IVFD: An Intelligent Video Forgery Detection Framework Leveraging InceptionV3 and GRU for Enhanced Forensics

Kumbham Bhargavi [1], M JAHIR PASHA[2], Rajitha Kotoju[3], M. Sree Vani[4]
[1]Associate Professor, Department of CSE, Keshav Memorial Institute of Technology, Hyderabad.
[2]Associate Professor, Department of Computer Science and Engineering (Data Science), Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal, Andhra Pradesh, INDIA.
[3]Assistant professor, Department of Computer Science and Engineering, Mahatma Gandhi Institute Of Technology, (MGIT), Hyderabad 500075, India.
[4]Professor, Department Of CSE, Bvrit Hyderabad College Of Engineering For Women, Hyderabad -500090

Article Info

Article history:

Received Nov 11, 2024
Revised Dec 26, 2024
Accepted Jan 9, 2025

Keyword:

Video Forgery Detection, Artificial Intelligence,
Deep Learning,
Hybrid Deep Learning,
Digital Forensics

ABSTRACT

Cloud computing-like services that are great at paying for and managing multimedia are fundamental technological innovations that have made it easier for individuals and organizations to adopt multimedia content. Thanks to social media, different people with different perspectives can voice their opinions and present data through photos and videos. However, video tampering is a significant issue because illegal modification of video content can easily mislead audiences and make it difficult for them to relate to reality. This is, therefore, a serious problem, as the consequences of video forgery are dire. Several image processing-based solutions have emerged to address video forgery. Artificial intelligence has recently allowed deep learning models to be trained extensively; hence, deep learning has been frequently used for video tampering detection. However, further work is still required to refine such models or develop hybrid models to improve the existing models' capabilities in identifying video forgeries and assisting digital forensics. We introduce a framework based on deep learning to automate the detection and localization of video forgeries. We offer a hybrid deep learning model that fuses Inception V3 with a Gated Recurrent Unit (GRU) as part of our framework. We also propose a new algorithm, Intelligent Video Forgery Detection (IVFD), to detect the forgeries and their invariants based on this hybrid model. Through empirical studies applied on a standard dataset, called the Deepfake Challenge dataset, we get an accuracy of 97.21%, which makes our hybrid deep learning model outperform many existing models. Since video content is prevalent in almost all applications in today's era, our design system should be laid on top of these applications, which can facilitate detecting the tampering of the videos and thereby contribute towards digital forensics.

Copyright © 2025 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Kumbham Bhargavi
Associate Professor, Department of CSE (AIML),
Keshav Memorial Institute of Technology, Hyderabad.
Email: bhargavikumbham@kmit.in

1. INTRODUCTION

Increased multimedia content usage is widespread today with the availability of distributed cloud computing and other storage infrastructures. The Multimedia content is in the form of Images, Videos, Text, Audio, etc. Due to the boom of numerous technologies, adversaries use image and video editing content to conduct illegal activities for different purposes. Hence, the authenticity of the multimedia content became a question mark. Widespread social problems are caused by deliberate misuse of multimedia content in many fields, and an automated method is required to detect such mischievous activities. Heuristic-based heuristic methods have traditionally been used in video tampering detection methods. Now that we have the big picture of artificial intelligence, with learning-based approaches, such as intense learning models, we have objects that can process or analyze content. They can find fake, altered, or modified content in videos.

Although considerable progress has been made in deep-learning-based video forgery detection, current methods perform unsatisfactorily on the effective fusion of spatial and temporal features. Self-supervised learning typically works very well with spatial data (required temporal dependencies), and traditional convolutional neural networks (CNNs) can be used to extract complex spatial patterns but cannot capture temporal dependencies (required to learn smooth representations). Thus, avoiding using complementary advantages of modern CNN architectures such as InceptionV3 for spatial feature extraction and sequential-based temporal for classification like GRU or LSTM is a key challenge in digital forensics. This paper proposes an effective video forgery detection using a hybrid deep learning framework based on IRRI20VEX InceptionV3 and GRU to overcome these shortcomings.

Several researchers have researched video tampering detection using various deep-learning models. We also fine-tuned hyperparameters that have recently improved on the pixel level to enhance performance gain for frame-level video anomaly detection (VAD)[1]. Worthy attempts have been accomplished in digital video forgery detection, especially concerning IoT and social media [2]. State-of-the-art watermarking techniques have been used in ensemble approaches and deep learning to enhance video content security against attackers [3]. To mitigate the threats posed by AI-generated content [4], algorithms for real-time deepfake detection have been developed. It has improved object detection while in motion through resilient hybrid deep neural networks [5]. CNN architectures have significantly improved computer vision through new design and optimization mechanisms [6]. Lastly, modern image and video forensics algorithms have defined reliable methods for detecting modified visual media assets [7]. The literature noted that digital forensics video forge red detection performance needs to be improved via deep learning models hybrid and patch-based combination.

More advanced forgeries — especially variations based on deepfake technology — pose a significant detection challenge, as deepfake technology can modify videos in particular ways. Enabling such deception is a generative model of sufficient sophistication. Notably, Generative Adversarial Networks (GANs), where tampered videos can now appear hyper-realistic, and key forged elements can be seamlessly incorporated into real-world footage. These forgeries are often less elaborate, where only the facial expressions are modified, the lip-sync is forged, or even background parts are modified, which can avoid detection by conventional techniques. High-fidelity face swaps, reenactments, and neural texture synthesis create forgeries with little to no artifacts, further complicating detection. Moreover, deepfake models are constantly advancing and improving at bypassing standard detection methods. To overcome these challenges, the models must identify spatial abnormalities, such as pixel-level distortions, and temporal anomalies, such as unnatural transitions or inconsistent motion patterns. From this perspective, the hybrid InceptionV3-GRU model performs best because it provides good spatial feature extraction and temporal sequence modeling capabilities to detect subtle inconsistencies that deepfake incorporates.

