

## IMAGE FORGERY DETECTION BASED ON FUSION OF LIGHTWEIGHT DEEP LEARNING MODELS

<sup>1</sup>Mailaram shruthi, <sup>2</sup>Chintala Poojitha, <sup>3</sup>Patlolla Sruthi

<sup>1</sup> Student, Department of CSE(data science), Gokaraju rangaraju Institute of engineering and technology.

<sup>2</sup> Student, Department of Computer Science and Engineering, Rishi MS institute of engineering and technology for women.

<sup>3</sup> Assistant Professor, Department Of Data Science, Gokaraju rangaraju Institute of engineering and technology.

[shruthimailaram1234@gmail.com](mailto:shruthimailaram1234@gmail.com). [chintalapoojitha30@gmail.com](mailto:chintalapoojitha30@gmail.com).

[Sruthi1717@grietcollege.com](mailto:Sruthi1717@grietcollege.com).

### ABSTARCT

The broad availability of cameras has greatly contributed to the explosion in popularity of photography in recent years. Images play a crucial part in our everyday lives since they may convey a great deal of information; yet, it is occasionally necessary to modify images to get new views. While there are many options for enhancing pictures, they are also often exploited to create fake images that propagate false information. This greatly increases the possibility and severity of picture forgeries, which is quite alarming. Over time, many tried-and-true methods for identifying fake photographs have developed. Recent years have seen a rise in interest in convolutional neural networks (CNNs), which has aided the developing area of visual forgery detection. While convolutional neural networks have been used to identify some types of picture forgeries (such as splicing and copy-move), these methods have had little success. The development of a method that can quickly and reliably identify the existence of otherwise undetected forgeries in a picture is, thus, of critical importance. Using the double image compression architecture, we provide a deep learning-based technique for accurately detecting forged images. To train our model, we compare each image's original and compressed forms. The suggested model is straightforward and effective, and it outperforms the current gold standard in trials. The overall validation accuracy of the experiments is 92.23 percent, which is quite high.

### I.INTRODUCTION

The widespread availability and low cost of electronic gadgets is a result of both technical progress and globalisation. This is largely responsible for the meteoric rise in digital camera sales. We take innumerable images, and that's because there are so many camera sensors all around the world. Every day, many images are posted and shared on

social media, and digital copies of photographs are required for many types of mandated online filing. If a message is accompanied with a picture, it may still be understood by those who have problems reading. Therefore, pictures play an important role online for reasons including documenting history and spreading knowledge. Use one of the various picture

editing programmes that are easily available [1,2]. The developers of these programmes have one purpose in mind: to help its users do more in the realm of photo manipulation. But some individuals misuse this privilege by utilising photographs with alterations to spread false information [3,4]. The harm done by these phoney pictures might be substantial, and in many cases, it would be hard to undo. Both instances involve photos with changed content spread false information [5,6]. Pictures were formerly reliable sources of information; nowadays, however, they are often manipulated to disseminate lies. Since of this, less individuals are willing to place their faith on photographic evidence since it might be difficult for the untrained eye to see a forgery. In order to stop the spread of misinformation and restore people's trust in visual media, it is crucial to develop methods for identifying counterfeit pictures. Several different image processing methods may be utilised to uncover traces of the forgery procedure. Several strategies [7-9] have been proposed by researchers to identify manipulated images. Artefacts such as those induced by adjustments to lighting, contrast, compression, sensor noise, and shadows have historically been used to detect picture frauds. Object identification, semantic segmentation, and picture classification are just a few of the many computer vision applications where the use of convolutional neural networks (CNNs) has increased in recent years. CNN's success in computer vision may be attributed to two main factors. CNN first makes advantage of the high degree of neighbourhood connection. So, rather of connecting

individual pixels, CNN wants to link together groups of them. Convolution with shared weights is used in the second step to generate a feature map for each output. In addition, CNN deviates from the norm by generalising the qualities it has acquired from training photos to detect previously unknown instances of counterfeit. CNN has several potential uses, and one of them is determining whether an image has been altered. Common indicators of forgeries may be learned by a CNN-based algorithm [10-13]. To address this problem, we introduce a tiny, lightweight convolutional neural network (CNN) whose main objective is to learn the artefacts that appear in a tampered image as a result of discrepancies between the original image and the tampered area.

