e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

IMAGE FORGERY DETECTION BASED ON FUSION OF LIGHTWEIGHT DEEP LEARNING MODELS

Y. Akhil Yadav[*1], Ramagiri Prathik[*2], K. Arun Kumar[*3], Dr. A. Lakshman[*4]

[*1,2,3]Student Of B. Tech Computer Science And Engineering, Department Of Information Technology, Malla Reddy College Of Engineering & Technology, Hyderabad, Telangana, India.

[*4]Assistant Professor, Department Of Computer Science And Engineering, Malla Reddy College Of Engineering & Technology, Hyderabad, Telangana, India.

ABSTRACT

Image forgery detection is one of the key challenges in various real time applications, social media and online information platforms. The conventional methods of detection based on the traces of image manipulations are limited to the scope of predefined assumptions like hand-crafted features, size and contrast. In this paper, we propose a fusion based decision approach for image forgery detection. The fusion of decision is based on the lightweight deep learning models namely SqueezeNet, MobileNetV2 and ShuffleNet. The fusion decision system is implemented in two phases. First, the pretrained weights of the lightweight deep learning models are used to evaluate the forgery of the images. Secondly, the fine-tuned weights are used to compare the results of the forgery of the images with the pre-trained models. The experimental results suggest that the fusion based decision approach achieves better accuracy as compared to the state-of-the-art approaches.

Keywords: SqueezeNet, MobileNetV2 And ShuffleNet.

I. INTRODUCTION

Images and videos are widely used as evidence in various contexts, including trials, insurance fraud, and social media. However, the easy accessibility of digital editing tools has given rise to questions about the authenticity of images. Image forensics authorities aim to develop technological innovations to detect image forgeries, which can be classified into copy-move and splicing categories. Various image forgery detection techniques have been proposed over the years, including those that exploit the artifacts left by multiple JPEG compression and camera based methods. Detecting forged images is essential as they can mislead people and threaten individuals' lives. Previous studies have attempted to identify copy-paste or splicing of forged areas in images by extracting various properties such as lighting, shadows, sensor noise, and camera reflections. Several researchers have assessed the credibility of images by determining whether they are authentic or forged. There are currently numerous techniques available for identifying forged regions in images that rely on detecting artifacts left by multiple JPEG compressions and other image manipulation techniques. Camera-based methods have also been explored, where detection is based on demosaicing regularity or sensor pattern noise. The irregularities in the sensor pattern are extracted and compared for anomalies. Using lightweight models is motivated by the need to prevent overfitting of convolutional neural network (CNN) architectures, as well as their ability to be easily deployed on resource constrained hardware and learn enriched representations. ShuffleNet is particularly efficient as it generates more feature map channels for a given computation complexity budget, which encodes more information and is crucial for the effectiveness of small networks. MobileNet utilizes deep-separable convolutions and has achieved state-of the-art results, demonstrating its effectiveness across a wide range of tasks. SqueezeNet, on the other hand, is optimized for fast processing speed in CNN systems with significantly fewer parameters than AlexNet, while maintaining standard accuracy. The utilization of lightweight models not only enables effective deployment on resource-restricted hardware but also helps in learning enriched representations. This paper proposes a decision fusion method that uses lightweight deep learning models for detecting image forgery. The method consists of two phases: feature extraction from images using SqueezeNet, MobileNetV2, and ShuffleNet without regularization in the first phase, and detection of image forgery using fine-tuned models with fusion and regularization in the second phase. The main contributions of this paper include the proposed decision fusion based system using lightweight models for image forgery detection, the two-phase implementation of the fusion system using pretrained and fine-tuned weights, and the reduction of false matches, false positive rate, and ultimately increasing the accuracy of the approach due to the utilization of lightweight models.

II. LITERATURE REVIEW

1. **"Kwon, M. et al. Detecting and localizing image splicing had become essential to fought against malicious forgery.."**

