Image Tampering Detection System

Ashay Sonak[1], Aman Sharma[1], Rohit Ramteke[1], Vishal Yadav[1], Shruti Kolte[2]

[1]Student, Department of Computer Science Engineering, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, India.

[2]Professor, Department of Computer Science Engineering, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, India.

Corresponding Author: ashay.sonak.as@gmail.com

Abstract: - In today's technical world, the digital image is a vital part of many application domains. The meaning of image forgery is the manipulation of digital images to hide important information or output false information. Due to the introduction of modern image processing tools, digital image forgery is at its peak. Copy-move forgery is one of the most commonly used techniques to perform image forgery. The aim of the proposed system is to detect and highlight the malpractices performed on modern-day digital images.

Key Words: —*Image forgery, Digital images, Image Tampering.*

I. Introduction

A digital image is an image or picture represented digitally. It is a numeric representation, normally binary, of a two-dimensional image. The digital image is a crucial means to distribute information on the Internet that is extensively used in almost every field. Some digital images might involve business secrets and even national security. Internet development and multimedia have made the process of distribution easy making the content security of pictures a crucial issue for scientists and engineers. Image processing can be used to convert a picture into a digital image and then manipulate it in order to extract desired data from it. Image processing mostly deals with the processing of images, pictures, video, etc. Image processing is any type of signal processing in which the input is an image, such as a photograph or a video frame, and the output is either an image or a set of image-related features or parameters. Image processing can include working with image zooming, image segmentation, image enhancement, video, and image compression.

Due to the advancements in technology and thus in image editing and processing software, it is very difficult to directly identify real images over fraudulent ones. This trend reveals major flaws and reduces the trustworthiness of digital photographs. Therefore, a need is felt to develop a system that can be used to check the authenticity and integrity of digital images as these images are usually used for important daily technical decisions and tasks.

II. Image Tampering

2.1 Copy-Move Forgery

Copy move forgery is a technique for producing a compound image by removing an object from one image and replacing it with another. It entails creating new items or hiding areas in the forged image utilizing spliced areas from the same or different image or photographs. This is frequently done with the goal of hiding an object from the image by covering it with a segment duplicated from another portion of the image.

2.2 Double Jpeg Compression Detection

Double compression in JPEG images occurs when a JPEG image is decompressed to the spatial domain and then resaved with a different (secondary) quantization matrix. Tampering with JPEG images often involves recompression, i.e., resaving the forged image in the JPEG format with a different compression quality factor after digital tampering, which may introduce evidence of double JPEG compression.

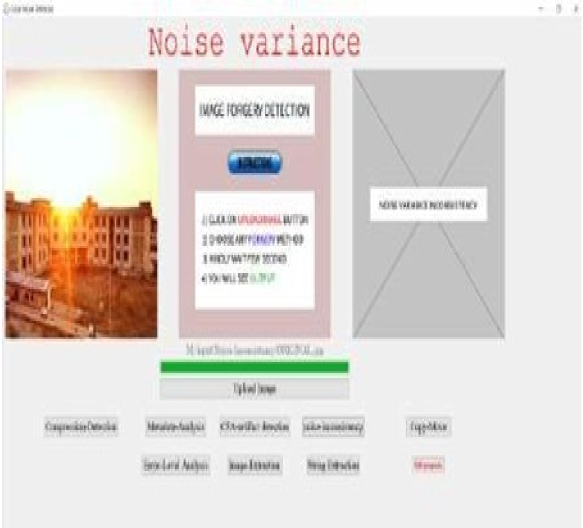
Manuscript revised April 24, 2022; accepted April 25, 2022.
Date of publication April 27, 2022.

This paper available online at www.ijprse.com

ISSN (Online): 2582-7898; SJIF: 5.59

2.3 Noise Variance Inconsistency

To mask the signs of the tampering process, the most widely employed method is noise. Variations or inconsistencies can also be caused by other factors such as colour, lighting, or texture. The original image usually has homogeneous noise all over it. As a result, finding noise irregularities in an image could indicate manipulated regions.



