IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207089|

Tampered Image Detection based on CFA Artifact

Divya Chethan H D, Ms. Sandhya N

Student, Department of MCA, Visvesvaraya Technological University, The National Institute of Engineering, Mysuru, India

Assistant Professor, Department of MCA, Visvesvaraya Technological University, The National Institute of Engineering, Mysuru, India

ABSTRACT: This paper introduces a tampered image detection method based on Color Filter Array (CFA) artifacts. With the rise of digital images in critical fields like legal evidence and media, ensuring their authenticity is paramount. Our approach exploits the unique CFA patterns introduced during image capture, which are difficult to replicate in tampered regions. The methodology includes pre-processing images, extracting features using DCT and SIFT techniques, and matching these features to detect inconsistencies. The system accurately identifies and highlights tampered areas, providing clear visual results. This method enhances detection accuracy and speed, offering a reliable tool for forensic analysis and contributing to the integrity of digital media.

I. INTRODUCTION

Since the invention of photography, image manipulation has evolved from a labor-intensive process to a straightforward task with the advent of digital photography. This ease of modification has led to significant social issues, including the reliability of media images and the alteration of photographs for aesthetic purposes. Consequently, research in image forgery detection has grown in both academia and industry. Tampering, broadly defined as any post-processing action on an image, can be detected using various methods. Targeted Tamper Detection techniques identify specific manipulations like re-compression or splicing, while Universal Tamper Detection methods reveal general post-processing without specifying the type. Local Tamper Detection techniques focus on inconsistencies within different regions of an image. Our research develops a technique for fine-grained forgery localization by analyzing Color Filter Array (CFA) artifacts, specifically bi-linear interpolation artifacts, to detect and localize tampering in images.

II. OBJECTIVES

Detection is based on finding resemblance present in different segments of image. Different methods, like the Discrete Cosine Transform and the Scalar Invariant Feature Transform, are used to classify authentic and fake images and detect the forgery portion based on the type of image. Based on both time and performance, assess how well these strategies work.

- **Real-Time Application for Forgery Detection:** This system ensures quick detection of image forgeries, crucial for social media, live video feeds, and news broadcasts. It provides timely responses to prevent the spread of misinformation and ensures content integrity.
- **Fake News and Evidence Detection:** The technology helps combat false information by reliably spotting altered images used to spread fake news. It also ensures that justice is based on genuine visual information, preventing the use of tampered evidence in judicial contexts.
- **Forensic Document and Analysis:** Businesses, educational institutions, and financial institutions can verify digital documents' authenticity to avoid forgeries. The project aims to provide forensic experts with tools to detect tampering in digital photos, supporting court cases and criminal investigations.
- **Court Use:** The technology offers reliable and accurate detection of altered photos, aiding jurors and judges in making well-informed decisions based on genuine visual evidence.
- **Protection of Intellectual Property:** By authenticating digital photos and identifying illicit modifications, the system supports copyright and trademark enforcement, contributing to the protection of intellectual property rights.
- **Digital Art and Security:** The technology verifies the authenticity of digital artworks, preserving the integrity of the art market. It also strengthens security measures by ensuring that surveillance footage remains untampered, providing reliable records of events and actions.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207089|

II. LITERATURE SURVEY

[1] Ma, W., Wei, B., & Liu, S. (2007). Image Tamper Detection Based on CFA Interpolation Consistency.
[2] Lukáš, J., Fridrich, J., & Goljan, M. (2006). CFA Interpolation Artifact Analysis for Image Forgery Detection.
[3] Popescu, A. C., & Farid, H. (2005). Detection of Region Duplication Forgery in Digital Images Using CFA Patterns.
[4] Goljan, M., & Fridrich, J. (2007). Forgery Detection Based on Demosaicing Artifacts.
[5] Dong, J., Wang, W., & Tan, T. (2013). A Survey of Digital Image Forensics.
[6] Al-Qershi, O. M., & Khoo, B. E. (2020). A Comprehensive Review of Image Forgery Detection Techniques.
[7] Bayar, B., & Stamm, M. C. (2016). Deep Learning-Based Forgery Detection in Digital Images.