The contributions of this work are: we present a novel framework based on deep learning for automatic detection and localization of video forgeries. Within this framework, we present a deep learning hybrid model combining Inception V3 and Gated Recurrent Unit (GRU). We also propose a novel algorithm based on the hybrid deep learning model and our proposed framework, namely Intelligent Video Forgery Detection (IVFD), for detecting forgeries and their invariants with high accuracy. We conducted extensive experiments on a well-known benchmark dataset (the Deepfake Challenge). We showed that our hybrid deep learning model achieves state-of-the-art results with a maximum accuracy of 97.21%, outperforming many existing deepfake detectors. Since all of the stated applications, today have some essential video components, we need to establish how our proposed system can be employed in actual applications for video tampering detection and help in the progress of digital forensics. The remainder of the paper is organized as follows: Section 2 reviews the literature by discussing different existing methods based on deep learning models for video forgery detection. Section 3 describes the proposed approach, which includes the deep learning model framework and video forgery detection algorithm. In Section 4, we present the results of our empirical study; in Section 5, we discuss the related work of this paper and its limitations. We conclude our work in Section 6 and suggest some future work.

2. RELATED WORK

There are several existing deep-learning models used for video tampering detection. Dilek and Dener [1] improved frame-level video anomaly detection (VAD) performance by tweaking hyperparameters and improving pixel-level anomaly detection techniques. Shafai et al. [2] used to increase the efficacy of digital video forgery detection, particularly for IoT and social network data. Aberna and Agilandeeswari [3] concentrated on developing watermarking methods by investigating ensemble approaches and deep learning integration for increased security and resilience, particularly in video domains. Kaur et al. [4] focused on creating reliable real-time deepfake detection algorithms in light of the growing dangers of modified AI-generated material. Sahoo et al. [5] investigated the resilient hybrid deep neural networks to improve the MOD-CVS model for object detection in motion.

Zhao et al. [6] improved CNN architectures in computer vision, paying particular attention to creative designs, regularization, and activation optimization. Tyagi and Yadav [7] concentrated on creating reliable approaches for utilizing cutting-edge picture and video fraud detection algorithms to identify and separate altered visual assets. Himeur et al. [8] enhanced deep domain adaptation (DDA) and deep transfer learning (DTL) for video surveillance systems (VSSs). Ray et al. [9] concentrated on improving data quality and efficiency by extending transfer learning for vision-based human activity identification. Ramesh et al. [10] examined federated and spatio-temporal representation learning and concentrated on improving SSL techniques for surgical computer vision.

Pazho et al. [11] improved a cilia’s scalability and real-time intelligence monitoring capabilities while prioritizing privacy protection and ethical issues. Suralkar and Kazi et al. [12] concentrated on improving the recognition of phony videos by utilizing transfer learning in autoencoders and hybrid CNN-RNN models. Chen et al. [13] optimized edge-cloud collaboration for real-time object detection in intelligent video surveillance to increase productivity and handle latency-sensitive jobs. Donato et al. [14] emphasized predictive analytics and IoT sensor integration for fault identification and system efficiency gains. It focuses on developing deep-learning applications in railway maintenance. Zhou et al. [15] tackled video segmentation problems despite recent advances in deep learning, emphasizing improving models and datasets.

Ding et al. [16] improved a deep learning-based system to provide reliable detection and timely services for ECE forensics in 5G HetNets. Verdoliva et al. [17] developed automatic systems to identify corrupted media and deepfakes to prevent their use in election fraud and disinformation. Stoyanova et al. [18] addressed legal, privacy, and encryption issues, created standards and tools for safe Internet of Things forensics, and ensured the accurate gathering and storage of digital evidence. Parveen et al. [19] used clustering methods to speed up block matching to improve picture forgery identification. Jiao et al. [20] investigated video object detection and focused on redundant data and real-time processing efficiency.

Unlu et al. [21] improved autonomous drone surveillance through lightweight detection algorithms and practical dual-camera configurations for a broader range of video surveillance applications. Nawaratne et al. [22] improved anomaly detection by applying deep learning and active learning techniques and expanding real-time video surveillance using ISTL. Du et al. [23] intended to use DNN feedback to enhance bandwidth and accuracy while utilizing DDS to transform video streaming protocols. Song et al. [24] concentrated on improving vehicle detection accuracy for highway surveillance systems employing YOLOv3 and ORB. Sharma et al. [25] studied deep learning-based object identification. They will examine GAN-based detectors, video object detection, real-time remote sensing, multi-domain detection, salient object recognition, weakly supervised, unsupervised, and multi-task learning.

Table 1. Comparative analysis of existing video forgery detection approaches, their methodologies, datasets, and limitations

Approach	**Methodology**	**Dataset Used**	**Limitations**
Dilek and Dener [1]	Fine-tuning hyperparameters for pixel-level anomaly detection	Custom anomaly detection dataset	Limited scalability to large, diverse datasets; focused only on pixel-level anomalies.
Shafai et al. [2]	IoT and social network-based digital video forgery detection	IoT-specific datasets	Lack of generalizability to non-IoT domains; limited analysis of temporal features.
Kaur et al. [4]	Deepfake detection using real-time algorithms	Deepfake Detection Challenge Dataset	Ineffective for subtle manipulations in dynamic scenes; does not incorporate spatial patterns.
Aberna and Agilandeeswari [3]	Ensemble deep learning-based watermarking for video security	Custom watermarking datasets	Focused on security rather than forgery detection, it does not address dynamic temporal artifacts.
Tyagi and Yadav [7]	Traditional image and video forgery detection algorithms	General image forgery datasets	Limited performance on video forgery; no integration of temporal dependencies.
Proposed Hybrid Model	Combination of InceptionV3 for spatial features and GRU for temporal patterns	Deepfake Detection Challenge Dataset	Excels in integrating spatial and temporal features; achieves state-of-the-art accuracy (97.21%).

