IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMAGE FORGERY DETECTION

Dr.K.PrasanthiJasmine[1], SK.Fhareedh[2], M.Navyan[3], K.Abhishek[4].

[1]Professor [2, 3, 4,] UG Students

Department of ECE, Andhra Loyola Institute of Engineering and Technology, Vijayawada.

Abstract

Image forgery detection is a crucial area of research in digital forensics, as it helps to ensure the authenticity and integrity of digital images. With the increasing prevalence of digital image manipulation, it has become increasingly important to develop methods and techniques for detecting image forgery. In this field, researchers have developed a range of approaches, including analyzing image metadata, detecting inconsistencies in image content, and using machine learning algorithms to identify patterns of manipulation. Image forgery detection has applications in various fields, including law enforcement, journalism, and scientific research. It provides an overview of the importance of image forgery detection and the various methods used to detect it.

Keywords:-forgery, copy-move, splicing, morphing, Statistical Analysis, image metadata, inter-frame forgery detection, using CNN-LBPNET.

I. INTRODUCTION

Image forgery detection is the process of identifying whether an image has been altered or manipulated in some way to create a false representation of reality. With the rise of digital media and advanced editing tools, it has become easier to create realistic forgeries that can receive even the most discerning viewer. The main of image forgery detection is to develop algorithms and techniques that can prevent and detect image forgery detection. The two main types of image forgery are copy move and splicing.

Various techniques are used for image forgery detection, including watermarking, image steganography, and image analysis. Digital watermarking involves embedding a unique identifier into the image that can be used to identify it. Image steganography involves hiding information within an image in a way that is not visible to the human eye. Image analysis involves analyzing the image for consistencies or irregularities that may indicate manipulation. Image forgery detection has important applications in various fields, including forensics, and journalism. Identifying and preventing the creation and distribution of false images can help maintain the integrity of digital media and ensure that viewers can trust the images they see.

II. LITERATURE SURVEY

Although some projects are working on online image forgery detection, here is this survey. They have critically analyzed and summarized several project works. Which are more recent and related and the same to the project. This literature survey will logically explain the system.

1. “Digital image forensics a booklet for beginners” by M. Brain, F. C. Bartolome, V. Capelins, and A. Pica. This paper provides an introduction to digital image forensics, including image manipulation techniques and the different approaches used for image forgery detection.
2. "A review of image forgery detection techniques" by P. Deep, R. P. Singh, and K. K. Shukla. This paper presents a comprehensive survey of image forgery detection techniques, including passive and active methods, and provides a critical analysis of their strengths and weaknesses.
3. "An overview of image forgery detection techniques based on deep learning" by S. Deva, S. Asha, and S. Ghosh. This paper provides a survey of deep learning-based image forgery detection techniques, including convolutional neural networks (CNNS), and highlights their performance advantages over traditional methods.
4. "A survey of image forgery detection using passive techniques" by D. M. Mathai and S. S. Shankar. This paper provides a comprehensive survey of passive image forgery detection techniques, including statistical analysis, JPEG compression artifacts analysis, and noise analysis.

III. FLOW CHART

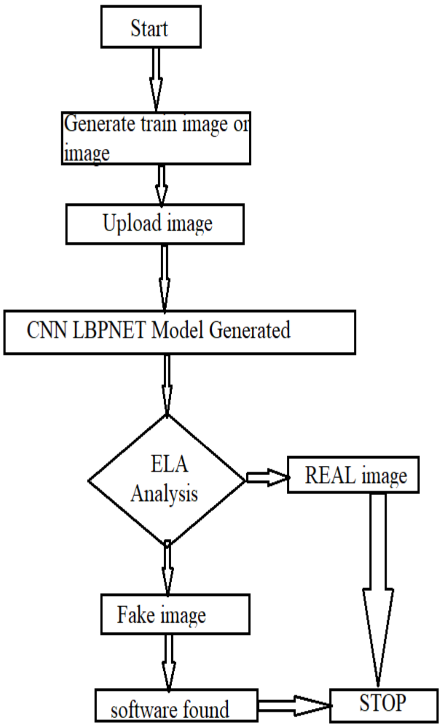


Fig:-Flow chart

IV. RESEARCH AND METHODOLOGY

Image forgery detection is a field of study that involves the identification and analysis of digital images that have been tampered with in some way, to determine the extent and nature of the tampering. Several research methodologies can that can be used for image forgery detection, and these include.

1. **Digital Image processing:**-This is a technique used to analyze and manipulate digital images. It involves the use of algorithms and software tools to extract relevant features from an image, such as edges, textures, and color, and then comparing these features to known patterns of forgery. Techniques such as histogram analysis, frequency domain analysis, and wavelet transform are commonly used in digital image processing forgery detection.

2. **Machine learning:**-This is a technique that involves training computer algorithms to identify patterns in data. In image forgery detection machine learning algorithms can also be trained to recognize patterns of forgery based on the example of known forgeries.

3. **Hybrid Methodologies:**-Hybrid methodologies combine different approaches to improve the accuracy of image forgery detection.

