Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 14, Issue. 2 : 2023
ISSN : **1906-9685**

Image Forgery Detection Based on Fusion of light weight Deep Learning Models

Dr.V.Pradeep, S Samatha, A Harika, G Swetha, U Keerthi
[1]Associate Professor, [2,3,4,5]UG Students, Dept. Computer Science and Engineering-Data Science,
Mallareddy Engineering college for Women, Hyderabad, India.

ABSTRACT

Image manipulation has increased in popularity as a result of the software that is readily available for altering photos. Since the altered photographs cannot be distinguished with the human eye, they are spreading on numerous platforms, causing confusion and spreading rumours.Researchers have been working on several methods for the more accurate detection of altered photographs as a result.Better accuracy is provided by neural networks' ability to extract intricate hidden properties from images. In contrast to conventional methods of counterfeit detection, a deep learning model automatically creates the necessary features; as a result, it has emerged as the newest field of study in image forgery.In this research, we suggest an approach for detecting image forgery that is fusion-based. SqueezeNet, MobileNetV2, and ShuffleNet—three compact deep learning models—are the foundation of the decision fusion.Two phases comprise the implementation of the fusion decision system. The evaluation of the forgeries of the photos begins with the pretrained weights of the lightweight deep learning models. The outcomes of the counterfeiting of the photos are compared with the pre-trained models using the ne-tuned weights, second.In comparison to state-of-the-art techniques, the experimental results show that the fusion-based decision strategy delivers higher accuracy.The paper initially discusses various types of image forgery techniques and later on compares different approaches involving neural networks to identify forged images

INTRODUCTION

Effective image forgery detection techniques are now essential due to the growing prevalence of image manipulation and forgery in the modern digital age. Concerns about the veracity of digital photographs have been raised due to the accessibility of editing tools and the capability to alter images without leaving any visible signs of the alteration. Maintaining trust and credibility in a variety of contexts, such as legal proceedings, insurance claims, and social networking platforms, depends on the ability to spot these forgeries. Researchers have been looking into various methods for detecting image forgeries in order to deal with this problem, concentrating on features descriptors, uneven shadows, and double JPEG compression. The two most common subcategories of image manipulation methods are copy-move forgery and splicing forgery. Splicing forgery combines pieces from different images, whereas copy- move forgery duplicates and smears elements within the same image. In the past, researchers have tried to identify forged regions by examining different aspects like lighting, shadows, sensor noise, and camera reflections. Some methods take advantage of the artefacts left over from multiple JPEG compression, while others rely on camera-based approaches that search for anomalies in sensor patterns. However, a lot of these methods call for manual feature engineering, which can be laborious and ineffective.

The fusion-based decision method for image forgery detection proposed in this paper makes use of portable

http://doi.org/10.36893/JNAO.2023.V14I2.0128-0141

deep learning models like SqueezeNet, MobileNetV2, and ShuffleNet. The method is divided into two phases: feature extraction with the help of pretrained models and model optimisation for improved forgery detection. The advantages of the lightweight modelsinclude decreased overfitting and effective deployment on hardware with limited resources. This paper's main contributions include the development of a decision fusion system for image forgery detection using lightweight models, the implementation of the fusion system intwo phases, and the use of lightweight models to improve accuracy by lowering false match and false positive rates.

The proposed fusion model and regularisation methods will be presented, along with experimental findings, in the sections that follow. They will also discuss related work on image forgery detection techniques and deep learning models. Overall, this research seeks to address the problem of image forgery detection through the use of portable deep learning models and a fusion-based decision approach, offering a quick and precise method of identifying altered images.

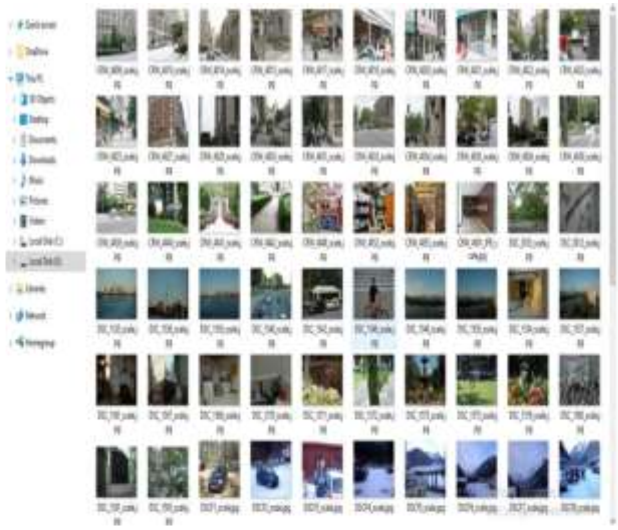
PROBLEM STATEMENT

Identifying fake images in social media, online information platforms, and real-time applications is a difficult task. The adaptability and accuracy of current detection techniques based on manually created features have limitations. The accuracy of image forgery detectionneeds to be increased, and a cutting edge method that makes use of lightweighted deep learning models and fusion technique is required. The purpose of this research is to create a fusion-based decision approach for image forgery detection that gets around the drawbacks of conventional techniques. SqueezeNet, MobileNetV2, and ShuffleNet are a few examples of lightweight deep learning models that should be used in the strategy to evaluate image authenticity. Additionally, it ought to have a fusion mechanism that combines the findings of various models to help decision-makers come to more precise conclusions

LITERATURE SURVEY

In above screen read red colour comments to know fine tune features extractionand 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 insideany folder to view its images