Oprea et al. [26] improved representation learning, and future work in deep learning-based video prediction will concentrate on enhancing loss functions, investigating novel architectures, and resolving stochasticity issues. Luo et al. [27] improved TSC for anomaly detection by improving similarity metrics, computational effectiveness, and increased dataset variety for a more comprehensive assessment. Chen et al. [28] involved maximizing the effectiveness of object recognition and tracking algorithms, such as YOLO V3 and SSD, on low-power devices. Pal et al. [29] concentrated on tackling granular computing difficulties by improving DL-based object recognition and tracking for various applications. Using deep learning, Mittal et al. [30] improved object recognition for low-altitude UAV datasets, emphasizing performance issues and enhancements.

Wu et al. [31] developed deep learning for object recognition, including using contextual information efficiently, producing proposals efficiently, and using AutoML and LVIS benchmarks. Johnston et al. [32] improved feature extraction from real videos to provide reliable video tampering technique detection. Zampoglou et al. [33] improved the quality of datasets using temporal annotations, improved annotation techniques, and investigated sophisticated voting algorithms for classification accuracy to improve video verification. Johnston and Elyan [34] utilized cutting-edge deep learning algorithms to address the quick growth of video tampering techniques, emphasizing universal detection and localization. Yang et al. [35] intended to maximize computational efficiency by streamlining the spatiotemporal trident network for improved tampering detection and localization accuracy.

Yang et al. [36] improved VTD-Net to maximize training stability and performance metrics for robust identification of adversarially created faces. Kaur and Jindal [37] developed DCNN-based techniques for effective inter-frame video tampering detection, emphasizing scalability and accuracy gains. Gu et al. [38] concentrated on improving VM power metering techniques, highlighting machine learning accuracy, and investigating topics such as power budgeting and energy-efficient scheduling. Costa et al. [39] for more accuracy and fewer false-positive rates while improving picture tampering detection utilizing cutting-edge machine learning algorithms. Ding et al. [40] increased visual quality and trick detectors by developing anti-forensics techniques for DeepFake films. The literature showed that deep learning models must be enhanced or hybridized to improve performance in video tampering detection. Traditional models of video forgery detection, such as CNN, LSTM, and ResNet50, are minimal. CNNs do well in extracting space features but cannot capture the temporal dependencies, essential for spotting discrepancies between frames in the video. LSTMs were built to model temporal sequences but are starkly lacking in capturing spatial information, like minor texture imperfections or edge artifacts in the frames. While ResNet50 is better at capturing spatial features with its deep residual layers, it is still limited in its capability to model time dependency. It does not suit sequential data like videos well. This underlines the importance of combining spatial and temporal analysis in a hybrid approach to overcome the limitation and enhance the efficacy of video forgery detection. Table 1 extensively compares the current literature on video forgery detection, encompassing the methods adopted, the crime/suspicious datasets employed, and their drawbacks. It shows where current models fall short (scalability, temporal-spatial, dataset diversity) and present proprietary, hybrid InceptionV3-GRU performances that set a new standard of excellence. Previous work that focused on video tampering detection relied on either CNNs (e.g., VGG16, ResNet50) [6], [10]– [12], or RNNs (e.g., LSTM) [7]– [9]. Still, they do not explicitly combine spatial feature extraction and temporal sequence modeling at each frame level. By combining InceptionV3 with GRU, our novel hybrid method addresses this key issue with an innovative end-to-end approach that leverages the complementary strengths of these architectures to capture fine-grained spatial features and temporal dependencies. It was asserted that this approach provides a broader detection mechanism to identify sophisticated manipulations, such as changes in facial expression and frame transitions, that traditional models overlook or do not accurately capture.

3. MATERIALS AND METHODS

This section provides more clear information regarding the deep learning-based framework, the proposed hybrid deep learning model, the underlying algorithm, dataset details, and how to evaluate the functionality of our methodology, enabling the identification of deep insights about the proposed approaches.

3.1. METHODS

Proposed an efficient video forgery detection using a deep learning model. Worry about the deep learning framework, as shown in Figure 1, which can process videos to detect forged content. The framework works by supervised learning to know something about the video and guess which portions have been tampered with. Preprocessing is done on the data we have. This step is crucial because in step here, the raw video data are evaluated, and based on the evaluation, the corrupted video part is either normalized or removed to give clean data for training the deep learning models. After preprocessing completion, we have to extract features (features Extraction) since we need features from the video to perform Video Tamper Detection (VT) more efficiently. The feature extraction phase is the most important as it can reduce dimensionality, thus helping to train better. We can now use features extracted from data to train the proposed hybrid deep learning model.

