e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com

IMAGE FORGERY DETECTION SYSTEM

Sumaira A. Shaikh[*1], Amar M. Sakore[*2], Prerana A. Kharat[*3], Sachin Raj[*4], Harshal R. Chavhan[*5]

[*1]Professor, Computer Engg., Sinhgad Academy Of Engineering, Pune, Maharashtra, India.

[*2,3,4,5]Student, Computer Engg., Sinhgad Academy Of Engineering, Pune, Maharashtra, India.

DOI: https://www.doi.org/10.56726/IRJMETS30944

ABSTRACT

Digital image forgery refers to the practice of misleading a viewer of a digital image by altering the image to hide some significant or crucial data. It is typically challenging to identify the portion of the original image that was altered. The identification of picture forgeries is crucial for maintaining the image's integrity. With the use of picture editing software, digital photos may now be easily edited thanks to the use of contemporary technology and photography. Consequently, it is essential to spot picture tampering activities. On the basis of object removal, object addition, and unexpected size adjustments in the image, image fraud detection can be carried out.

I. INTRODUCTION

In the modern era, there is an abundance of digital imagery available to us. Previously, we had complete faith in the purity and authenticity of this imagery, but modern technology has eroded that faith. From prestigious publications to the media sector, legal proceedings, retail stores, academic journals, political campaigns, and the photographic satire that lands in our inboxes and on social media. Photographs that have been altered are showing up more frequently. Without a doubt, the authenticity of images is a major concern right now. To confirm the validity of the altered image, there are two basic categories of image forgery detection. The first is the Active approach, and the second is the Passive way, and they are both further detailed in the literature. Watermarking and Steganography are two main categories under the active methods where the authentic information is inserted into the digital image. When it's necessary to check the legitimacy of the photograph, the previously saved information is used to shed light.

The most common approach to fake an image using passive methods is a copy-move forgery. It involves copying from the image and pasting it back into the original image.

Different ways to manipulate an image:

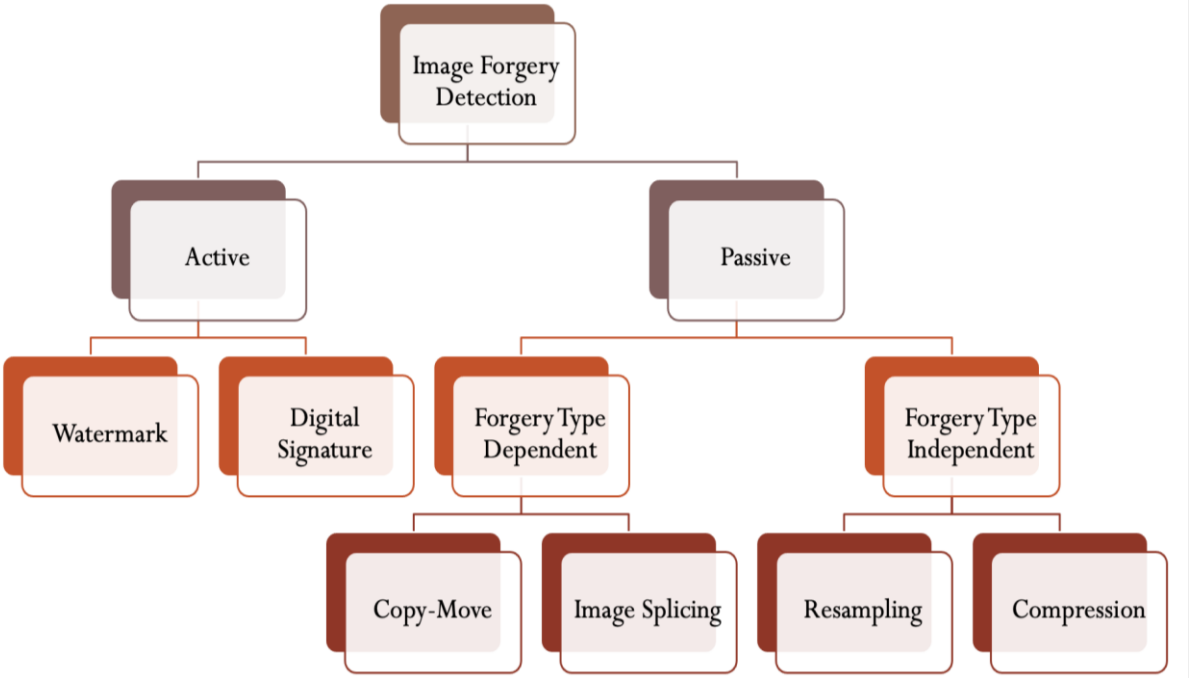
1. Image Splicing: Copying regions from an authentic image and paste them to other images.
2. Copy-Move: Copies and pastes regions within the same image.
3. Removal: Eliminates regions from an authentic image followed by in painting.

