# FORGERY DETECTION USING COMPUTER VISION TECHNIQUES

# AGENDA

- Introduction
- Existing solutions
- Methodology
- Block Diagram
- Advantages
- Limitations
- Conclusion

# INTRODUCTION TO IMAGE FORGERY DETECTION

- The explosion of social networking services, there has been a monumental increase in the volume of image data.
- Moreover, the development in image processing software such as Adobe Photoshop has given a rise to doctored images. Such doctored images a can be used for malicious purposes such as spreading false information and inciating violence.
- This image forgery detection project allows users to **detect even the slightest signs** of forgery in an image. This project is developed using Python programming language and some of the libraries available in it.

# LITERATURE SURVEY

| S.NO | AUTHOR | TITLE | OBSERVATION | LIMITATIONS |
|---|---|---|---|---|
| 1 | Gajanan K. Birajdar | Digital image forgery detection using passive techniques: A survey | This article surveys recent developments in blind digital image forgery detection techniques without requiring prior knowledge of the image. | require significant computational resources or may not be scalable for large datasets |
| 2 | Navpreet Kaur Gill | A review paper on digital image forgery detection techniques | The article discusses recent developments and limitations of passive digital image forgery detection techniques that do not require pre-embedded information in the image. | This paper discusses about all the techniques only |
| 3 | Tu K. Huynh | A survey on Image Forgery Detection techniques | This paper provides a survey of image forgery detection techniques for both copy-move and spliced images, classifying them into groups based on their methods and summarizing achievements, limitations, and future work. | “differences may be caused by resampling, blur, image features or camera features. Although there are many suggested algorithms, each of them still has limitation.” |

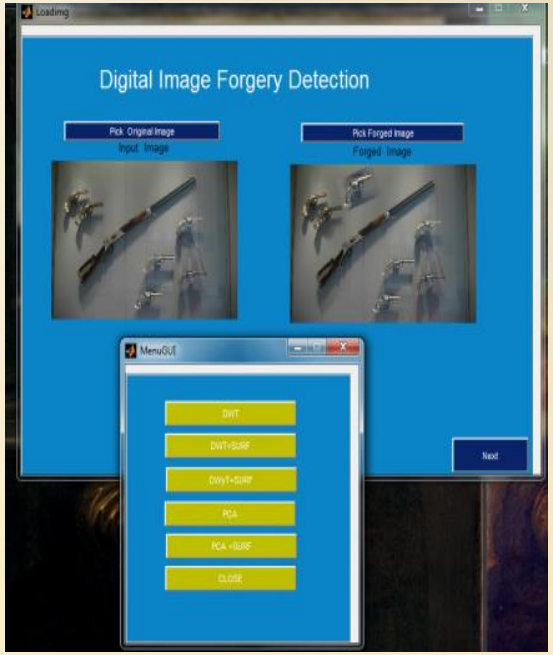
# LITERATURE SURVEY

| S.NO | AUTHOR | TITLE | OBSERVATION | LIMITATIONS |
|---|---|---|---|---|
| 4 | Gajanan K. Birajdar | A bibliography of pixel-based blind image forgery detection techniques | This paper surveys various digital image forgery detection techniques, including copy-move, splicing, resampling, and retouching, with a focus on pixel-based methods that don't require prior knowledge of tampering type. It emphasizes the need for robust image authentication methods in the face of growing digitization. | 1)High False Positive Rate<br>2)Limited Applicability |
| 5 | Tanzeela Qazi | Survey on blind image forgery detection | The survey covers blind digital image forgery detection techniques for copy/move, splicing, and retouching. | The limitations of this techniqueare the higher computational time and poor performance forthe identical or smooth areas |
| 6 | Kunj Bihari Meena | Image Forgery Detection: Survey and Future Directions | Reviews existing methods for detecting image forgery and categorizes various forgery detection techniques, highlighting the need for continued attention in this field due to increasingly sophisticated image manipulation tools.. | The review focuses on existing methods and may not provide new insights or approaches for detecting image forgery. |

# EXISTING SOLUTIONS OF THE PROBLEM

Image forgery detection is a challenging task in machine learning . there are various existing solutions for detecting image forgery, and some of the most popular approaches are:

1. Copy-Move Forgery Detection: In this technique, the image is divided into smaller blocks, and duplicate blocks are identified in the image.
2. Splicing Forgery Detection: Splicing forgery detection focuses on identifying regions in an image where two or more images have been combined to create a new image.



