JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IMAGE FORGERY DETECTION USING MD5 AND OPENCV

[1]K Jagadeeswari, [2]P Lakshmi Priyanka, [3]V Ganesh, [4]M Nayum Basha, [5]B Mamatha

[1]Assistant Professor,[2345]Student
[12345]Department of Artificial Intelligence& Data Science
[12345]Annamacharya Institute of Technology & Sciences, Tirupati,
Andhra Pradesh – 517520 India

***Abstract*: With the rise of sophisticated image editing tools, verifying the authenticity of digital images has become increasingly challenging. This work focuses on detecting image forgery by utilizing a hybrid approach that combines MD5 hashing and OpenCV-based visual analysis. The process begins by generating an MD5 hash for each image, serving as a unique digital identifier. If two images produce the same hash, they are considered identical. However, even minor edits can change the hash, helping to flag altered images. To complement this, OpenCV is employed to perform pixel-level and structural comparisons between images. This allows for detection of subtle modifications such as splicing, cloning, or region tampering that might evade hash-based detection alone. By merging the fast, lightweight nature of MD5 hashing with the detailed visual inspection capabilities of OpenCV, the system ensures a more robust method for identifying image manipulations. This approach can be particularly useful in digital forensics, media validation, and secure archival systems.**

***Keywords*—Image forgery detection, MD5, OpenCV, image comparison, hashing.**

I. INTRODUCTION

In today's digital era, images are essential tools in fields like journalism, social media, law enforcement, and documentation. However, the ease with which images can be manipulated using advanced editing tools has led to a surge in image forgery. These alterations can have serious consequences—ranging from spreading misinformation to tampering with evidence in legal proceedings. Traditional, manual methods of identifying forged images are often inefficient and prone to human error, especially when dealing with subtle manipulations. This has created a growing demand for reliable and automated methods to verify image authenticity.

This project addresses the issue by introducing an image forgery detection system that leverages two powerful tools: MD5 hashing and OpenCV. The approach integrates cryptographic hashing to detect structural changes and visual analysis techniques to uncover tampering at the pixel level. MD5 (Message Digest Algorithm 5) generates a unique digital fingerprint for every image. Any small alteration in the image results in a different hash, enabling quick detection of tampering. OpenCV, an open-source computer vision library, provides tools to perform in-depth visual comparisons, identifying inconsistencies such as copy-move forgery or local edits that may not affect the overall hash. Together, these methods form a dual-layered solution for accurate and fast image verification.

A. Objective of the Study

The primary aim of this study is to develop a robust, automated system for detecting image forgery using MD5 hashing and OpenCV-based visual comparison. As image tampering becomes more sophisticated, it is increasingly difficult for humans to detect such changes without the aid of technology. This project proposes an efficient framework that combines the speed of MD5 hashing with the accuracy of visual inspection through OpenCV. The goal is to ensure digital image integrity across various sectors by providing a solution that is scalable, reliable, and easy to deploy.

B. Scope of the Study

This study focuses on building an image verification system that compares two input images to determine if they are identical or if one has been altered. The system first uses MD5 hashing to generate and compare hash values for both images. If the hashes differ, it immediately flags a discrepancy. If the hashes match, the system proceeds with OpenCV-based visual analysis to inspect for pixel-level changes that might not affect the hash. By combining cryptographic checks with visual validation, the system ensures comprehensive detection of image tampering. Additionally, verified

images can be stored in a secure database for future reference or audits. This system is intended for use in real-world scenarios such as news reporting, digital content verification, and legal documentation.

C. Problem Statement

Despite the widespread use of images in digital communication, verifying their authenticity remains a challenge due to the availability of powerful editing tools. Current detection methods are either too simplistic or computationally demanding, often failing to catch subtle manipulations. This project proposes a balanced approach that uses MD5 hashing for fast, structural verification and OpenCV for deep visual analysis. By combining these techniques, the system aims to detect both obvious and hidden modifications, offering a dependable solution for image forgery detection.

II. Related Work

The rapid advancements in image editing software and the ever-meressing dependence on visual data for digital commutacation have tunned image forgety detection into a very important area of research Moch work has been done to improve forgery detection accuracy and reliability by using different techniques which mclude cryptographic hashing functions and computer-vision algorithms. The present literature survey makes an attempt to indicate some major contributions concerning the integration of MD OpenCV and SHA256 in connection with image forgery detection [1].