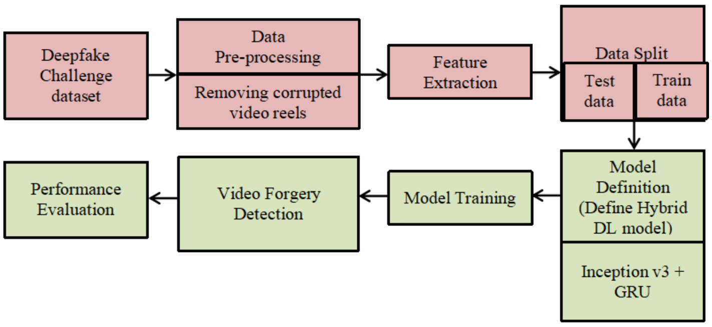

Figure 1. Proposed deep learning framework for video forgery detection

The dataset is split into two segments: training and testing sets. The training set is for training, while the test set is for testing the model when a forgery is detected. The testing data is samples without a class label, acting like unseen data, which is required to validate the performance of the proposed hybrid deep learning model. Once the model has been trained, it is saved on secondary storage and can be used in all required situations. The model is loaded into the main memory to detect video forgery, and forgeries in the supplied test video are identified. The hybrid deep learning model can also be tested on the test data, but more unlabeled samples are included in the test data. The reason for this is that the model's performance can only be assessed when we can measure the algorithm's predictions against the ground truth.

3.2. Hybrid Deep Learning Model

We then presented a hybrid deep learning model based on a GRU–-Inception V3 model that captures the given video frame's spatial and temporal features. We want to differentiate between what part of the video is forgery and what is original. In this component of the proposed model, the pre-trained model Inception V3 is used to get a better performance of this model. It is shown in heat map one in Figure 2 that it is structured to feed every video outline to highlight locally. Inception V3 — known for its multi-scale convolutional filters, can capture texture and edge-related features, even complex and abstract parts. It has a fundamental role in identifying the needed artifacts that help distinguish between true and fake content.) Also, transfer learning has been added, and it improves the model's performance. As a retrained model, it learned representations of different image features, enabling it to converge faster within the hybrid deep learning architecture.

Once spatial features have been extracted from video frames, the proposed hybrid deep learning model utilizes GRU to handle sequential data with temporal context, as this model can effectively learn temporal dependencies. A recurrent GRU neural network can store information across sequences, taking into account the time series aspect of data. It is an essential feature for understanding the video's content and identifying whether it is Real or Fake. GRU's temporal properties help identify unnatural transitions, changes in illumination, and differences in facial expressions, all of which might be difficult to catch. As the video frames are passed through the layers within the GRU network, it identifies patterns and learns details important to differentiate forged content from actual content.

InceptionV3 is a state-of-the-art convolutional neural network that has proven effective in extracting spatial features from images and video frames thanks to its one-dimensional multi-scale convolutional filters and optimized architecture. It retains detailed spatial information (edges, textures, and complex visual structures display high performance in detecting localized tampering in video frames. Conversely, GRU is a kind of recurrent last neural network that is excellent for sequentially modeled temporal dependencies. Unlike LSTM, which has complex gating mechanisms, its simpler architecture helps it to remember relevant information over time. Hence, inconsistencies (like unnatural lighting or transitions) can be found in the video. InceptionV3 and GRU have been used because they offer complementary advantages, i.e., while InceptionV3 extracts spatial features from an image, GRU creates a time-sequence from the vectors generated by InceptionV3, overcoming issues posed by standalone CNN or RNN model (CNN is good for extracting spatial features, and RNN which is good for sequential data). This hybrid method guarantees a thorough examination of video information, resulting in a much more effective forgery recognition capability in the case of dynamic footage, which is validated by the earlier work.

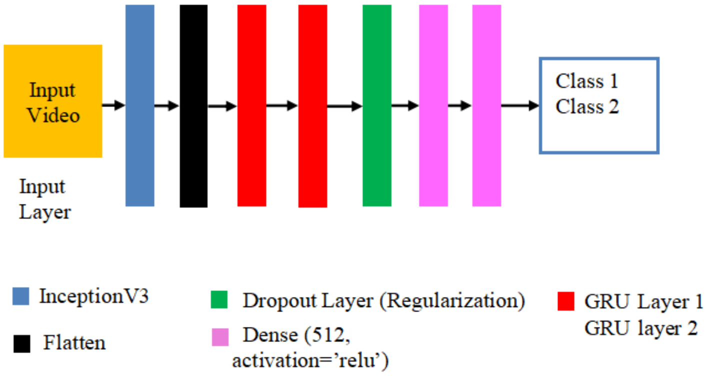

Figure 2. Proposed hybrid deep learning model for video forgery detection

In Figure 2, This hybrid deep learning architecture in GRU layers is motivated by the fact that every GRU layer produces some desired outputs that can be further fed into the next GRU layers. Such design enables the model to leverage low-level and high-level features in the temporal domain for better discrimination among video frames. Such a framework allows the hybrid deep learning model to learn the short- and long-term dependencies across video frames. To mitigate the overfitting challenge, the model applies an additional dropout layer. Based on the features extracted in the time domain, the hybrid model performs a decision that helps to differentiate between forgery and authentic content. Then, at the end of the model, some dense layers are added to better understand the temporal and spatial trends and make the trends multiplicated to achieve a more accurate solution. The last dense layer uses the Sigmoid with one neuron, deciding whether a video is forged. Hence, the model performs binary classification based on the test samples and their content in this step.

A novel hybrid deep learning model that can use state-of-the-art convolutional layers like Inception V3 and recurrent neural network layers to develop a system that can extract fine-grained features from videos. Inception V3 is one of the most popular pre-trained models that extract features from video data successfully. Due to its unique architecture, the complex patterns in the image content can be extracted for visualizations. It combines inception modules, and the functionality is finally concatenated. Global average pooling and normalization capability are helpful in the proposed hybrid deep learning model. In this hybrid model, the GRU part of LSTM architecture makes it suitable for sequential data with its layered structure. When integrated with Inception V3, the approach systematically acquires spatial and temporal characteristics, assuring more discernibility for video forgery detection.