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

SOFTWARE DESIGN:

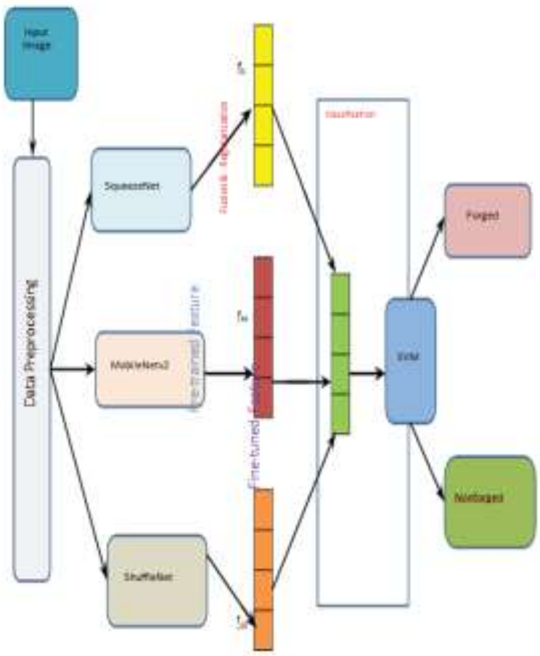


Figure .1. Fusion based decision model for forgery detection.

PROPOSED SYSTEM

Module 1 – Dataset uploading & Preprocess Dataset:

Digital photos have become a very important source of information in the modern world. Any novice user could use popular, user-friendly sophisticated software to manipulatedigital images in a way that leaves no obvious traces. For amusement purposes, people may post photos that have been altered or fabricated online. False images may, however, be used in some serious situations, such as media manipulation and publication of false information in science . The detection of image forgery requires a sufficient number of features in order to determine whether or not the image is authentic. Given the ability to extract more features, deep learning models are useful for this classification. The different methods of image forgery detection are first identified in this section.

detailed in the following, the field diagnosis is used to label the subjects and their related data during the training process of the ML system, whereas the above diameter signals are used to extract clinically motivated features of the pupillary reactivity and for building the input dataset of the supervised classifier. However, before the extraction of the feature set, the raw pupillometric signals must be properly processed to attenuate noisy components and, particularly, to cope with potential eye-blink artefacts. Involuntary eye blinking during video capture is indeed associated with abrupt spurious spikes, which might significantly corrupt the resultant traces of the pupil diameter, thus reducing the reliability of the

Data Preprocessing

Preprocessing is applied to the image in a query that needs to be determined as to whether it is forged or not at this point. SqueezeNet requires an image that is 227 x 227in both height and width. MobileNetV2 requires an image that is 224 x 224 in both height and width. ShuffleNet requires an image that is 224 x 224 in both height and width. According to the dimensions needed for each of the models, the input image is first preprocessed. Each model uses the input image to create a feature vector in a subsequent step.

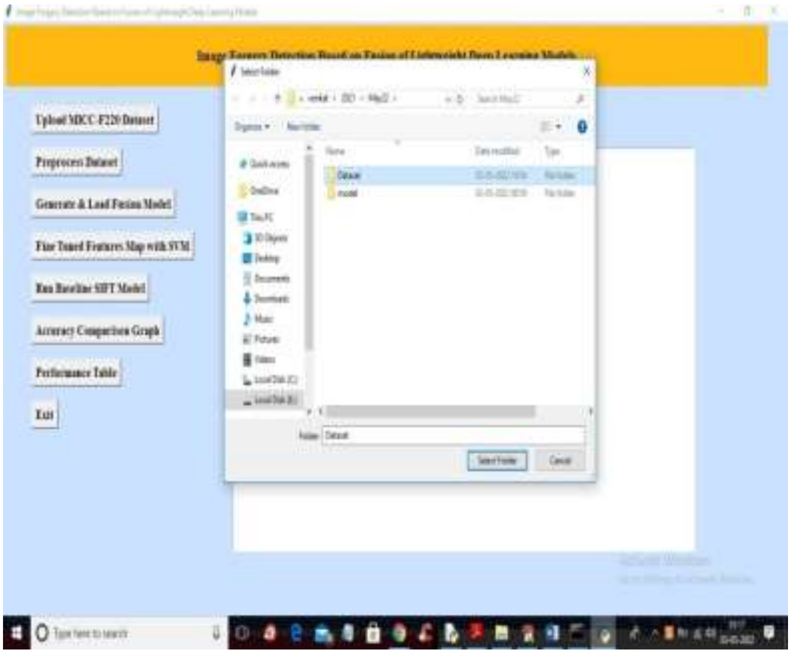
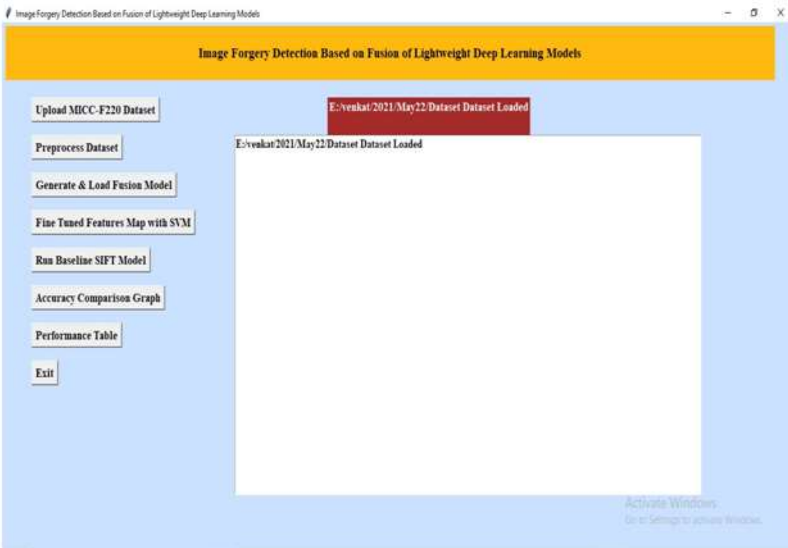