II. IMAGE FORGERY DETECTION TECHNIQUES

Forgery identification determines the genuineness of pictures. Different methods have been developed to verify verified photos. In this study, we categorise several techniques into two groups:

- Active techniques
- Passive techniques

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com



Active Forgery Identification Techniques

An active forgery detection technique needs information that has already been retrieved or implanted. Eg. Watermark, Digital signature

Passive Forgery detection Techniques

Passive methods, popularly known as blind methods, merely uses the image itself for its authentication and integrity. This approach makes the assumption that, even if there are no obvious signs of tampering in the image, tampering may still affect the underlying statistics due to noise inconsistencies, image blurring, image sharpening, forgery through copy-move, and image inpainting, among other things.

Techniques that depend on the type of counterfeit done on the image, such as splicing, are designed to distinguish only specific kinds of forgeries.

Techniques that are independent of fraud can identify forgeries based on artefact traces left behind by the sharpening and blurring process as well as irregularities caused by shade and light effects.

III. HARDWARE AND SOFTWARE REQUIREMENTS

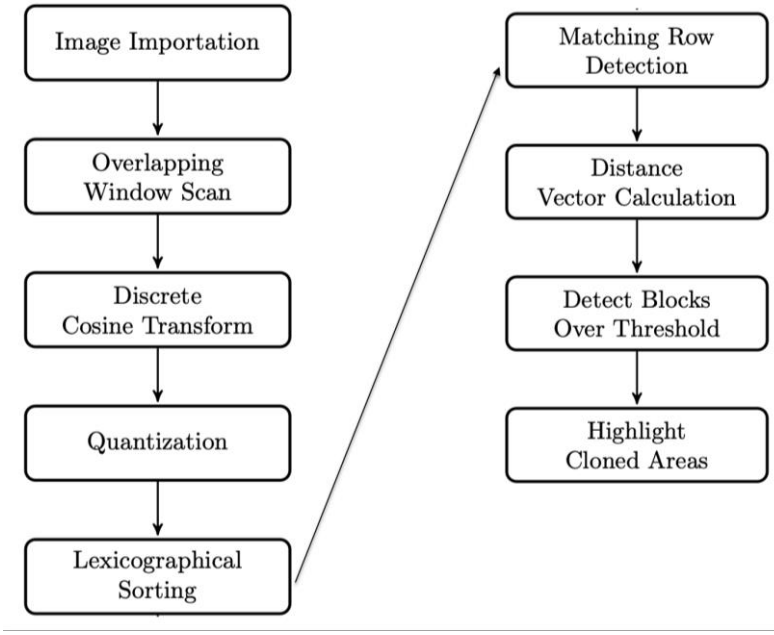
Software	Description
Operating System	Microsoft Windows 10
Database server	MySQL
Web Server	Xampp
Programming IDE	Jupyter Notebook , Google Collab
Browser	Google Chrome , Microsoft Edge

Hardware	Description
Processor	Intel Core i7 @ 2.70 GHz
Memory	8.00 GB
Hard Disk Space	256 GB
Device	HP Pavilion
Others	Other required standard computer peripherals, such as keyboard and mouse.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com

IV. CLONE DETECTION ARCHITECTURE

The problem of clone detection, also known as "copy-move detection," is crucial for picture authenticity. Clones are a unique type of image alteration where a portion of the original image is cloned, maybe altered in size, rotation, or other ways, and then pasted in a different area of the original image



