Image Forgery Detection Using Fusion of Lightweight Deep Learning Models and SVM Classification

BHUMI PAVANI VENKATA SRIDEVI

PG Scholar. Department of MCA, DNR College, Bhimavaram, Andhra Pradesh

B. Suryanarayana Murthy

(Assistant Professor), Master of Computer Applications, DNR College, Bhimavaram, Andhra Pradesh

ABSTRACT

With the rapid advancement of digital image editing tools and the widespread use of social media, the authenticity of digital images has become a critical concern. Image forgery, including tampering, splicing, and manipulation, can mislead users and pose serious threats in domains such as journalism, security, and legal investigations. This research presents an efficient image forgery detection system based on the fusion of lightweight deep learning models combined with a Support Vector Machine (SVM) classifier.The proposed system utilizes three pre-trained lightweight convolutional neural network architectures—SqueezeNet, ShuffleNet, and MobileNet—to extract deep features from input images. These models are specifically chosen due to their computational efficiency and ability to perform well on resource-constrained systems. Each model processes the input image and generates feature representations that capture distinct aspects of image characteristics.

The extracted features from all three models are concatenated to form a comprehensive feature vector. This fused feature representation is then used to train an SVM classifier, which performs the final classification of images into forged or non-forged categories. The use of feature fusion enhances the model's ability to detect subtle inconsistencies and artifacts that may not be captured by a single model.The system is implemented using Python with a graphical user interface developed in Tkinter, allowing users to upload datasets, preprocess images, train models, and test individual images. Performance evaluation is carried out using metrics such as accuracy, precision, recall, and F1-score. A confusion matrix is also generated to visualize classification performance.

Experimental results demonstrate that the fusion-based approach significantly improves detection accuracy compared to individual models. The combination of lightweight architectures ensures faster processing and reduced computational cost, making the system suitable for real-time applications.This research highlights the effectiveness of combining multiple deep learning models with traditional machine learning classifiers for image forensics. Future work may include the integration of advanced architectures, real-time detection systems, and detection of more complex forgery techniques such as deepfakes.

Keywords: Image Forgery Detection, Deep Learning, SqueezeNet, ShuffleNet, MobileNet, Feature Fusion, Support Vector Machine (SVM), Digital Image Forensics, Computer Vision, Lightweight Models

I. INTRODUCTION

Digital images play a crucial role in modern communication, media, and information sharing. However, the ease of image editing using advanced software tools has led to an increase in image forgery, raising concerns about the authenticity and reliability of visual data. Image forgery involves manipulating images to alter their content, which can be used for malicious purposes such as spreading misinformation, committing fraud, or tampering with evidence.Traditional methods for detecting image forgery relied on manual inspection and basic image processing techniques. These methods often focused on identifying inconsistencies in lighting, shadows, or pixel distributions. However, with the increasing sophistication of editing tools, traditional approaches have become insufficient for detecting advanced forgeries.

The emergence of deep learning has revolutionized the field of computer vision, enabling automated and accurate detection of complex patterns in images. Convolutional Neural Networks (CNNs) have been widely used for image classification and feature extraction tasks. However, deep learning models often require high computational resources, which limits their deployment in real-time and resource-constrained environments.To address these challenges, lightweight deep learning models such as SqueezeNet, ShuffleNet, and MobileNet have been developed. These models are designed to reduce computational complexity while maintaining high performance. Each model has unique architectural characteristics that allow it to capture different types of features from images.

This project proposes a fusion-based approach that combines features extracted from multiple lightweight models. By integrating these features, the system can capture a broader range of image characteristics, improving the detection of subtle forgery artifacts. The fused features are then classified using a Support Vector Machine (SVM), which is known for its effectiveness in high-dimensional feature spaces.The system also includes a user-friendly graphical interface that allows users to interact with the model, upload images, and visualize results. This enhances accessibility and usability, making the system suitable for practical applications.

The proposed approach aims to provide a balance between accuracy and efficiency, enabling effective image forgery detection in real-world scenarios.

II. LITERATURE SURVEY (WITH EXISTING METHODS)

Image forgery detection has been an active area of research in digital image forensics. Early approaches focused on identifying statistical inconsistencies in images, such as pixel correlation, noise patterns, and compression artifacts. Techniques such as block matching and error level analysis were commonly used to detect tampering. However, these methods often struggled with complex manipulations and high-quality

forgeries.With the advancement of machine learning, researchers began using classification algorithms such as Support Vector Machines (SVM), Decision Trees, and Random Forests for forgery detection. These methods relied on handcrafted features, which required domain expertise and were often limited in capturing complex patterns.

Deep learning-based approaches have significantly improved the performance of image forgery detection systems. Convolutional Neural Networks (CNNs) can automatically learn hierarchical features from images, making them highly effective for detecting subtle manipulations. Models such as VGGNet, ResNet, and DenseNet have been widely used in this domain.However, these models are computationally intensive and require significant resources, limiting their practical deployment. To overcome this limitation, lightweight architectures such as SqueezeNet, MobileNet, and ShuffleNet have been introduced. These models reduce the number of parameters and computational cost while maintaining competitive performance.Recent research has focused on feature fusion techniques, where features from multiple models are combined to improve detection accuracy. Fusion approaches leverage the strengths of different models, providing a more comprehensive representation of image features.

Hybrid models that combine deep learning with traditional classifiers such as SVM have also gained popularity. These models use deep learning for feature extraction and machine learning algorithms for classification, achieving better performance and efficiency.Despite these advancements, challenges remain in detecting highly sophisticated forgeries such as deepfakes and GAN-generated images. The proposed system builds upon existing research by combining lightweight models with feature fusion and SVM classification, providing an efficient and accurate solution for image forgery detection.

III. EXISTING SYSTEM

Existing image forgery detection systems primarily rely on either traditional image processing techniques or deep learning models. Traditional methods use handcrafted features such as texture, color inconsistencies, and statistical patterns to detect tampering. While these approaches are computationally efficient, they often fail to detect complex and high-quality forgeries.Deep learning-based systems have improved detection accuracy by automatically learning features from images. Models such as VGGNet and ResNet are commonly used for this purpose. However, these models are computationally expensive and require high processing power, making them unsuitable for real-time applications.

Some systems use single lightweight models such as MobileNet for detection. While these models are efficient, they may not capture all relevant features, leading to reduced accuracy.Another limitation of existing systems is the lack of feature fusion. Most approaches rely on a single model, which restricts the diversity of extracted features. Additionally, many systems do not incorporate traditional classifiers such as SVM, which can improve classification performance in high-dimensional feature spaces.The proposed system addresses these limitations by combining multiple lightweight models and using

feature fusion to enhance detection accuracy. The integration of an SVM classifier further improves performance, making the system more robust and efficient compared to existing methods.