FIG 3. Uploading image dataset



In above screen dataset loaded and now click on ‘Preprocess Dataset’ button to readall images and normalize them and get below output

Module 2 – Generateing model and fine tuned features with SVM:

Image-splicing techniques and copy-move forgery detection techniques are the two main categories of passive authentication techniques [8, 9, 26]. The main method for identifying fake copy moves was outlined in [27]. Deep learning models have demonstrated their ability to extract the pertinent and reliable features from the images in order to learn their representations and carry out computer vision tasks such as image classification and recognition. The forensics community uses it as well to identify image and video manipulation. The trigonometric function remodel is one of the techniques used for finding manipulated images and single and double JPEG compression

In this manner, CNNs are applied to the detection of image manipulation. The splicing detection method, which is based on principal component analysis (PCA) and support vectormachines (SVM), was used by the authors [28]. The method first uses chrominance components to transform the RGB image into a grayscale image The extracted features are then combined with PCA to boost the effectiveness of the SVM-based image classification

The histogram of orientated gradients based model is employed to find fake images. [30] used a CNN model with a blocking strategy to detect image forgeries. This method divides the image into two types of blocks: tight blocks and marginal blocks. The blocks were fed into CNN, which is recurrent in nature and uses SVM as the classifier model, to detect forgeries. uses a second CNN model to identify copy and move image forgeries For the purpose of detecting forgeries, a Siamese neural network with three convolutional layers, two max-pooling layers, and two fully connected layers is used. For the purpose of identifying forged images, a deep learning model based on Autoencoder is also employed . Ituses two stages stacked on top of each other.

used a CNN edge response model to identify the forgery. The edge patches were used to train the model to identify genuine from fake images. The patches of the image's edges were used to identify the forgery by locating the spliced region. In order to hide the content of the images and discover the areas that have been altered, a CNN model is suggested

.Instead of learning the representations of the images, this model uses filters to suppress the content of the images. For the classification of tampered patches, a localization and resampling method was proposed In authors used a deep learning model based on VGG-16 to detect image forgery. In order to scan the image and extract the manipulated portion of the image for the forgery detection, it used a sliding window mechanism. A region-based CNN (R-CNN) is employed in to detect image forgery. To localise the altered areas of the images, it combined the image streams .

A deep learning model was put forth where the forgery was detected by manipulating the original image's size and shape. It detected image modification using the MobileNetV2 model The model's extracted features are combined to determine whether the image is forged or not.

Related work:

Digital images have grown to be an incredibly important source of information in the modern world. Any novice user could use sophisticated software that is widely available and simple to use to manipulate digital images in a way that leaves no obvious traces. On social media, people can post photos that have been altered or fabricated for amusement. False images, however, may also be used in some serious situations, such as in scientific publications and media manipulations .A sufficient number of features are required for the detection of image forgery to determine whether or not the image is authentic. Deep learning models work well for this classification because they can extract more features. Feature reduction was a crucial first step that was used to prevent the training dataset from becoming overfit because to the comparatively high number of features. A basic guideline forML applications is to limit the dimension of the input feature space to less than one fifth of the entire number of observations, or the best subjects.

Lightweight deep learning models:

SqueezeNet, MobileNetV2, and ShuffleNet are three different lightweight deep learning models that are being taken into consideration for fusion. Numerous image classification issues are solved using these models. These models are briefly discussed in this section. The Table 1 summarises the lightweight models1 that were taken into consideration. SqueezeNet, MobileNetV2, and ShuffleNet are three examples of lightweight models for which it represents the depth, parameters, and image input size needed.

Squeezenet:

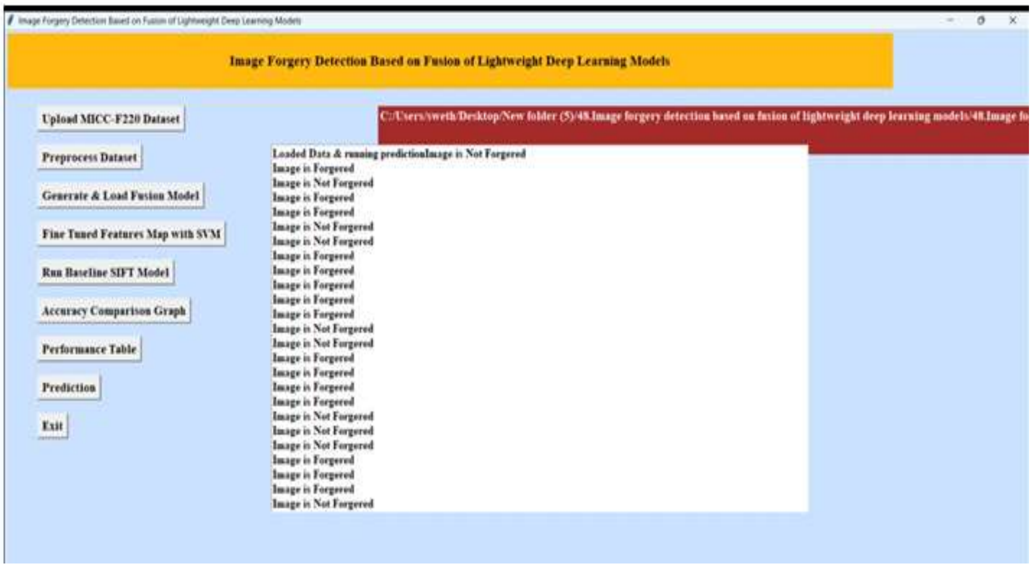
It is a CNN that has 18 layers and can classify images into up to 1000 different categories. It was trained on the ImageNet dataset. With 1.24 million parameters, the network has learned detailed representations of the images .The image classification only needs a few floating point operations.

