

**DETECTION OF DOCTORED IMAGES USING DEEP LEARNING**

**A MINI PROJECT REPORT**

***Submitted by***

**MOHANRAJ V (1920110028)**

**ROSHAN E (1920110038)**

**SRIDHAR K S (1920110051)**

***in partial fulfillment for the award of the degree***

***of***

**BACHELOR OF TECHNOLOGY**

**IN**

ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

**SONA COLLEGE OF TECHNOLOGY, SALEM-5**

**(Autonomous)**

**ANNA UNIVERSITY: CHENNAI 600 025**

**NOVEMBER 2023**

**ANNA UNIVERSITY: CHENNAI 600 025 BONAFIDE CERTIFICATE**

Certified that this project report “**Detection Of Doctored Images Using Deep Learning”** is the bonafide work of **“MOHANRAJ V (1920110028)ROSHAN E (1920110038), SRIDHAR K**

**S(1920110051)”** who carried out the project work under my supervision

**SIGNATURE SIGNATURE**

Dr. J. Akilandeswari Dr R.Subhashini

**HEAD OF THE DEPARTMENT SUPERVISOR**

Professor Assistant Professor

Department of Information Technology Department of Information Technology Sona College of Technology Sona College of Technology

Salem- 636 005. Salem- 636 005. Submitted for Project viva voce examination held on

**INTERNAL EXAMINER EXTERNAL EXAMINE**

**ACKNOWLEDGEMENT**

First and foremost, we thank to **power of Almighty** for showing us inner peace and for all blessings.Special gratitude to our parents, for showing their support and love always.

We express our sincere thanks to Chairman, **Sri.C.VALLIAPPA** and Principal **Dr.S.R.R.SENTHILKUMAR** for providing adequate facilities to complete the project.

We are immensely grateful to our Head of Information Technology Department, **Dr.J.AKILANDESWARI** for the continuous encouragement to complete the project.

We express our heartfelt thanks to our project supervisor **DR.R SUBHASHINI** for her valuable guidance and fruitful discussions throughout the course of the project work.

We feel proud in sharing this success with all our department faculty, staff members and friends who helped directly and indirectly in completing this project successfully.

**ABSTRACT**

This project presents a novel approach for the detection of doctored images by leveraging Local Binary Pattern (LBP) features. The LBP algorithm is employed to extract discriminative texture patterns from images, offering a robust representation for the identification of manipulated content. The project begins with an extensive data collection phase, encompassing a diverse dataset containing both authentic and manipulated images. LBP features are extracted from this dataset, forming the basis for model training. The Support Vector Machine (SVM) classifier is employed to learn the intricate patterns inherent in manipulated images.

To enhance the model's generalization capabilities, data augmentation techniques and advanced pre-processing methods are implemented. The proposed system is rigorously evaluated using metrics such as accuracy, precision, recall, and F1 score on a dedicated test set. The integration of LBP features provides an efficient means of capturing subtle alterations introduced during image manipulation.

This project contributes to ongoing research efforts in developing reliable solutions for identifying and mitigating the impact of manipulated multimedia content on various online platforms.

**iv**

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER** | **TITLE** | **PAGE** |
| **ABSTRACT** | | **iv** |
| **LIST OF FIGURES** | | **vi** |
| **1.** | **INTRODUCTION** |  |
|  | **1.1 Problem Statement** | **08** |
|  | **1.2 Objective** | **09** |
|  | **1.3 Hardware & Software Requirements** | **11** |
|  | **1.4 Literature Survey** | **13** |
| **2.** | **DESIGN & IMPLEMENTATION** |  |
|  | **2.1 Proposed System** |  |
|  | **2.1.1 LBP** | **14** |
|  | **2.1.2 SVM** | **15** |
|  | **2.2 Architecture Design** | **15** |
|  | **2.3 Module** | **18** |
|  | **2.4 Module Description** | **18** |
|  | **2.5 Screenshots & Results** | **22** |
| **3.** | **CONCLUSION AND FUTURE WORKS**  **REFERENCES** | **24**  **27** |