A major challenged to localize spliced areas was to discriminate between authentic and tampered region with intrinsic properties such as compression artifacts. They proposed cat-net, an end-to-end fully convolutional neural network including rgb and dct streams, to learned forensic features of compression artifacts on rgb and dct domains jointly. The proposed method outperforms state-of-the-art neural networks for localizing spliced regions in jpeg or non-jpeg images. Wu, Y. et al. To fight against real-life image forgery, which commonly involves different types and combined manipulations, they propose a unified deep neural architecture called mantra-Net. Unlike many existing solutions, mantra-Net is an end-to-end network that performs both detection and localization without extra pre-processing and post processing. Manifold is a fully convolutional network and handles images of arbitrary sizes and many known forgery types such splicing, copy move, removal, enhancement, and even unknown types. Zheng, L. et al. Editing a realworld photo through computer software or mobile applications was one of the easiest things one could did today before sharing the doctored image on one's social networking sites. Although most people did it for fun, it was suspectable if one concealed an objected or changed someone's faced within the image. Rony, J. et al. Used state-of-the-art deep learned models for cancer diagnosis presents several challenges related to the nature and availability of labeled histology images. In this surveyed, deep weakly-supervised learned models were investigated to identified and locate diseases in histology images, without the needed for pixel-level annotations. Given training data with global image-level labels, these models allowed to simultaneously classify histology images and yield pixel-wise localization scores, thereby identifying the corresponding regions of interest.

2. **"Meena, et al. This age of digitization, digital images were used as a prominent carrier of visual information."**

Images were becoming increasingly ubiquitous in everyday life.Unprecedented involvement of digital images could be seen in various paramount fields liked medical science, journalism, sports, criminal investigation, image forensic, etc., where authenticity of image was of vital importance. Various tools were available free of costed or with a negligible amount of costed for manipulating images. Some tools could manipulate images to such an extent that it became impossible to discriminate by human visual system that image was forged or genuine. Hence, image forgery detection was a challenging area of researched. Abdel-Basset M, et al. Understanding was considered a key purpose of image forensic science in ordered to found out if a digital image was authenticated or not. It could be a sensitive task in case images were used as necessary proof as an impact judgment. It's known that there were several different manipulating attacks but, this copy moved was considered as one of the most common and immediate one, in which a region was copied twice in ordered to give different information about the same scene, which could be considered as an issue of information integrity. The detection of this kind of manipulating had been recently handled used methods based on sift.

3. **"Kekre HB, et al. Image hashing techniques used to generate hash valued for each image in the database"**

These hash values generated for images could been used for content based image retrieval, image database indexing, and image authentication, avoiding, and mitigating the tampering of digital images. In the information era, the increasing availability of multimedia data in digital form had led to a tremendous growth of tools to manipulate digital multimedia. To ensured trustworthiness, multimedia authentication techniques had emerged to verify content integrity and prevent forgery. A novel approached was proposed for forgery detection used image hashing, experimental results showed that even slightest of image tempering could been detection with the proposed technique. Zhou P, et al. (2018) [18] Image manipulation detection was different from traditional semantic objected detection because it pays more attention to tampering artifacts than to image content, which suggests that richer features needed have been learned. They proposed a two stream faster r-cnn network and train it end-to-end to detect the tampered regions given a manipulated image. One of the two streams was a rgb stream whose purpose was to extract features from the rgb image input to found tampering artifacts liked strong contrast difference, unnatural tampered boundaries, and so on. The other was a noise stream that leverages the noise features extracted from a steganalysis rich model filter layer to discover the noise inconsistency between authentic and tampered regions. They then fuse features from the two streams through a bi linear pooling layer to further incorporate spatial co-occurrence of these two modalities. Experiments on four standard image manipulation datasets demonstrate that our two-stream framework outperforms each individual stream, and achieves state-of-the-art performance compared to alternative methods with robustness to resizing and compression.

4. **"Kuznetsov A. et al. Proposed an algorithm for detecting one of the most used types of digital image forgeries-splicing."**

The algorithm was based on the use of the vgg-16 convolutional neural network. The proposed network architecture took image patches as input and obtains classification results for a patch: original or forgery. On the training stage they select patches from original image regions and on the borders of embedded splicing. Bunk J, et al. (2017) [20] Resampling was an important signature of manipulated images. They proposed two methods to detect and localize image manipulations based on a combination of resampling features and deep learned. In the first method, the radon transform of resampling features were computed on overlapping image patches. Deep learned classifiers and a gaussian conditional random field model were then used to create a heatmap. Tampered regions were located used a random walker segmentation method. In the second method, resampling features computed on overlapping image patches were passed through a long short-term memory (lstm) based network for classification and localization. They compare the performance of detection/localization of both these methods.