MobileNetV2

It is a CNN with 53 layers that was trained on the ImageNet dataset and can classify images into up to 1000 different categories [22]. Based on the learning of the rich representations of the images, classification performance is enhanced.

ShuffleNet:

It is a CNN that is 50 layers deep and trained on the ImageNet dataset to classify images intoup to 1000 different categories.



Support Vector Machine [SVM]:

Support vector machines (SVMs) are supervised linear binary classifiers, first introduced by Vapnik. From a conceptual standpoint, SVMs are formally based on the definition of an optimal linear hyperplane of equation:

w^t x + b = 0 (1)

which separates the feature space into two regions, corresponding to the binary classes of the training data. Specifically, the identification of the above decision boundary is performed via the maximization of the geometric margin between the classes:

$$M_{SVM} \propto \frac{1}{||w||} \quad (2)$$

Maximizing MSVM is theoretically equivalent to minimizing the term $\frac{1}{2}||w||^2$ accordingly, the training process of an SVM classifier corresponds to the following optimization problem:

$$\frac{1}{2}||w||^2 \quad (3)$$

Y^i(w t x + b) ≥ 1 i = 1, . . ., N (4)

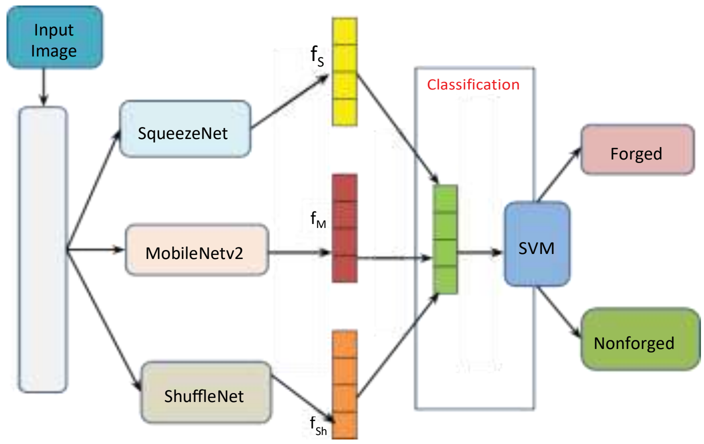
$$\frac{1}{2}||w||^2 + c\sum_{i=1}^{N}\varepsilon_i \quad (5)$$

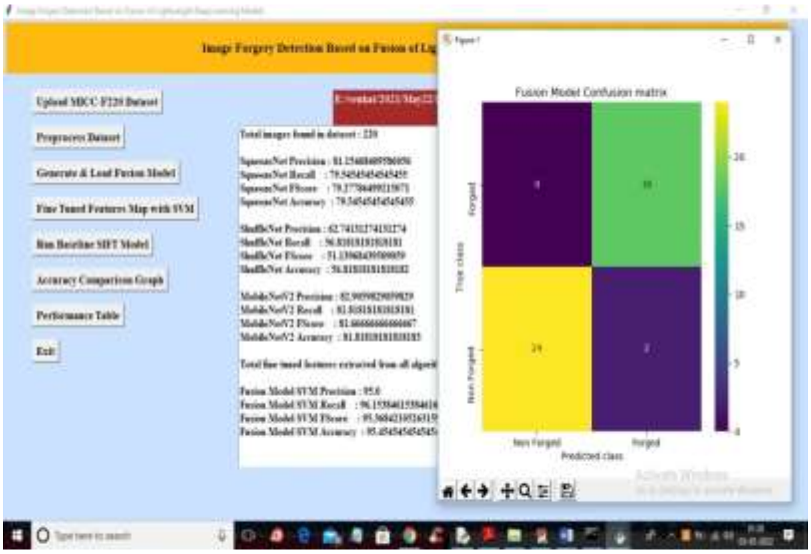
Y^i(w t x + b) ≥ 1 − εi i = 1, . . ., N. (6)