Bhatia and Ghosal (2018) proposed a hybrid approach using MIDS and SHA algorithms to generate unique hash values for image swathentication. Their study demonstrated that combming multiple lashing techniques eulances detection accuracy and provides robustness agamst various emage manipulations, emphasizing the value of hybrid cryptographic approaches in forgery detection systems [2].

Chen and Zhang (020) conducted a comprehensive survey on image forgesy detection techniques hased on visual features, highlighting the effectiveness of using OpenCV in conjunction with machine learning algorithms. The study concluded that visual inconsistencies at the pitel level can be accurately detected using computer vision tools, significantly improving the system's ability to identify subtle tampering [3].

Thang and Wang (2019) explored hashing functions like MLIS and SHA256 integrated with OpenCV for detecting forgenes in digital images. Their research confirmed that cryptographic hash functions offer high-speed detection of mage alterations, while OpenCV adds a layer of visual verification to ensure comprehensive analysts [4].

Sharma and Kumar (2017) imrodnced a method that comhines MIDS hashing and pixel-level comparison for detecting tampered regions in images Their findings showed that MD5 efficiently identifies changes in image data, and the use of OpenCV for structural comparison further validates the authenticity of the marge [5].

Singh and Arora (2016) evahated deep learning models for image forgery detection in comparison to traditional hashing methods. While deep learning demonstrated promising results in classification, the authors concluded that integrating simpler approaches like MDS and OpenCV could offer a more metastable and pet fumance-balanced soluhon for real-world applications [6].

Zhan and Liu (2021) developed an image authentication system ning SHA256, citing its superior cryptographic strength compared to MIDS Their work emphasized the enhanced security and reliability of SHA256 in forgery detection, especially in sectors requiring high data integrity such as legal and governmental doza [7].

Patel and Mehta (2018) investigated OpenCV's capability in real-time forgery detection, focusing on visual discrepancies such as splicing cropping and resizing. Their research demonstrated OpenCV's effectiveness is capturing minor yer critical image alterations that may be missed by hashing techniques alone [8].

Khan and Ahmed (2017) proposed a combined approach uning image hashing and visual analysis techniques. The integration of cryptographic and computer vision methods improved detection accuracy and speed confirming the benefits of a dual-layered strategy for robust image verification [9].

Li and Yu (2019) enhanced forgery detection by combining SHA256 with visual festare matching sing OpenCV Their approach proved effective in detecting both localazed and global tampering, offering a rehable framework suitable for ingh-stakes cuvnomments such as forensic movestaganous [10].

Lastly, Singh and Gupta (2000) presented a system that utilizes MDS and SHA256 hashing in conjunction with pixel analysis via OpenCV Their stady reported that the proposed system outperforms conventional methods by detecting even minor manipulations, thereby validating the effectiveness of a multi-layered detecnon mochanun [11].

III. Architecture Details

Modules

1. Image Upload Module

Function: This module allows users to upload two digital images that need to be compared for potential forgery. It manages image file input and ensures the files are ready for further processing.

Features:

Provides an easy-to-use interface for selecting and uploading images.

Supports commonly used image formats such as JPEG and PNG.

Validates file types and handles unsupported format errors gracefully.

2. MD5 Hash Generation Module

Function: This module creates a unique MD5 hash for each uploaded image. These hashes serve as digital signatures, which help determine whether any change has been made to the images.

Features:

Calculates MD5 hash values for both images.

Compares the two hash values to check for integrity and detect any tampering.

Offers hash outputs for transparency and verification steps.

3. Image Comparison Using OpenCV Module

Function: OpenCV is used here to perform a detailed visual comparison between the two uploaded images. Unlike hashing, which detects binary changes, OpenCV highlights visual discrepancies at the pixel level.

Features:

Performs pixel-by-pixel comparison to detect subtle image modifications.

Identifies changes such as cropping, object insertion, or color alterations.

Can generate visual overlays or difference maps to clearly show altered regions.

4. Forgery Detection Module

Function: This component evaluates the results from both the MD5 and OpenCV modules to determine whether the uploaded images are identical or tampered.