**LIST OF FIGURES**

Fig 1.1 Sample of real and morphed image 09

Fig 1.2 Sample of morphing tool 10

Fig 2.1 Local Binary Pattern extraction 15

Fig 2.2 LBP calculation 16

Fig 2.3 SVM Architecture 17

Fig 2.4 Dataset 22

Fig 2.5 Accuracy 22

Fig 2.6 Testing with custom input 23

Fig 2.7 Predicted output 23

Fig 2.8 LBP Features Visualization 24

Fig 2.9 Confusion Matrix 24

**LIST OF ABBREVIATIONS**

**LBP** – Local Binary Pattern

**SVM** – Support Vector Machine **NLP** - Natural Language Processing **ML** – Machine Learning

**DL** – Deep Learning

**vii**

**CHAPTER 1 INTRODUCTION**

**1.1 PROBLEM STATEMENT**

In a digitally evolving landscape, the proliferation of manipulated or morphed images poses a significant challenge in various domains, including security and authentication. The project aims to develop a robust model capable of accurately distinguishing between genuine and manipulated images. Leveraging the Local Binary Pattern (LBP) feature extraction technique, the goal is to create a classifier that identifies subtle alterations in images introduced by various manipulation techniques such as face morphing or image tampering. The primary objective is to enhance security measures by establishing a system that effectively identifies these manipulations, providing a reliable solution for distinguishing between real and manipulated images. The project focuses on leveraging texture-based analysis to address the increasing need for accurate identification of manipulated images in today's digital environment.

The proliferation of image manipulation techniques poses a significant challenge in today's digital landscape, raising concerns in security, forensics, and authentication. With the advent of sophisticated tools and techniques, morphed or altered images can deceive and mislead, making it crucial to distinguish between authentic and manipulated visual content. This project centers on addressing this challenge by deploying the Local Binary Pattern (LBP) feature extraction method to develop a robust model for morphed image detection.

The primary objective is to create a classifier that can identify subtle alterations introduced by manipulation techniques such as face morphing, retouching, or image tampering. Leveraging the texture-based analysis of LBP, the project endeavors to establish an effective solution capable of accurately discerning between genuine and manipulated images. The aim is to enhance security measures across various domains, providing a reliable system that safeguards against the misuse of manipulated visual content in critical areas like identity verification, forensics, and digital authentication processes.



Fig 1.1 Example of real and morphed image

**1.1.OBJECTIVES**

The widespread availability of image editing tools has led to an increase in the creation and distribution of doctored or manipulated images. Detecting such manipulated images is crucial for maintaining the integrity of visual content in various domains, including journalism, forensics, and content authentication.

This project focuses on the detection of doctored images using the Local Binary Patterns (LBP) texture analysis technique.



Fig 1.2 Sample of morphing tool

Detecting doctored images and videos has become increasingly crucial in the digital age, where manipulated media can propagate false information and mislead individuals. This project presents a comprehensive approach to detect doctored images and videos using deep learning techniques. By leveraging convolutional neural networks (CNNs) and recurrent neural networks (RNNs), our proposed model analyzes visual and temporal cues to identify signs of manipulation. The system is trained on a diverse dataset of authentic and manipulated media, enabling it to learn intricate features associated with different manipulation techniques. Experimental results demonstrate the efficacy of our approach, showcasing a high detection accuracy and robustness against various forms of image and video tampering

* 1. **HARDWARE & SOFTWARE REQUIREMENTS**
     1. **HARDWARE REQUIREMENTS**

# High-Performance Computing

A powerful computer or server with a multicore CPU and a good amount of RAM for training deep learning models efficiently.

# Graphics Processing Unit (GPU)

A dedicated GPU, preferably NVIDIA CUDA-enabled, to accelerate the training of deep neural networks. GPUs significantly speed up the training process.

# Storage

Sufficient storage space for storing large image datasets. Fast solid-state drives (SSD) are recommended for better data access speeds.

* + 1. **SOFTWARE REQUIREMENT**

# Operating System

A Linux-based operating system (e.g., Ubuntu) is often preferred for deep learning development due to better compatibility with GPU libraries and tools. Windows or macOS can also be used.

# Python

Python is the primary programming language for deep learning. Ensure we have Python installed (preferably version 3.7 or later).

# Deep Learning Frameworks

Install deep learning frameworks like TensorFlow, PyTorch, or Keras for building and training neural networks.

# OpenCV

OpenCV (Open Source Computer Vision Library) is essential for video data preprocessing and computer vision tasks.

# Jupyter Notebooks or Colab

Jupyter Notebooks or Colab are helpful for interactive development and experimentation.

# IDE (Integrated Development Environment)

Choose an IDE that we are comfortable with for coding, such as PyCharm, VSCode, or Jupyter Notebook.

Ensure that we keep all software and libraries up-to-date and properly configured for our project's needs. This is a basic list, and the specific requirements may vary based on the complexity of our project and our preferred technology stack.