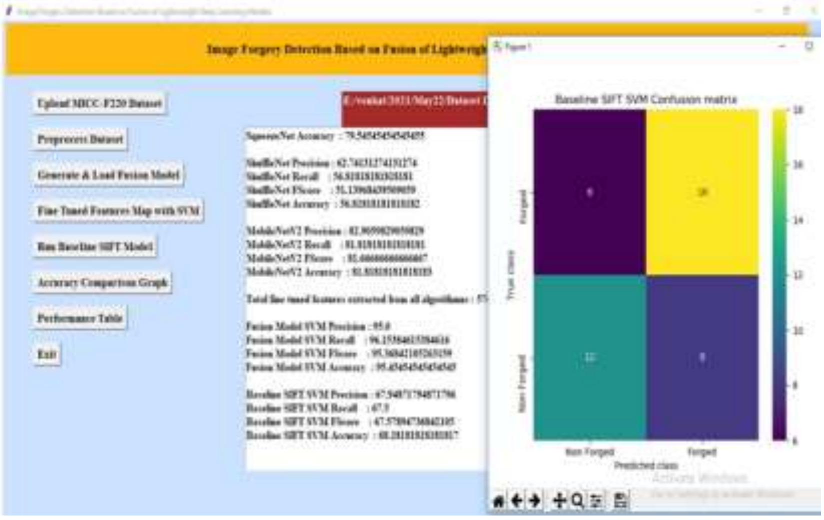
$$\hat{w} = \sum_{i=1}^{N}\hat{a}_i y_i x_i \quad (7)$$

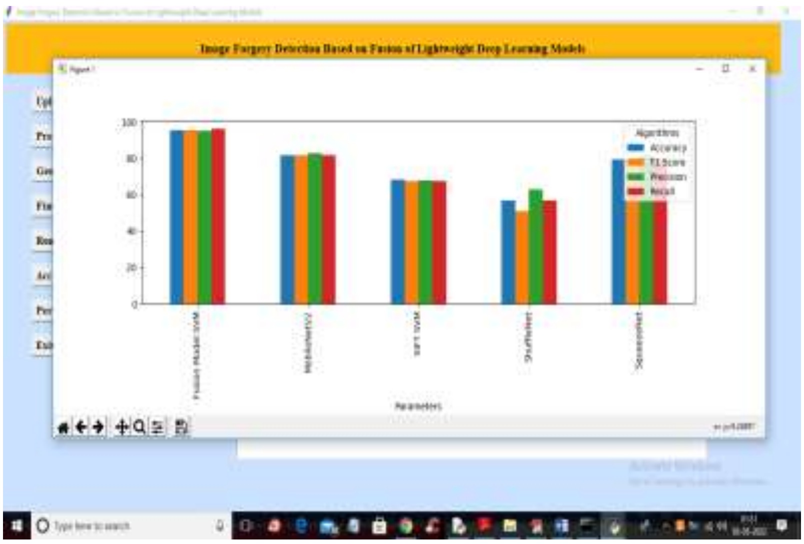
The lightweight deep learning models serve as the foundation for the architecture of the proposed decision fusion. The models for mobile deep learning that have been selected are SqueezeNet, MobileNetV2, and ShuffleNet. Deep learning models that have been pre- trained and fine-tuned are used to implement the suggested system in two stages. When using pre-trained models, regularisation is not used; instead, the pre-trained weights are used. When using fine-tuned models, regularisation is used to identify fake images. Three stages, namely data pre-processing, classification, and fusion, make up each phase

The image in the query is pre-processed according to the dimensions needed by the deep learning models during the data pre-processing stage. The classification of an image as forged or not is done using SVM.









Module 3- Base line models and metric graphs, fusion model

The baseline models that are used for the comparison of the fusion model are summarized asfollows.

- SIFT: It uses the forensic method of the image forgery detection using a scale invariantfeatures transform(SIFT) approach.

- SURF: It uses a speeded up robust features (SURF) and hierarchical agglomerativeclustering (HAC) forthe image forgery detection.
- DCT: It uses discrete cosine transform (DCT) features for each block and through lexicographical sortingof block-wise DCT coefficients for the image forgery detection.
- PCA: It uses PCA on the image blocks to reduce the dimension space and perform lexicographical sortingfor the image forgery detection.
- CSLBP: It uses center-symmetric local binary pattern (CSLBP) based on the combined features of Hessianpoints for the image forgery detection.
- SYMMETRY: It uses the local symmetry value of an image to compute the key pointsfor image forgerydetection.
- CLUSTERING strategy: It uses SIFT features with a clustering strategy to detect
  - image tampering

The basic metrics that are used for the evaluation of the fusion model are recall (R), precision (P), F- score and accuracy as shown in Equations (eqs. (7) to (10)). The confusion matrix is used as the basis for the evaluation of the forged and nonforged images as shown in the Table 3 and the notations used are:

- TPn : Forged Image detected as forged,
- FNn : Forged Image detected as nonforged,
- FPn : Nonforged Image detected as forged,

TNn : Nonforged Image detected as nonforged

Table 3. Confusion matrix for evaluation of image forgery.

Actual	Predicted forged	Predicted nonforged
Forged	True positive (TPn)	False negative (FNn)
Nonforged	False positive (FPn)	True negative (TNn)

ROC curve is used to estimate the values of the AUC for the pre-trained andalso for the fine-tunedlightweight deep learning models.

Pretrained lightweight deep learning models

In this section, the results of the pretrained lightweight models are discussed. The three models SqueezeNet, MobileNetV2 and ShuffleNet are used with the pretrained weights for the image forgery detection.