III. METHODOLOGY

The project's methodology encompasses the following key steps:

- In copy-move image forgery, a strong connection between copied and pasted elements of an image can be utilized to detect areas of the image that have been tampered with. The methods used to identify fakes are as follows.

1. Context Understanding
Understanding image tampering by analyzing inconsistencies in CFA (Color Filter Array) artifacts, which are unique patterns introduced during image sensor processing.
Example:
Input: "A digitally tampered photograph where a portion of the image has been altered."

2. Pre-processing
The input images are pre-processed to enhance detection accuracy. This includes converting images to grayscale, resizing, and applying low-pass filters.
Example:
Task: Converting an RGB image to grayscale to simplify the analysis of CFA patterns.

3. Feature Extraction
Extracting feature vectors that capture the unique CFA artifacts. This involves breaking the image into smaller blocks or analyzing key points within the image.
Example:
Method: Dividing the image into overlapping blocks and extracting features related to CFA patterns from each block.

4. Matching
Comparing the extracted features to detect similarities or inconsistencies that indicate tampering.
Example:
Algorithm: Using lexicographical sorting to organize and match feature vectors, identifying duplicated or altered regions.

5. Filtering
Applying filtering techniques to reduce false positives and enhance detection reliability. This involves morphological operations to refine the detection results.
Example:
Method: Using morphological operations to eliminate isolated mismatches and focus on significant tampered areas.

6. Analysis
Analyzing the filtered results to identify and localize the tampered regions within the image. This includes examining the statistical properties of the detected features.
Example:
Task: Determining the exact boundaries of the tampered regions based on the inconsistencies in CFA patterns.

7. Output Generation
Producing a final output that highlights the tampered regions, providing a visual representation of the detection results.
Example:
Result: Generating an image with marked tampered regions, along with a confidence score indicating the likelihood of tampering.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207089|

IV. TOOLS AND TECHNOLOGIES REQUIRED

Hardware Requirements

Processor : Oct Core onwards, i3, i5, i7 etc.…
Processor Speed : 2.4 GHz
RAM : 2 GB+
Hard Disk Space : 256 GB plus or 256 SSD card plus

Software Requirements

Operating System : Windows 7 and Higher
Software : MATLAB

V. CONCLUSION

The rise of digital photography has made image manipulation more accessible, leading to widespread concerns about the authenticity of images. Detecting tampered images is crucial for maintaining trust in media and advertising. Research in this area focuses on three main techniques: targeted tamper detection for specific manipulations like cloning and splicing, universal tamper detection for generic alterations, and local tamper detection for identifying inconsistencies across different image regions. Our work improves this field by developing a fine-grained forgery localization method using Color Filter Array (CFA) artifact analysis, specifically targeting bi-linear interpolation artifacts. This approach enhances tamper detection accuracy and provides reliable image authentication, beneficial for applications in journalism and forensics.

REFERENCES

[1] Ma, W., Wei, B., & Liu, S. (2007). Image Tamper Detection Based on CFA Interpolation Consistency.
[2] Lukáš, J., Fridrich, J., & Goljan, M. (2006). CFA Interpolation Artifact Analysis for Image Forgery Detection.
[3] Popescu, A. C., & Farid, H. (2005). Detection of Region Duplication Forgery in Digital Images Using CFA Patterns.
[4] Goljan, M., & Fridrich, J. (2007). Forgery Detection Based on Demosaicing Artifacts.
[5] Dong, J., Wang, W., & Tan, T. (2013). A Survey of Digital Image Forensics.
[6] Al-Qershi, O. M., & Khoo, B. E. (2020). A Comprehensive Review of Image Forgery Detection Techniques.
[7] Bayar, B., & Stamm, M. C. (2016). Deep Learning-Based Forgery Detection in Digital Images.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details