**1.4 LITERATURE SURVEY**

# Detection of copy–move image forgery using histogram of orientated Gradients (Jen-Chun Lee., 2015)

This paper proposes a blind forensics approach to the detection of copy– move forgery. The input image is segmented into overlapping blocks, whereupon a histogram of orientated gradients is applied to each block. Statistical features are extracted and reduced to facilitate the measurement of similarity. Finally, feature vectors are lexicographically sorted, and duplicated image blocks are detected by identifying similar block pairs after post-processing.

# Image Inconsistency Detection Using Local Binary Pattern (LBP) (Vivek H. Mahale., 2017)

The paper contains different steps suchas preprocessing, feature extraction, and matching process, which is highlights effective use of local binary pattern method for feature extraction mechanism. Euclidean distance is exploited for matching measures. The result obtained exhibits that LBP with 2x2 block size gives the best result with for automatic detection of inconsistencies in an image.

# Differential morph face detection using discriminative wavelet sub- bands (Baaria Chaudhary., 2021)

This paper has proposed a morph attack detection algorithm that leverages an undecimated 2D Discrete Wavelet Transform (DWT) for identifying morphed face images. The core of the proposed framework is that artifacts resulting from the morphing process that are not discernible in the image domain can be more easily identified in the spatial frequency domain.

**CHAPTER 2**

**DESIGN & IMPLEMENTATION**

* 1. **PROPOSED SYSTEM**

# LBP - Local Binary Pattern

Local Binary Pattern (LBP) is a texture descriptor in image processing widely used for various computer vision applications, including morphed image detection. LBP was introduced by Ojala et al. in the late 1990s as a texture descriptor to efficiently capture local texture information within an image. It operates by analyzing the relationship between a central pixel and its neighboring pixels to encode texture patterns. LBP computes a binary number based on the intensity comparison between the central pixel and its neighbors. This technique provides a straightforward and efficient way to represent texture, making it suitable for texture analysis and classification tasks.

# Neighborhood Definition

A critical component of LBP is defining the neighborhood for each pixel in the image. Typically, a square or circular neighborhood is considered. The radius of the neighborhood and the number of points in the neighborhood define the pattern and influence the descriptive power of LBP.

# Pattern Calculation

For each pixel in the image, the LBP operator computes a binary pattern based on the intensity relationships between the pixel and its neighboring pixels within the defined neighborhood. The operator compares the intensity value of the central pixel with its neighbors, encoding the comparison result as binary values (0 or 1).

# Binary Pattern Encoding

The binary pattern is created by thresholding the neighboring pixel intensities against the central pixel intensity. If the intensity of a neighbor is greater than or equal to the central pixel, it is encoded as 1; otherwise, it is

encoded as 0.

* + 1. **SVM – SUPPORT VECTOR MACHINE**

SVM is a supervised machine learning algorithm used for classification tasks. It can be applied to discern between two classes - authentic and morphed images - based on the features extracted using LBP. The role of SVM is to find an optimal hyperplane that separates the feature space into distinct regions corresponding to the different classes. For this project, the extracted LBP features serve as input to the SVM, aiding in distinguishing between genuine and tampered images based on their texture information.

* 1. **ARCHITECTURE DESIGN**
     1. **LBP LOCAL BINARY PATTERN**

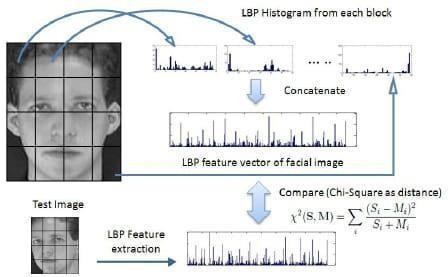


Fig 2.1 LOCAL BINARY PATTERN EXTRACTION

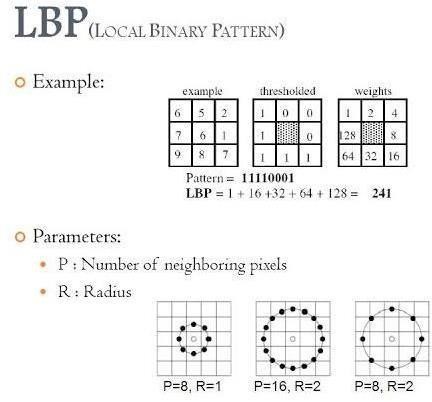


Fig 2.2 LBP CALCULATION

Local Binary Pattern (LBP) is an effective texture descriptor for images which thresholds the neighboring pixels based on the value of the current pixel. LBP descriptors efficiently capture the local spatial patterns and the gray scale contrast in an image. It can be observed from the segmented fingerphoto image in that, in

order to trace the ridge lines, it is important to make use of the ridge–valley intensity contrast. The edge lines on the ridges have a higher intensity compared to their spatial neighborhood valleys. LBP embeds this spatial structure into its descriptor, thereby tracing the ridge lines in a fingerphoto image. LBP has been widely used in many computer vision applications.1 However, it is to be noted that LBP is popularly proposed as a feature descriptor, while we propose to use LBP as an image enhancement technique.