3.3. Algorithm Design

We have an algorithm for Intelligent Video Forgery Detection(IVFD): an Automated AI-based forgery Detection in Videos Algorithm. That is, the algorithm is directed to identify such forgery types by means of the deep learning model or the hybrid deep learning model proposed in this paper. This method has been used in real-time video forensics since it can accurately detect video alterations.

Algorithm: Intelligent Video Forgery Detection (IVFD)
Input: Deepfake Detection Challenge dataset D
Output: Video forgery detection results R, performance statistics P

```
Begin
D'←Preprocessing(D)
(T1, T2, T3)←DataPreparation(D')
F←FeatureExtration(T1)
Configure hybrid DL model m
Compile m
m'←TrainTheModel(F, T1, m)
Persist m'
Load m'
F←FeatureExtraction(T2)
R←VideoForgeryDetection(m', F, T2)
P←FindPerformance(ground truth, R)
Print R
Print P
End
```

Algorithm 1. Intelligent Video Forgery Detection (IVFD)

In this paper, we propose Algorithm 1, which detects video forgeries automatically based on the hybrid model. It is a supervised algorithm that consists of two phases: the training data phase and the testing database. The hybrid deep learning model is trained over a training set during the training phase. This dataset is preprocessed, and features are extracted to improve the quality of the training process before training starts. Steps such as normalization and data cleaning are involved in Data Preprocessing. Data preprocessing helps get better data quality with clear formatting to prepare for machine learning. This step is an essential process since it increases the accuracy of the deep learning model. The dataset is split into three sets — the training set, the test set, and the validation set, respectively — used during different steps of the algorithm. Feature extraction is the step that allows you to find relevant features for choosing the class label and then arrange these in the form of a vector.

After the training, the hybrid DL model and the required compilation and training were configured. Later, the model that was trained is stored for modification and use. The saved model is loaded back into the memory and predicts the forgery in the given test videos during the testing phase. The ground truth vs. the predicted label by the algorithm tested is then used to software a confusion matrix for bees that forms the basis for evaluation once the algorithm is tested. The performance of a model is measured based on several metrics, such as loss and accuracy. Abstract: The provided algorithm uses a combined deep learning model approach to boost the detection performance of fakery videos. In real-world applications, this algorithm helps with digital forensics by revealing which sections of videos have been altered.

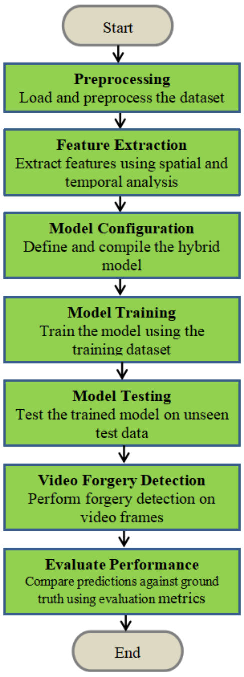
Start
Preprocessing
Load and preprocess the dataset
Feature Extraction
Extract features using spatial and temporal analysis
Model Configuration
Define and compile the hybrid model
Model Training
Train the model using the training dataset
Model Testing
Test the trained model on unseen test data
Video Forgery Detection
Perform forgery detection on video frames
Evaluate Performance
Compare predictions against ground truth using evaluation metrics
End

Figure 3. Flowchart of the intelligent video forgery detection (IVFD) algorithm

The layout of the step-by-step algorithm is illustrated in the flowchart shown in Figure 3. Data Pre-processing Before running the actual algorithm, raw video data is cleaned and normalized. This is further carried out in the spatial and temporal domain, and Features are extracted to make it easier. Using the preprocessed data, the hybrid deep learning model, which combines InceptionV3 and GRU, is defined, compiled, and trained. After training completion, the model is validated with new data to identify fake content within the processed video frame. Performance is measured by comparing the predictions to ground truths using metrics.

3.4. Dataset Details

The empirical study uses a Deepfake Detection Challenge dataset, as available in [41]. Description: A wide variety of real and fake video content designed for digital forensics research. An example of class imbalance is the set used in this research, the Deepfake Detection Challenge dataset, which has many more samples in one of the FAKE classes than the other class, the REAL class. An imbalance between both classes may result in a biased model, trained heavily on the majority class and thus decreasing the model's generalization. There are some techniques to solve this matter. One can use oversampling methods, like in the case of SMOTE, there are synthetic examples generated for the minority class that help in balancing the data. Also, also while training the model, you can give class weight to the minority class (high), so it will force the model to learn from these samples, and errors are penalized more. Moreover, we can apply data augmentation strategies. For example, we can flip, crop, or rotate a few frames in the "REAL" class and boost the diversity among the minority samples. Implementing these strategies can make the model more robust and better generalize unknown data.

3.5. Evaluation Methodology

Our method is evaluated using metrics based on the confusion matrix, as depicted in Figure 4 since we have used a learning-based approach (supervised learning).

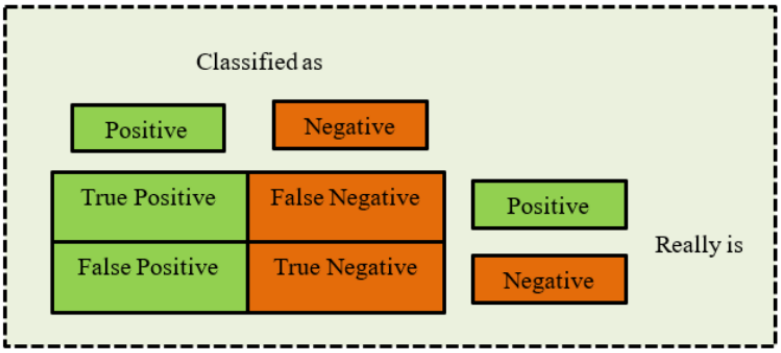

Figure 4. Confusion matrix

Based on the confusion matrix, the predicted labels of our method are compared with the ground truth to arrive at performance statistics. Eq. 1 to Eq. 4 express different metrics used in performance evaluation.

$$\text{Precision (p)} = \frac{TP}{TP+FP} \tag{1}$$

$$\text{Recall (r)} = \frac{TP}{TP+FN} \tag{2}$$

$$\text{F1-score} = 2 * \frac{(p * r)}{(p+r)} \tag{3}$$

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \tag{4}$$

The measures used for performance evaluation result in a value that lies between 0 and 1. These metrics are widely used in machine learning research.