FORGED JPEG IMAGE

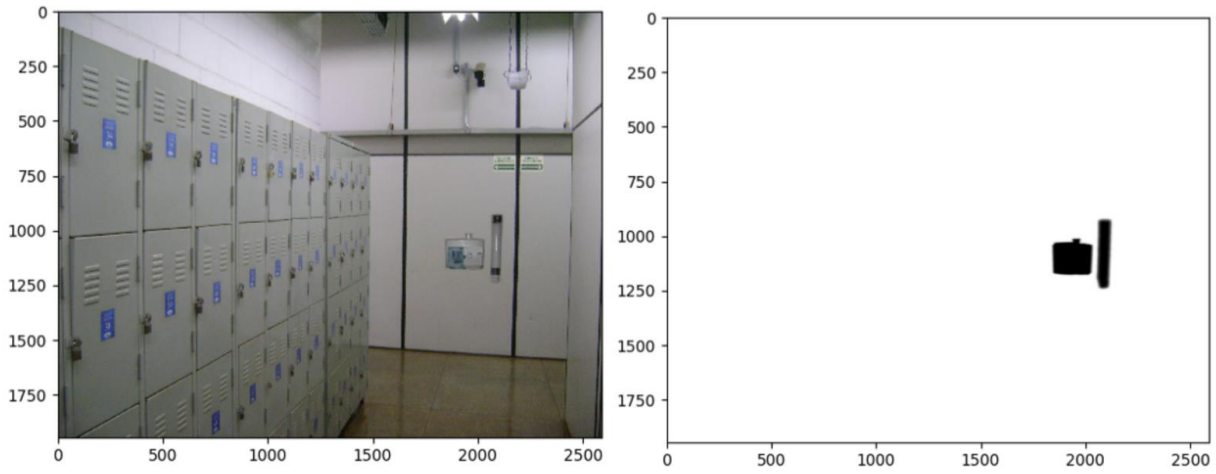
CLONE DETECTION RESULT

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com

V. METHODOLOGY

DATASET:

Only the trained set is utilized for this project. It has two directories: one with perfect photographs and the masks that go with them, the other with bogus images. A fake image's mask is a black-and-white (not grayscale) image that shows the fake image's spliced region. The spliced region is represented by the black pixels in the mask, which represent the area in the source image where alteration was done to produce the forged image.



The dataset includes 450 false photos and 1050 real images. Normally, colour images consist of three channels, one for each of the colours red, green, and blue; however, occasionally a fourth channel for yellow may be present. Our dataset contains a variety of 1, 3, and 4 channel pictures.

ANNOTATING IMAGES:

We chose to use an open supply for our work because we underestimated the time needed to name the pictures. After the photographs were annotated, all of the files were saved in the txt format.

VI. CONCLUSION

In the proposed system, we have implemented different concepts of image forgery detection algorithms. The system is capable of taking input image and give out suitable outputs to solve the obstacle of forged images. The system can be used in law and enforcements and cyber security to help the user to differentiate between legitimate and tampered images. The system can be used to help the user to differentiate between legitimate and tampered images.

VII. REFERENCES

[1] Image forgery detection: a survey of recent deep-learning approaches [Marcello Zanardelli , Fabrizio Guerrini, Ricardo Leonardi & Nicola Adami]-2022

[2] Image Forgery Detection using Deep Learning: A Survey [Zankhana J. Barad Mukesh M. Goswami]-2020

[3] A Survey on Image Forgery Detection Using Different Forensic Approaches [Akram Hate Saber, Mohd Ayyub Khan]-2020

[4] A Review on Copy-Move Image Forgery Detection Techniques [Zaid Nidhal Khudhair, Farhan Mohamed and Karrar A. Kadhim]-2019

[5] A Survey on Image Forgery Detection Using Different Forensic Approaches [Akram Hatem Saber, Mohd Ayyub Khan, Basim Galeb Mejbel]-2020

[6] A Study on Image Forgery Detection Techniques [Shijo Easowa*, Dr. L. C. Manikandanb], International Journal of Computer (IJC) -2019

[7] A Systematic Study of Image Forgery Detection [Dr. Santhosh Kumar (Guru Nanak Institute of Technology)]-2018

[8] An Analysis of Image Forgery Detection Techniques[Chandan Deep Kaur, Navdeep Kanwal]- 2019.

[9] Image Forgery Detection Using Analysis of CFA Artifacts Yogesh Katre 1, Prof. Gajendra Singh Chandel,

International Journal of Advanced Technology in Engineering and Science Volume No.02, Special Issue No. 01, September 2014.

[10] Image Forgery Localization via Fine-Grained Analysis of CFA Artifacts Pasquale Ferrara, Tiziano Bianchi, Member, IEEE, Alessia De Rosa, and Alessandro Piva, Senior Member, IEEE, IEEE Transactions on Information Forensics and Security, Vol. 7, No. 5, October 2012.

[11] An Overview of Image Steganography T. Morkel 1, J.H.P. Eloff 2, M.S. Olivier 3 Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

[12] Effective Python-59 specific ways to write better python 1st Edition by Brett Slatkin, 2015.

[13] Detection of Image Forgery[Shubham Sharma , Sudeeksha Verma , Swapnil Srivastava]-2020.

[14] A Review on Digital Image Forgery Detection[Jahnavi Ega, Deepak Sri Sai Krishna, V. M. Manikandan]-2021.

[15] Image forgery and its detection: A survey[M. Arun Anoop]-2015.