III. METHODOLOGY

The architecture of the proposed decision fusion is based on the lightweight deep learningmodels. The lightweight deep learning models chosen are SqueezeNet, MobileNetV2, and ShuffleNet. The proposed system is implemented in two phases i.e., with pre-trained and fine-tuned deep learning models. In the pre-trained model's implementation, regularization is not applied, and the pre-trained weights are used and for the fine-tuned implementation, regularization is applied to detect image forgery. Each phase consists of three stages namely, data pre-processing, classification, and fusion. In the data pre-processing stage, the image in the query is pre-processed based on the dimensions required by the deep learning models. SVM is used for the classification of the image as forged or non-forged. The dataset used for the experiment is benchmark publicly available MICC-F220 of 110 nonforged images and 110 forged images with 3 channels i.e. color images of size 722 × 480 to 800 × 600 pixels. From the dataset 154 images are chosen randomly for training purposes and remaining for testing purpose.

Data preprocessing:

In this stage, the image in a query that needs to be identified whether it is forged or not is subjected to preprocessing. The height and width of the image required for SqueezeNet is 227×227. The height and width of the image required for MobileNetV2 is 224×224. The height and width of the image required for ShuffleNet is 224×224. The input image is preprocessed first based on the dimensions required for each of the models. Each model then takes the input image to produce feature vector in further stages.

Lightweight deep learning models:

The different lightweight deep learning models that are considered for fusion are SqueezeNet, MobileNetV2, and ShuffleNet. These models are used for the image classification problems numerously. In this section, these models are discussed briefly. The lightweight models1 considered are summarized as shown in the Table 1. It represents the depth, parameters and the image input size required for the lightweight models namely, SqueezeNet, MobileNetV2, and ShuffleNet. SqueezeNet is a CNN trained on the ImageNet dataset with 18 layers deep and can classify the images up to 1000 categories. The network has learned rich representations of the images with 1.24 million parameters. It requires only a few floating point operations for the image classification.

MobileNetV2 is a CNN trained on the ImageNet dataset with 53 layers deep and can classify the images up to 1000 categories. The performance of the classification is improved based on the learning of the rich representations of the images. ShuffleNet It is a CNN that is also trained on the ImageNet dataset with 50 layers

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

deep and can classify the images up to 1000 categories.

TECHNOLOGIES USED:

DEEP LEARNING:

Deep learning is a branch of machine learning which is based on artificial neural networks. It is capable of learning complex patterns and relationships within data. In deep learning, we don't need to explicitly program everything. It has become increasingly popular in recent years due to the advances in processing power and the availability of large datasets. Because it is based on artificial neural networks (ANNs) also known as deep neural networks (DNNs). These neural networks are inspired by the structure and function of the human brain's biological neurons, and they are designed to learn from large amounts of data. Deep Learning is a subfield of Machine Learning that involves the use of neural networks to model and solve complex problems. Neural networks are modeled after the structure and function of the human brain and consist of layers of interconnected nodes that process and transform data.The key characteristic of Deep Learning is the use of deep neural networks, which have multiple layers of interconnected nodes. These networks can learn complex representations of data by discovering hierarchical patterns and features in the data. Deep Learning algorithms can automatically learn and improve from data without the need for manual feature engineering.Deep Learning has achieved significant success in various fields, including image recognition, natural language processing, speech recognition, and recommendation systems. Training deep neural networks typically requires a large amount of data and computational resources. However, the availability of cloud computing and the development of specialized hardware, such as Graphics Processing Units (GPUs), has made it easier to train deep neural networks.

In a fully connected Deep neural network, there is an input layer and one or more hidden layers connected one after the other. Each neuron receives input from the previous layer neurons or the input layer. The output of one neuron becomes the input to other neurons in the next layer of the network, and this process continues until the final layer produces the output of the network. The layers of the neural network transform the input data through a series of nonlinear transformations, allowing the network to learn complex representations of the input data.In summary, Deep Learning is a subfield of Machine Learning that involves the use of deep neural networks to model and solve complex problems. Deep Learning has achieved significant success in various fields, and its use is expected to continue to grow as more data becomes available, and more powerful computing resources become available. The project "image forgery detection based on fusion of lightweight deep learning models" integrates various technologies across different stages of its implementation. Here's a breakdown of the technologies typically employed.

Programming Languages:

Python: Widely used for its extensive libraries and frameworks suitable for machine learning and data analysis tasks.

Deep Learning Libraries:

TensorFlow: An open-source machine learning framework developed by Google, commonly used for building and training neural network models, including artificial neural networks.

Keras: A high-level neural networks API, often used in conjunction with TensorFlow for building and training neural network models with ease.