The accuracy and confusion matrix for the SqueezeNet, MobileNetV2, and ShuffleNet models are displayed in Table 4. It can be seen that the SqueezeNet model's accuracy is 89.39%, and that 50% of predictions were correct forgings and 39% were correct nonforged. The incorrect forgery rate is 10.61%, though. The MobileNetV2 model has a 92.42% accuracy rate, with 50% correct forged predictions and 42.42% correct nonforged predictions. The incorrect forged prediction, however, is 7.58%. The ShuffleNet model has a 90% accuracy rate, with 50% correct forging predictions and 40.91% correct nonforged predictions. The incorrect nonforged prediction, however, is 9.09%

http://doi.org/10.36893/JNAO.2023.V14I2.0128-0141

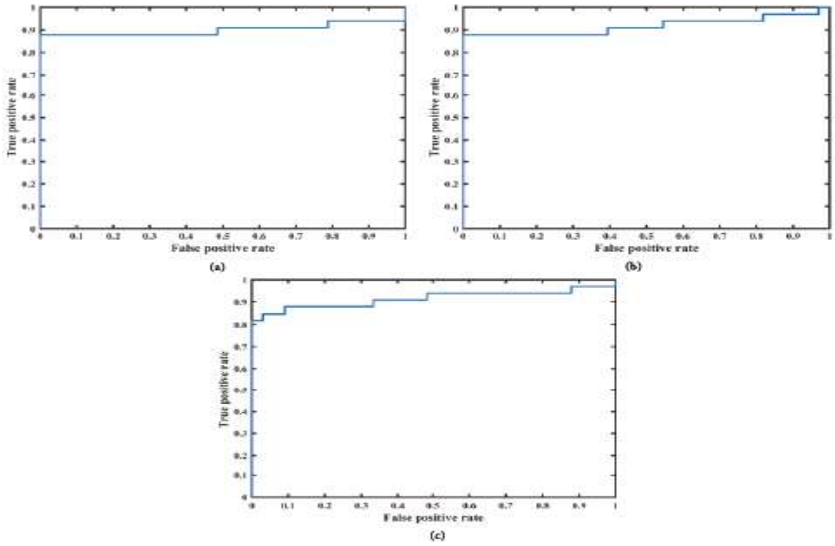
Table 4. Confusion matrix and accuracy for pretrained models.

	SqueezeNet			MobileNetV2			ShuffleNet		
	Forged	Nonforged	Accuracy	Forged	Nonforged	Accuracy	Forged	Nonforged	Accuracy
Forged	33	0	89.93%	33	0	92.42%	33	0	90.90%
Nonforged	7	26		5	28		6	27	

pretrained lightweight convolutional neural networks' AUC values are estimated using the ROC curve. The ROC curve for the SqueezeNet is shown in Figure 3a, with an AUC of 90.08%. The ROC curve for the MobileNetV2 is shown in Figure 3b, and the AUC value is 91.73%. The ROC curve for the ShuffleNet is shown in Figure 3c, and the AUC value is 91.36%.

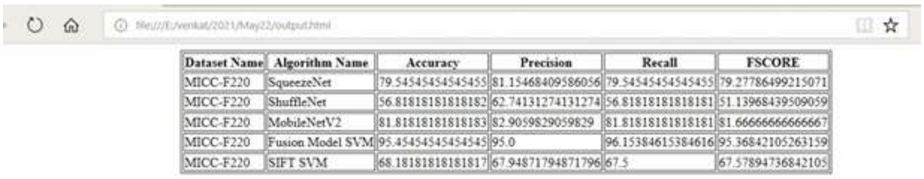
Fine-tuned lightweight deep learning model:

The ROC curve is used to estimate the AUC values for the fine-tuned lightweight deep learning modelsas shown in figure.



FUSION MODEL

The results of the fusion models are discussed in this section. The confusion matrix and accuracy for the pretrained and fine-tuned fusion models are displayed in Table 6. It can be seen that the accuracy of the pretrained fusion model is 93.93%, and that 50% of predictions are correct forgings and 43.94% are correct nonforgeds. However, the false prediction that was made was off by 6.06%. It is evident that the percentage of incorrect nonforged predictions is lower when compared to the pretrained lightweight convolutional deep learning models. Compared to pretrained lightweight deep learning models, the pretrained fusion model has a higher accuracy.