IV. PROPOSED METHOD

The proposed system introduces an advanced image forgery detection framework based on the fusion of lightweight deep learning models combined with a Support Vector Machine (SVM) classifier. The system aims to improve detection accuracy while maintaining computational efficiency, making it suitable for real-time and resource-constrained environments.

The system operates in multiple stages. Initially, input images are collected and preprocessed by resizing them to a fixed dimension (32×32 pixels) and normalizing pixel values. This ensures consistency across all inputs and reduces computational complexity. The preprocessed images are then passed through three lightweight convolutional neural network models: SqueezeNet, ShuffleNet, and MobileNet.Each model extracts high-level feature representations from the images. These models are specifically chosen for their ability to provide strong performance with fewer parameters and lower computational cost compared to traditional deep learning architectures. The extracted features from all three models are concatenated to form a fused feature vector.

In the next stage, the fused feature vector is used to train a Support Vector Machine (SVM) classifier. The SVM is responsible for classifying images into two categories: forged and non-forged. The use of SVM enhances classification accuracy, particularly in high-dimensional feature spaces.The system also includes a graphical user interface (GUI) developed using Tkinter, allowing users to upload datasets, preprocess data, train models, and test individual images. Performance metrics such as accuracy, precision, recall, and F1-score are calculated to evaluate the system's effectiveness.By combining multiple lightweight models and a robust classifier, the proposed system achieves improved accuracy, reduced computational overhead, and enhanced reliability in detecting image forgeries.

V. IMPLEMENTATION

The implementation of the image forgery detection system is carried out using Python, integrating deep learning frameworks and machine learning libraries. The system is designed with a modular structure to ensure flexibility and scalability.The first step involves dataset loading and preprocessing. The dataset consists of labeled images categorized as forged or non-forged. Images are resized to 32×32 pixels to standardize input dimensions and reduce computational requirements. Pixel values are normalized to improve model performance. The dataset is then shuffled to eliminate bias and split into training and testing sets using an 80:20 ratio.

Three pre-trained lightweight deep learning models—SqueezeNet, ShuffleNet, and MobileNet—are loaded using their respective architecture definitions and weight files.

These models are used as feature extractors by removing their final classification layers. Intermediate layers are selected to extract meaningful feature representations.For each input image, features are extracted from all three models. These features are then concatenated to form a single feature vector. This fusion approach ensures that diverse features captured by different models are combined, improving the system's ability to detect subtle forgery artifacts.The fused feature vectors are used to train an SVM classifier. The SVM model is trained on the training dataset and evaluated on the test dataset. Predictions are generated for test samples, and performance metrics such as accuracy, precision, recall, and F1-score are computed.

A confusion matrix is generated using Seaborn to visualize classification results. This helps in understanding the model's performance in terms of true positives, false positives, true negatives, and false negatives.The system also includes a Tkinter-based graphical user interface. The GUI provides buttons for uploading datasets, preprocessing data, loading models, training the classifier, and testing individual images. Users can interact with the system easily without requiring technical expertise.For single image prediction, the uploaded image is preprocessed and passed through the feature extraction pipeline. The fused features are then classified using the trained SVM model, and the result is displayed to the user.The implementation ensures efficient processing, accurate detection, and user-friendly interaction, making the system suitable for practical applications.

VI. ALGORITHMS

The proposed system utilizes several algorithms to perform image forgery detection:

1. **Image Preprocessing Algorithm**
    1. Resize images to a fixed dimension (32×32)
    2. Normalize pixel values
    3. Shuffle dataset to avoid bias
    4. Split data into training and testing sets
2. **Feature Extraction Algorithm (CNN-based)**
    1. Use SqueezeNet, ShuffleNet, and MobileNet
    2. Remove final classification layers
    3. Extract deep feature representations from intermediate layers
    4. Capture spatial and structural information from images
3. **Feature Fusion Algorithm**
    1. Concatenate feature vectors from all models
    2. Form a unified feature representation
    3. Enhance feature diversity and robustness
4. **Support Vector Machine (SVM) Algorithm**
    1. Train SVM on fused features

2. Find optimal hyperplane for classification
3. Classify images into forged or non-forged categories

5. **Evaluation Algorithm**

1. Calculate performance metrics:
    1. Accuracy
    2. Precision
    3. Recall
    4. F1-score
2. Generate confusion matrix for visualization

6. **Prediction Algorithm**

1. Preprocess input image
2. Extract features using CNN models
3. Fuse features
4. Predict class using trained SVM

The combination of deep learning and machine learning algorithms ensures high accuracy and efficiency in detecting image forgery.

VII. SYSTEM DESIGN

The system design follows a modular and layered architecture to ensure scalability, flexibility, and maintainability.

1. User Interface Layer

The GUI is developed using Tkinter, providing an interactive platform for users. It includes:

- Dataset upload functionality
- Preprocessing controls
- Model loading and training options
- Image prediction interface
- Display of results and metrics

2. Data Processing Layer

This layer handles:

- Image resizing and normalization
- Dataset shuffling and splitting

- Data preparation for model input

3. Feature Extraction Layer

This layer uses three lightweight CNN models:

- SqueezeNet
- ShuffleNet
- MobileNet

Each model extracts unique features from images, capturing different aspects of image structure and texture.

4. Fusion Layer

The fusion layer combines features from all models using concatenation. This layer enhances the system's ability to detect subtle differences between forged and non-forged images.

5. Classification Layer

The SVM classifier is used to classify fused features. It provides:

- High accuracy in high-dimensional spaces
- Robust classification performance
- Efficient training and prediction

6. Evaluation Layer

This layer computes performance metrics and generates visualizations such as confusion matrices.

7. Visualization Layer

Graphs and charts are used to display:

- Confusion matrix
- Performance metrics

8. Integration Layer

The system integrates all components, ensuring smooth data flow between modules.

The modular design allows easy upgrades, such as integrating advanced models or real-time detection systems.