PyTorch: Another open-source machine learning library, particularly favored for its dynamic computation graph, often preferred by researchers and practitioners for deep learning tasks.

Scikit-learn: A versatile machine learning library in Python, offering various algorithms for classification, regression, clustering, and dimensionality reduction, useful for tasks such as data preprocessing and model evaluation.

Data Visualization Tools:

Matplotlib: A popular plotting library in Python, widely used for creating static, interactive, and animated visualizations.

Seaborn: Built on top of Matplotlib, Seaborn offers enhanced aesthetics and additional plot types for statistical

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

data visualization.

Plotly: A versatile visualization library offering interactive plots and dashboards, often utilized for exploratory data analysis and presentation of results.

Data Processing and Analysis Tools:

Pandas: A powerful data manipulation library in Python, commonly used for data wrangling, cleaning, and analysis tasks.

NumPy: A fundamental package for scientific computing in Python, providing support for arrays, matrices, and mathematical functions essential for numerical computations.

Development Environments:

Jupyter Notebook: A web-based interactive computing environment ideal for data exploration, prototyping, and collaborative development.

MODULES DESCRIPTION:

Project Modules:

1. Collecting dataset
2. Data Pre-Processing Stage
3. Fusion model and regularization
4. Data Splitting

1. Collecting dataset:

The dataset used for the experiment is benchmark publicly available MICC-F220 of 110 Non forged images and 110 forged images with 3 channels i.e. color images of size 722 × 480 to 800 × 600 pixels.

2. Data Pre-Processing Stage:

In this stage, the image in a query that needs to be identified whether it is forged or not is subjected to preprocessing. The height and width of the image required for SqueezeNet is 227×227. The height and width of the image required for MobileNetV2 is 224×224. The height and width of the image required for ShuffleNet is 224×224. The input image is preprocessed first based on the dimensions required for each of the models. Each model then takes the input image to produce feature vector in further stages.

$$Y_{fusion} = [Y_1 + Y_2 + ... + Y_T]$$

$$f_{fusion} = \frac{m-w}{s} + 1 * \frac{n-w}{s} + 1$$

3. Fusion model and regularization:

The proposed system uses lightweight deep learning models with pretrained weights for image forgery detection. The system is implemented as a fusion of the decision of these models. The input image is first passed to the lightweight models to obtain their respective feature maps. The feature maps from SqueezeNet, MobileNetV2, and ShuffleNet are denoted fs,fm,fsh. The output feature map from the pretrained lightweight deep learning model is used for the fusion model, which is a combination of the feature maps obtained from the lightweight models. This feature map, denoted as fp = fs + fm + fsh.

The fusion model uses feature map fp as a local descriptor for an input patch to extract the features of the image. The image for the fusion model is represented as a function Yfusion = f(x) where x is the patch in the input image. For a test image size m×n, a sliding window of size p×p is used to compute the local descriptor Yfusion is computed as shown in the equation where Y1, Y2, , YT represents the descriptors of the patches of the image obtained from the deep learning models. It is obtained as a concatenation of all the input patches xi and the new image representation is given by equation where s is the size of the stride used for transforming the input patch, this new image representation fusion is used as the feature map for the classification by the SVM as forged or nonforged.

For fine tuning of the parameters of the fusion model, the initialization of the weight kernels is used as shown in

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

Equation. In this equation Wf represents the weights of the fusion model, Ws represents the weights of the SqueezeNet model, Wm represents the weights of the MobileNetV2 model and Wsh represents the weights of the ShuffleNet model. The weight of the fusion model Wf is initialized as shown in Equation. The initialization of the weights acts as a regularization term and facilitates the fusion model to learn the robust features of detecting the forgery rather than the complex image representations.

$$W_f = [W_{sj} W_{mj} W_{shj}] j = 1, 2, 3$$

$$W_f = [W_s^{4k-2} W_m^{4k-2} W_{sh}^{4k}] \text{ where } k = [[j+1] mod 11] + 1$$

4. Data Splitting :

The splitting of data to validate whether the class values generated from Deep Learning model and actual class values are same or not based on the result evaluation to know the performance rate of our Deep Learning model. In this work we using two different algorithms. To perform Deep Learning model we have Shuffle the data in the ratio of 80:20, 80% is for training the model and remaining 20% is for testing the model. To perform Deep Learning algorithm we have splitted the dataset into10-cross-folds from which first 9 folds are used for training the model and last fold is for the testing the model and so on by using k-cross-fold-validation technique.

