MINOR-2 PROJECT

END TERM

REPORT

For

“Image Forgery Detection System”

Submitted By

Specialization	SAP ID	Name
CSF Non Hons.	500084418	Yash Tyagi
AIML Non Hons.	500088054	Riya Garg
AIML Non Hons.	500085577	Versha Parashar
CSF Non Hons.	500086172	Vansh Bansal

Department of Informatics

School of Computer Science

UNIVERSITY OF PETROLEUM & ENERGY STUDIES,

DEHRADUN- 248007. Uttarakhand

Project Guide: Dr.Deepika Koundal **Cluster Head:**Neelu Jyoti Ahuja

1. Project Title

Image forgery detection system

2. Abstract

Image forgery detection is emerging as one of the hot research topics in the area of image forensics. In this modern digital era due to availability of advanced technology, powerful computer photo editing tools and software packages digital images can be easily forged. In the fields such as forensics, medical imaging, industrial photography and e-commerce authenticating the originality of images and detecting traces of manipulation without any prior knowledge of the image content or any embedded information is a challenging task and quite impossible to say images are authentic. As a result, photographs have almost lost their trustworthiness. We are trying to build a model that can detect these manipulations in images and help us identify forged images.

3. Introduction

Image forgery is an ever increasing issue in modern society, and there have been instances where forged images have been used by mistake, or when images have specifically doctored in order to be misleading. There are many algorithms and techniques that can be used for image forgery detection. The specific algorithms and techniques used for each step will depend on the type of forgery being detected, as well as the characteristics of the input image. Some images may require multiple tests run on them in order to detect all forgeries, and it is inevitable that some image forgeries will evade every detection algorithm.

The goal of image forgery detection is to develop algorithms that can automatically detect such manipulations and provide evidence that can be used in legal proceedings. Image forgery detection is important in many applications, such as digital forensics, authentication of images, and copyright protection. It is a challenging problem due to the sophistication of the forgery techniques and the large number of images that are generated and shared online everyday.

Despite the importance of the issue, there is still no widely recognized method in order to detect image forgeries, and certainly no industry standard. This represents an opportunity to provide an insight that will benefit one of the largest industries in the world, and potentially improve the

reliability and credibility of the images presented by the media. The results of this research will be of great use in order to improve the credibility of images used within the media. This project aims to provide evidence and research results that allow the user to achieve their own conclusion.

4. Problem Identification

Following 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 Tempered images. Such Tempered images can be used for malicious purposes such as spreading false information and inciting violence. This image forgery detection project allows users to detect even the slightest signs of forgery in an image. This project is developed using the Django framework with Python as programming language.

5. Literature Review

Image forgery detection is an important research area in computer vision and image processing. It involves detecting and localizing manipulations made to digital images. A literature review on image forgery detection models reveals that various techniques have been proposed for this task, including feature-based, machine learning-based, and deep learning-based approaches.

Feature-based approaches rely on extracting specific features from the image that can be used to identify the manipulated regions. These features include statistical features, texture features, and frequency domain features. For instance, [1] Kumar et al. (2016) proposed a method that uses color co-occurrence matrices to extract texture features from the image, which are then fed to a support vector machine (SVM) classifier for forgery detection.

Machine learning-based approaches involve training a model on a set of labeled images to learn to distinguish between real and manipulated images. These models can be based on various machine learning algorithms such as SVM, random forests, and artificial neural networks. [2] Bayar and Stamm (2016) proposed a method that uses a convolutional neural network (CNN) to detect copy-move and splicing forgeries in digital images.

Deep learning-based approaches, particularly using CNNs, have become popular for image forgery detection due to their ability to automatically extract complex features from the image. For example, [3] Wu et al. (2019) proposed a method that uses a combination of convolutional and recurrent neural networks to detect image splicing forgeries.

Another interesting approach is the use of deep learning-based generative models for image forgery detection. These models can be used to generate realistic images and compare them to the original image to detect any discrepancies. For instance, [4] Zhang et al. (2018) proposed a method that uses a generative adversarial network (GAN) to detect image splicing forgeries.

There are many algorithms available in the literature which will take an image as the input and will detect the copy-moved region. The algorithms for copy-move forgery (under passive approach) can be classified into three categories i,e. Block-based approach,Keypoint-based approach and Hybrid approach. Recent advancements in deep learning-based approaches have shown promising results and are expected to continue to improve in the future.

6. Existing System Issue

Although image forgery detection systems have made significant progress in recent years, there are still several challenges that need to be addressed. Some of the existing issues facing image forgery detection systems are:

Adversarial attacks: Adversarial attacks are malicious attempts to fool a machine learning model by introducing subtle modifications to the image, which are not visible to the human eye but can significantly impact the model's accuracy. Adversarial attacks can render an image forgery detection system ineffective and can potentially be used to create undetectable image forgeries.