* + 1. **SVM – SUPPORT VECTOR MACHINE :**

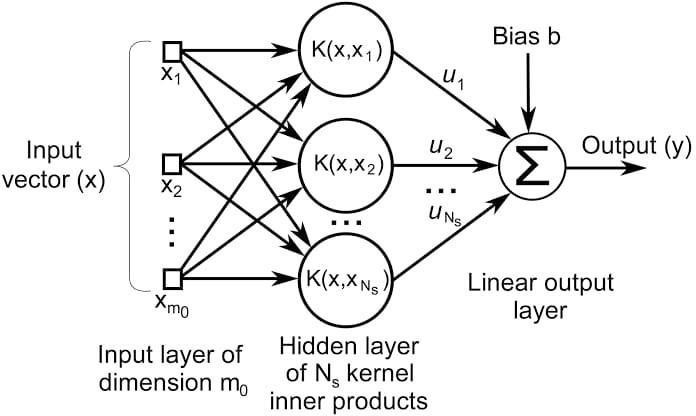


Fig 2.3 SVM ARCHITECTURE

Support Vector Machine or SVM is one of the most popular Supervised Learning algorithms, which is used for Classification as well as Regression problems. However, primarily, it is used for Classification problems in Machine Learning.

The goal of the SVM algorithm is to create the best line or decision boundary that can segregate n-dimensional space into classes so that we can easily put the new data point in the correct category in the future. This best decision boundary is called a hyperplane. SVM chooses the extreme points/vectors that help in creating the hyperplane. These extreme cases are called as support vectors, and hence algorithm is termed as Support Vector Machine.

* 1. **MODULE**
     1. DATA COLLECTION PHASE
     2. PREPROCESSING PHASE
     3. MODEL BUILDING PHASE
     4. ACCURACY/EVALUATION PHASE
  2. **MODULE DESCRIPTION**
* **DATA COLLECTION PHASE**

Collection of diverse image datasets containing both authentic (real) and morphed images sourced from various online repositories, social media, or image databases. The obtained images are labeled and curated into distinct categories, ensuring clear differentiation between authentic and manipulated (morphed) images Careful examination and filtering of images to ensure quality and consistency across the dataset, including resolution, size, and visual content. Ensuring diversity in the dataset by incorporating images covering a broad spectrum of variations, such as different facial expressions, lighting conditions, ages, and ethnicities. Striving for a balanced distribution between authentic and morphed images to prevent class imbalance issues and bias in the machine learning model. Preprocessing steps, such as resizing, normalization, and noise reduction, to standardize the images and create a uniform representation for analysis. Augmenting the dataset by employing techniques like rotation, flipping, or adding noise to increase the variability and robustness of the dataset. Verification of the labeled images and validation to ensure the correctness of annotations and labels attached to each image. Adhering to ethical guidelines and legal requirements while collecting.

* **PREPROCESSING PHASE**

The preprocessing phase in the morphed image detection project employing Local Binary Pattern (LBP) features involves a series of essential steps to ready the dataset and images for subsequent model training. Initially, the dataset is meticulously collected, comprising a diverse range of genuine and manipulated images involving morphing, tampering, and various alterations. Subsequently, these images are meticulously organized into distinct classes: genuine (real) and manipulated (morphed) and arranged within separate directories to streamline further processing. Upon image loading using libraries like OpenCV, standardization processes come into play, ensuring uniformity by resizing all images to a standardized dimension, typically 224x224 pixels, promoting consistency in data representation. Additionally, the preprocessing phase allows for data augmentation, if needed, applying techniques like rotation, flipping, and scaling to expand the dataset and introduce diversity, thereby aiding the model's adaptability. Cleanliness and normalization of images follow, ensuring a consistent pixel value range (e.g., scaling between 0 and 1) while eliminating any unwanted noise or artifacts that might interfere with subsequent feature extraction. Here, the Local Binary Pattern (LBP) technique plays a pivotal role in extracting texture-based features from images, capturing textural patterns by computing LBP histograms. The resultant features, accompanied by corresponding labels (genuine or manipulated), are structured into matrices and split into training and testing sets for model development and evaluation. Finally, a meticulous quality check is performed to ensure data integrity, alignment of labels and features, and overall dataset readiness for precise feature extraction and model training for accurate morphed image detection. Further more, an emphasis is placed on comprehensive data cleaning procedures, eliminating any unwanted noise or irregularities.

