iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.70883

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Image Source Identifier with Video Deepfake and Forgery Detection using Conventional and Recurrent Neural Networks

Rahul Daga[1], Pranav Patil[2], Parth Rajopadhye[3], Arihant Awate[4], Manasvi Patil[5], Deepali Joshi[6]
Dept.of Information Technology Vishwakarma Institute of Technology Pune, India

Abstract: ***This paper presents a model which addresses two important forensics analysis i.e. source camera identification and deepfake/forgery detection for videos.Camera identification of images is implemented using CNN based Photo Response Non-Uniformity noise patterns and for Deepfake/Forgery we have used RNN based model that analyzes temporal and spatial inconsistencies. The source identification model is trained on multiple mobile cameras whereas the deepfake model captures the frame-wise variations and deepfake artifacts,The experimental results of the model validate the robustness of the system with an overall approximate of 93% accuracy providing a comprehensive framework for Digital Media Forensics.***
Keywords: Convolutional and Recurrent Neural Networks, Deepfake, Forgery, Digital Media Forensics

I. INTRODUCTION

With many advancements in cloud technologies and widespread availability of image and videos, the authenticity and integrity of digital media has been challenging for substantiation. Deepfakes and forgeries have a substantial increase with various level of threats in different domains of forensics such as cybersecurity, journalism etc.Deepfakes and forgery are generated artificially[7] using software like photoshop and many more leading to a high threat level for individuals being a victim of this. With extensive manipulative media today, ranging from photo alterations to hyper realistic deepfake video generation, the concerns regarding the credibility and misleading use of these techniques have increased.

The origin and the source of images taken plays a critical role for investigating the forensic reports. The analyst identifies the source camera from which the images are taken[4]. Images taken from a camera taken digitally inherit the sensor properties of the camera sensor, each device having its own unique feature in their design[12]. Since each camera sensor creates a distinct Photo Response Non Uniformity pattern, it gives us the camera traces as there is manufacturing imperfections which keeps it consistent across all images taken from the same device. For source camera identification we have implemented a CNN based model that extracts and classifies the PRNU noise pattern to attribute an image to its source camera.

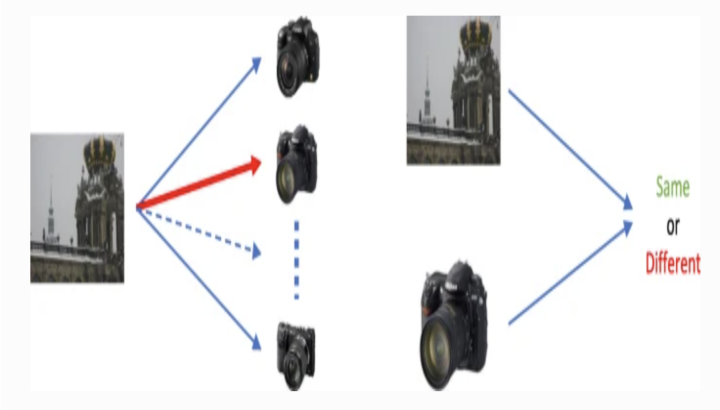


Figure 1: Basics of the system

In concurrence of advancements in image processing techniques, the emergence of sophistical deepfake technologies has created new challenges for media authenticity verification. Deepfakes are generally based on GAN (Generative Adversarial Networks), which creates hyper-realistic synthetic videos. Deepfakes can be used for positive tasks but widely are used in many malicious uses[5].

