



*WebStack - Portfolio Project - Pitch*

Group project Portfolio Project Presentation

# IMD - Image forgery Detection

A copy-move and block-based image forgery  
detection



# List Of Team Members

- Lenge Dandung Joshua

E-mail- [maticsjnr@gmail.com](mailto:maticsjnr@gmail.com)

Github - [@hendrixxD](#)



# Description Of The Project

Imagine a world where you can trust the authenticity of every image you see. With the rise of digital media, image forgery has become a growing concern, with fake images used for everything from propaganda to financial fraud. My solution is an image forgery detection system that uses advanced algorithms to detect copy-move and block-based forgeries.

My system will leverages cutting-edge image processing techniques to analyze an image and identify regions that have been manipulated. By comparing the textures and patterns of different regions, my algorithms can identify inconsistencies and determine whether an image has been tampered with or not. This will allows me provide my users with a high level of confidence in the authenticity of any image.

With this system, my goal is to provide a powerful tool for journalists, investigators, and anyone who needs to verify the authenticity of digital images. By detecting forgeries with a high degree of accuracy, I can help protect the integrity of digital media and prevent the spread of digital misinformation.



# Learning Objectives

Understanding the basics of image processing: Learning the fundamentals of how images are captured, stored, and manipulated in digital form, and how they can be analyzed using various techniques.

Understanding the principles of machine learning: Gaining a basic understanding of the principles of machine learning, including supervised and unsupervised learning, training data, and model evaluation.

Familiarizing with image forgery detection techniques: Exploring the various image forgery detection techniques, including copy-move and block-based forgery detection, and understanding how they work.


Implementing a machine learning pipeline: Building a complete end-to-end pipeline for image forgery detection, including data preparation, feature extraction, model training, and evaluation.

Evaluating and improving the model: Learning how to evaluate the performance of a machine learning model, and how to improve its accuracy by tuning hyperparameters and using more advanced techniques.



# Technologies To Be Used

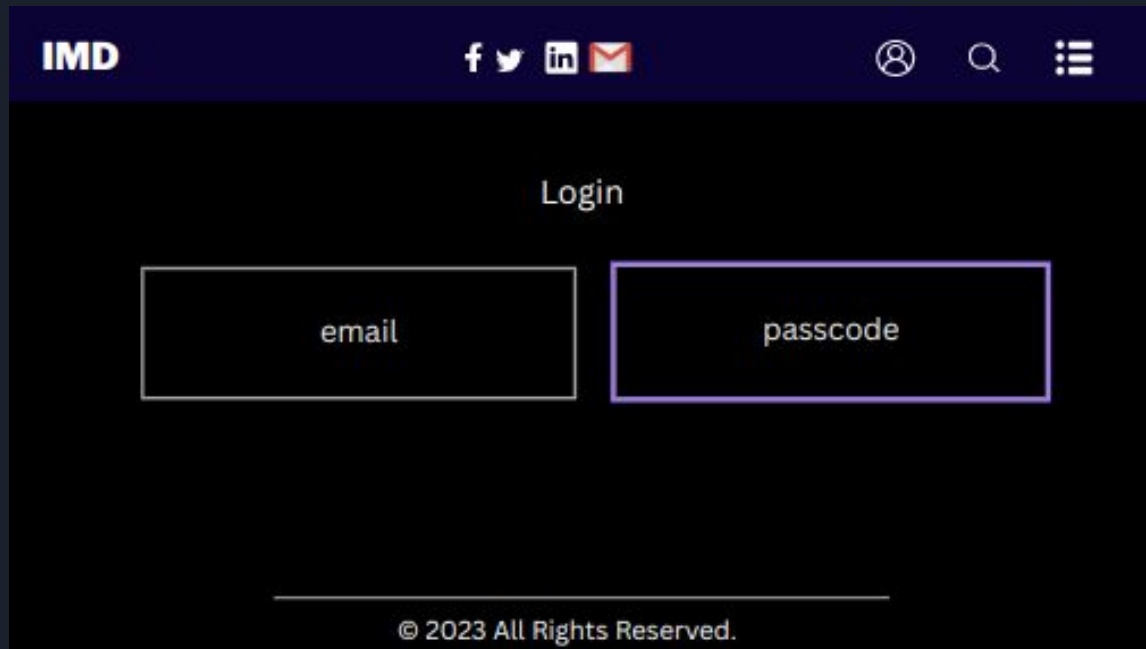
- **Flask:** Flask is a lightweight web framework in Python that can be used to build a simple API for image forgery detection
- **OpenCV:** OpenCV is an essential library for image processing in Python. It provides a wide range of functions and algorithms for analyzing and manipulating digital images, including the ability to detect edges, perform image filtering, and extract features. For the task of image forgery detection, OpenCV can be used to preprocess images and extract relevant features that can be used for further analysis.
- **scikit-learn:** scikit-learn is a popular machine learning library in Python that provides a range of algorithms for classification, regression, and clustering. For the task of image forgery detection, scikit-learn can be used to train and evaluate machine learning models that can detect copy-move and block-based forgeries