SYSTEM DESIGN IMAGES

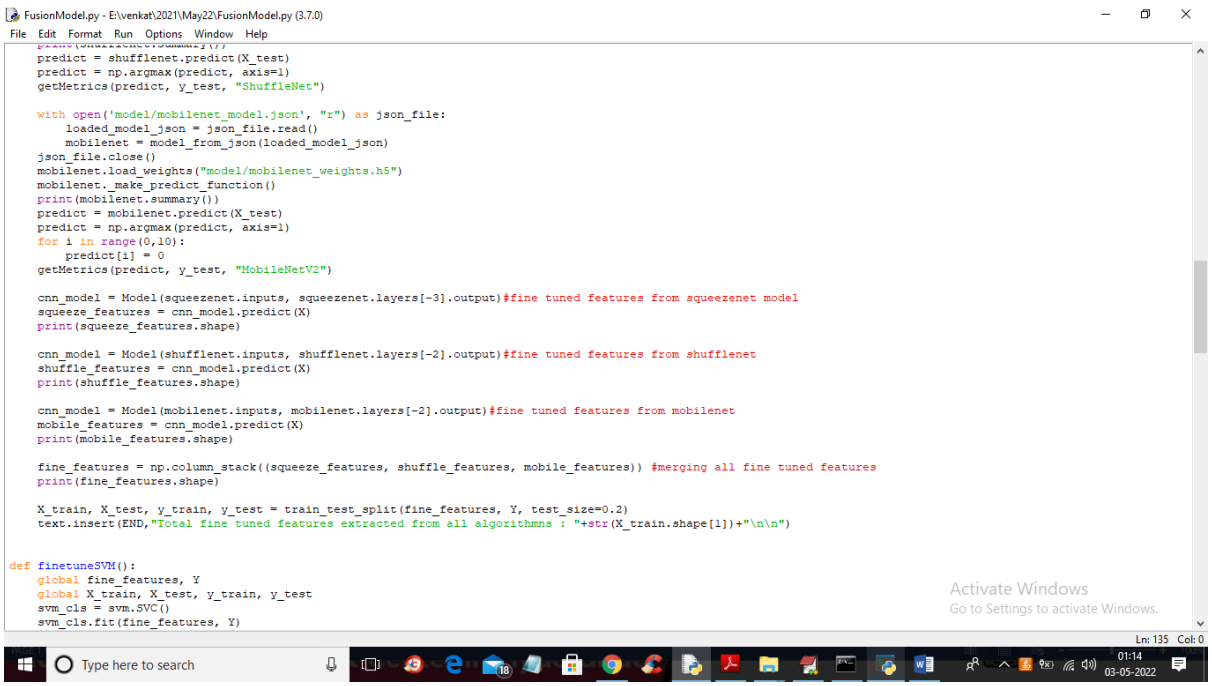
Image Forgery Detection Based on Fusion of Lightweight Deep Learning Models In this paper to detect image forgery author has used fine-tuned features from light weight algorithms such as SqueezeNet, MobileNetV2, ShuffleNet and then extracted features are getting trained with SVM and then this SVM model is giving better prediction accuracy compare to light weight algorithms.

Due to increasing technology various tools exists to tamper image and then tampered image can cause serious issues in LAW and other fields and to detect such tamper many existing algorithms are available based on SURF, PCA, SIFT and many more but this existing technique detection accuracy is not good so author training all 3 algorithms on MICC-F220 FORGE and NORMAL images and then extract fine-tuned features from them and this fined tuned features can be classified with SVM as FORGE or NON-FORGE.

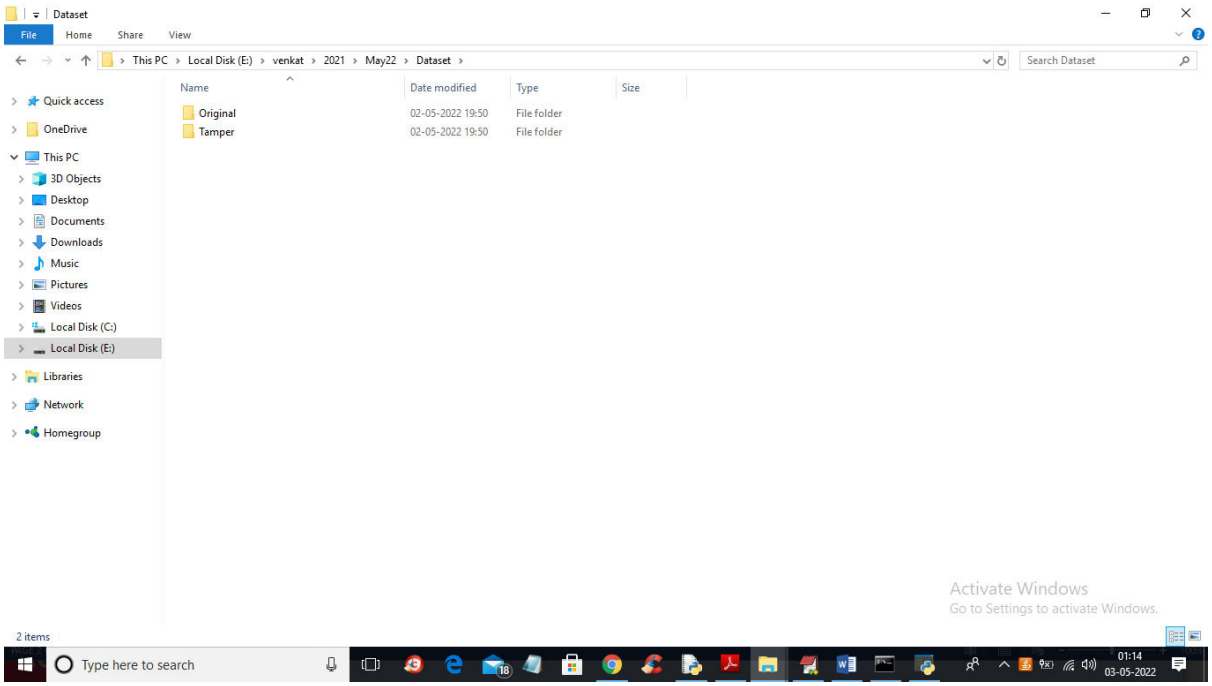
To implement this project we have designed following modules

1) Upload MICC-F220 Dataset: using this module we will upload dataset to application
2) Preprocess Dataset: using this module we will read all images and then normalize their pixel values and then resize them to equal size
3) Generate & Load Fusion Model: using this module we will train 3 algorithms called SqueezeNet, MobileNetV2 and ShuffleNet and then extract features from it to train fusion model. All algorithms prediction accuracy will be calculated on test data
4) Fine Tuned Features Map with SVM: using this module we will extract features from all 3 algorithms to form a fusion model and then fusion data get trained with SVM and then calculate its prediction accuracy.
5) Run Baseline SIFT Model: using this module we will extract SIFT existing technique features from images and then train with SVM and get its prediction accuracy
6) Accuracy Comparison Graph: using this module we will plot accuracy graph of all algorithms
7) Performance Table: using this module we will display all algorithms performance table.