©IJRASET: All Rights are Reserved

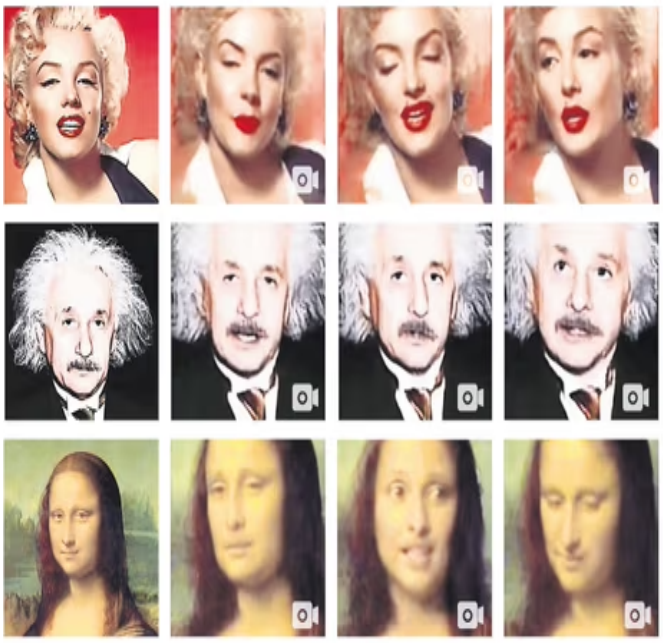


Figure 2: Deepfake and Forgery.

Given in the above images is the deepfake videos created where the faces of the portraits appears to be moving like a video.
An RNN model has been implemented in this project which helps analyze sequential video frames to detect deepfake content. With this unified approach we tend to strengthen digital forensic investigations.

II.RELATED WORK

Guru Swaroop Bennabhaktula et al. [3] used a Deep Learning Model for Source Camera Device Identification from Videos with 28 device VISION dataset to test and train their model. With this evaluation they have achieved 74.70% accuracy. With a similar evaluation on the QUFVD dataset resulted their model to achieve 88.5% accuracy. Various ConvNets were used to conduct this experiment.
Wen-Chao Yang et al. [4] used a new approach for PRNU analysis. The experimental outcomes provided a low processing time and very low FRR. SCI/V method was used in video forensics.
Peipeng Yu et al. [5] surveys the current research status of deepfake video detection which revealed that the recent deepfake video detection methods are still insufficient and cannot be applied in real life.
Akash Chintha et al. [6] have used a combined convolutional latent representationwith bidirectional recurrent structures and entropy-based cost functions. Here an XceptionNet CNN model is used as a salient and efficient facial feature representation which are bidirectional recurrence layer. For visual deepfakes, FaceForensics++ and Celeb-DF datasets were which demonstrates robustness of methods implemented.
Shraddha Suratkar et al. [7] have analyzed the problem the generalizability in order to make the network robust to all kind of attacks. The paper presents models with better accuracy of deepfake detectors. Models are trained on DFDC dataset and FaceForesics++ and achieves a score of 94% and 98% respectively.
Muhammad Javed et al. [8] proposed a model based on two deep neural architectures, MesoNet4 and ResNet101. The model is evaluated on diverse datasets, including CelebV1, and CelebV2. Further the evaluation of the integrated hybrid empathizes the efficiency in identifying the deepfake content streaming.
Apurv Jindal [9] proposed a model for deepfake forgery detection, used the LTSM model network with ResNet50 as a pre-trained model. The model achieves the highest accuracy of 93.59%.
Mehdi Kharrazi et al. [10] have experimented with 150 images from 3 different models. SVM model was used to classify the data from all the different camera models and the accuracy achieved of the final model is 88.02%

©IJRASET: All Rights are Reserved

Xiangui Kang et al. [11] propose a Camera Reference Phase SPN which is Sensor Pattern Noise extraction method, which enhances identification accuracy. It demonstrates the superiority in resisting JPEG compression and achieving better ROC performance compared to all existing techniques.

Na Huang et al. [12] introduces a method using CNN to learn CSNP. The approach enhances accuracy and minimizes data requirements, making it suitable for forensic investigations with limited training samples. This method achieves a 99.8% accuracy, outperforming earlier approaches. And the future work aims to address challenges like lighting variations and overfitting with larger datasets.

David Freire-Obregon et al. [13] have also proposed a hybrid model combining ResNet50 and Vision Transformers. This proposed method describes a CNN architecture which detects and identifies with 98% accuracy. This is carried out by using the images captured from different mobile device cameras.

Yangjing Long and YizhenHusang in [14] have worked on the model that integrates a 3D CNN and LSTM layers for extracting spatiotemporal features from video frames. They have used the FaceForensics++ datasetwhich achieves a 94.78% accuracy. This study also emphasizes a few preprocessing which includes face detection and alignment for better performance which is a robust architecture for real-time and accurate deepfake analysis.

Tong Qiao et al. [15] proposed a model for source camera identification based on identification of unique noise pattern of every different camera model. The study is based on LRT i.e. Likelihood Radio Test and the performance of the presented model is theoretically established.