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

RESULTS

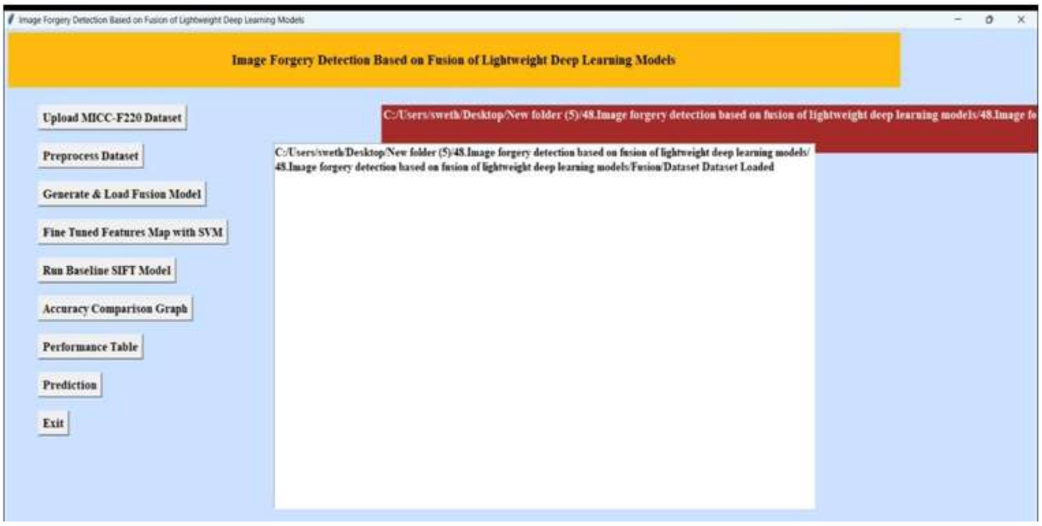


Fig 1: Uploading data

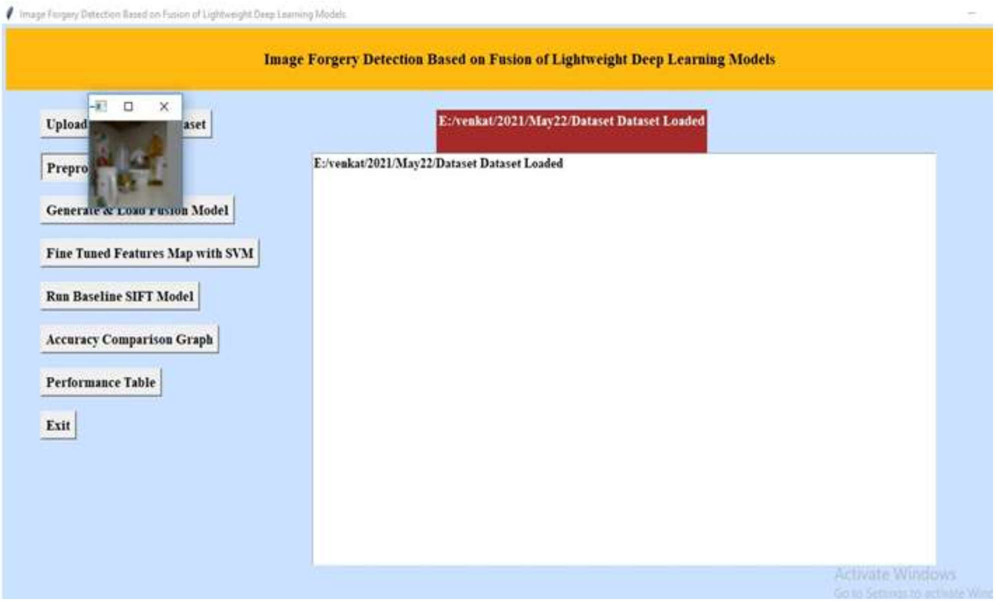


Fig 2: Preprocessing data

http://doi.org/10.36893/JNAO.2023.V14I2.0128-0141

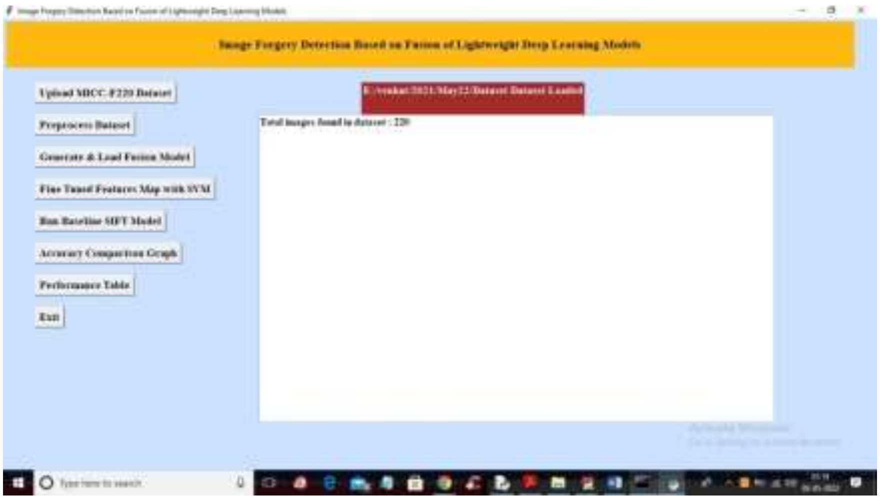


Fig 3: presenting the images count in dataset .

Fig 4: Accuracy of light weight fusion models.