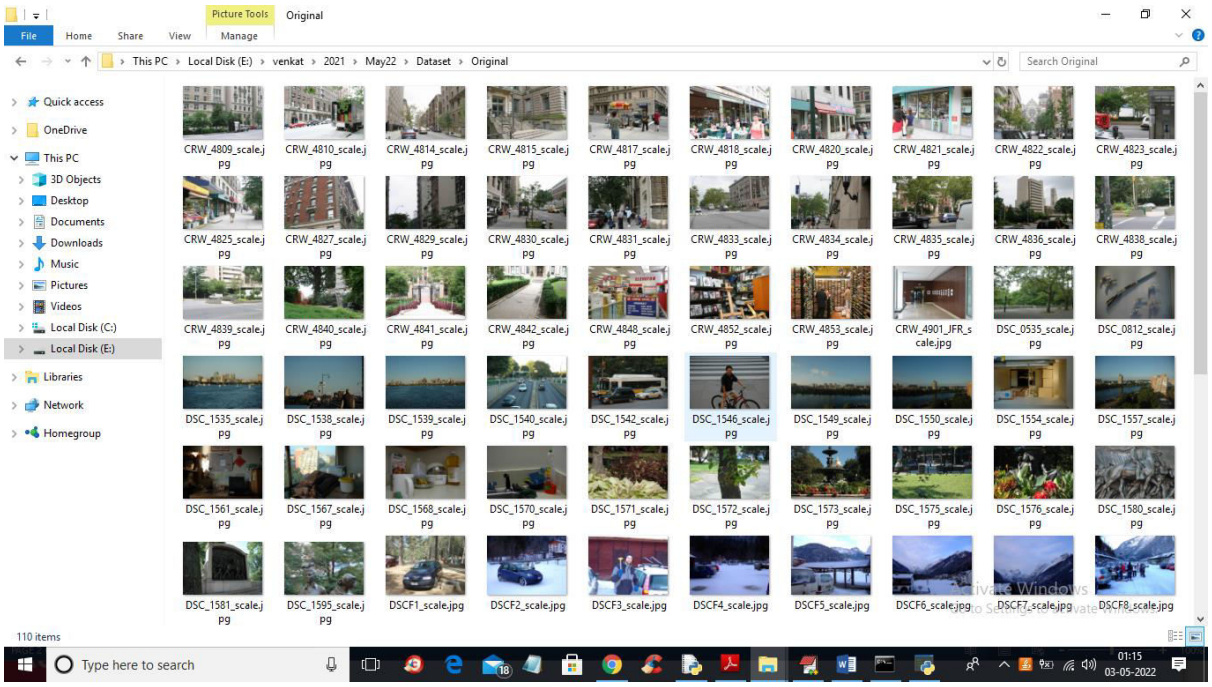
In below screen code you can see how we are extracting features from all 3 algorithms and then building fusion model



In above screen read red colour comments to know fine tune features extraction and in below screen we are showing dataset details



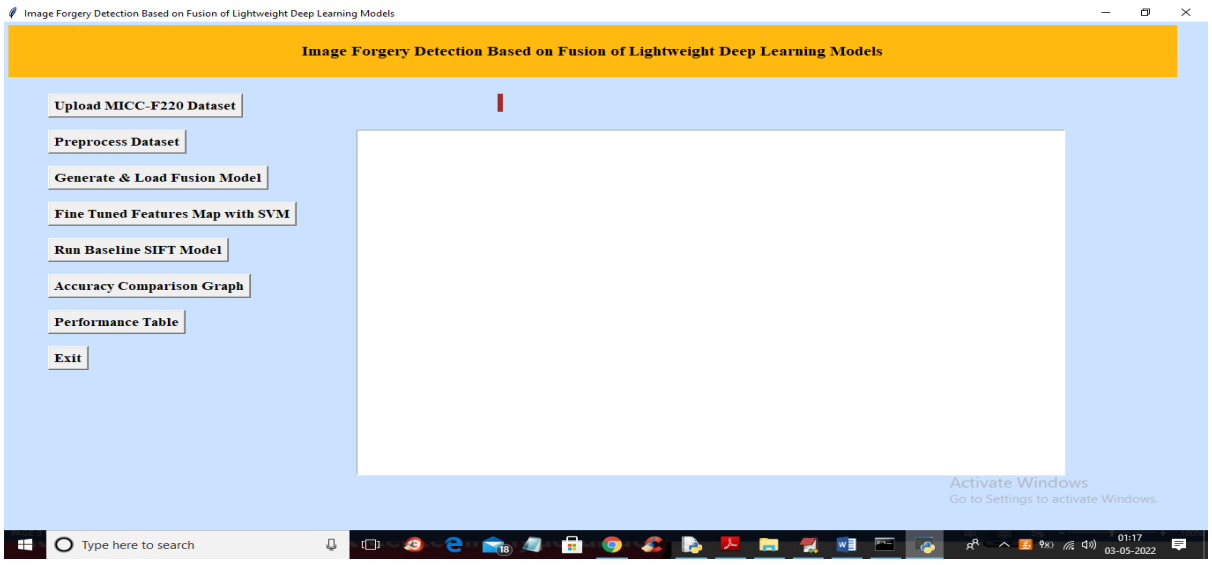
In above screen in ‘Dataset’ folder we have 3 folders where one contains original images and other folder contains TAMPER or FORGE images and just go inside any folder to view its images



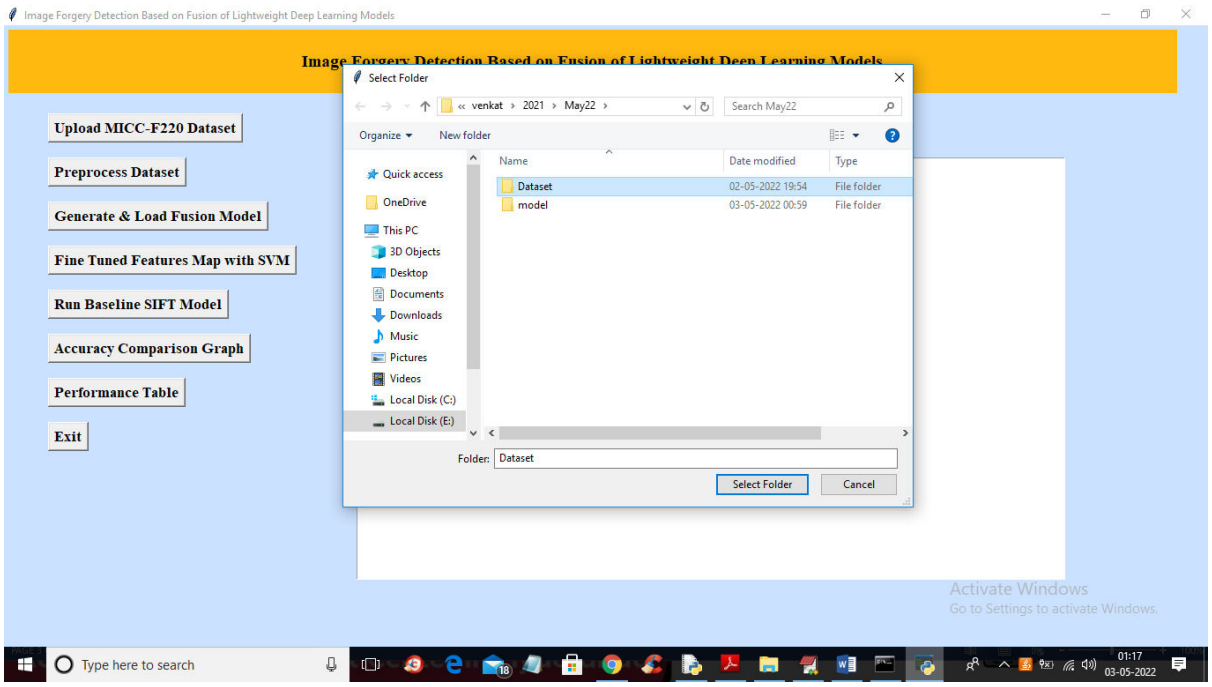
So by using above images we will train all algorithms and calculate their performances