Bo Wanrg et al. [16] have proposed an effective source camera identifier model which is based on a multi-class SVM classifier. The accuracy of the identifier is 98%. on average whereas 96.9% for the three Canon cameras.

Davide Cozzolino et al. [17] have proposed a model to leverage the image noise pattern in conditions like cropped images, or compressed images. The model achieves an average accuracy of 60.05% and a large gain with respect to the conventional method.

III. TECHNOLOGY USED

A. Tenserflow

A free open-source software library for dataflow and differentiable programming across a range of tasks. It is a symbolic math library and also used for machine learning applications such as neural networks.

B. Numpy

It is a general-purpose array processing package. It provides a high performance multi-dimensional container of generic data. Arbitrary data-types can be defined using Numpy which allows to seamlessly and speedily integrate with a wide variety of database,

C. Pandas

An open-source Python Library providing high performance data manipulated and analysis tool using its powerful data structure. Python with pandas is used in wide range of fields including academic, and commercial domains.

D. Matplotlib

This library is used for generating plots, histogram, power spectra, charts etc. It can be used in python script shells, web application servers etc.

E. Scikit-learn

Scikit-learn provides a range of supervised and unsupervised learning algorithms via a consistent interface in Python. It is licensed under a permissive simplified BSD license and is distributed under many Linux distributions, encouraging academic and commercial use.

These systems in our project are used to design and train the deep learning model for accurate classification of source cameras and deepfake detections. The Numpy library supports efficient numerical operations, hence helps in PRNU noise extraction and image preprocessing. Similarly, Scikit-learn aided in evaluation metrices, and implementation of classifiers for the system. Together, these libraries form robust foundation for both analytical and machine learning components of the system.

IV. SYSTEM ARCHITECTURE AND DESIGN

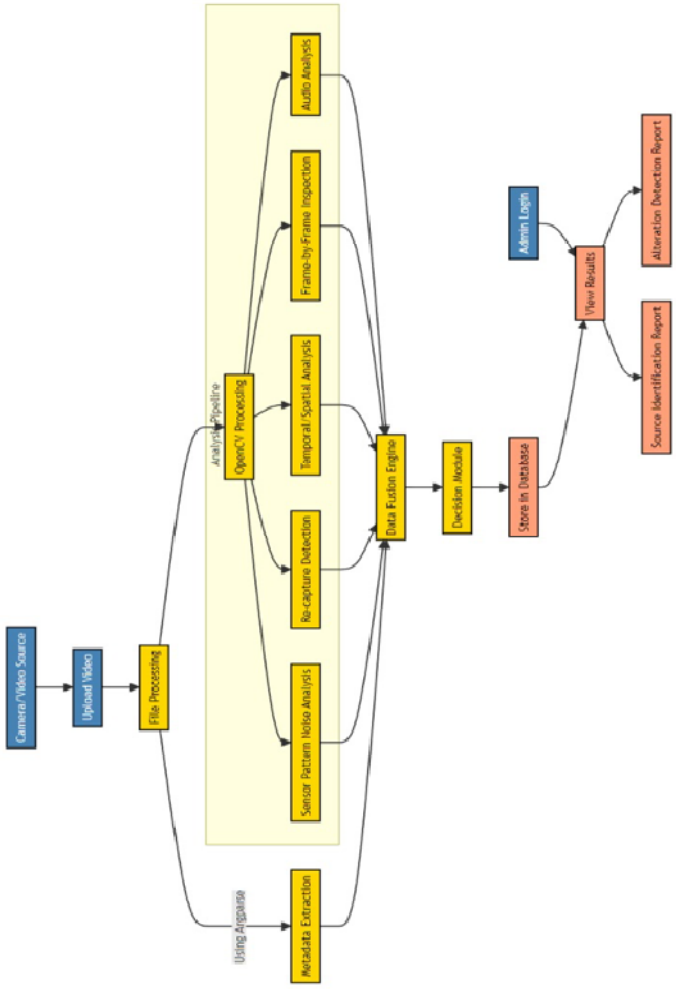


Figure 3: System Basic Flow

The architecture presents a pipeline for the system of Source Camera Identification and deepfake detection. The system takes input as videos and images from a camera source. This is then followed by file processing then, metadata extraction and another analysis pipeline. This core analysis pipeline leverages OpenCV and includes modules for noise pattern sensors for analysis, frame-by-frame inspections, spatial temporal inconsistencies. Each of the data feeds into the data fusion engine that integrates multimodal evidence to enhance decision accuracy.