# EXISTING SOLUTIONS OF THE PROBLEM

3. Camera-Based Forgery Detection: This technique focuses on detecting whether an image is captured by a digital camera or created using computer software.
4. Steganography Detection: Steganography is the practice of hiding information inside an image. Steganography detection is based on identifying the changes in the image's statistical properties that are caused by the hidden information.
5. Deep Learning-Based Forgery Detection: In recent years, deep learning-based approaches have shown significant promise in detecting image forgery. These methods use convolutional neural networks (CNNs) to extract features from the image and classify it as authentic or forged.

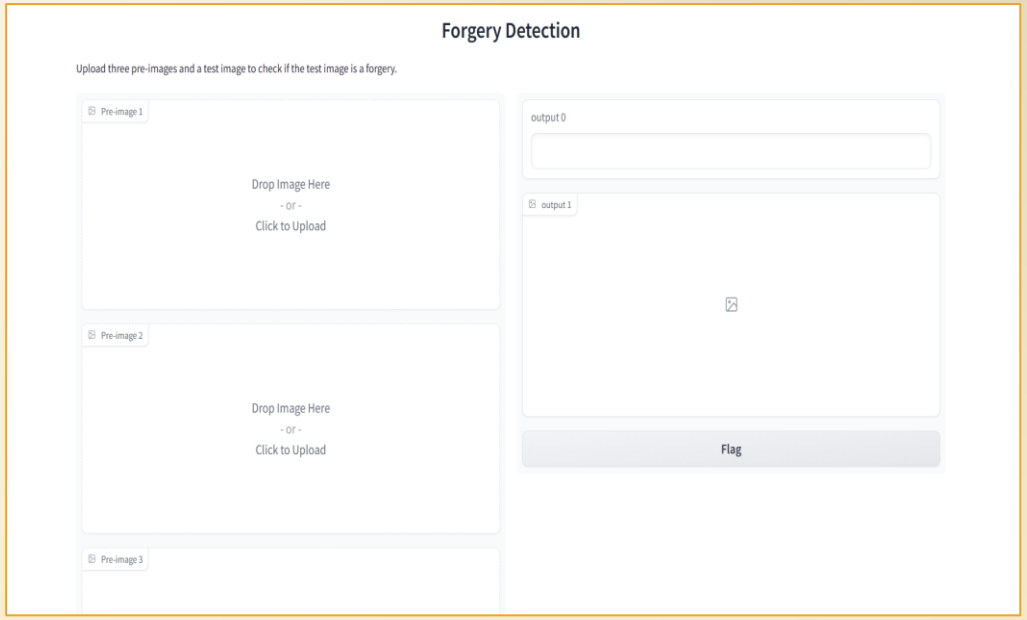
# METHODOLOGY

The methodology for image forgery detection generally involves the following steps:

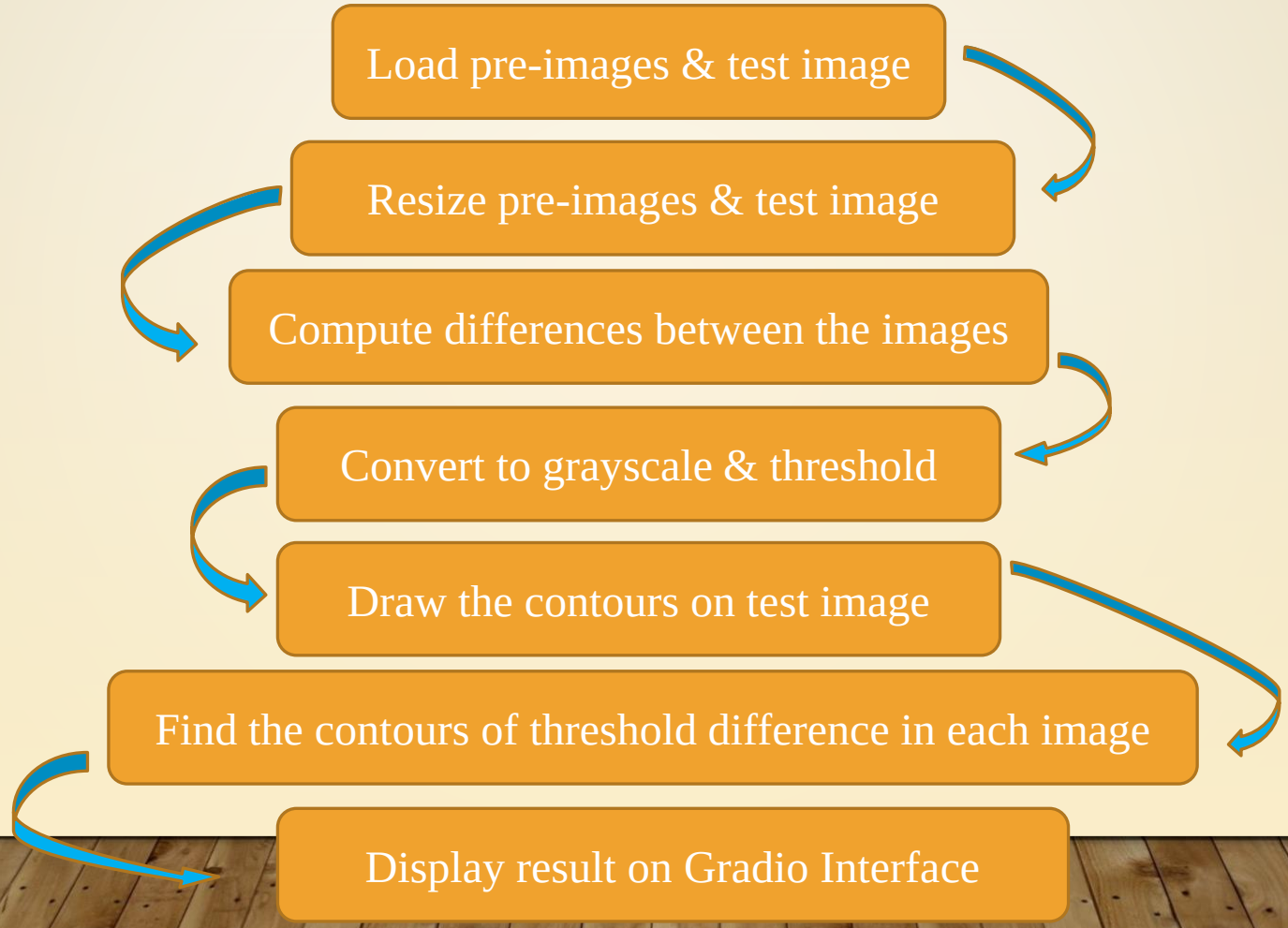
1. Load three pre-images and a test image.
2. Resize all the images to fit within a maximum size.
3. Compute the absolute difference between each pre-image and the test image, resulting in three difference images.
4. Convert the difference images to grayscale and threshold them to highlight the significant differences.

# METHODOLOGY

5. Find the contours of the differences in each image using OpenCV's findContours function.
6. Draw the contours on the test image using OpenCV's rectangle function.
7. If there are no contours in any of the difference images, mark the test image as authentic. Otherwise, mark it as a forgery.
8. Display the result along with the original test image on the Gradio interface.



