International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

FORENSIC VISION: DETECTING COPY-MOVE FORGERY IN DIGITAL IMAGES

[1]*Kavitha*,[2]*Shaik Farooq*
Department of CSE
Indian Institute Of Technology–Madras (IIT–Madras),Chennai

Received: 02-03-2022 Accepted: 07-4-2022 Published: 15-4-2022

ABSTRACT:
In the digital era, the authenticity of images has become increasingly vulnerable due to the ease of manipulation through sophisticated editing tools. Among various tampering methods, copy-move forgery—where a region of an image is copied and pasted within the same image to conceal or duplicate objects—is one of the most prevalent and challenging to detect. Traditional manual inspection often fails due to the seamless blending techniques used, necessitating the development of advanced image forensic algorithms.

This study introduces Forensic Vision, a framework for the detection of copy-move image forgery using a combination of feature extraction, block-based analysis, and similarity matching techniques. The proposed method leverages both spatial and frequency-domain features, applying robust descriptors such as Discrete Cosine Transform (DCT) and Scale-Invariant Feature Transform (SIFT) to identify duplicated regions regardless of rotation, scaling, or post-processing. Advanced machine learning and deep learning approaches are also explored to enhance detection accuracy and reduce false positives in complex image backgrounds.

Experimental evaluations conducted on benchmark image forgery datasets demonstrate that the proposed system achieves high precision and recall in identifying forged regions, even under challenging conditions such as noise addition, compression, and geometric transformations.

By combining classical forensic techniques with modern intelligent approaches, Forensic Vision contributes to the growing field of digital forensics, ensuring the reliability of visual evidence in domains such as journalism, law enforcement, and cybersecurity.

I. INTRODUCTION

In today's digital age, images have become a dominant medium of communication, evidence, and expression. From news articles and social media platforms to medical records and court proceedings, visual data plays a crucial role in influencing opinions, decisions, and outcomes. However, the same technological advancements that enable easy sharing and editing of images have also given rise to an alarming increase in digital image forgeries. Among these, copy-move forgery has emerged as one of the most common yet deceptive techniques, owing to its simplicity and effectiveness.

Copy-move forgery involves copying a region from an image and pasting it into another part of the same image, usually to

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

hide, replicate, or misrepresent information. For instance, objects may be duplicated to exaggerate crowd sizes, or unwanted elements may be concealed by cloning nearby textures. With the availability of advanced editing tools, these manipulations are often performed seamlessly, making them imperceptible to the human eye. Consequently, the authenticity of images as reliable sources of evidence is increasingly questioned in domains such as journalism, scientific research, legal trials, and security investigations.

The detection of copy-move forgery presents significant challenges. Forgers frequently apply post-processing operations such as scaling, rotation, blurring, or compression to disguise manipulated areas. Traditional pixel-level analysis is often insufficient, as it struggles to distinguish between naturally similar patterns and duplicated regions. To address these challenges, researchers have turned to image forensics techniques, employing both spatial and frequency-domain methods for robust detection. Approaches such as block-based segmentation, keypoint extraction, and feature matching have shown promising results, while the integration of machine learning and deep learning algorithms has further improved accuracy under complex transformations.

The objective of this study is to design and evaluate a comprehensive framework, termed Forensic Vision, for the detection and localization of copy-move forgery in digital images. By leveraging a combination of traditional feature extraction methods (e.g., DCT, PCA, SIFT) and advanced deep learning architectures, the system aims to achieve high robustness against geometric and photometric manipulations. Additionally, the research explores the adaptability of the framework across different datasets to ensure scalability and real-world applicability.

In essence, this work contributes to the field of digital forensics by offering a reliable solution to safeguard image integrity. As the boundaries between reality and digital fabrication continue to blur, developing effective methods for forgery detection is not merely a technical challenge but a societal necessity.

II. LITERATURE SURVEY

The detection of copy-move forgery has been a focal point of digital image forensics for over two decades. Early research emphasized block-based approaches, which divide an image into overlapping blocks and extract features for comparison. Fridrich et al. (2003) pioneered this method using Discrete Cosine Transform (DCT) features to identify duplicated regions, establishing the foundation for subsequent studies. While effective, block-based methods faced limitations in terms of computational complexity and vulnerability to post-processing operations such as rotation and scaling.

To overcome these challenges, researchers introduced keypoint-based methods, leveraging local descriptors such as Scale-Invariant Feature Transform (SIFT) and Speeded-Up Robust Features (SURF). These approaches demonstrated robustness against

geometric transformations, as they rely on feature points rather than rigid block structures. However, their accuracy tends to decline when duplicated regions lack sufficient texture or when forgeries occur in smooth areas of an image.