V. METHODOLOGY

A. Source Camera Identification

The source camera identification model utilizes a 6-layer neural network that will identify and separate one image from other using PRNU. The vector input can be denoted as:

$$x \in \mathbb{R}^n$$

And each layer of the neural network performs linear transform and a non-linear function just after:

$$h_i = \sigma(W_i \, . \, h_i - 1 + b_i)$$

… (1)

With b_i and W_i being the weight of the matrix and σ being the activation function.
The final layer in the neural network applies the softmax function to produce a probability distribution over the number of camera classes given as:

$$\hat{y_j} = \frac{e^{2j}}{\sum_{k=1}^{K} e^{2k}} \text{ for } j = 1, 2, \ldots, K$$

... (2)

The categorical entropy loss can be given as of the network can be given as:

$$\mathscr{L} = -\sum_{j=1}^{K} y_j \log(\hat{y_j})$$

… (3)

with $y_j$which is true label encoded.
This CNN architecturewhich detects and identify the source not only detects the mobile device but also the embedded the camera of the mobile used to capture the image. The experiment for source camera identification is carried out using the images MICHE-I dataset.
The total number of trainable parameters used are: 813, 733

Layer (type)	Output Shape	Param #
Conv2d_1	(None, 62, 62, 32)	896
max_pooling2d_1	(None, 31, 31, 32)	0
Conv2d_2	(None, 29, 29, 32)	9248
max_pooling2d_2	(None, 14, 14, 32)	0
flatten_1	(None, 6272)	0
dense_1	(None, 128)	802944
dense_2	(None, 5)	645

Table 1: CNN Layers

B. Deepfake and forgery detection

For deepfake detection we have used the FaceForensics++ datasetand our own new dataset for training and testing of our model. The model employs a ResNet-50 architecture.ResNetutilizes residual connections to facilitate the training of deep networks.
In the training process:

1) *Data Preprocessing:* Videos are extracted in the form frames. On extraction normalization is applied to match the input with the pre-trained model requirements of the ResNet model.
2) *Feature extraction:*Frames extracted then undergoes a mapping process. As the data propogates through the network and post the final processing, a gloabal pooling layer condenses the spatial dimensions of the feature maps.
3) *Classification:* Now, as the features are fully extracted they are fed into the layer with the softmax function for the classifier to classify the input as real or deepfake.

The residual block of the model computes:

$$y = \mathcal{F}(x, \{\mathcal{W}_i\}) + x \quad \ldots (4)$$

Where $\mathcal{F}(x)$ is the residual mapping and x is the input to the block. And the final output for this is y.

The ResNet50 architecture is given below with # param = 25.0×10^6

Stage	Output	ResNet-50 (32x4d)
conv1	112 x 112	7 x 7, 64, stride 2
conv2	56 x 56	$\begin{bmatrix} 1\times1, 128 \\ 3\times3, 128, C=32 \\ 1\times1, 256 \end{bmatrix} \times 3$
conv3	28 x 28	$\begin{bmatrix} 1\times1, 256 \\ 3\times3, 256, C=32 \\ 1\times1, 512 \end{bmatrix} \times 4$
conv4	14 x 14	$\begin{bmatrix} 1\times1, 512 \\ 3\times3, 512, C=32 \\ 1\times1, 1024 \end{bmatrix} \times 6$
conv5	7 x 7	$\begin{bmatrix} 1\times1, 1024 \\ 3\times3, 1024, C=32 \\ 1\times1, 2048 \end{bmatrix} \times 3$
	1 x 1	Global average pool 1000-d fc, softmax

Table 2: ResNet-50 architecture

VI. RESULTS AND DISCUSSION

A table that describes the model accuracy with all camera models is given as:

Model Name	Sequence Strength	Accuracy
model_84_acc_10	10	84.376
model_87_acc_20	20	87.942
model_89_acc_40	40	89.389
model_91_acc_60	60	91.709
model_92_acc_80	80	92.552
model_93_acc_100	100	92.822

Table 3: Accuracies according to the sequence strength

Given the above are the accuracy of the deepfake detection model.
Similarly, the model for source camera identification the confusion matrixof experimentation is given as:

	Precision	Recall	f1-score	support
0.0	0.91	0.80	0.85	862
1.0	0.30	0.54	0.38	138
Accuracy			0.93	1000
Macro avg	0.61	0.67	0.62	1000
Weighted avg	0.83	0.76	0.79	1000

Table 4: Confusion Matrix for source camera identification

Screenshots of Implementation

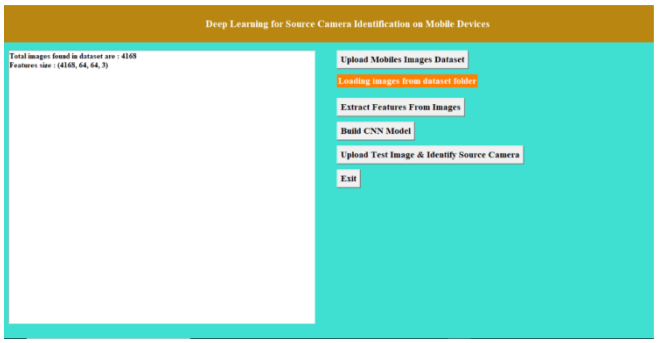


Figure 4: Implementation (dataset uploading)

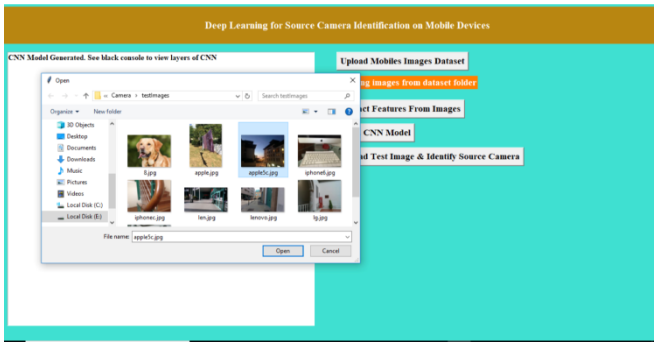


Figure 5: Implementation (Using test images)

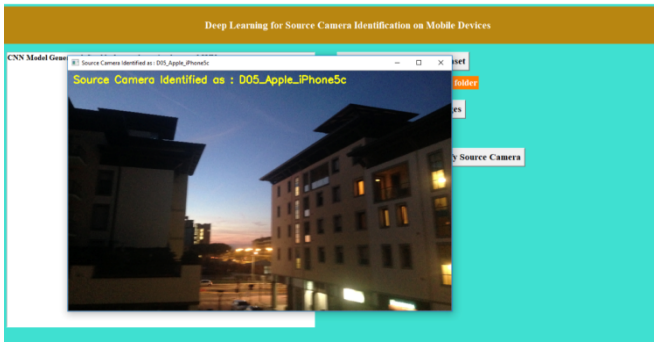


Figure 6: Implementation (Prediction)

This is the camera source identification part. Here we can see first you have to upload the images from the dataset, extract the feature, build CNN model and then upload test images and identify the source camera.

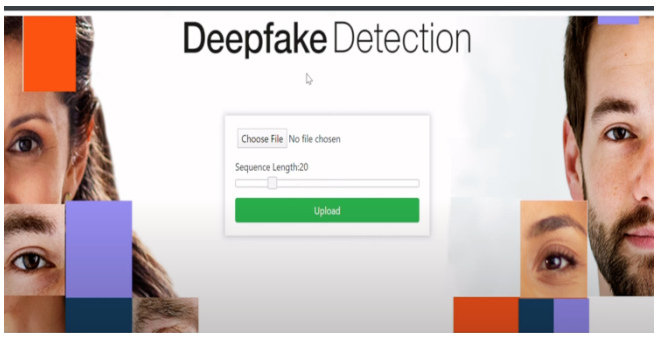


Figure 7: Deepfake Implementation

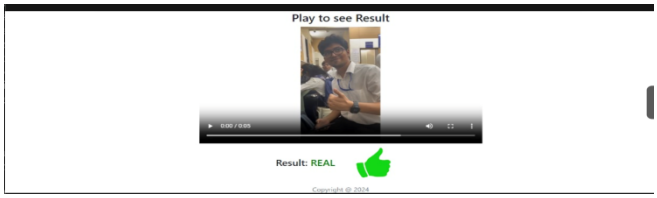


Figure 8: Prediction

Above given here is the deepfake detection part. When we upload our images, it asks for the sequence strength which is the total number frames we want our video to be distributed in, with that the video is processed and the features are extracted in the backend and the model gives out the output result with accuracy based on number of frames it is distributed.