# BLOCK DIAGRAM



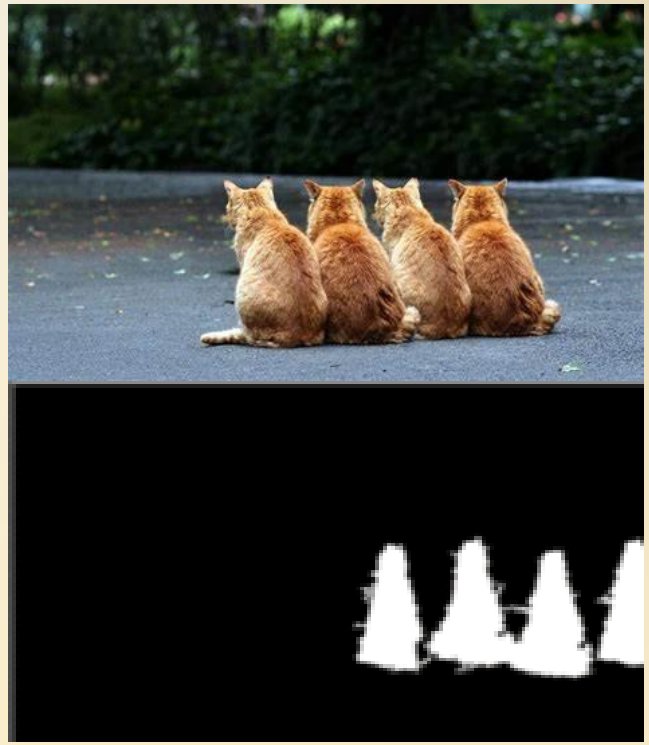
# USED PACKAGES

- The language we used for implementation is python. Because python is freeware and opensource , high level programming language , platform independent portability these are the  features of python .

- In python programming platform we used the packages:
  1. Numpy
  2. OpenCV
  3. Gradio

# ADVANTAGES

- Including increased accuracy and reliability
- Improved security, and reduced costs.
- It is possible to detect any malicious alterations or manipulations.
- Can be used to identify copyright infringement.
- Protect sensitive information from unauthorized access.



# LIMITATIONS

- Image forgery detection can also be vulnerable to false positives, where an image is incorrectly identified as being altered when it is not.
- Limited Generalizability.
- Need of the source image.

# CONCLUSION

- Image forgery detection is an important tool for detecting malicious alterations or manipulations of digital images. It can help to protect sensitive information from unauthorized access and to identify copyright infringement.
- Image forgery detection can be time consuming and expensive, but it can also be used to detect subtle changes in an image and to reduce costs.

# REFERENCES


- Birajdar, G. K., & Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. *Digital investigation*, *10*(3), 226-245.
- Gill, N. K., Garg, R., & Doegar, E. A. (2017, July). A review paper on digital image forgery detection techniques. In *2017 8th international conference on computing, communication and networking technologies (ICCCNT)* (pp. 1-7). IEEE.
- Huynh, T. K., Huynh, K. V., Le-Tien, T., & Nguyen, S. C. (2015, January). A survey on image forgery detection techniques. In *The 2015 IEEE RIVF International Conference on Computing & Communication Technologies-Research, Innovation, and Vision for Future (RIVF)* (pp. 71-76). IEEE.

# REFERENCES


- Qureshi, M. A., & Deriche, M. (2015). A bibliography of pixel-based blind image forgery detection techniques. *Signal Processing: Image Communication*, *39*, 46-74.
- Qazi, T., Hayat, K., Khan, S. U., Madani, S. A., Khan, I. A., Kołodziej, J., ... & Xu, C. Z. (2013). Survey on blind image forgery detection. *IET Image Processing*, *7*(7), 660-670.
- Meena, K. B., & Tyagi, V. (2019). Image forgery detection: survey and future directions. *Data, Engineering and Applications: Volume 2*, 163-194.

# THANK YOU