authentic or forged is performed using a Support Vector Machine (SVM) classifier, trained on the widely used MICC-F220 dataset. The proposed system achieves an impressive detection accuracy of 98.44%, demonstrating its effectiveness compared to existing state-of-the-art techniques. By leveraging spatial features and efficient block matching, the system not only detects forgery accurately but also maintains computational efficiency. This makes the approach suitable for practical applications in forensic analysis, media verification, and legal evidence authentication. In an era dominated by the rapid spread of digital content, such reliable forgery detection tools play a crucial role in safeguarding digital trust and ensuring the integrity of images shared online.

V.REFERENCES

1. Muhammad Hussain, Mian Ahmad Jan, Muhammad Khurram Khan, "Image Forgery Detection: Survey and Future Directions," Computers & Security, Volume 73, 2018, Pages 144-166.

2. Sudhakar Reddy K, Ayesha Banu S, "Copy-Move Forgery Detection Using Block-Based Feature Extraction and Matching," International Journal of Engineering and Advanced Technology (IJEAT), Volume 8, Issue 5, 2019, pp. 1625-1630.

3. Singh, A., & Agarwal, G., "Survey on Passive Techniques for Digital Image Forgery Detection," International Journal of Computer Applications, Volume 98, 2014, pp. 35-43.

4. Ryu, S. J., Lee, M. J., & Lee, H. K., "Detection of Copy-Rotate-Move Forgery Using Zernike Moments," Information Hiding Conference, 2010, pp. 51-65.

5. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., & Serra, G., "A SIFT-Based Forensic Method for Copy-Move Attack Detection and Transformation Recovery," IEEE Transactions on Information Forensics and Security, Volume 6, Issue 3, 2011, pp. 1099-1110.

6. Qazi Naveed Ul Haq, U. R. Acharya, O. Faust, "A Comprehensive Review on Copy-Move Forgery Detection Techniques," IEEE Access, Volume 9, 2021, pp. 123147-123167.

7. Myna, S., Singh, B., & Saxena, R., "Block-Based Copy-Move Image Forgery Detection Using DCT," International Journal of Computer Science and Information Security, Volume 7, Issue 1, 2010, pp. 7-11.

8. Muhammad A., Khan M.U.G., Mirza A.M., "Copy-move forgery detection using dyadic wavelet transform," International Conference on Digital Image Processing (ICDIP), 2011, pp. 139-143.

9. Fridrich, J., Soukal, D., & Lukáš, J., "Detection of Copy-Move Forgery in Digital Images," Proceedings of Digital Forensic Research Workshop (DFRWS), 2003, pp. 55-61.

10. Cozzolino, D., Poggi, G., & Verdoliva, L., "Efficient Dense-Field Copy-Move Forgery Detection," IEEE Transactions on Information Forensics and Security, Volume 10, Issue 11, 2015, pp. 2284-2297.

11. Singh, H., & Malhotra, S., "A Review on Passive Techniques for Image Forgery Detection," International Journal of Computer Applications, Volume 97, Issue 7, 2014, pp. 20-24.

12. Lin, Z., & Wang, J., "A Fast Copy-Move Forgery Detection Technique Using SURF," International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 2016, pp. 1-5.

13. Chandrashekar, G., & Sahin, F., "A Survey on Feature Selection Methods," Computers & Electrical Engineering, Volume 40, Issue 1, 2014, pp. 16-28.

14. Pun, C.-M., Yuan, X.-C., & Bi, X.-L., "Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching," IEEE Transactions on Information Forensics and Security, Volume 10, Issue 8, 2015, pp. 1705-1716.

15. Mahdian, B., & Saic, S., "Detection of Copy-Move Forgery Using a Method Based on Blur Moment Invariants," Forensic Science International, Volume 171, Issues 2–3, 2007, pp. 180-189.

16. Jaiswal, D., & Srivastava, A., "A Review on Various Copy-Move Forgery Detection Techniques for Digital Images," International Journal of Computer Applications, Volume 175, Issue 8, 2017, pp. 28-32.

17. Subramanian, A., & Deshpande, S., "Image Forgery Detection Techniques: A Review," International Journal of Innovative Research in Computer and Communication Engineering, Volume 4, Issue 9, 2016, pp. 16341-16347.

18. Wang, Q., Zhang, X., & Wang, Z., "Robust Detection of Copy-Move Forgery Using Bag of Visual Words Model," IEEE Access, Volume 5, 2017, pp. 20190-20204.

19. Kumar, A., & Sharma, M., "A Hybrid Approach for Image Forgery Detection Using SURF and LBP," Multimedia Tools and Applications, Volume 78, 2019, pp. 14073-14091.

20. Dixit, P., & Bhushan, B., "An Enhanced Method for Copy-Move Forgery Detection Using Hybrid Feature Extraction," Journal of King Saud University - Computer and Information Sciences, 2022 (In Press).