4. EXPERIMENTAL RESULTS

This section presents the results of our empirical study using the proposed framework implementation, a hybrid deep learning model, and the underlying algorithm for the automatic detection of forgeries. Utilizing a benchmark dataset collected from [41], the experimental results demonstrate that our hybrid deep learning model outperforms many state-of-the-art deep learning models.

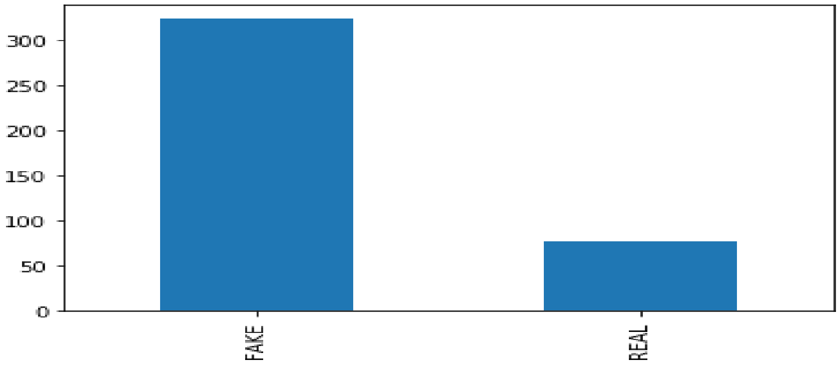

Figure 5. Data distribution dynamics in the dataset with fake and real videos

Figure 5 shows the dataset's distribution regarding two classes, "FAKE" and "REAL." Class designations are shown on the x-axis, and the number of instances in each class is shown on the y-axis. The class "FAKE" has a substantially greater count than "REAL," suggesting that the two classes in the dataset are out of balance.

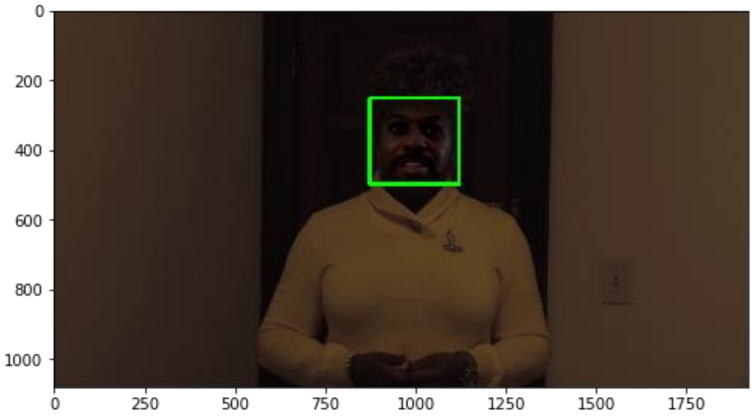

Figure 6. An actual video frame

As presented in Figure 6, A sample of the actual video frame is provided, while Figure 7 shows a sample of the tampered video frame.

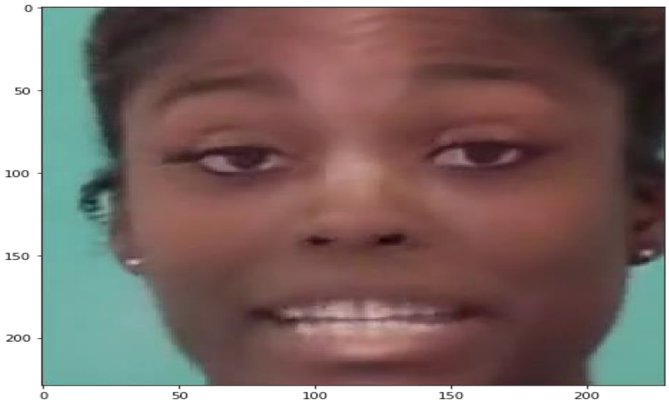

Figure 7. A tampered video frame

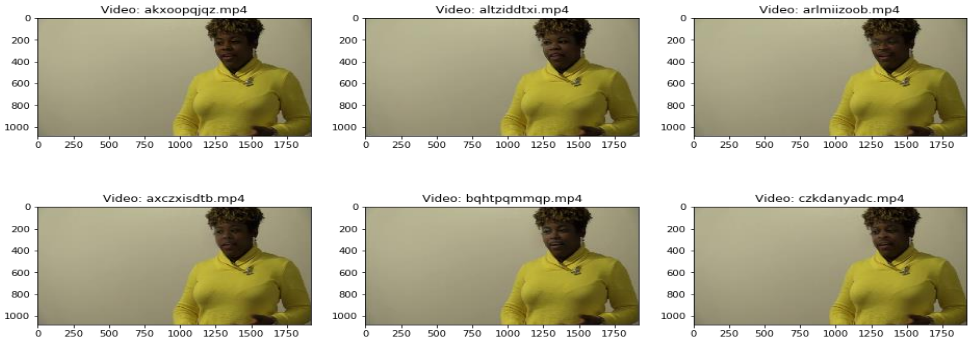

Figure 8. An excerpt of a sample of video frames in the dataset

Figure 8 shows an excerpt from a sample of video frames in the dataset. It has several video frames that form a video.