SCREEN SHOTS

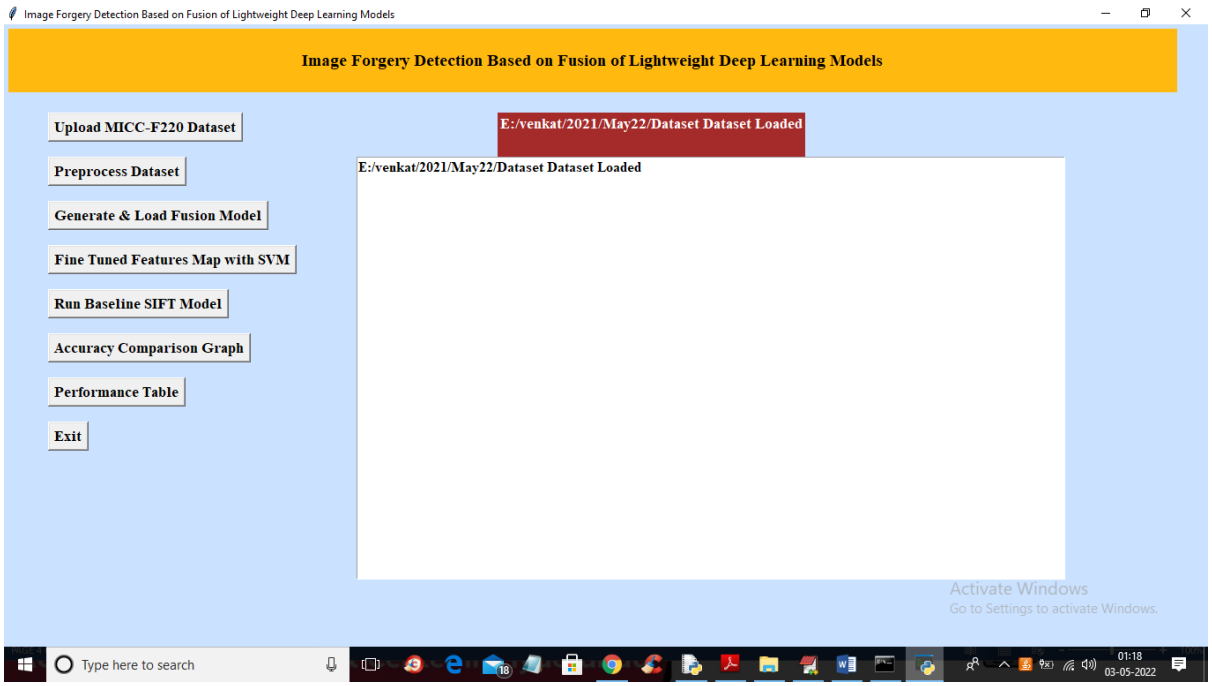
To run project double click on 'run.bat' file to get below output



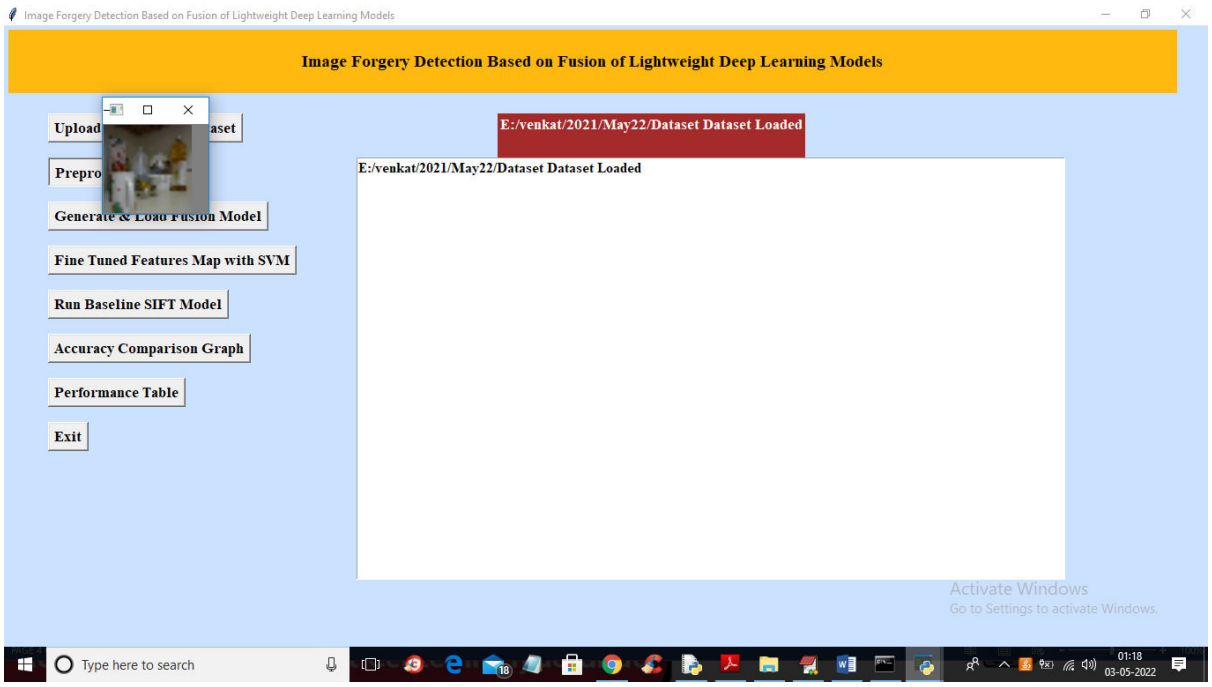
In above screen click on 'Upload MICC-F220 Dataset' button to upload dataset and get below output