- 
- **Bcrypt:** Bcrypt is safer. It's made to be slower, this makes it harder for an attacker to brute force a password. It can be configured to iterate more and more which is useful since CPU's are getting more powerful.
  - **Amazon S3[Simple Storage Service]:** Amazon S3 as the best third-party service for storing and retrieving large amounts of image data. Amazon S3 is designed for scalability and reliability, and provides a range of features for managing and securing your data. It can also be easily integrated with other AWS services for added functionality, making it a good choice for building a robust image forgery detection system.

# Home page



# Login Page



A mockup of a login page with a dark blue header and a light blue body. The header contains the 'IMD' logo, social media icons for Facebook, Twitter, LinkedIn, and Email, and user interface icons for a profile, search, and menu. The main content area is titled 'Login' and features two input fields: 'email' and 'passcode'. The 'passcode' field is highlighted with a red border. At the bottom, a copyright notice reads '© 2023 All Rights Reserved.'.

IMD

f t in e

⦿ 🔍 ☰

Login

email

passcode

© 2023 All Rights Reserved.



# Signup Page

IMD

f t in e

⦿ 🔍 ☰

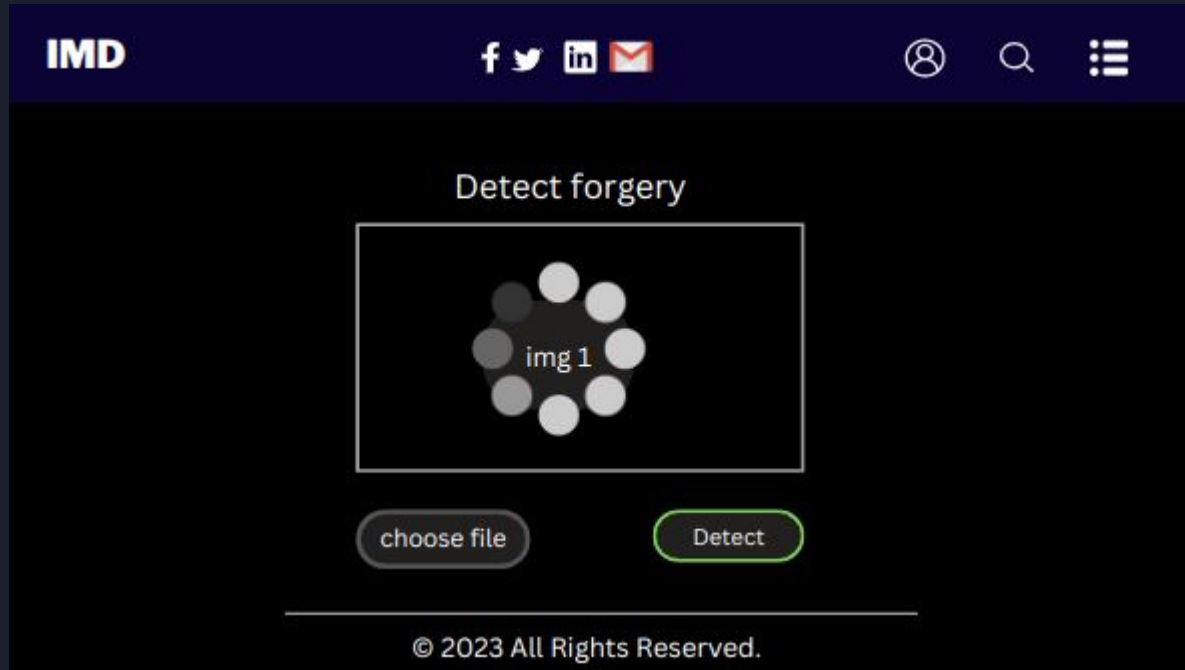
Signup

email	passcode
email	passcode

---

© 2023 All Rights Reserved.

# Image Upload To Detect Forgery



# Results Page