K-Cross folds technique is a technique in which we train our model using the subset of the data- set and then evaluate using the complementary subset of the data-set. It is a popular method because it is simple to understand and because it generally results in a less biased or less optimistic estimate of the model. The data in the datasets are in hundreds which is not sufficient for the model to train so to perform both the algorithm we are using K cross fold technique. We have selected k-cross- fold technique because Fusion algorithm is a lazy learner which means the algorithm takes much time to learn the training data so it is the best choice to select this technique because in this method we will divide the dataset into k . The technique has a single parameter called k that refers to the number of groups that a given data sample is to be split into. As such, the procedure is often called k-fold cross-validation. When a specific value for k is chosen, it may be used in place of k in the reference to the model, such as k=10 becoming 10-fold cross-validation.

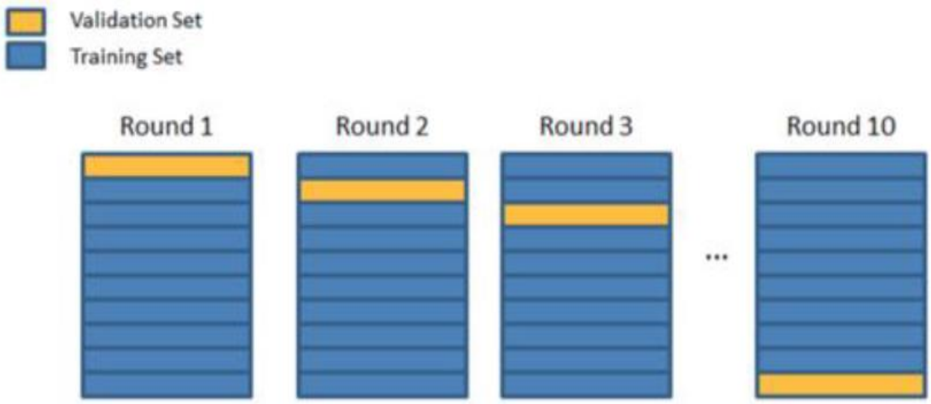

Fig 1:

It's observed that the datasets consists of the same class together so the algorithm will work bias and its performance rate will decrease so as to overcome this problem we have randomly selected the data from the dataset and splitted it into the format of 80:20. 80% of the data from the dataset is for the training the model and 20% of the data from the dataset is for testing the model. It is a popular method because it is simple to understand and because it generally results in a less biased or less optimistic estimate of the model.

The proposed approach uses SVM as a classifier, which is known for its popularity and efficiency in binary classification. The performance of the approach is evaluated at the image level using various performance

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

metrics, such as precision, recall (TPR), false positive rate (FPR), F-score, and accuracy.

Process/Algorithm

1. SqueezeNet:

SqueezeNet is a deep neural network architecture designed for efficient use of computational resources, particularly in terms of model size and computational power required for inference. It was introduced to address the challenge of deploying large neural networks on resource- constrained devices, such as mobile phones or embedded system. It is a CNN trained on the ImageNet dataset with 18 layers deep and can classify the images up to 1000 categories. The network has learned rich representations of the images with 1.24 million parameters. It requires only a few floating point operations for the image classification.The main goal of SqueezeNet is to maintain a good balance between model accuracy and computational efficiency, making it suitable for deployment on devices with limited resources. It has been widely used in applications where real-time or low-latency processing is crucial, such as in mobile and embedded systems.

2. MobileNetV2:

MobileNetV2 is a neural network architecture specifically designed for mobile and edge devices, emphasizing efficiency and performance in terms of both model size and computational requirements. It is the successor to the original MobileNet, and it incorporates several improvements to enhance its accuracy and efficiency. It is a CNN trained on the ImageNet dataset with 53 layers deep and can classify the images up to 1000 categories. The performance of the classification is improved based on the learning of the rich representations of the images. ShuffleNet It is a CNN that is also trained on the ImageNet dataset with 50 layers deep and can classify the images up to 1000 categories. MobileNetV2 is well-suited for applications where computational resources are limited, such as on mobile devices, but high accuracy is still desired. It has been widely adopted for various computer vision tasks, including image classification, object detection, and segmentation on resource-constrained devices.