VII. CONCLUSION

In this paper we successfully implement a deep learning application, for the source camera identification and deepfake detection of videos. This addresses the current challenges faced by the digital media authentication sector. Employing a CNN architecture for deepfake and source identification, the model accurately facilitates the information required.

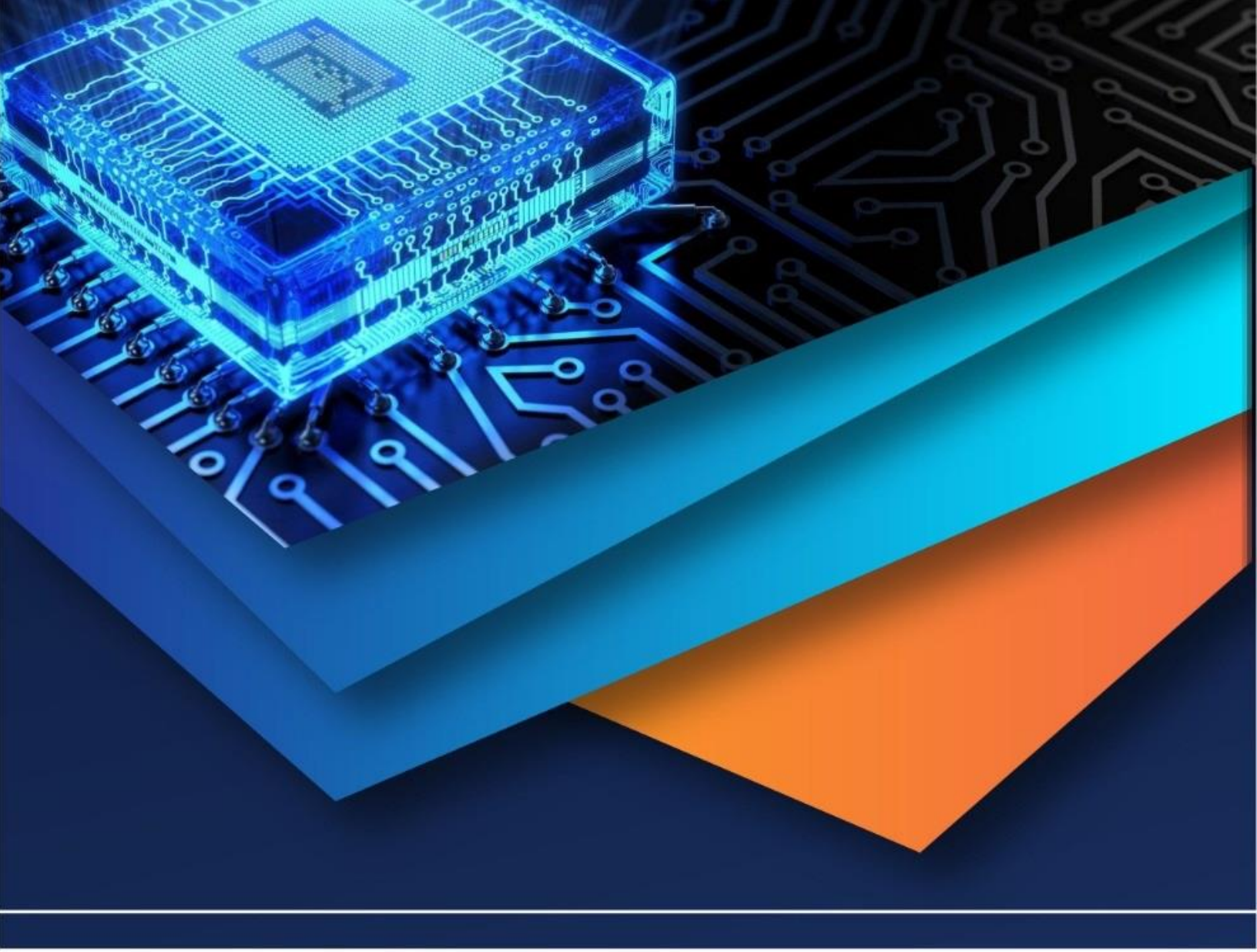
The highly efficient deepfake module leveraging ResNet-50 based on CNN architecture with accuracies within the range of 84% - 93% also helps in addressing the concern of subtle artifacts introduced during synthetic content generation. And source camera identification also based on CNN architecture giving the accuracy up to 93% plays a crucial role in forensic investigations, and provenance of digital content. The integration of these modules in a unified analytical pipeline enhances the system's reliability.