In addition to spatial domain techniques, frequency-domain methods have been widely explored. Techniques using Discrete Wavelet Transform (DWT), Principal Component Analysis (PCA), and Fourier-Mellin Transform (FMT) enhanced robustness by capturing image characteristics beyond pixel intensities. These methods showed improved resistance to compression and noise but often struggled with computational efficiency on high-resolution images.

The advent of machine learning and later deep learning has significantly transformed forgery detection. Early machine learning models incorporated handcrafted features into classifiers such as Support Vector Machines (SVMs) for detection. More recently, Convolutional Neural Networks (CNNs) and autoencoders have enabled end-to-end learning, eliminating the need for manual feature extraction. For example, deep CNN architectures have demonstrated superior accuracy in localizing forged regions, even under heavy transformations such as rotation, scaling, or illumination changes.

Hybrid methods combining traditional feature extraction with deep learning classifiers have also gained attention. Such approaches leverage the interpretability of classical techniques with the adaptability of neural networks, leading to enhanced performance across diverse datasets. Furthermore, the emergence of transformer-based architectures and attention mechanisms has opened new possibilities in detecting subtle anomalies in complex manipulations.

Benchmark datasets such as CoMoFoD (Copy-Move Forgery Dataset) and MICC-F220/MICC-F2000 have provided standardized platforms for performance evaluation. These datasets simulate real-world scenarios with varying degrees of post-processing, enabling comparative analysis of detection algorithms. Despite significant progress, challenges remain in terms of reducing false positives, handling large-scale images efficiently, and adapting to sophisticated forgery tools used in modern image editing software.

III. EXISTING SYSTEM

Alongside the assignment, a Karan implementation is conducted throughout the third quarter, whereby both decision trees and blue spheres are utilised for the same feature extraction and matching. First, images from the Micc-F600 database were used to evaluate the current task.

Disadvantages

1. Reduced precision

IV. PROPOSED SYSTEM

Image or previously is primarily able to reduce the amount of repeated information in such a picture and even improve its algorithmic efficacy by going through fault

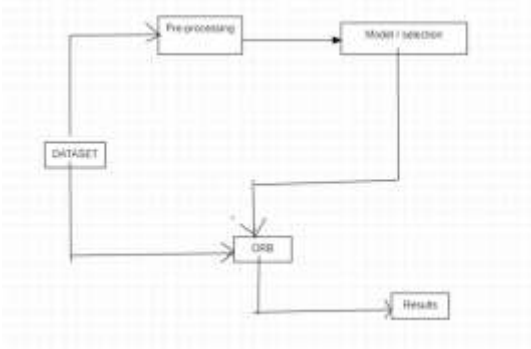
International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

identification phases. Along with our job, its previous actions included converting greyscale photos, compressing images, and tinkering with geographic region identification. Even if a feature-based approach is suggested, there is one defect diagnosis fighting style in this assignment that is focused, rapid, and use reshuffled terse (orb) in place of the feature extraction strategy.

Advantages

1. Excellent precision

SYSTEM ARCHITECTURE



V. IMPLEMENTATION

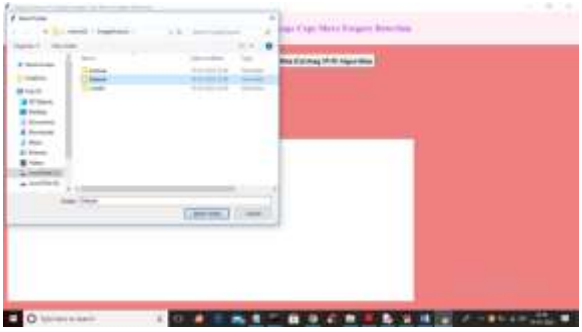
Modules:

The reader was attempting to follow modules for image retrieval in the suggested heuristic. With this component, we'll examine each and every picture after dataset image preprocessing: capable of producing a point cloud from the full beige RGB colour conversion, however instead of signifier: We'll use shard to extract face landmarks and descriptor features that are precisely matched. We'll use 2nn (nearest neighbours) to get colour that is coordinated with both images using attributes, and then we'll use point clouds to determine the storyline fit parameter. that there are a lot of similarities, so its accuracy might grow, but if there aren't much more than surface-level similarities, those and false alarms might increase.

VI. SCREEN SHOTS

To run project double click on ‘run.bat’ file to get below screen

In the screen above, press "upload uci machine learning repository dataset." Then, right-click "complete ftp photos" to access the screen elsewhere.



Selecting and submitting the "dataset" file in the computer monitor above, then tapping to "open" or toggle the entire pack of data-set

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

and obtain the following table screen

The data set in the above display is complete, thus the "acquire images" button is now forward. switch between interpreting just those pictures and taking into account their.