3. ShuffleNet:

ShuffleNet is a neural network architecture designed to achieve high performance with reduced computational complexity, making it suitable for deployment on resource-constrained devices, including mobile phones and edge devices. It was introduced to address the challenge of balancing the trade-off between model accuracy and computational efficiency. ShuffleNet aims to strike a balance between model efficiency and accuracy, and it has been widely adopted in applications where computational resources are limited. The architecture has proven effective for tasks such as image classification and object detection on devices with constraints in terms of memory, processing power, and energy consumption.

IV. RESULTS AND ANALYSIS

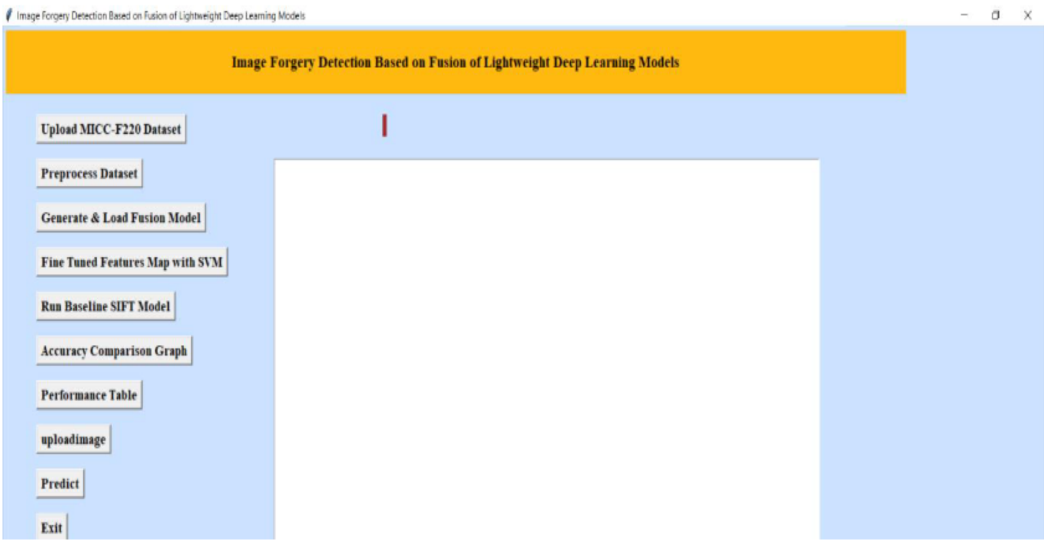

Fig 2: Homepage

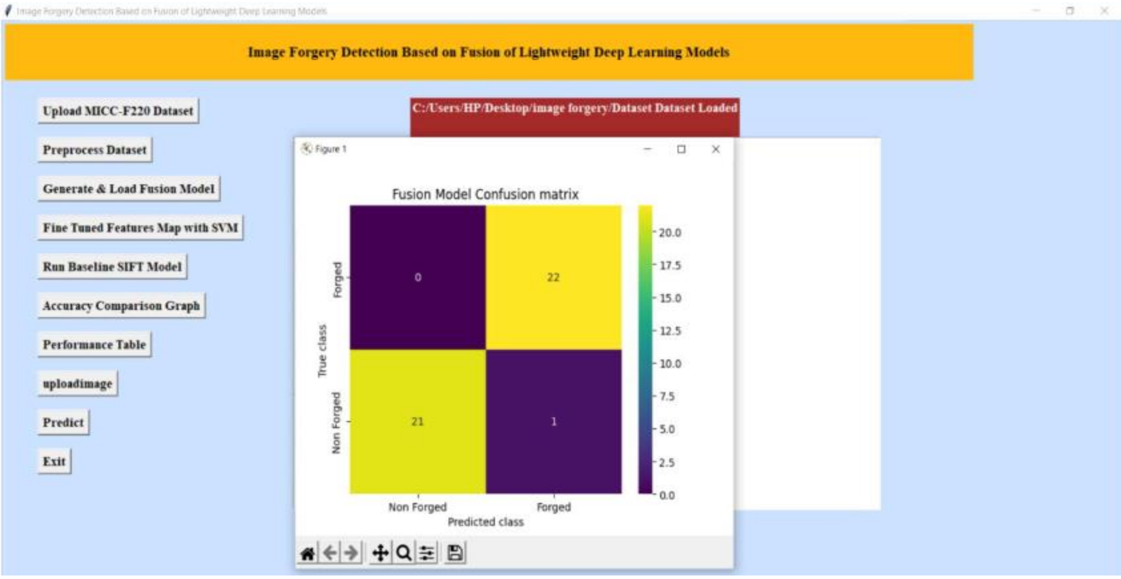

Fig 3: Fusion Model Confusion Matrix

Fig 4: Accuracy Comparison Model

Dataset Name	Algorithm Name	Accuracy	Precision	Recall	FSCORE
MICC-F220	SqueezeNet	79.54545454545455	81.15468409586056	79.54545454545455	79.27786499215071
MICC-F220	ShuffleNet	56.81818181818182	62.74131274131274	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