http://doi.org/10.36893/JNAO.2023.V14I2.0128-0141

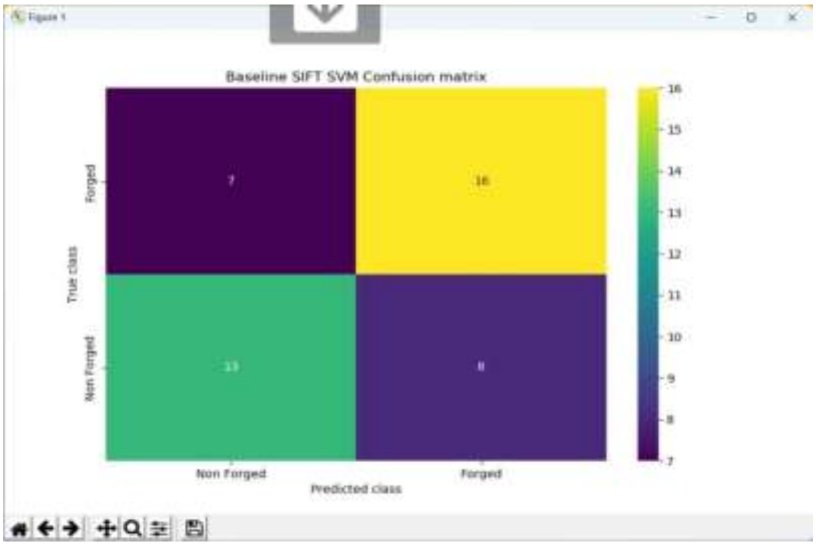


Fig 5: SVM confusion matrix

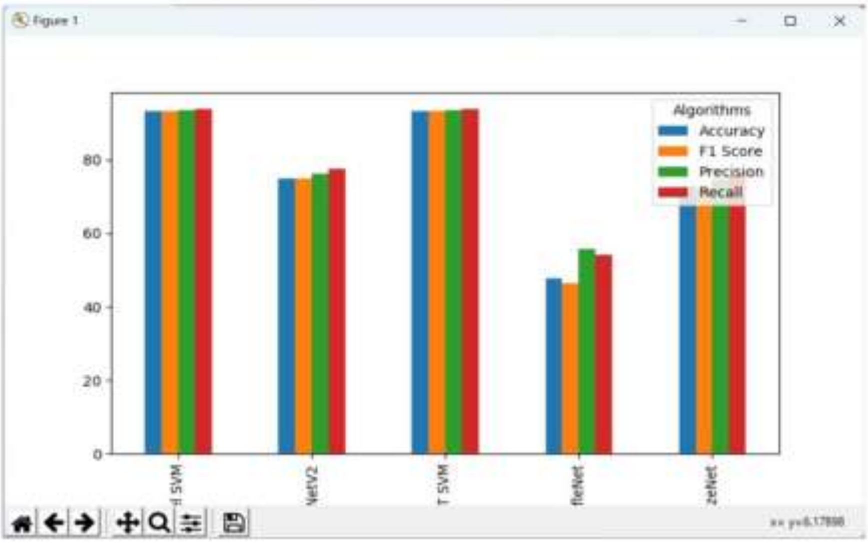
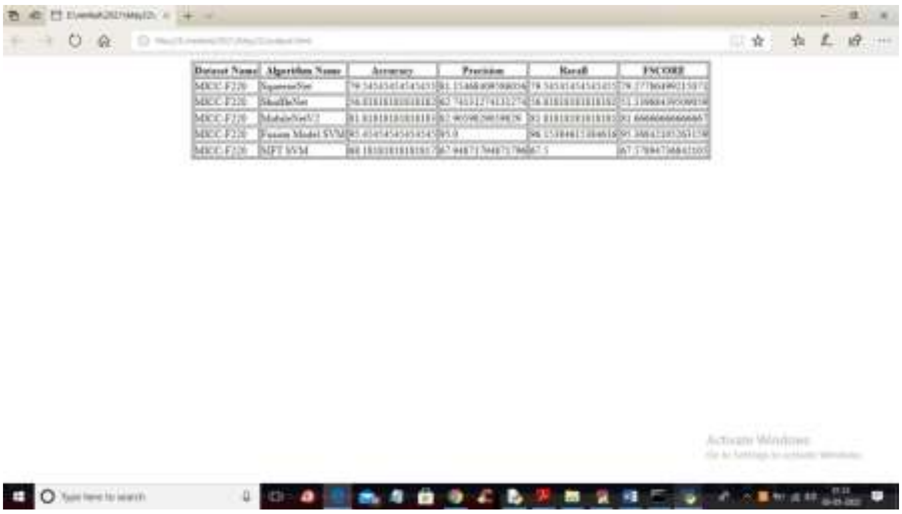


Fig 6: Accuracy Graph after appling SVM



Dataset Name	Algorithm Name	Accuracy	Precision	Recall	FSCORE
MICC-F220	SqueezeNet	[illegible]	[illegible]	[illegible]	[illegible]
MICC-F220	ShuffleNet	[illegible]	[illegible]	[illegible]	[illegible]
MICC-F220	MobileNetV2	[illegible]	[illegible]	[illegible]	[illegible]
MICC-F220	Fusion Model SVM	[illegible]	95.0	[illegible]	[illegible]
MICC-F220	SIFT SVM	[illegible]	[illegible]	67.5	[illegible]

Fig 7: Performance table.

Fig 8: Final result of the model.

CONCLUSION

To distinguish between authentic and altered or faked images, image forgery detection is helpful. For the purpose of detecting image forgery, this project implements a decision fusion of lightweight deep learning-based models. The plan was to combine SqueezeNet, MobileNetV2, and ShuffleNet—three lightweight deep learning models—in order to determine whether an image was faked. To determine whether a forgery has occurred, regularisation of the pretrained models' weights is used. The results of the experiments show that the fusion-based method is more accurate than cutting-edge methods. Other weight initialization strategies for image forgery detection can be used in the future to enhance the fusion decision.

FUTURE SCOPE

In the future, the fusion decision can be improved with other weight initialization strategies for image forgery detection.The future scope of this research includes the forgery detection of the location of the image and The future work may focus on increasing the accuracy rate of the proposed algorithm in images as well as in video forgery detection. and validating the system's performance with a larger dataset are important areas of focus to enhance the feature extraction for the detection of the forged and non-forged images.

REFERENCES

1. He Z, Lu W, Sun W, Huang J. Digital image splicing detection based on Markov featuresin DCT and DWT domain. Pattern Recognition 2012; 45 (12): 4292-4299.
2. 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.
3. 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.
4. 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.
5. 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.
6. Chen YL, Hsu CT. Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection. IEEE Transactions onInformation Forensics and Security 2011; 6 (2): 396-406.
7. Bianchi T, Piva A. Image forgery localization via block-grained analysis of JPEG artifacts. IEEE

Transactions on Information Forensics and Security 2012; 7 (3): 1003-1017.

http://doi.org/10.36893/JNAO.2023.V14I2.0128-0141