Features:

Combines hash comparison and pixel analysis results.

Declares the image as forged if either the MD5 values differ or OpenCV detects differences.

Notifies the user about the outcome with relevant details.

5. Database Storage Module

Function: Stores verified authentic images (those that passed both MD5 and OpenCV checks) in a database for secure record-keeping and future verification.

Features:

Maintains a collection of verified images with associated metadata.

Supports retrieval and auditing of stored images.

Ensures secure handling and access control for stored image data.

6. User Interface (UI) Module

Function: Offers an interactive front-end for users to engage with the system, upload files, and view comparison outcomes.

Features:

User-friendly interface for image selection and result visualization.

Displays computed MD5 hashes and highlights visual differences.

Provides immediate feedback on whether images are identical or altered.

IV. EXISTING METHODOLOGY

Image forgery detection using OpenCV and MD5 typically involves a mix of visual analysis and data integrity checks. MD5 is mainly used to verify the integrity of an image by generating a unique hash value. If even a single pixel is altered, the MD5 hash will change, making it easy to detect that some modification has occurred—though it won't show where or what was changed. On the other hand, OpenCV is used for more in-depth analysis to localize and understand the forgery. Techniques like copy-move detection use OpenCV's feature extraction and matching tools (such as SIFT or template matching) to find duplicated regions within an image, which is common in forgeries. Another method is error level analysis, where the image is recompressed and differences between the original and recompressed versions are analyzed to reveal areas with varying compression levels, hinting at tampering. Image splicing can also be detected by analyzing edges or noise patterns using OpenCV. Inconsistencies in edge smoothness or noise distribution can suggest that parts of different images were combined. These methods don't need pre-embedded data and are known as passive forgery detection techniques. Combining MD5 with OpenCV-based visual analysis can provide both verification and localization of tampered content.

.

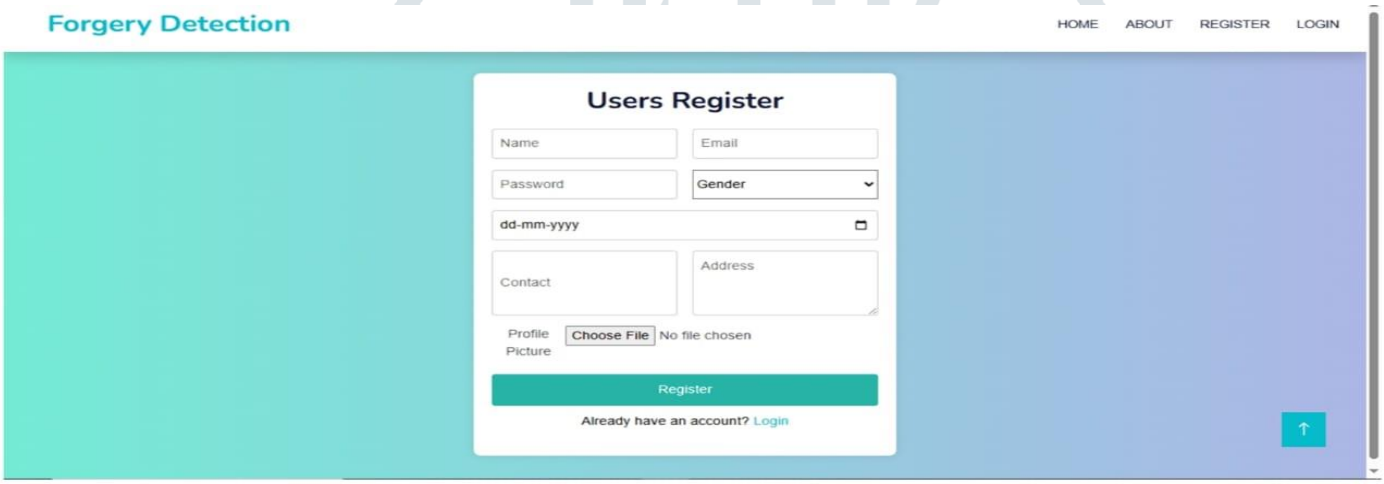
V. PROPOSED METHODOLOGY

The proposed image forgery detection system combines the efficiency of MD5 hashing with the precision of OpenCV-based visual analysis to verify the authenticity of digital images. The process begins by generating an MD5 hash for each image, which acts as a digital fingerprint. Since even a minor alteration in the image, such as modifying a single pixel, results in a completely different hash, this method provides a fast and effective way to detect tampering. The system compares the hashes of two images—if they differ, the image is flagged as modified.