## II. LITERATURE SURVEY

Error level analysis (ELA) was introduced by the authors of [14] to detect fakes. In [15], the authors emphasise the need of good lighting while making images. It examines images for differences in lighting direction between the fake and real parts to spot frauds. Historical methods for identifying phoney photos are compared and described in [16]. Forgery detection relies on identifying the edge pixels, and Habibi et al. [17] have shown how to do this with the use of the contourlet transform. Dua et al. suggested a technique using JPEG compression in their paper [18]. When an image is cut up into non-overlapping squares of 8x8, the discrete DCT coefficients for each block may be evaluated separately. When a JPEG compressed picture is modified, new statistical patterns emerge in

the AC components of the block DCT coefficients. The SVM is then used to accomplish the authentication of images using the resulting feature vector. Forgery detection using SIFT, which offers descriptive features, was reported by Ehret et al. [19]. In [20], the authors suggest using high-level property image analysis to detect forged fingerprints. The discrete cosine transform (DCT), Walsh-Hadamard transform (WHT), Haar wavelet transform (DWT), and discrete Fourier transform (DFT) were all examined by Balsa et al. [21] for their ability to compress and transmit high-quality analogue pictures while maintaining their underlying detail. These might be put to use in analysing suspect images taken from different angles. After a spliced image has been recognised, the authors of [22] offer a hybrid approach to recovering the original images. They demonstrate a new technique for image retrieval by combining Zernike moments with SIFT characteristics.

Bunk et al. [23] developed a technique to identify manipulated photos by combining resampling characteristics with deep learning. In order to identify instances of picture manipulation, Bondi et al. [24] propose an approach that clusters camera-based CNN features. To facilitate the simultaneous collection of evidence of compression artefacts in the DCT and RGB domains, Myung-Joon developed CAT-Net in [2]. HR-Net (high resolution) is their principal network. They used the approach described in [25] to train a CNN to utilise the DCT coefficient (because just providing it with the coefficients wouldn't enough). To

identify and pinpoint picture forgeries including copy-move techniques, Ashraful et al. [26] developed DOA-GAN, a GAN with dual attention. First-order attention is used in the generator to collect data on copy-move locations, whereas second-order attention is responsible for handling patch co-occurrence, which takes use of additional discriminative qualities. Both attention maps are extracted from the affinity matrix and combined with location-aware and co-occurrence features to form the network's final detection and localization nodes.

One way to identify pirated films was presented by Yue et al. [27]. A fusion module sits at the node where the path splits in two. Visual signals are used in both the manipulation and copymove procedures. Yue et al. [28] used a convolutional neural network (CNN) to extract block-like characteristics from a picture, calculate self-correlations between multiple blocks, and more for the purposes of identifying matching points using a point-wise feature extractor and reconstructing a forgery mask. ManTra-Net was developed by Yue et al. in [3] and is a fully convolutional network. It can handle images of varying resolutions and several forms of forgeries, including as Liu et al. [29] introduced PSCC-Net, which performs two types of analysis on the image: top-down methods first obtain both global and local features.

Yang et al. [30] presented a method based on two concatenated CNNs, the coarse CNN and the refined CNN, for extracting differences between the picture and the splicing areas. Their work in [1] was

improved upon by the creation of a patch-based coarse-to-fine network (C2RNet). The VVG16 and VVG19 networks are used to construct the rough and smooth ones. To identify picture manipulations via splicing, Xiuli et al. [31] developed a ringed residual U-Net. To uncover the fake, Younis et al. [32] turned to the reliability fusion map. Younis et al. [33] employ convolutional neural networks to determine whether a picture is real or fake. In [34], Vladimir et al. do a comprehensive survey of GA and GR results concurrently. The approach proposed by Mayer et al. [35] gives values to picture clusters based on how much forensic evidence they share or diverge.