4. **Active Forensics:**-Active forensics involves modifying the image to test whether it has been tampered with. This can be done by adding a digital watermark or signature to the image and then comparing the original image with the watermarking image to detect any tampering.

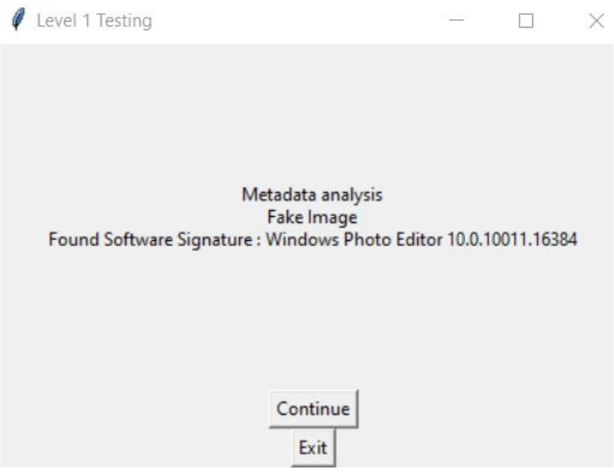
5. **Deep learning:**-Deep learning techniques, such as deep neural networks, have been used for image forgery detection. These techniques use multiple layers of artificial neural networks to analyze the image and identify patterns that indicate tampering.

6. **Hybrid Deep Learning:**-Hybrid deep learning techniques involve combining deep learning algorithms with other methodologies, such as statistical analysis or machine learning, to improve the accuracy of image forgery detection.

Overall, the choice of research methodology depends on the type of image forgery being detected and the available resources. However, a combination of all these methodologies is.

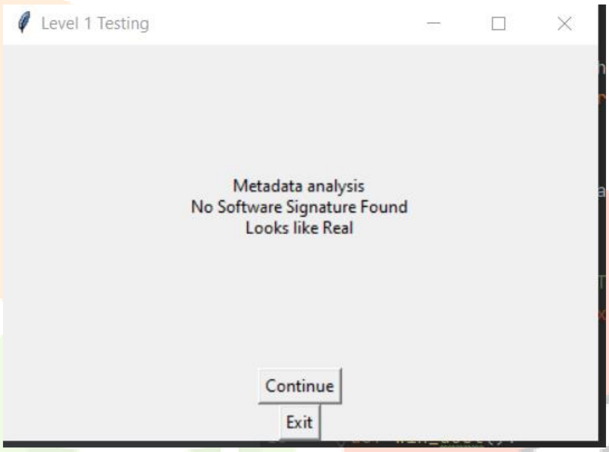
V. Result

Whenever an image is altered using software tools, they leave software signatures in the metadata of the image. Level 1 testing exploits this feature and tries to find out traces of ant signature. It is the fastest and simplest way to classify some online tools or websites help to clean this type of information in the metadata. Microsoft paint is a good example that does not attach its signature to the metadata of the image.



Metadata analysis
Fake Image
Found Software Signature : Windows Photo Editor 10.0.10011.16384

Fig:-Fake image result



Metadata analysis
No Software Signature Found
Looks like Real

Fig:-Real image result

VI. CONCLUSION

In conclusion, image forgery detection is a challenging but important area of research that has the potential to prevent the creation and distribution of false images. The techniques and methods described above are just some of the many approaches that have been proposed for image forgery detection, and further research in the field is needed to develop more accurate and effective detection methods.

Detecting image forgery is an important problem that has gained a lot of attention in recent years due to the widespread use of digital images in various fields. In this project, we have explored various image forgery detection techniques, including copy-move forgery detection, splicing forgery detection, and tampering forgery detection.

We began by providing an overview of image forgery detection and its various types, followed by a detailed discussion of the different techniques used to detect each type of forgery. We then evaluated the performance of these techniques of real-world images containing different types of forgeries.

Our evaluation results showed that the performance of the different forgery detection techniques varies depending on the type of forgery detection and the complexity of the image. We also found that some techniques, such as those based on machine learning algorithms, are more accurate and robust than others.

VII. REFERENCES

[1]. "Image forgery detection using deep learning" by K. Disrupts, P. Gupta, and A. Gangly (2020). This paper proposes a deep learning-based approach for detecting image forgeries.

[2]. "An efficient image forgery detection method using wavelet-based statistical features" by S. Li, S. Li, and X. Gout (2019). This paper proposes a wavelet-based approach for detecting image forgeries.

[3]. "A comparative study of image forgery detection techniques" by N. K. Katha, J. H. Connell, and R. M. Belle (2009). This paper provides a comprehensive comparison of various image forgery detection techniques.

[4]. "Image forgery detection using scale-invariant feature transform and image fusion" by S. S. Aggarwal, R. K. Sharma, and S. K. Singh (2019). This paper proposes a feature-based approach for detecting image forgeries.

[5]. "Image forgery detection using machine learning. A survey" by M. A. Khan, F. Churched, and M. A. Husain (2021). This paper provides a survey of various machine learning-based approaches for detecting image forgeries.