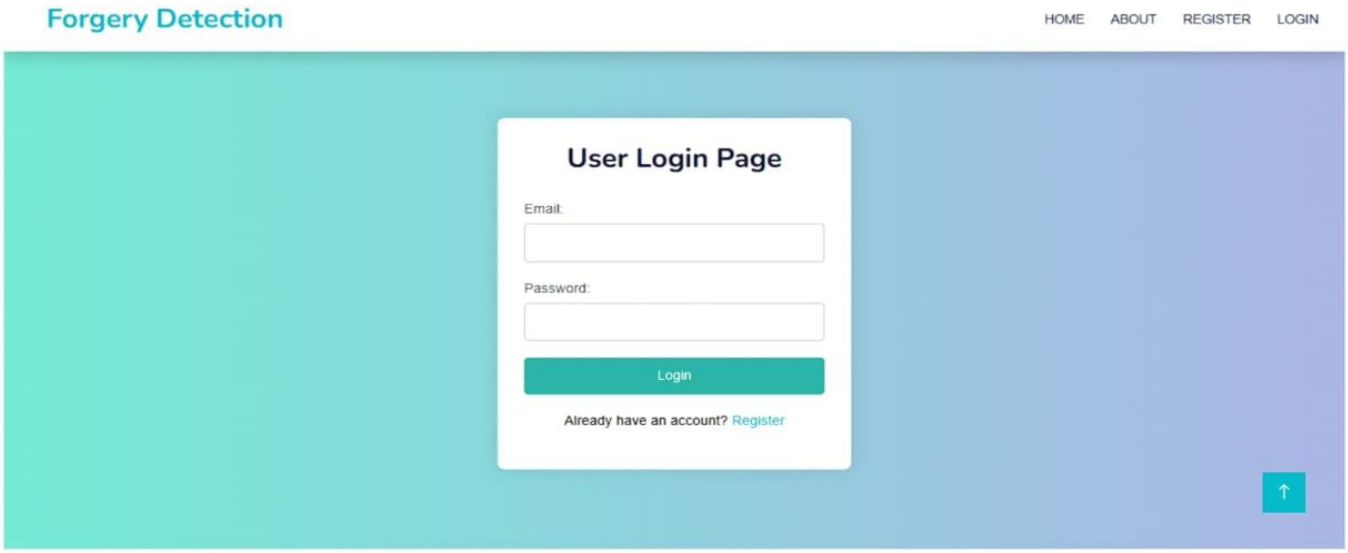
However, some sophisticated image forgeries might not cause significant changes in the hash value. To overcome this limitation, the system incorporates OpenCV for detailed pixel-level analysis. OpenCV compares the structural and visual elements of the images, identifying manipulations such as object insertion, splicing, or region duplication that might go undetected through hashing alone. If both the MD5 hash and the OpenCV visual comparison confirm image similarity, the image is considered authentic and securely stored. This dual-approach ensures both speed and accuracy in detecting image forgeries, making it a practical tool for digital forensics, journalism, and content authentication.