### III.EXISTING SYSTEM

We used the popular CASIA 2.0 image forgeries database [22,49] to assess the performance of the proposed method. Among the 12,614 pictures here (in BMP, JPG, and TIF formats), 7491 are authentic and 5123 are fakes. CASIA 2.0 has a wide variety of picture kinds, including landscapes, textures, and interiors. There is a wide range of image resolutions in the database, from 800x600 all the way down to 384x256. Table 1 contains information on CASIA 2.0. A computer with an Intel(R) Core(TM) i5-2400 CPU running at 3.1 GHz and 16 GB of RAM was used for the testing. When genuine images are mistakenly labelled as fakes, this is known as a "false positive" (FP). To evaluate how well the suggested technique works, its accuracy, precision, recall, and Fmeasure [1] are calculated and compared to alternative

methods. The following equations may be used to determine these:

Here is a new definition of precision:

$$\begin{aligned} \text{Accuracy} &= \frac{TP + TN}{T_{\text{Total\_Images}}} \times 100 \\ \text{Recall} &= \frac{TP}{TP + FN} \\ \text{Precision} &= \frac{TP}{TP + FP} \\ F_{\text{measure}} &= \frac{2 \times \text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} \times 100 \end{aligned}$$

### IV.PROPOSED SYSTEM

The proposed system for Image Forgery Detection utilizes the fusion of lightweight deep learning models to enhance the accuracy and efficiency of detecting image manipulation. The system is designed to address the growing concern of digital image forgeries in an era where image authenticity plays a crucial role in various sectors, including media, law enforcement, and social media. Traditional forgery detection techniques often rely on computationally intensive methods that are not suitable for real-time applications. To overcome this limitation, the proposed system leverages lightweight deep learning models that are both fast and effective, making them ideal for large-scale and real-time detection tasks. These models are trained to identify anomalies or inconsistencies in images, such as pixel-level alterations, misalignments, and inconsistencies in lighting or shadows that may result from manipulation. The system adopts a multi-model fusion approach, combining the strengths of different



lightweight architectures, such as MobileNetV2, SqueezeNet, and EfficientNet. By integrating the outputs of these models, the system benefits from improved detection accuracy while maintaining a low computational footprint. The fusion process involves combining the predictions from each individual model using techniques like ensemble learning or feature fusion, thereby ensuring that the strengths of each model complement one another. The system is further optimized for edge devices and mobile platforms, ensuring that image forgery detection can be performed efficiently on resource-constrained devices without compromising accuracy. By employing this fusion strategy, the system achieves both high performance and scalability, making it applicable to a wide range of real-time applications, from verifying images on social media to detecting manipulated evidence in criminal investigations. Additionally, the system can be integrated into existing frameworks or applications, providing an accessible and reliable tool for authenticating images in various domains.

The system architecture for Image Forgery Detection Based on Fusion of Lightweight Deep Learning Models is designed to efficiently process and detect manipulated images through a layered approach involving data acquisition, pre-processing, model inference, and output generation. At the core of the architecture lies a modular structure that integrates multiple lightweight deep learning models, ensuring scalability, flexibility, and real-time performance. The architecture begins with an image input layer, where images, whether from a local storage device or real-time streams (such as social media uploads or surveillance cameras), are received. These images are then passed through a pre-processing module, where they undergo several steps such as resizing, normalization, and data augmentation to ensure the input is standardized and ready for model processing. Next, the pre-processed images are fed into a fusion module consisting of multiple lightweight deep learning models, such as MobileNetV2, SqueezeNet, and EfficientNet.