Noise variance

IMAGE FORGERY DETECTION

1) CLICK ON UPLOADIMAGE BUTTON
2) CHOOSE ANY FORGERY METHOD
3) KINDLY WAIT FEW SECONDS
4) YOU WILL SEE OUTPUT

Fig.1. Noise variance inconsistency detection using the proposed system

2.4 Metadata Analysis

The information and exact features of a single image file are referred to as photo metadata. Date created, creator, file name, content, themes, and other details are frequently included. More complex features can be extracted using image metadata including origin device, origin software, dimensions, time created, compression details, etc.

2.5 Error Level Analysis

Image error level analysis is a technique for detecting changes to compressed (JPEG) images by detecting the distribution of errors introduced after the image is resaved at a specified compression rate. ELA works by re-saving the image at 95% compression and comparing the results to the original. Because of their distinctive characteristics in the ELA depiction, modified areas are immediately visible. ELA algorithm takes factors like shadows, eyes, and reflections into consideration to display hidden details of the input image.

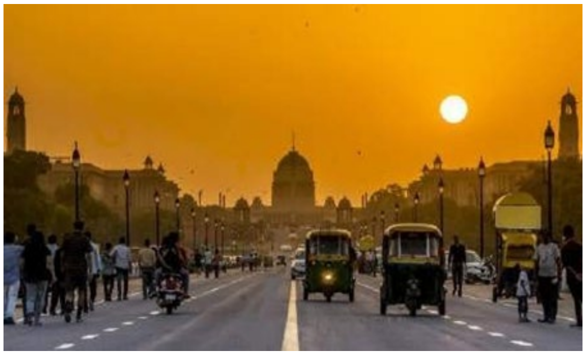


Fig.2. Input image for ELA

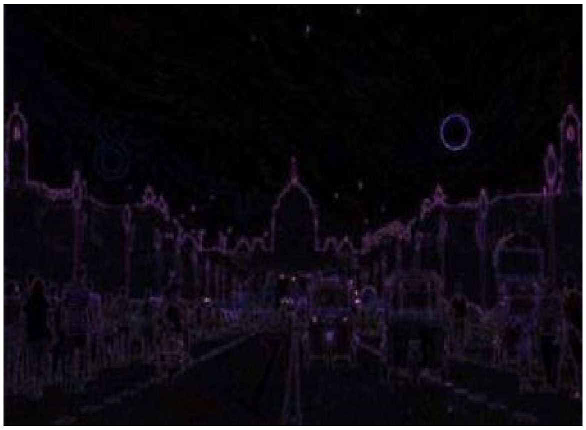


Fig.3. Output of ELA using the proposed system

2.6 String Extraction

Binary structures, binary data, and textual values are commonly found in media files. All possible textual values are extracted using the strings analyzer. A string is any succession of text letters and spaces in technical terms. When strings are retrieved from a file, binary or non-printable characters are not displayed. The file is parsed by the string’s extractor. It shows every byte sequence that might be used to create text characters.

2.7 Image Extraction

The most common cover objects for steganography are photographs. Many various picture file formats exist in the realm of digital photographs, the majority of which are designed for specialized applications. Different steganographic algorithms exist for these various image file types. Image stegnography is hiding information that is easily not visible to human eye. Image extraction is the process of extraction of this hidden information.

Fig.4. Input image for image extraction

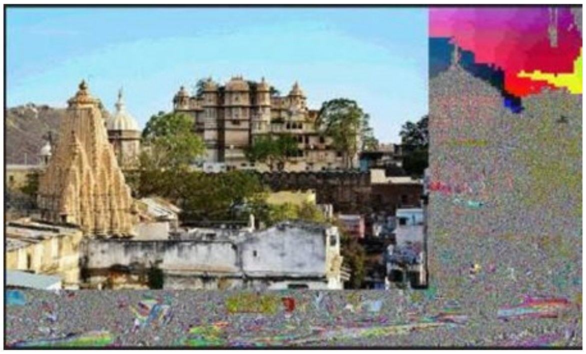


Fig.5. Output of input image for image extraction using the proposed system.