VI. RESULTS AND ANALYSIS

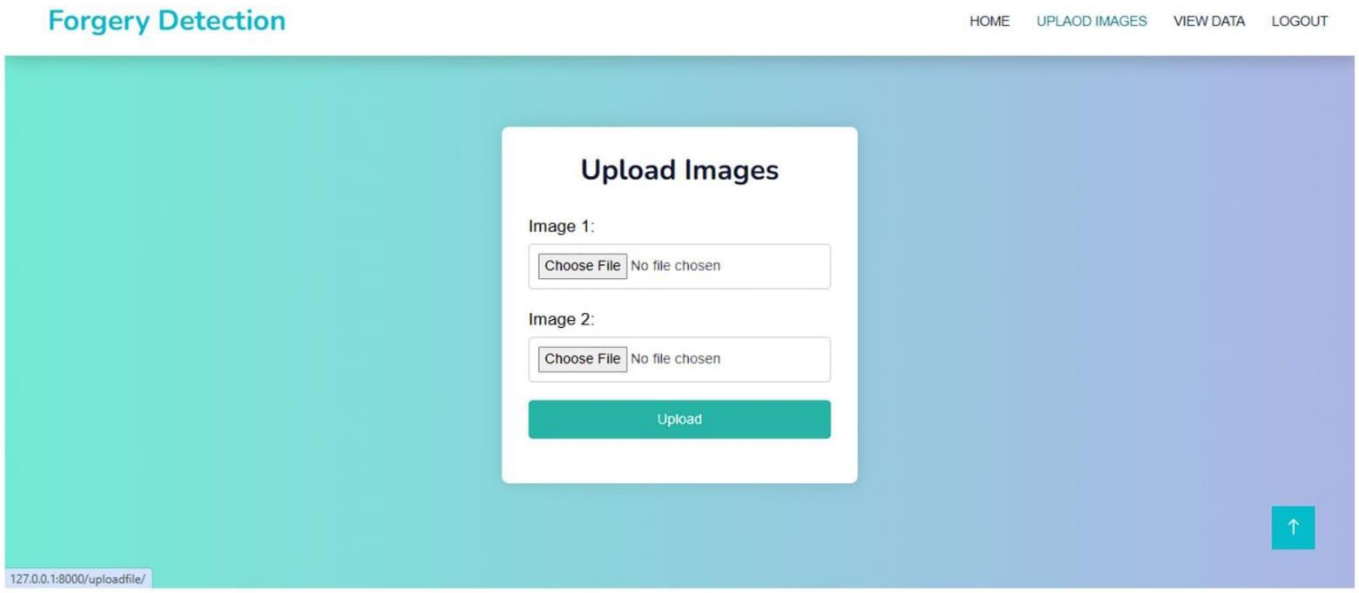
Registration Page: here user can register