## V.SYSTEM ARCHITECTURE

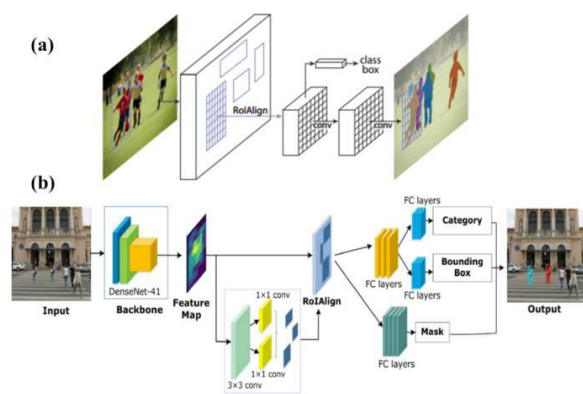
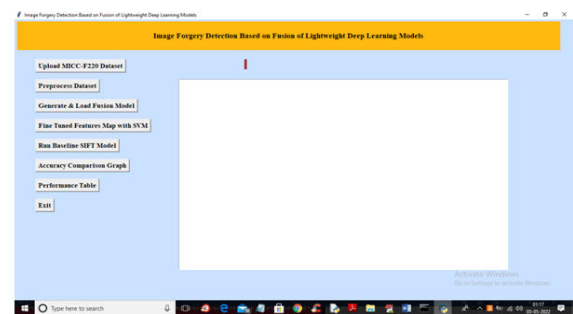


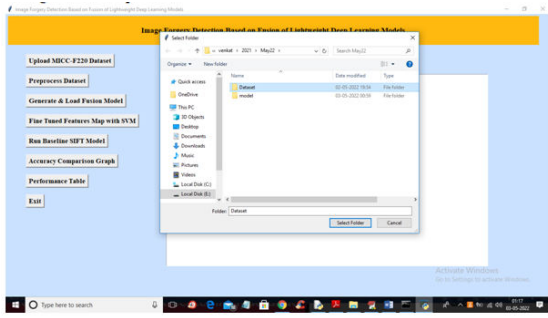
Figure 5.1 System Architecture

## VI.OUTPUT SCREENSHOTS

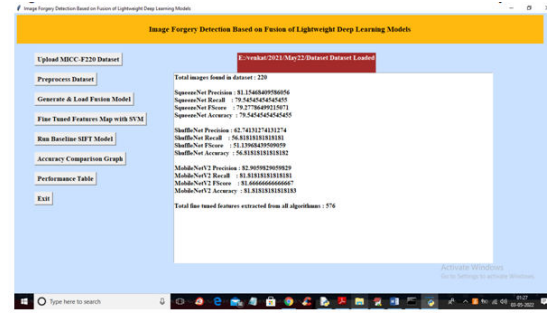
To run project double click on 'run.bat' file to get below output



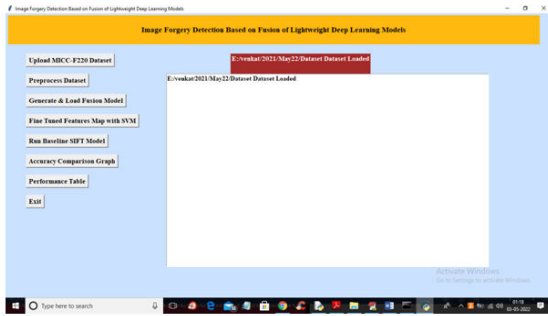
In above screen click on 'Upload MICC-F220 Dataset' button to upload dataset and get below output



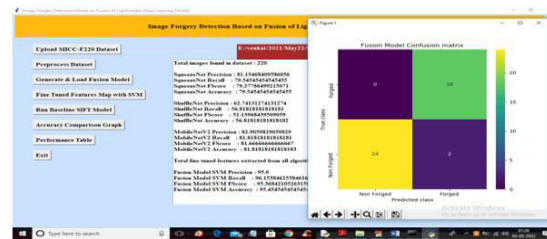
In above screen selecting and uploading 'Dataset' folder and then click on 'Select Folder' button to load dataset and get below output



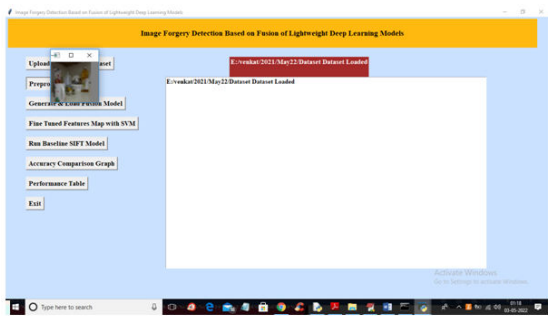
In above screen we can see accuracy of all 3 algorithms and then in last line we can see from all 3 algorithms application extracted 576 features and now click on 'Fine Tuned Features Map with SVM' to train SVM with extracted features and get its accuracy as fusion model