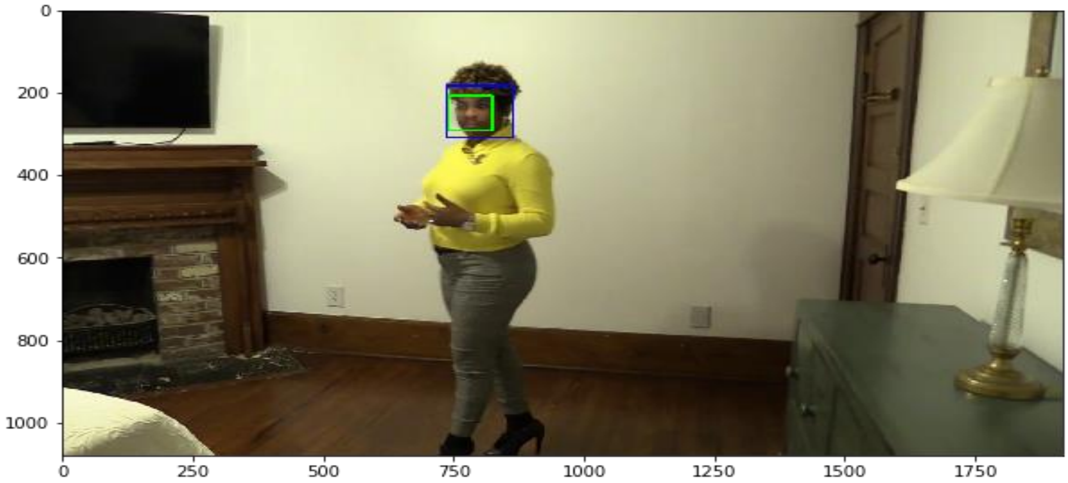

Figure 9. Tampering detection results using a hybrid deep learning technique

As presented in Figure 9, it is evident that the face portion of the person is detected as tampered with, and it is accurate as per the ground truth.

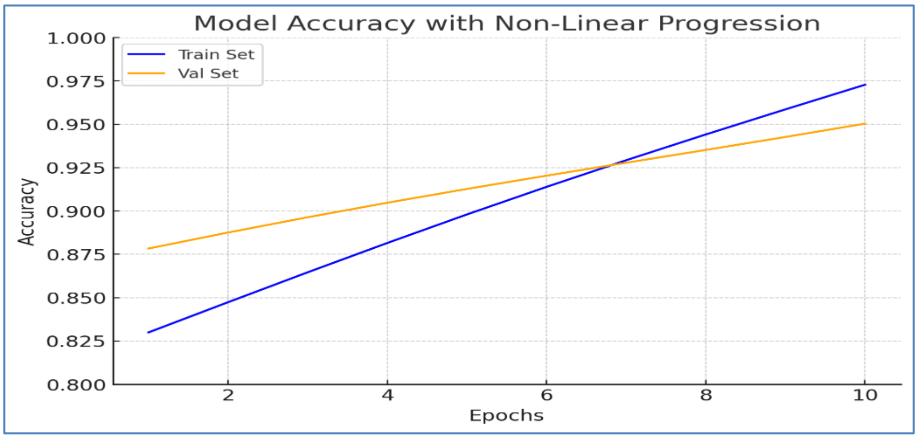

Figure 10. Accuracy of the deep learning model against several epochs

As presented in Figure 10, the proposed deep learning hybrid deep learning model accuracy in training and validation is visualized against several epochs until the convergence.

Table 2. Performance comparison among deep learning models in video forgery detection

Forgery Detection Model	Precision	Recall	F1 score	Accuracy
Baseline CNN	90.13	91.26	90.6	91.9
Baseline LSTM	76.32	76.21	75.83	76.32
VGG16	84.13	84.72	84.82	85.61
ReseNet50	83.57	83.66	83.06	83.71
Hybrid Model (InceptionV3+GRU) (Proposed)	96.51	96.3	97.26	97.21

Table 2 shows the performance of various deep learning models, including the proposed hybrid model for video forgery detection. The empirical observations were made using several performance metrics such as precision, recall, F1 score, and accuracy.