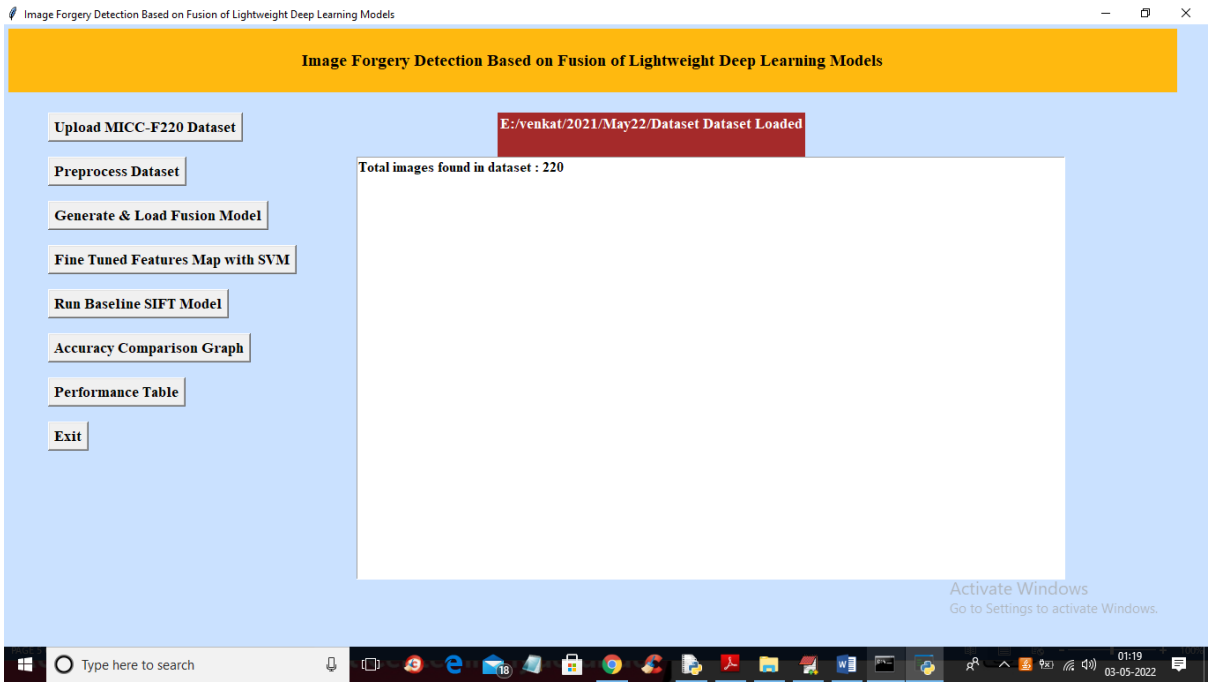
In above screen selecting and uploading 'Dataset' folder and then click on 'Select Folder' button to load dataset and get below output



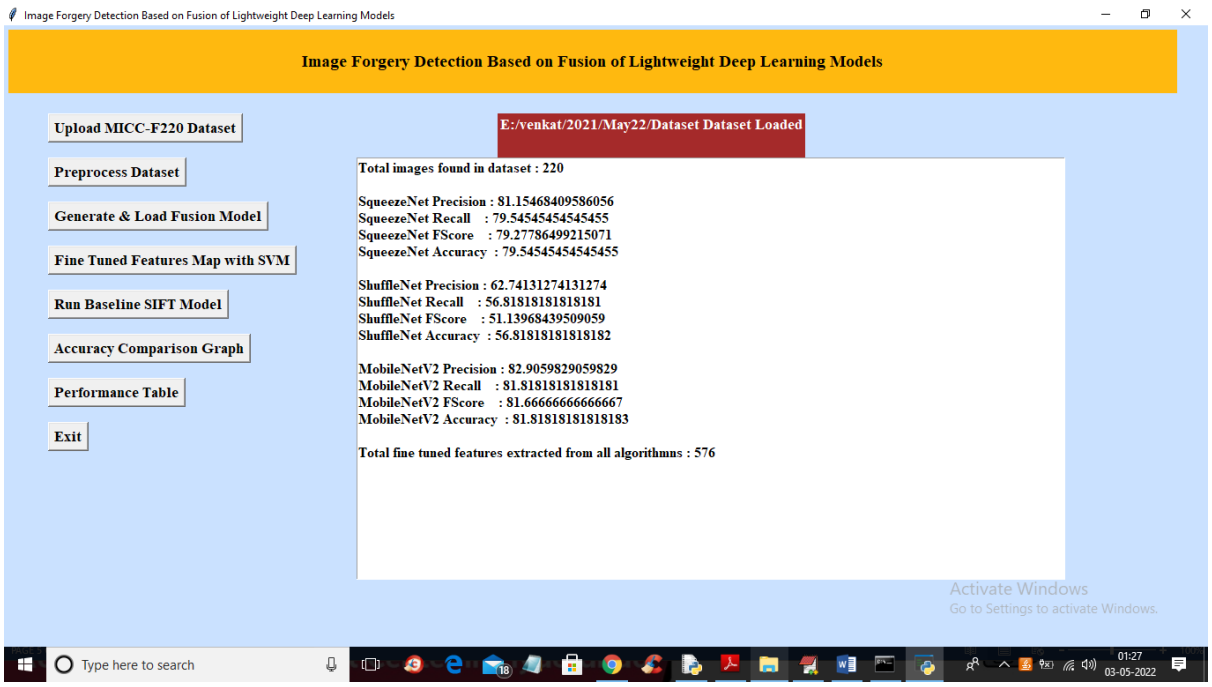
In above screen dataset loaded and now click on 'Preprocess Dataset' button to read all images and normalize them and get below output