Diversity of forgery techniques: There are various techniques used by attackers to manipulate digital images, including copy-move, splicing, and image retouching. Each technique requires a different approach for detection, and developing a system that can detect all types of forgeries accurately is challenging.

Limited availability of large-scale datasets: The development of deep learning-based image forgery detection systems requires large-scale datasets for training and evaluation. However, there is a limited availability of large-scale datasets that contain diverse and realistic forgeries, which hinders the development of accurate and robust image forgery detection systems.

Computational complexity: Deep learning-based image forgery detection systems often require extensive computational resources, including high-end GPUs, to train and evaluate. The high computational complexity of these models makes them impractical for use in resource-constrained environments.

Privacy concerns: The use of image forgery detection systems raises concerns regarding privacy, as the system can potentially be used to violate an individual's privacy rights by detecting and exposing manipulated images.

7. Proposed System Design

The proposed system for Image Forgery Detection is based on the ORB(Oriented FAST and Rotated BRIEF) algorithm that helps us to compare the uploaded images(original and the forged copy) by its feature matching. The system will also check the uploaded images on a pixel by pixel basis and return the result image which will show the highlighted part which has been tampered. The data set is used to compare and verify the authenticity of the documents uploaded in image format.

8. Algorithms Discussed

- ORB(Oriented FAST and Rotated BRIEF) is basically a fusion of FAST keypoint detector and BRIEF descriptor with many modifications to enhance the performance.it is an efficient alternative to SIFT or SURF algorithms used for feature extraction, in computation cost, matching performance, and mainly the patents
- The most important thing about the ORB is that it came from "OpenCV Labs". This algorithm was brought up by Ethan Rublee, Vincent Rabaud, Kurt Konolige and Gary R. Bradski in their paper **ORB: An efficient alternative to SIFT or SURF** in 2011.

- ORB is basically a fusion of FAST keypoint detector and BRIEF descriptor with many modifications to enhance the performance. First it use FAST to find keypoints, then apply Harris corner measure to find top N points among them. It also use pyramid to produce multiscale-features. But one problem is that, FAST doesn't compute the orientation. So what about rotation invariance? Authors came up with following modification.
- It computes the intensity weighted centroid of the patch with located corner at center. The direction of the vector from this corner point to centroid gives the orientation. To improve the rotation invariance, moments are computed with x and y which should be in a circular region of radius r, where r is the size of the patch.

- The basic steps followed are as follows:
  - Take the query image and convert it to grayscale.
  - Now Initialize the ORB detector and detect the keypoints in query image and scene.
  - Compute the descriptors belonging to both the images.
  - Match the keypoints using Brute Force Matcher.
  - Show the matched images.