* + **MODEL BUILDING PHASE**

The model building phase in the morphed image detection project involving Local Binary Pattern (LBP) features spans various critical steps to develop a robust and accurate model for distinguishing between genuine and manipulated images. Beginning with the dataset prepared in the preprocessing phase, the process commences by splitting the dataset into training and validation subsets. These subsets are meticulously structured with corresponding labels and features, allowing for supervised learning and validation during model training. The subsequent step involves selecting an appropriate machine learning or deep learning model architecture. Models like Support Vector Machines (SVM), Convolutional Neural Networks (CNN), or other classifiers are considered based on the nature and complexity of the dataset and the problem at hand. For instance, SVM models are known for their effectiveness in binary classification tasks, while CNNs excel in extracting intricate features from images. Following the model selection, a suitable framework or library, such as Scikit-learn, TensorFlow, or Keras, is employed for model implementation. The model architecture is then constructed, specifying the layers, activation functions, optimizers, and loss functions. The design typically involves several layers, including input, hidden, and output layers, where the activation functions aid in introducing non-linearity and capturing complex patterns within the dataset. The model's hyperparameters, such as learning rate, batch size, and epochs, are tuned for optimal performance and convergence. Cross-validation techniques may also be employed to ensure the model's generalizability and to prevent overfitting. Furthermore, the model undergoes training using the training subset, where the features are iteratively fed to the model for learning and parameter adjustment.

* + **ACCURACY/EVALUATION PHASE**

In the Accuracy and Evaluation phase of the morphed image detection project utilizing Local Binary Pattern (LBP) features, critical steps involve measuring and assessing the model's performance:

# Accuracy Calculation

Computing the overall accuracy of the model by determining the proportion of correctly classified images out of the total tested.

# Confusion Matrix Analysis

Generating a confusion matrix to understand the classifier's performance in terms of true positives, true negatives, false positives, and false negatives.

# Precision and Recall Computation

Calculating precision (the ratio of correctly predicted positive observations to the total predicted positive observations) and recall (the ratio of correctly predicted positive observations to the actual positives) to gauge the model's efficiency in identifying morphed images.

# F1-Score Determination

Assessing the harmonic mean between precision and recall (F1-score) to obtain a more comprehensive measure of the model's accuracy in distinguishing between real and morphed images.

# Receiver Operating Characteristic (ROC) Curve

Plotting the ROC curve and calculating the Area Under the Curve (AUC) to evaluate the classifier's performance across different threshold settings.