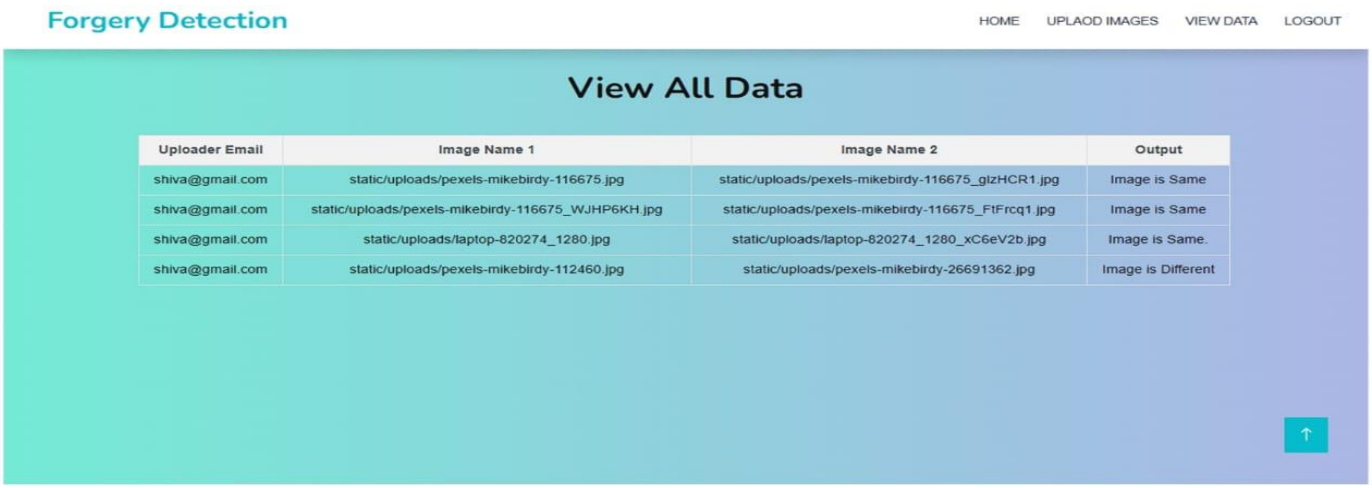
Login Page: here user can login



Upload Page: User can upload file here



View Page: User can view all the data



VII. CONCLUSION

The proposed system demonstrates an effective and practical approach to image forgery detection by integrating MD5 hashing and OpenCV-based visual analysis. This dual-layered method leverages the strengths of both cryptographic and image processing techniques to accurately detect manipulations in digital images. MD5, as a lightweight and fast hashing algorithm, generates unique hash values for each image. Any minor modification in the image content results in a different hash value, making it an efficient way to detect tampering at t2he data level. By comparing these MD5 hashes, the system quickly identifies structural changes or inconsistencies between two images. Complementing the hashing technique, OpenCV offers detailed pixel-level analysis that can detect subtle visual modifications that might not alter the file's hash. These include localized edits such as cloning, splicing, cropping, or the addition of foreign elements to the image. OpenCV enables a thorough comparison by highlighting differences in the visual content, thus ensuring that even undetected alterations from the hash comparison can be caught. The combination of MD5 and OpenCV provides a balanced and efficient framework that ensures digital image authenticity. This system can be widely applied in fields like journalism, law enforcement, legal documentation, and digital forensics where verifying image credibility is crucial. With its user-friendly design and robust accuracy, the system ensures only genuinely altered images are flagged, reducing false positives and enhancing trust in visual content.

VIII. REFERENCES

1. Bhatia P & Ghosal S (2018) "Image Forgery Detection Using Hybrid MIDS and SHA Algorithms" International Journal of Comprater Science and Engmeering, 7(5), 112-121
2. 2) Chen, S. & Zhang, Y. (2020). "A Survey on Intage Forgery Detechon Techniques Based on Visual Features" Journal of Degital Forensics, 13(3), 55-68

3. 3) Zhang, J., & Wang Z (2019) "Forgery Detection in Digital Images Using Hashing Functions and OpenCV Journal of Image Processing and Computer Vision, 34(2), 98-106
4. 4) Shania, S., & Клани, A. (2017). "Detechon of Image Tampering Using MD5 Hasling, and Pixel Comparison" International Journal of Computer Vision and Image Processing, 8(2) 76-83
5. 5) Singh. V & Arora, R. (2016). "Deep Learning Models for Image Forgery Detection" Proceedings of the International Conference on Machine Learnung, 45(4), 234-240
6. 6) Zhao L. & Lim. X (2021) "SHA256-Based Image Authentication and Forgery Detection System. IEEE Transacions on Image Processing, 30(1), 23-34
7. 7) Patel, H., & Mehta. P. (2018). "OpenCV Based Real Time Forgery Detection in Digital Images." Journal of Real-Time Systems, 40(6), 1005-1017.
8. 8) Khan, M. & Ahmed, M. (2017) "Combining Image Hashing with Visual Analysis for Forgery Detection luzernational Journal of Digital Imaging and Forensics, 18(2), 210-219.
9. 9) Li, X. & Yu, L. (2019) "Enhanced Image Forgery Detection with SHA256 and Visual Feature Matching International Journal of Image and Graphics, 26(3) 189-200
10. 10) Singh. A., & Gupta, 5. (2020). "hoage Forgery Detection Using Hashing and Pixel Analysis." Journal of Information Security, 9(5), 112-11
11. 11) Kamar A & Ram, S. (2018) "Hybrid Image Forgery Detection Using SHA256 and Feature Extraction Journal of Computer Vision and Image Processing, 20(2), 85-96
12. 12) Kauz, A. & Aura. N. (2020). "Comparative Analysis of Image Forgery Detection Techniques. A Survey." International Journal of Computer Applications, 12(6), 45-58
13. 13) Slamma, R. & Mota, M. (2019). "Security Enlunicemens m Image Forgery Detection Usmy OpenC International Conference on Artificial Intelligence and Image Processang, 23(4), 512-524.
14. 14) Pati, S., & Nayak. P. (2017). "Image Forensics Uung OpenCV and Cryptograpluc Haslung." Journal of Computer Security and Cryptography, 11(1), 101-115
15. 15) Ahmed, R., & Singh. V. (2021) "Image Forgery Detection Using Cryptographir and Vimal Analysis" Computer Vision and Image Analysis. 28(7), 303-311