VIII. FUTURE WORK

Future enhancements may involve incorporating temporal analysis to better capture the inconsistencies and faults which slightly improves the accuracy of the model to detect deepfakes or forgeries. Using transformer-based architectures, can improve the overall performance and provide better accuracies in both source camera and deepfake identification models.

REFERENCES

[1] "Source Camera Attribution from Videos"- Husrev TahaSencar. Book series of Advances in Computer Vision and Pattern Recognition, 2022
[2] "Deepfake Detection"– Siwei Lyu. Book Series of Advances in Computer and Pattern Recognition, 2022
[3] "Source Camera Device Identification from Videos" – Guru Swaroop Bennabhaktula, Derrick Timmerman, Enrique Alegre, George Azzopardi. SN Computer Science Journal, 2022
[4] "A fast source camera identification and verification method based on PRNU analysis for use in video forensic investigations" – Wen-Chao Yang, JaijunJiang, Chung-Hao Chen. Multimedia Tools and Applications Journal, 2020
[5] " A Survey on Deepfake Video Detection" - Peipeng Yu, Zhihua Xia, Jianwei Fei, Yujiang Lu. IET Biometrics Journal, 2020
[6] "Recurrent Convolutional Structure for Audio Spoof and Video Deepfake Detection" – Akash Chintha, Bio Thai, Saniat Javid Sohrawardi, Kartavya Bhatt, Andrea Hickerson, Matthew Wright, Raymond Ptucha. IEEE Journal of Selected Topics in Signal Processing, Vol 14, No. 5, 2020
[7] "Deepfake Video Detection Using Transfer Learning Approach" – Shraddha Suratkar, Faruk Kazi. Arabian Journal for Science and Engineering, 2023
[8] "Real-Time Deepfake Video Detection Using Eye Movement Analysis with a Hybrid Deep Learning Approach" –Muhammab Javed, Zhaohui Zhang, Fida Hussain Dahri, Asif Ali Laghari. MDPI Electronics Journal 2024
[9] "Deepfake Video Forgery Detection" – Apurv Jindal. IRE Journals, Volume 6 Issue 12, 2023
[10] "Blind Source Camera Identification" –Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon. IEEE International Conference on Image Processing, 2004
[11] "Enhancing Source Camera Identification Performance With a Camera Reference Phase Sensor Pattern Noise" – Xiangui Kang, Yinxiang Li, Zhenhua Qu, Jiwu Huang. IEEE Transactions on Information Forensics and Security, Vol 7, No. 2, 2012
[12] "Identification of the Source Camera of Images Based on Convolutional Neural Network" – Na Huang, Jingsha He, Xinggang Xuan, Gongzheng Liu, Chengyue Chang. Journal of Digital Investigations, 2018
[13] "Deep learning for Source Camera Identification on mobile devices" – David Freire-Obregon, Fibo Narducci, Silvio Barra, Modesto Castrillon-Santana. Journal of Pattern Recognition Letters, 2018
[14] "Image Based Source Camera Identification using Demosaicking" – Yangjing Long, Yizhen Haung. IEEE International Conference on Image Processing, 2006
[15] "Source Camera Device Identification Based on Raw Images" – Tong Qiao, Florent Retraint, Remi Cogranne, Thanh Hai Thai. IEEE International Conference on Image Processing, 2015
[16] "Source Camera Identification Forensics Based on Wavelet Features" – Bo Wang, Yiping Guo, Xiangwei Kong, Fanjie Meng. Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009
[17] "Combining PRNU and noiseprint for robust and efficient device source identification" – Davide Cozzolino, Francesco Marra, Diego Gragnaniello, Giovanni Poggi, Luisa Verdoliva. EURASIP Journal on Information Security 2020



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)