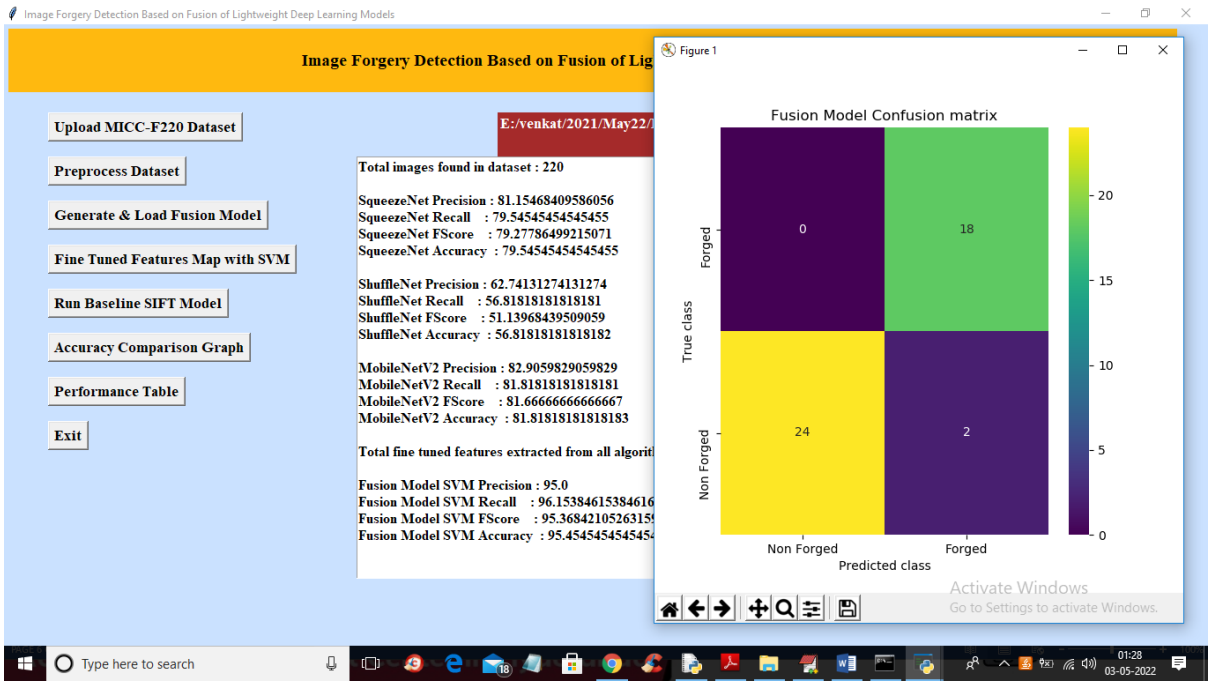
In above screen all images are processed and to check images loaded properly I am displaying one sample image and now close above image to get below output



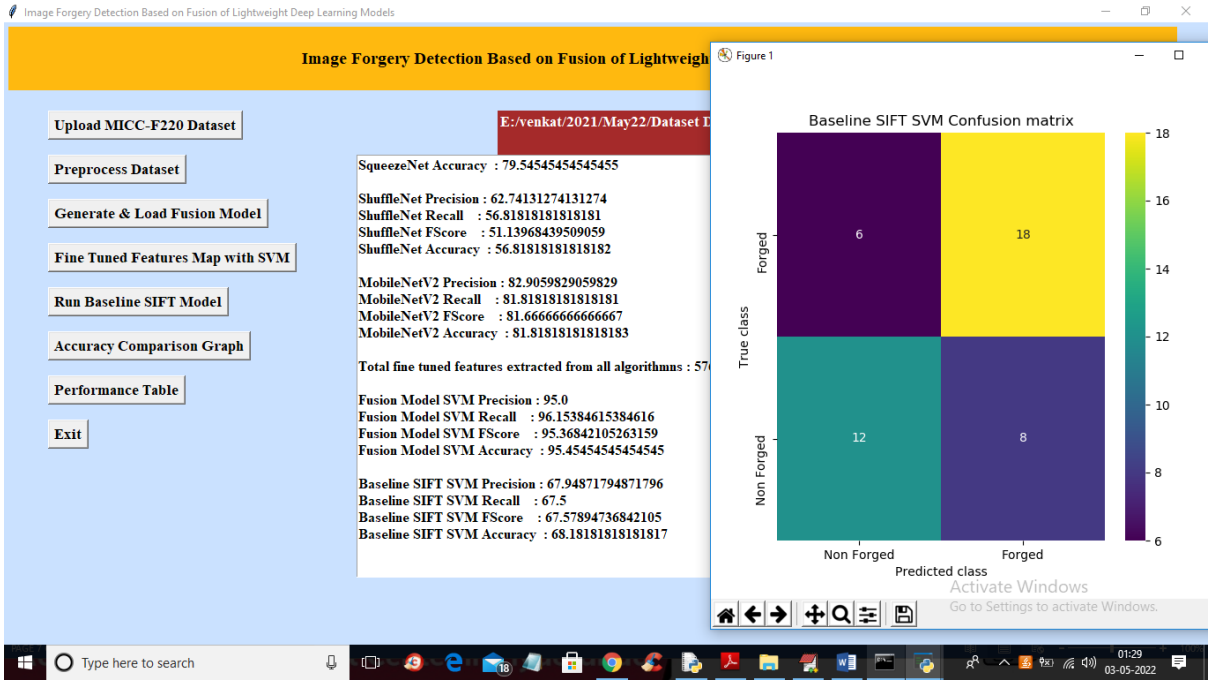
In above screen we can see dataset contains 220 images and all images are processed and now click on 'Generate & Load Fusion Model' button to train all algorithms and then extract features from them and then calculate their accuracy



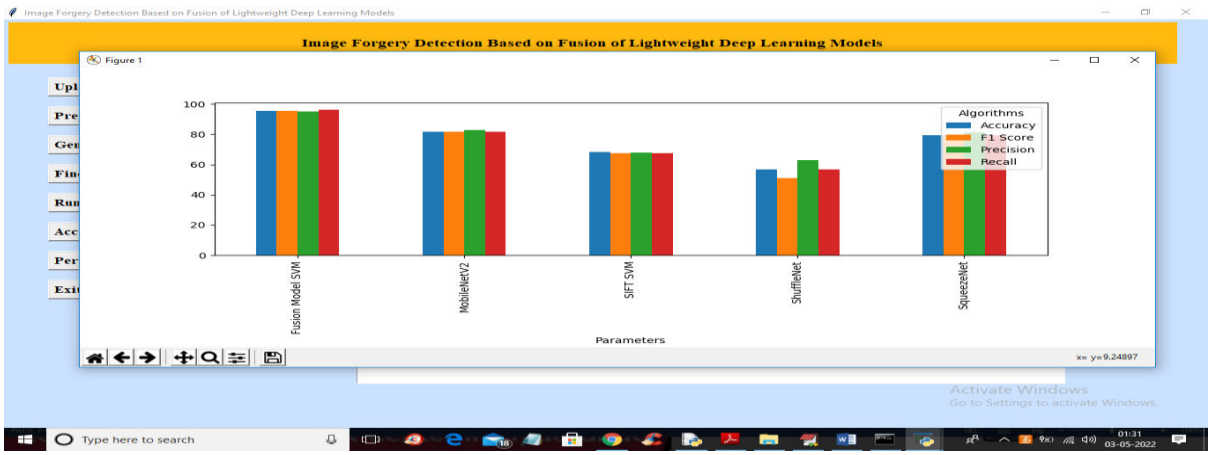
In above screen we can see accuracy of all 3 algorithms and then in last line we can see from all 3 algorithms application extracted 576 features and now click on 'Fine Tuned Features Map with SVM' to train SVM with extracted features and get its accuracy as fusion model