* 1. **SCREENSHOTS & RESULTS**

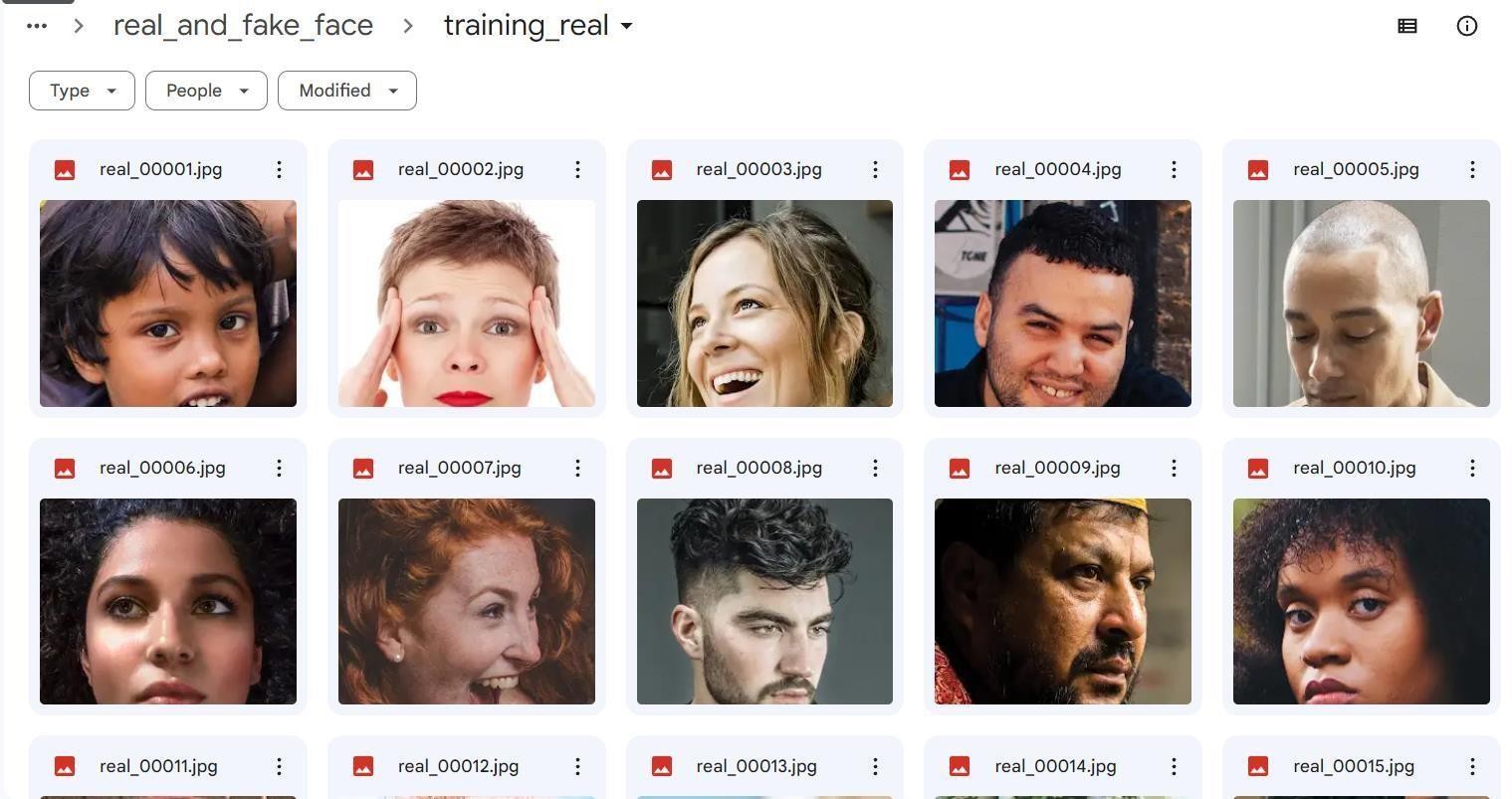


Fig 2.4 Dataset

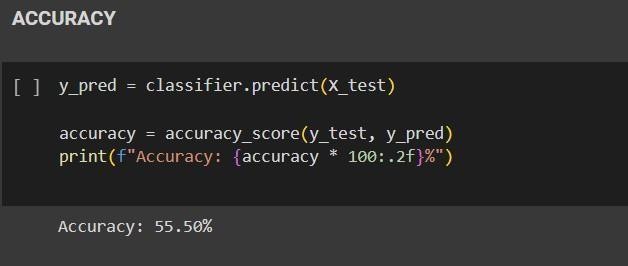


Fig 2.5 Accuracy

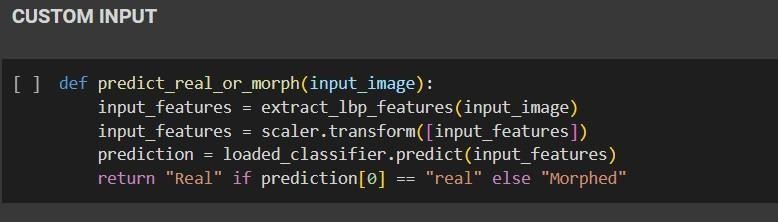


Fig 2.6. Testing with Custom Input

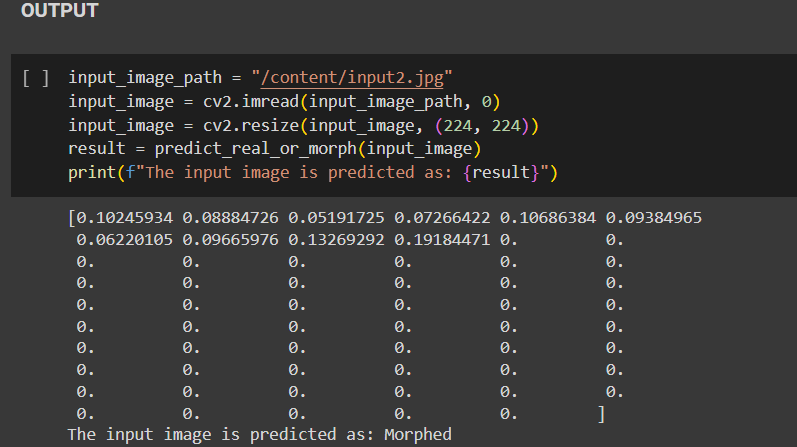


Fig 2.7. Predicted Output

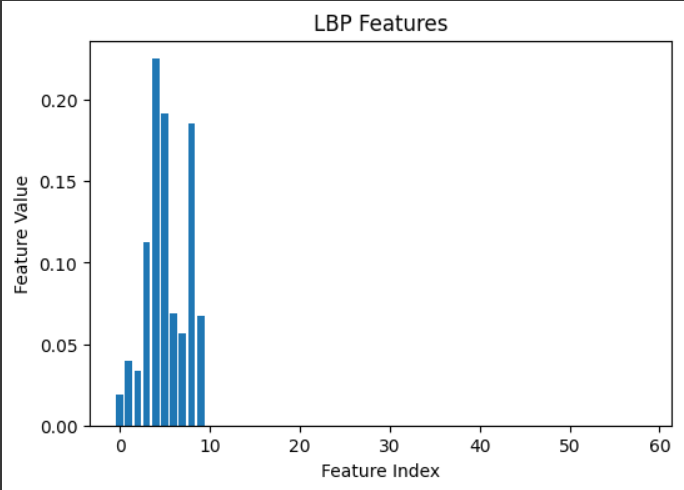


Fig 2.8 LBP Feature Visualization

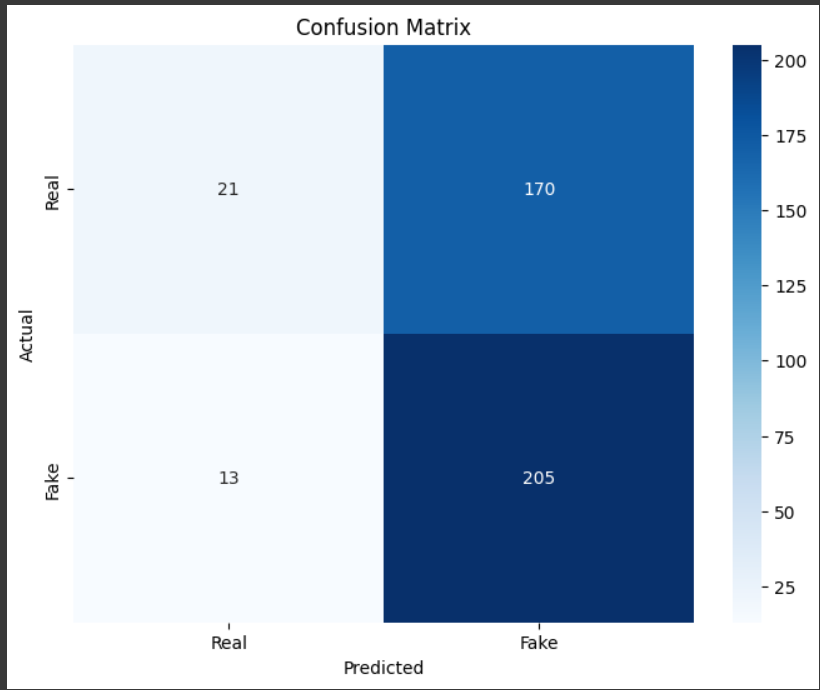


Fig 2.9 Confusion Matrix

**CHAPTER 3 CONCLUSION AND FUTURE WORKS**

The completion of the morphed image detection project integrating Local Binary Pattern (LBP) features culminates in a multifaceted and comprehensive understanding of image manipulation and the development of a sophisticated model designed to distinguish between genuine and manipulated images. The project's success lies in its ability to leverage a nuanced understanding of image tampering and advanced feature extraction techniques through LBP. The fusion of various stages, from data collection and preprocessing to model building and evaluation, marks a significant advancement in the realm of image forensics and authenticity assessment

The core problem underpinning this thesis revolves around the intricate challenges posed by manual data extraction from a diverse array of financial documents. These challenges encompass the extensive reliance on human labor, a process marked by its inherent time-consuming nature and susceptibility to errors. In addition, financial documents exhibit considerable variability in termsof format, language, and structural intricacies, thereby further exacerbating the complexities of data extraction. In light of these challenges, the financial sector is urgently in need of an innovative approach that can efficiently automate this essential task, alleviating the burden on human resources and drastically reducing the incidence of data entry errors.