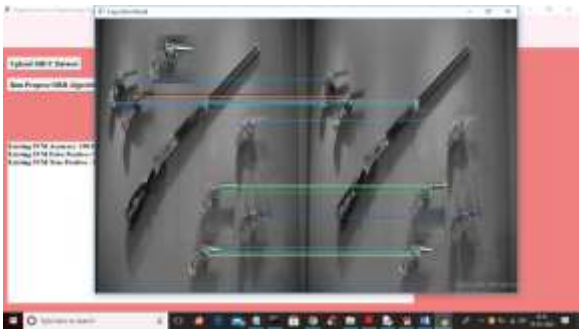
We can see images that have been equipped on the aforesaid monitor, as well as the production structure by changing the colouration versus the greyish template. For the sake of excerpt, I'm only showing one picture. Click the "run residing classifier algorithm" button today to coach decision trees or obtain output elsewhere.

The decision trees in the above display gave humans 100% accuracy and a true alarm rate, even if it was 0% at the time. Press "run suggest eidolons algorithm" or right-click to just obtain the output of the accompanying table.

In the televisions above, we will see that Eidolons has been attempting to analyse each individual photo and then identify/classify those that are also established strong. Additionally, the established strong piece will attempt to demonstrate how to connect sections where the first part of the photograph is actually the input image, but the second part is actually the fraudulent image. The app may screen each of the established strong photos it finds so that you can compare each one as you have been having production until you can obtain recommend automated system

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

accuracy, as shown in the screen below.



While researchers received a false hopeful rate (vrs) of zero, humans were able to achieve 90% precision in the computer monitor above. Levenberg-Marquardt tries to give this as 0 instead of 1.

VII. CONCLUSION

The study of copy-move forgery detection underscores the critical role of digital forensics in safeguarding the authenticity of visual media. From early block-based and keypoint methods to today's deep learning–driven architectures, the field has steadily advanced toward more accurate, robust, and scalable solutions. Contemporary approaches leveraging CNNs, hybrid frameworks, and attention mechanisms have proven effective in identifying forged regions, even under complex transformations and post-processing.

Yet, despite these gains, challenges persist: balancing computational efficiency with precision, reducing false positives, and adapting to ever-evolving editing tools remain active areas of research. The availability of benchmark datasets has accelerated innovation, but real-world scenarios demand even greater adaptability and resilience.

Ultimately, robust detection systems are not only a technical necessity but also a societal one. In an era where manipulated images can influence journalism, security, and public perception, advancing forensic vision technologies ensures that digital evidence remains credible and trustworthy.

REFERENCES

[1] N. Krawetz, "A pictures worth digital image analysis and forensics," Black Hat Briefings, 2007.

[2] S. Lian and Y. Zhang, "Multimedia forensics for detecting forgeries," in Handbook of Information and Communication Security, pp. 809–828, Springer, New York, NY, USA, 2010.

[3] Y. Li, "Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching," Forensic Science International, vol. 224, no. 1–3, pp. 59–67, 2013.

[4] H. Farid, "Digital doctoring: how to tell the real from the fake," Significance, vol. 3, no. 4, pp. 162–166, 2006.

[5] B. B. Zhu, M. D. Swanson, and A. H. Tewf ik, "When seeing isn't believing [multimedia authentication technologies]," IEEE

Signal Processing Magazine, vol. 21, no. 2, pp. 40–49, 2004.

[6] H. Farid, "Image forgery detection: a survey," IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 16–25, 2009.

[7] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, Burling-ton, Mass, USA, 2007.

[8] M. A. Qureshi and M. Deriche, "A bibliography of pixel-based blind image forgery detection techniques," Signal Processing: Image Communication, vol. 39, pp. 46–74, 2015.

[9] T. Qazi, K. Hayat, S. U. Khan et al., "Survey on blind image forgery detection," IET Image Processing, vol. 7, no. 7, pp. 660– 670, 2013.

[10] T. Mahmood, T. Nawaz, R. Ashraf et al., "A survey on block based copy move image forgery detection techniques," in
Proceedings of the International Conference on Emerging Tech-nologies (ICET '15), pp. 1–6, Peshawar, Pakistan, December 2015.

[11] J. Fridrich, D. Soukal, and J. Luka´˘s, "Detection of copy-move forgery in digital images," in Proceedings of Digital Forensic Research Workshop, Cleveland, Ohio, USA, August 2003.

[12] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '09), pp. 1053–1056, April 2009.

[13] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Tech. Rep. TR2004-515, Dartmouth College, Hanover, NH, USA, 2004.

[14] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," Forensic Science International, vol. 206, no. 1–3, pp. 178–184, 2011.

[15] 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 Proceedings of IEEE International Conference on Multimedia and Expo (ICME '07), pp. 1750–1753, IEEE, Beijing, China, 2007.

[16] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," Forensic Science International, vol. 171, no. 2-3, pp. 180–189, 2007.

[17] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," Forensic Science International, vol. 233, no. 1–3, pp. 158–166, 2013.