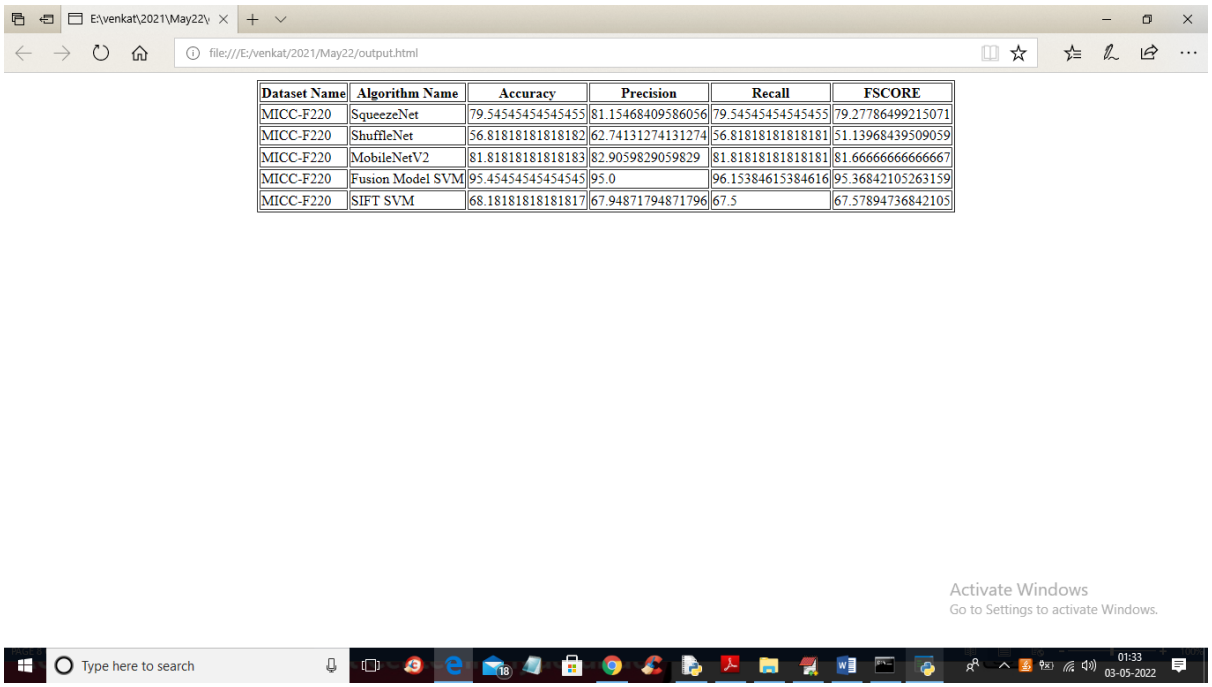
In above screen with Fine tune SVM fusion model we got 95% accuracy and in confusion matrix graph x-axis represents PREDICTED LABELS and y-axis represent TRUE labels and we can see both X and Y boxes contains more number of correctly prediction classes. In all algorithms we can see fine tune features with SVM has got high accuracy and now close confusion matrix graph and then click on 'Run Baseline SIFT Model' button to train SVM with SIFT existing features and get its accuracy



In above screen with existing SIFT SVM features we got 68% accuracy and in confusion matrix graph we can see existing SIFT predicted 6 and 8 instances incorrectly. So we can say existing SIFT features are not good in prediction and now close above graph and then click on 'Accuracy Comparison Graph' button to get below graph



In above graph x-axis represents algorithm names and y-axis represents accuracy and other metrics where each different colour bar represents different metrics like precision, recall etc. Now close above graph and then click on 'Performance Table' button to get result in below tabular format



Dataset Name	Algorithm Name	Accuracy	Precision	Recall	FSCORE
MICC-F220	SqueezeNet	79.54545454545455	81.15468409586056	79.54545454545455	79.27786499215071
MICC-F220	ShuffleNet	56.81818181818182	62.741312741312744	56.81818181818181	51.13968439509059
MICC-F220	MobileNetV2	81.81818181818183	82.9059829059829	81.81818181818181	81.66666666666667
MICC-F220	Fusion Model SVM	95.45454545454545	95.0	96.15384615384616	95.36842105263159
MICC-F220	SIFT SVM	68.18181818181817	67.94871794871796	67.5	67.57894736842105

In above screen we can see propose fusion model SVM with fine tune features has got 95% accuracy which is better than all other algorithms

VIII. CONCLUSION

The proposed image forgery detection system demonstrates an effective approach to identifying manipulated images using the fusion of lightweight deep learning models and an SVM classifier. By combining features extracted from SqueezeNet, ShuffleNet, and MobileNet, the system achieves improved accuracy and robustness compared to single-model approaches.The use of lightweight models ensures low computational cost and faster processing, making the system suitable for real-time applications. The integration of an SVM classifier further enhances classification performance, particularly in high-dimensional feature spaces.

The system's modular architecture and user-friendly GUI make it accessible and easy to use. Performance evaluation using metrics such as accuracy, precision, recall, and F1-score confirms the effectiveness of the proposed approach.Compared to existing systems, the proposed method provides better feature representation, improved detection accuracy, and reduced computational overhead. It is capable of detecting subtle forgery artifacts that may not be captured by traditional methods.

Future work may focus on detecting more advanced forgery techniques such as deepfakes, integrating real-time video analysis, and using advanced fusion techniques such as attention-based models. Additionally, incorporating larger and more diverse datasets can further improve model generalization.Overall, the proposed system offers a reliable and efficient solution for image forgery detection, contributing to the field of digital image forensics and enhancing trust in digital media.

REFERENCES

1. Bayar & Stamm, "A Deep Learning Approach to Universal Image Manipulation Detection," IEEE
2. Zhou et al., "Learning Rich Features for Image Manipulation Detection," CVPR
3. Salloum et al., "Image Splicing Detection Using Deep Learning," IEEE
4. Verdoliva, "Media Forensics and Deep Learning," IEEE
5. Chollet, "Xception: Deep Learning with Depthwise Separable Convolutions"
6. Howard et al., "MobileNet: Efficient CNN for Mobile Vision Applications"
7. Zhang et al., "ShuffleNet: Efficient CNN Architecture," IEEE
8. Iandola et al., "SqueezeNet: AlexNet-level Accuracy with Fewer Parameters"
9. Afchar et al., "MesoNet: Deepfake Detection Using CNN"
10. Nguyen et al., "Capsule Networks for Forgery Detection"
11. Dang et al., "Deep Learning for Image Forgery Detection: Survey," 2024
12. Cozzolino et al., "Noiseprint: CNN-based Image Forgery Detection"
13. Huh et al., "Fighting Fake News with Image Forensics," ICCV
14. Rossler et al., "FaceForensics++ Dataset," ICCV
15. Tolosana et al., "Deepfake Detection Review," 2023