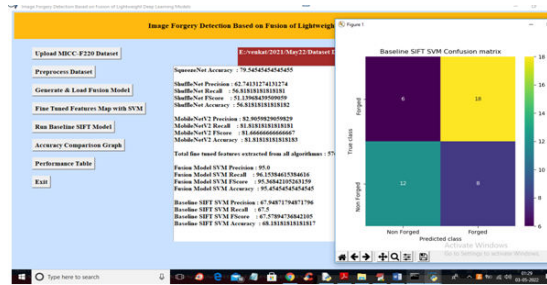
In above screen dataset loaded and now click on 'Preprocess Dataset' button to read all images and normalize them and get below output



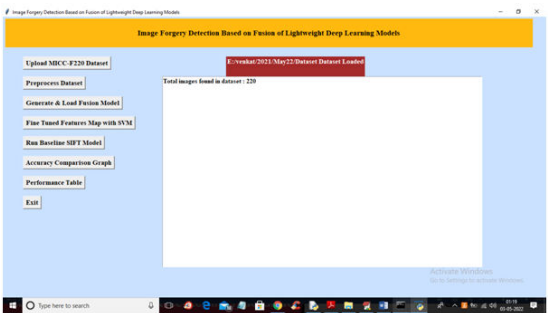
In above screen with Fine tune SVM fusion model we got 95% accuracy and in confusion matrix graph x-axis represents PREDICTED LABELS and y-axis represent TRUE labels and we can see both X and Y boxes contains more number of correctly prediction classes. In all algorithms we can see fine tune features 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



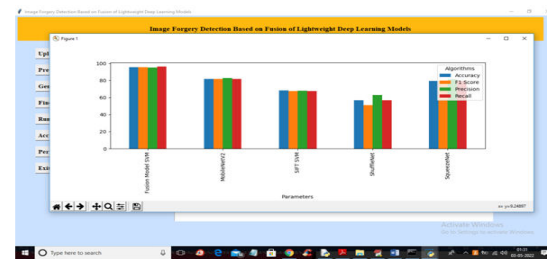
In above screen all images are processed and to check images loaded properly I am displaying one sample image and now close above image to get below output



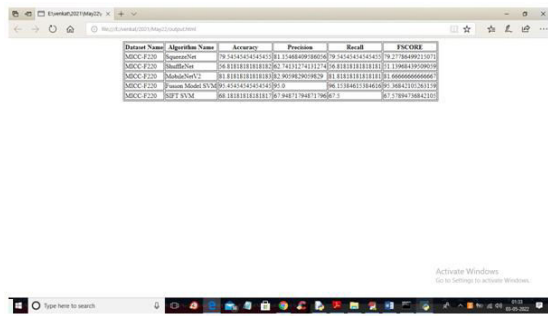
In above screen with existing SIFT SVM features we got 68% accuracy and in confusion matrix graph we can see existing SIFT predicted 6 and 8 instances incorrectly. So we can say existing SIFT features are not good in prediction and now close above graph and then click on 'Accuracy Comparison Graph' button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



In above 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 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	F1 SCORE
MSCC-F220	DeepNet	79.14444444444444	79.14444444444444	79.14444444444444	79.14444444444444
MSCC-F220	ShuffleNet	84.11111111111111	84.11111111111111	84.11111111111111	84.11111111111111
MSCC-F220	ResNet50	89.11111111111111	89.11111111111111	89.11111111111111	89.11111111111111
MSCC-F220	Fusion Model SVM	95.45454545454545	95.45454545454545	95.45454545454545	95.45454545454545
MSCC-F220	RF SVM	88.11111111111111	88.11111111111111	88.11111111111111	88.11111111111111