Fig 5: Performance Table

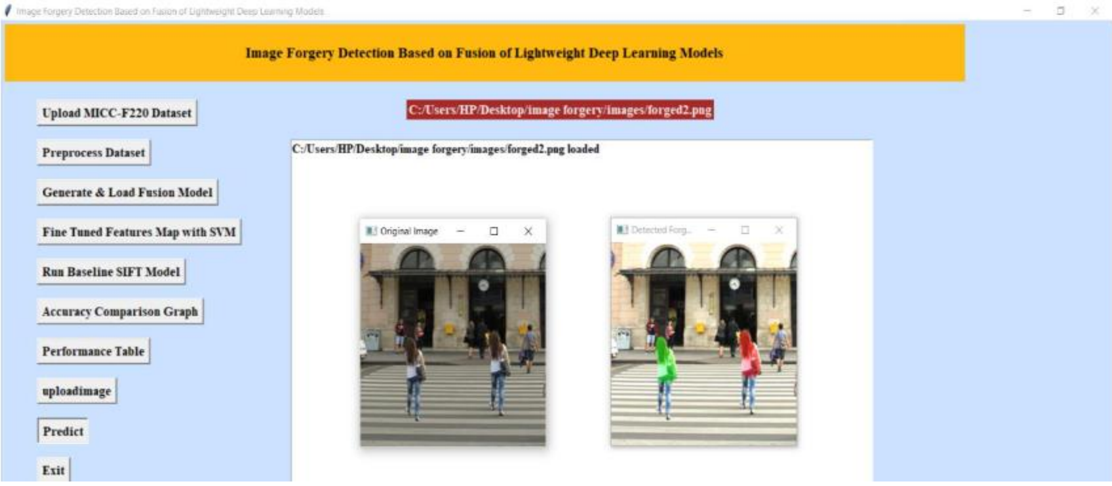

Fig 6: Actual Outcome

V. CONCLUSION

In conclusion, Image forgery detection based on the fusion of lightweight deep learning models offers a promising and efficient solution to address the challenges associated with identifying manipulated images. The fusion of multiple lightweight models provides a comprehensive approach, leveraging the strengths of different models to enhance accuracy, adaptability, and real-time detection capabilities. Image forgery detection helps to differentiate between the original and the manipulated or fake images. In this paper, a decision fusion of lightweight deep learning based models is implemented for image forgery detection. The idea was to use the lightweight deep learning models namely SqueezeNet, MobileNetV2, and ShuffleNet and then combine all these models to obtain the decision on the forgery of the image. Regularization of the weights of the pretrained models is implemented to arrive at a decision of the forgery. The experiments carried out indicate that the fusion based approach gives more accuracy than the state-of-the-art approaches. In the future, the fusion decision can be improved with other weight initialization strategies for image forgery detection.

In conclusion, Image Forgery Detection Based on Fusion of Lightweight Deep Learning Models represents a significant advancement in the field of image forensics, offering a powerful and versatile solution to combat the increasing challenges of image forgery and tampering. By combining the strengths of multiple lightweight deep learning models, the. system achieves a high level of accuracy in detecting various types of image manipulations, ensuring the integrity and authenticity of visual content. The fusion of lightweight deep learning models addresses the limitations of individual models, resulting in a more robust and reliable forgery detection system. The approach effectively analyzes image pixel values, structures, and patterns, making it adept at identifying even subtle alterations that could otherwise go undetected by traditional methods. This capability enhances the system's effectiveness in detecting both sophisticated and common image forgeries, fostering greater trust in digital media and promoting the use of authentic and unaltered visual content.

VI. REFERENCES

[1] Amerini, T. Uricchio, L. Ballan, and R. Caldelli, "Localization of JPEG Double Compression Through Multi-Domain Convolutional Neural Networks," 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2017, pp. 1865-1871, doi:10.1109/CVPRW.2017.233.