2.8 CFA Artifact Detection

The CFA is made up of a mosaic of spectrally selective filters that are organized in an interleaved pattern such that each pixel registers just one of the color spectrum's components. Image counterfeiting can be detected by analyzing the artefacts left in the image by the interpolation process. In an ideal world, an image from a digital camera would exhibit demosaicking artefacts on every group of pixels corresponding to a CFA element in the absence of any subsequent processing.

III. Result And Discussion

The system is functional in identifying and extracting Double JPEG Compression Detection, Copy-Move Detection, CFA Artifact Detection, Error Level Analysis, String Extraction, Image Extraction, Metadata Analysis out of input image. The home page of the UI consists of an image displaying box and an output displaying box. The user is provided with ten different interactive buttons and useful instructions at the center for the convenience of the user. The user needs to click on the "Upload Image" button which will open a pop-up file manager box allowing them to choose the input image out of local drive.

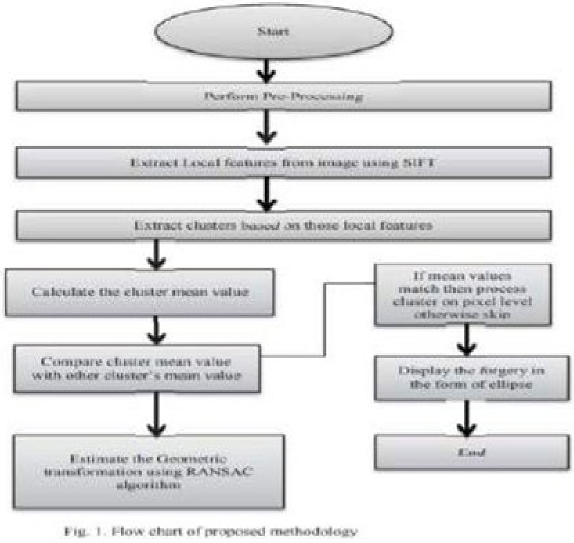

Start
Perform Pre-Processing
Extract Local features from image using SIFT
Extract clusters based on those local features
Calculate the cluster mean value
Compare cluster mean value with other cluster's mean value
Estimate the Geometric transformation using RANSAC algorithm
If mean values match then process cluster on pixel level otherwise skip
Display the forgery in the form of ellipse
End
Fig. 1. Flow chart of proposed methodology

Fig.6. Process flow diagram

The system allows the user to choose any of the techniques and produce suitable outputs through output window on the UI or pop-up windows or in the forms of images. The system works locally on the system without the requirement of network access.

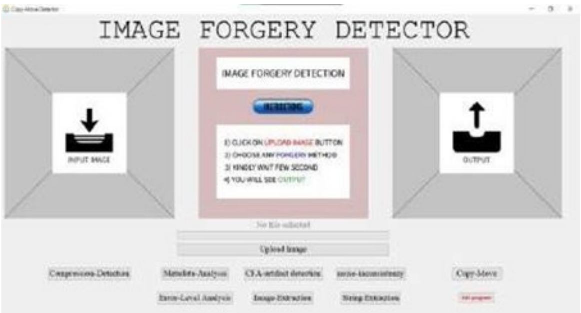


IMAGE FORGERY DETECTION

1) CLICK ON UPLOAD IMAGE BUTTON
2) CHOOSE ANY FORGERY METHOD
3) KINDLY WAIT FEW SECOND
4) YOU WILL SEE OUTPUT

Fig.7. Homepage UI

IV. Conclusion

In the proposed system, we have implemented eight 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.

References

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

[2]. A Review on Copy-Move Image Forgery Detection Techniques [Zaid Nidhal Khudhair, Dr. Farhan Mohamed,

Karrar A. Kadhim], Journal of Physics: Conference Series, Volume 1892, Issue 1, article id. 012010 (2021).

[3]. A Systematic Study of Image Forgery Detection [Dr. Santhosh Kumar (Guru Nanak Institute of Technology)] August 2018 Journal of Computational and Theoretical Nanoscience 15(8).

[4]. A Study on Image Forgery Detection Techniques [Shijo Easowa*, Dr. L. C. Manikandanb], International Journal of Computer (IJC) (2019) Volume 33, No 1, pp 84-91.

[5]. 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.

[6]. 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.

[7]. 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.