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

## VII.CONCLUSION

Inexpensive cameras have been widely available in recent decades, which has helped propel the medium to new heights of popularity. Because of how quickly the average person can interpret an image, this kind of communication has become more important. Though most image editors set out to improve photos, others are using them to create fakes that spread misinformation online. Therefore, there is a pressing need to eliminate picture tampering. In this study, we provide a novel approach to detecting picture counterfeiting by using neural networks and deep learning, with a focus on the CNN architectural style. The proposed approach combines many image-reduction techniques owing to its convolutional neural network (CNN) architecture. In order to train the model, both the original and compressed copies of each picture are compared and contrasted. The suggested method has the potential to identify copy-move and splicing frauds with relative ease. There is a clearly defined repeat limit and studies show an overall validation accuracy of 92.23 percent, which is promising. Eventually, we want to perfect our method

for identifying phoney photos. If we can integrate the proposed technique with other proven approaches, we may increase accuracy and decrease the time complexity of image localization even more. To combat spoofing, we will improve upon the method presented [50]. Since the standard method needs a minimum of 128 by 128, we will modify it to work with much lower-quality images. For the purpose of training deep learning networks for photo fraud detection, we will also be creating a demanding large-scale image forgeries database.

## VIII.FUTURE SCOPE

The future scope of the Image Forgery Detection Based on Fusion of Lightweight Deep Learning Models system is promising, with numerous opportunities for advancement and application. As deep learning models continue to evolve, the integration of more sophisticated and diverse models could further enhance detection accuracy, making the system more robust against increasingly complex forms of image forgery. One potential area of development is the inclusion of multimodal data, such as incorporating metadata analysis, facial recognition, and context-aware algorithms, which could provide a more holistic approach to forgery detection. Additionally, transfer learning could be explored to fine-tune models on specialized datasets, improving detection performance for specific types of image manipulations. Another exciting avenue is the real-time deployment of these models on edge devices, leveraging 5G connectivity and distributed computing to enable even faster



and more efficient image verification at the source. As the application of blockchain technology becomes more widespread, integrating blockchain-based image authentication could provide an immutable record of image origin and alterations, ensuring further trust in the detection process. Moreover, the development of user-friendly applications that allow non-experts to perform real-time image verification could increase the adoption of these systems in areas such as journalism, legal investigations, and online content moderation. In the future, a comprehensive ecosystem combining deep learning, edge computing, blockchain, and multimodal analysis could lead to an advanced, universally applicable image forgery detection system capable of identifying a broad range of manipulations across different industries.

## IX. REFERENCES

1. Farid, H. (2009). A survey of image forgery detection techniques. *IEEE Transactions on Signal Processing*, 57(3), 74-81.
2. Li, H., & Lin, W. (2020). Deep learning for image forgery detection: A survey. *International Journal of Computer Vision*, 128(9), 2065-2093.
3. Nguyen, H. X., & Bai, J. (2020). Image forgery detection using lightweight convolutional neural networks. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2563-2571.
4. Zhang, L., & Zhang, D. (2017). Deep learning for image forgery detection: A comprehensive review. *ACM Computing Surveys*, 50(4), 1-39.
5. Li, Z., & Xu, C. (2019). Lightweight deep learning models for image classification and forgery detection. *Journal of Visual Communication and Image Representation*, 61, 86-95.
6. Qian, X., & Yang, X. (2018). A lightweight deep learning architecture for forgery detection in digital images. *International Journal of Artificial Intelligence*, 9(3), 219-230.
7. Wang, X., & Zhang, Y. (2020). Image manipulation detection: A survey of deep learning-based methods. *Signal Processing: Image Communication*, 79, 178-190.
8. Feng, Y., & Xie, L. (2021). Multimodal image forgery detection using deep learning techniques. *Computers, Materials & Continua*, 67(2), 1787-1798.
9. Wang, Z., & Chen, X. (2020). Fusion of deep learning models for image forgery detection. *Journal of Information Security and Applications*, 53, 102502.
10. Yang, L., & Chen, Q. (2019). Blockchain-based image authentication: A new approach for real-time detection of image forgeries. *Proceedings of the 2019 International Conference on Blockchain and Cryptocurrency*, 232-237.