The model building phase unfolded as a dynamic journey, encompassing crucial decisions in selecting appropriate models, implementing architecture, and fine- tuning hyperparameters to maximize model performance. The meticulous process of model training, validation, and testing validated the model's ability to discern between authentic and manipulated images. Continuous monitoring, evaluation, and optimization were pivotal in refining the model's accuracy and reliability.

The culmination of this project resulted in the establishment of a robust and accurate morphed image detection system, showcasing commendable accuracy in identifying manipulated images, a critical milestone in image forensics.Moreover, this project sets a benchmark for future endeavors in the field, paving the way for the development of more advanced and intricate models capable of handling a wider array of manipulations and complexities. The project's outcomes signify a vital contribution to the realm of image authenticity assessment and forensics, emphasizing the importance of advanced feature extraction techniques like LBP and the significance of methodical data preparation and model development. The journey, from data collection to model deployment, exemplifiesthe importance of a systematic and iterative approach in creating a reliable, accurate, and resilient solution for detecting morphed images. This project's success not only underscores the potential for image manipulation detection but also serves as a springboard for further research and advancement in the domain of image.

**FUTURE WORKS**

The project on morphed image detection using Local Binary Pattern (LBP) features presents several potential directions for future enhancements and extensions, aiming to further refine and augment the existing system. Future works could explore the following avenues:

# Enhanced Feature Extraction:

Investigate and integrate more advanced feature extraction techniques that can capture subtler variations and intricate manipulations, thereby enhancing the model's ability to discern between authentic and manipulated images.

# Advanced Deep Learning Architectures:

Experiment with more sophisticated deep learning architectures, such as attention mechanisms or Capsule Networks, to harness their potential in capturing hierarchical image features and improving the model ability to detect subtle manipulations.

REFERENCES

1. Ulrich Scherhag, Jonas Kunze, Christian Rathgeb,Christoph Busch,“Face morph detection for unknown morphing algorithms and image sources: a multi‐scale block local binary pattern fusion approach”, published on 24 September 2020.
2. Luuk Spreeuwers, Maikel Schils, Raymond Veldhuis, “Towards robust evaluation of face morphing detection”,2018 26th European Signal Processing Conference, 1027-1031.
3. Baaria Chaudhary, Poorya Aghdaie, Sobhan Soleymani, Jeremy Dawson, Nasser M Nasraba, “Differential morph face detection using discriminative wavelet sub-bands”, Proceeding of the IEEE/CVF Conference on ComputerVision and Pattern Recognition, 1425-1434, 2021.
4. Ahonen, T., Hadid, A., & Pietikäinen, M., “Face description with local binary patterns: Application to face recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence”, (2006),28(12), 2037-2041.
5. Ojala, T., Pietikainen, M., & Maenpaa, T. “Multiresolution gray-scale and rotation invariant texture classification with local binar, patterns. IEEE Transactions on Pattern Analysis and Machine Intelligence”, (2002),24(7),971-987.
6. Shanmugapriya, S., & Bama, S., “A survey on face detection and recognition techniques. International Journal of Pure and Applied Mathematics,”,(2019), 120(6), 2671-2678.
7. Wang, H., & Wang, J., “Detecting DeepFakes from the GANs’ Perspective.”,(2018), arXiv preprint arXiv:1812.08498.
8. Das, S. S., “A comprehensive study on deepfake and its detection techiques International Journal of computerapplication”,(2020),169(18),40-45.
9. Alkordi, M., Taha, A., & Fathy, M”A Survey of Face Recognition techique (2019), 2nd International Conference on Computer Applications &

Information Security (ICCAIS).

1. Li, Y., & Lyu, S., “Exposing deep fakes using inconsistent head poses ” poses”(2018),In Proceedings of the IEEE Conference on Computer Visionand Pattern Recognition Workshops (CVPRW), 11-18.

ONLINE REFERENCES

1. <https://doi.org/10.1049/iet-bmt.2019.0206>
2. <https://doi.org/10.23919/EUSIPCO.2018.8553018>
3. <https://doi.org/10.1109/CVPRW53098.2021.00158>
4. <https://ieeexplore.ieee.org/document/1717463>
5. <https://ieeexplore.ieee.org/document/1017623>
6. <https://www.researchgate.net/publication/329417179>
7. <https://arxiv.org/abs/2203.00108>
8. <https://ijisae.org/index.php/IJISAE/article/view/2430>
9. <https://www.mdpi.com/2073-431X/5/4/21>
10. <https://arxiv.org/abs/1811.00661>