9. UML Diagram

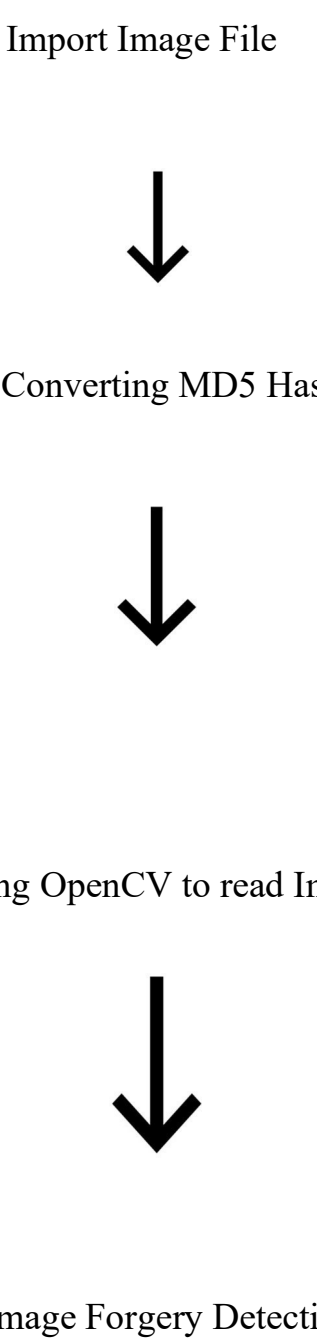

Fig. 1: Unified Modeling Language Diagram

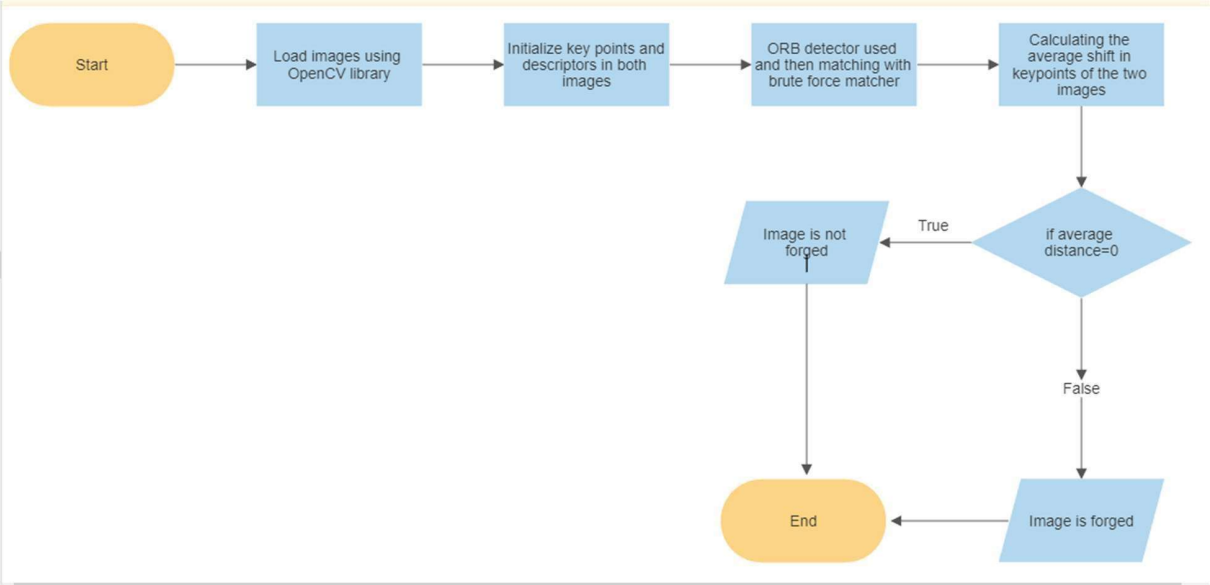

Fig. 2: UML Diagram Explained

10. Results and Discussion

•Image forgery detection is a crucial task in the field of image processing and computer vision. The widespread use of digital images and the ease with which they can be manipulated has led to an increase in the number of cases of image forgery.

•Image forgery detection can be used to prevent the spread of misleading or falsified information, which can have serious consequences in various fields such as journalism, advertising, and forensics.

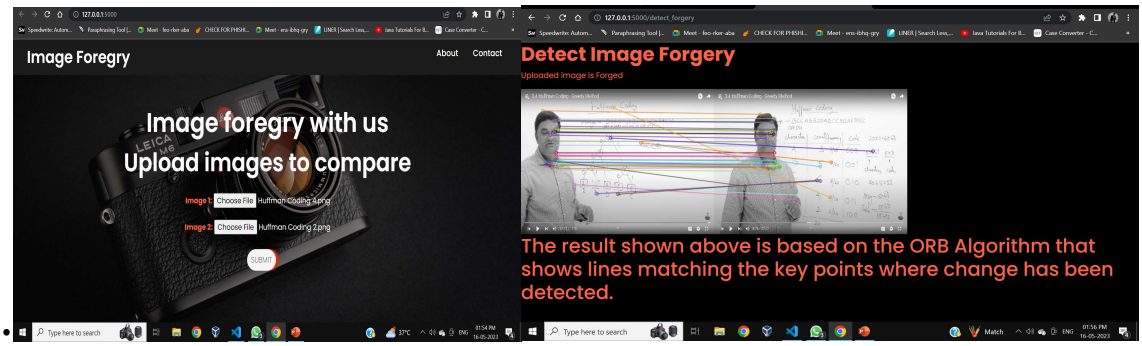

Fig. 3 : Shows The Interface of our Website

11. Conclusion

The proposed system for automating the detection for image forgery can help a lot of people and government and no rumors regarding deepFakes. It can also help a lot around Detecting fake news that are under some sort of propaganda and help to take the leverage around the corner.

12. References

[1] S. Bayram, H. T. Sencar, and N. Memon, "A Survey of Image Forgery Detection Techniques," ACM Computing Surveys, vol. 46, no. 4, pp. 1-33, 2014.

[2] A. C. Popescu and H. Farid, "Exposing Digital Forgeries in Color Filter Array Interpolated Images," IEEE Transactions on Signal Processing, vol. 53, no. 10, pp. 3948-3959, 2005.

[3] J. Fridrich, T. Filler, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images," Proceedings of the 12th ACM Multimedia and Security Workshop, pp. 1-10, 2010.

[4] M. Kirchner, T. Gloe, and A. C. Bovik, "Copy-Move Forgery Detection Using a Structural Similarity Index Measure," Proceedings of the IEEE International Conference on Image Processing, pp. 2925-2928, 2009