[2] B Xiao, Y Wei, X Bi, W Li, J Ma. “Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering”, Information Sciences, Volume 511, Pages 172-191, 2020, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2019.09.038.

[3] Zhang Y, Goh J, Win LL, Thing VL. Image region forgery detection: a deep learning approach. SG-CRC 2016; 2016: 1-11.

[4] Goh J, Thing VL. A hybrid evolutionary algorithm for feature and ensemble selection in image tampering detection. International Journal of Electronic Security and Digital Forensics 2015; 7 (1): 76-104

IRJMETS

e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

[5] Sutthiwan P, Shi YQ, Zhao H, Ng TT, Su W. Markovian rake transform for digital image tampering detection. In: Shi YQ, Emmanuel S, Kankanhalli MS, Chang S-F, Radhakrishnan R(editors). Transactions on Data Hiding and Multimedia Security VI. Lecture Notes in Computer Science, Vol. 6730. Berlin, Germany: Springer; 2011, pp. 1-17

[6] He Z, Lu W, Sun W, Huang J. Digital image splicing detection based on Markov features in DCT and DWT domain. Pattern Recognition 2012; 45 (12): 4292-4299.

[7] Chang IC, Yu JC, Chang CC. A forgery detection algorithm for exemplar-based inpainting images using multi-region relation. Image and Vision Computing 2013; 31 (1): 57-71.

[8] Rhee KH. Median filtering detection based on variations and residuals in image forensics. Turkish Journal of Electrical Engineering & Computer Science 2017; 25 (5): 3811-3826.

[9] Lamba AK, Jindal N, Sharma S. Digital image copy-move forgery detection based on discrete fractional wavelet transform. Turkish Journal of Electrical Engineering & Computer Science 2018; 26 (3): 1261-1277.

[10] Lin Z, He J, Tang X, Tang CK. Fast, automatic, and fine-grained tampered JPEG image detection via DCT coefficient analysis. Pattern Recognition 2009; 42 (11): 2492-2501.

[11] Kwon, M.J.; Yu, I.J.; Nam, S.H.; Lee, H.K. CAT-Net: Compression Artifact Tracing Network for Detection and Localization of Image Splicing. In Proceedings of the 2021 IEEE Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, 5–9 January 2021; pp. 375–384.

[12] Wu, Y.; Abd Almageed, W.; Natarajan, P. Mantra-Net: Manipulation Tracing Network for Detection and Localization of Image Forgeries With Anomalous Features. In Proceedings of the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach, CA, USA, 15–20 June 2019; pp. 9535–9544.

[13] Zheng, L.; Zhang, Y.; Thing, V.L. A survey on image tampering and its detection in real- world photos. J. Vis. Commun. Image Represent. 2019, 58, 380–399.

[14] Rony, J.; Belharbi, S.; Dolz, J.; Ayed, I.B.; mccaffrey, L.; Granger, E. Deep weakly supervised learning methods for classification and localization in histology images: A survey. Arxiv 2019, arxiv: abs/1909. 03354.

[15] Meena, K.B.; Tyagi, V. Image Forgery Detection: Survey and Future Directions. In Data, Engineering and Applications: Volume 2; Shukla, R.K., Agrawal, J., Sharma, S., Singh Tomer, G., Eds.; Springer: Singapore, 2019; pp. 163–194. JOURNAL OF CRITICAL REVIEWS ISSN- 2394-5125 VOL 10, ISSUE 03, 2023 31

[16] Abdel-Basset M, Manogaran G, Fakhry AE, El-Henawy I. 2-Levels of clustering strategy to detect and locate copy-move forgery in digital images. Multimedia Tools and Applications 2018; 79: 5419-5437. Doi: 10.1007/s11042- 018-6266-0

[17] Kekre HB, Mishra D, Halarnkar PN, Shende P, Gupta S. Digital image forgery detection using Image hashing. In: IEEE International Conference on Advances in Technology and Engineering (ICATE); Mumbai, India; 2013. Pp.1-6. Doi: 10.1109/icadte.2013.6524736

[18] Zhou P, Han X, Morariu VI, Davis LS. Learning rich features for image manipulation detection. In: IEEE Conference on Computer Vision and Pattern Recognition (CVPR); Salt Lake City, UT, USA; 2018. Pp. 1053-1061

[19] Kuznetsov A. Digital image forgery detection using deep learning approach. Journal of Physics: Conference Series 2019; 1368 (3): 032028. Doi: 10.1088/1742-6596/1368/3/032028.