ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, 2022

IMAGE FORGERY DETECTION USING IMAGE PROCESSING

[1]Sagar Babu Jeldi, [2]Chennaiahkate, [3]D. Chinni, [4]T.Prasanthi
[1,2,3,4]Department of Computer Science and Engineering, St. Peter's Engineering College, Hyderabad, Telangana, India.
sagarbabu@stpetershyd.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.

INTRODUCTION

A digital image is essentially a visual representation of a two-dimensional object or scene, stored and processed
in numerical format, typically as binary data. This numerical representation allows digital images to be easily manipulated, stored, transmitted, and analyzed by computers and other digital systems. The proliferation of digital images in various fields—ranging from social media, medical imaging, remote sensing, to national security—highlights the increasing importance of ensuring their authenticity and integrity. In today's digital age, digital images serve as a powerful means to convey, store, and distribute information across the Internet, making them an integral part of many day-to-day applications. However, the widespread use of digital images has also introduced new challenges, especially concerning image security. Certain digital images may contain sensitive information, such as business secrets, classified government data, or evidence in legal proceedings. The rise of the Internet and multimedia technologies has simplified the distribution of these images, but it has also opened the door to potential security threats. Image tampering, forgery, and manipulation are increasingly common, with powerful software tools enabling anyone to alter or edit digital content, often with minimal effort. As a result, the authenticity and reliability of digital images have become pressing concerns for scientists, engineers, and security experts.

The manipulation of images undermines trust in the visual information people encounter and can lead to serious consequences when fake images are mistaken for genuine ones. The difficulty of detecting forgeries stems from the fact that digital editing tool are highly sophisticated, enabling seamless alterations that leave no visible traces. Techniques like image splicing (inserting elements from one image into another), copy-move forgery (duplicating and repositioning parts of the same image), and retouching (altering colors or textures) can be applied with precision, making manual detection almost impossible.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, 2022

IMAGE TAMPERING

2.1 Copy-Move Forgery

Copy-move forgery, also known as region duplication, occurs when a part of the image is copied and pasted into another area of the same image. The purpose of this forgery is typically to conceal or duplicate certain objects or areas within an image. Since the copied part is from the same image, factors like noise, color balance, and texture remain consistent, making it more difficult to detect.

2.2 Double Jpeg Compression Detection

Double JPEG compression detection is a technique used to identify whether an image has been saved multiple times in the JPEG format, which can be a sign of tampering. JPEG compression is lossy, meaning it reduces image quality by discarding some of the data during the saving process. When an image is manipulated, and the edited version is resaved as a JPEG, the compression artifacts change, revealing traces of editing.

2.3 Noise Variance Inconsistency

Noise is a random variation in pixel values caused by the sensor or environmental factors. In a tampered image, noise patterns may vary across different regions, especially if the tampered area was edited separately or resaved with different compression settings.

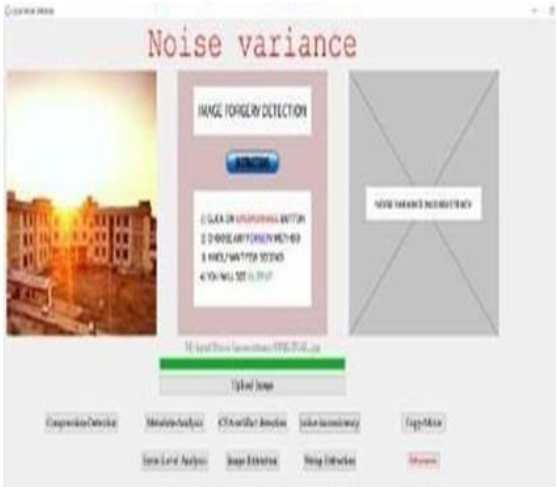

Fig.1. Noise variance inconsistency detection using the proposed system

2.4 Metadata Analysis

Metadata, specifically Exif (Exchangeable Image File Format) data, contains crucial information about an image's properties, including the camera model, timestamp, geolocation, and camera settings. By analyzing metadata, forensic analysts can detect inconsistencies that indicate tampering or manipulation.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, 2022

2.5 Error Level Analysis

Error Level Analysis (ELA) is a technique used to detect differences in image compression levels, which can indicate areas of manipulation. ELA works by visualizing the compression artifacts in an image, making it easier to spot discrepancies between the original and tampered sections.

Fig.2. Input image for ELA

Fig.3. Output of ELA using the proposed system

2.6 String Extraction

In media files, data can appear in the form of binary structures, binary data, or textual values. The **strings analyzer** helps extract any readable text from these files. Technically, a "string" refers to any sequence of letters and spaces. When the analyzer retrieves strings from a file, it filters out binary or non-printable characters, leaving only readable text. This process involves parsing the file to show every sequence of bytes that could represent text.

2.7 Image Extraction

Photographs are the most common type of files used for steganography, where hidden information is embedded within an image. There are many digital image formats, each suited for specific uses, and different steganographic methods are used for each type. In image

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, 2022

steganography, information is concealed in a way that is not visible to the human eye. The process of image extraction involves uncovering this hidden information.

Fig.4. Input image for image extraction

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

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.

2.8 CFA Artifact Detection

Most digital cameras use a Color Filter Array (CFA) to capture color images. CFA artifacts refer to the patterns left behind by the demos icing process, where the sensor interpolates colors to produce a full-color image. In a tampered image, these patterns may become inconsistent, revealing signs of manipulation.

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.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 10, 2022

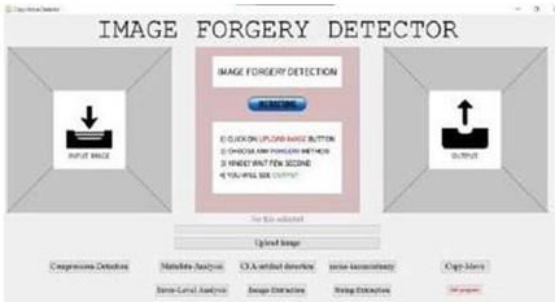

Fig.7. Homepage UI

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.