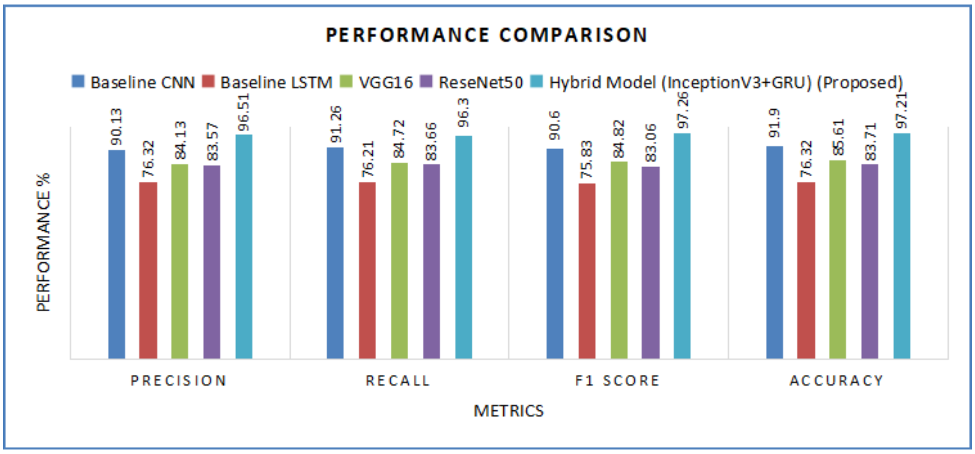

Figure 11. Performance comparison of different video forgery detection models

Figure 11 illustrates the performance comparison among all the deep learning models used for video forgery detection. The proposed methodology uses artificial intelligence, where the models learn from labeled data. These trained models then detect tampered video content, significantly improving video forensics. Regarding performance comparison, the baseline CNN model achieved a precision of 90.13%, the baseline LSTM reached 76.32%, the VGG16 model obtained a precision of 84.13%, and the ResNet50 model achieved 83.57%. The proposed hybrid model excelled, achieving an accuracy of 96.51%. Regarding recall, the baseline CNN achieved 91.26%, the baseline LSTM reached 76.21%, the VGG16 model obtained 84.72%, and the ResNet50 model achieved 83.66%. In contrast, the proposed hybrid model achieved an impressive recall rate of 96.3%. For the F1 score, the baseline CNN model achieved 90.6%, the baseline LSTM reached 75.83%, the VGG16 model obtained 84.82%, and the ResNet50 model achieved 83.06%. Again, the proposed hybrid model outperformed the others with an F1 score of 97.26%. Finally, regarding accuracy, the baseline CNN model reached 91.9%, the baseline LSTM achieved 76.32%, the VGG16 model obtained 85.61%, and the ResNet50 model achieved 83.71%. The proposed hybrid deep learning model exhibited the highest accuracy, 97.21%.

The proposed hybrid model achieves the best performance scores fortified through its incorporation of output layer of space and time-selected extraction mechanisms. InceptionV3, that includes multi-scale convolutional filters, is also better equipped for recognizing spatial features like edges, localized tampering, and textures in each individual video frame. This is followed by a Gated Recurrent Unit (GRU), a type of recurrent neural network, which learns temporal dependencies and thus can identify sequential inconsistencies (e.g., a sudden change in lighting, unnatural facial transitions, or mismatched expressions between frames). The two modeling architectures together give the hybrid model granular spatial analysis ability and temporal dependence modeling, addressing the potential limitations of either component in isolation. Furthermore, dropout layers and dense connections help to prevent overfitting, while transfer learning also enhances the model's ability to converge quickly on elaborate datasets. Empirical results show this combined interplay of InceptionV3 and GRU enables the hybrid model to surpass both baseline CNNs and RNNs, along with modern architectures such as ResNet50, to yield state-of-the-art metrics across precision, recall, F1-score, and accuracy.

Table 3. Comparative analysis of the proposed hybrid model with state-of-the-art video forgery detection models

Model	**Methodology**	**Dataset**	**Metrics**
Dilek and Dener [1]	Fine-tuning pixel-level anomaly detection	Custom dataset	Accuracy: 91.2%, F1-Score: 89.7%
Shafai et al. [2]	IoT and social network forgery detection	IoT-specific datasets	Accuracy: 87.5%, Precision: 86.8%, Recall: 85.3%
Kaur et al. [4]	Real-time deepfake detection	Deepfake Detection Challenge	Accuracy: 92.4%, Precision: 91.5%, F1-Score: 91.0%
Aberna and Agilandeeswari [3]	Ensemble DL-based watermarking	Custom watermarking dataset	Accuracy: 88.6%, Recall: 87.4%, F1-Score: 87.9%
Proposed Hybrid Model (InceptionV3 + GRU)	Hybrid spatial-temporal feature extraction	Deepfake Detection Challenge	Accuracy: **97.21%**, Precision: **96.51%**, F1-Score: **97.26%**

Table 3 compares the performance of the proposed hybrid model (InceptionV3 + GRU) with the existing video forgery detection models mentioned in the literature. It compares cross-methodologies and datasets with significant performance metrics such as accuracy, precision, and F1 score. The proposed model achieves the maximum performance metrics of 97.21% in accuracy and 97.26% in the F1 score, beating the others. As a result, the hybrid model is likely more powerful than other models because it deals with both spatial inconsistency and temporal inconsistency, which allows the hybrid model to work most efficiently when detecting advanced deepfake edits, which would serve to influence the field of video forensics and other similar areas of study.

5. DISCUSSION

As cloud infrastructure and the related ecosystem have emerged, there has been an unprecedented rise in the adoption of multimedia content by individuals and organizations. The third reason is that the multimedia objects can be administered cheaply whilst hosted in the cloud. On the other hand, social media applications where people of all classes share images and video forms of information offer room for adversaries to manipulate such content, which may cause severe social problems for the publishers of the multimedia content. The prevalence of video content in our digital lives has made video forgery or tampering a real and urgent issue to tackle. Multimedia objects are modified and misused for various gains. Thus, it is necessary to develop techniques that can automatically identify preserved video contents related to digital forensics that have been tampered with. In today's world, video forensics is a golden source for detecting the forgery in videos, which helps in exact reality measurement and preserving the social order. In this paper, we propose a video forgery detection system using Artificial Intelligence based on InceptionV3 and GRU hybrid model for video forgery detection. This is the reason for improving these deep learning models, as current deep learning models can interpret multimedia content; however, there is still a need to improve how to visualize and examine the issue. We have carefully combined existing models to create our hybrid model, which can efficiently detect forgeries in videos, and we believe that our proposed system can outperform the existing models. Nevertheless, the proposed system does have limitations, as outlined in Section 5.1.

5.1. Limitations

The limitations of the proposed system for video forgery detection are highlighted in Table 8. While the hybrid model proposed here can offer performance superiority, training data is limited over existing players. Hopefully, the system needs to generalize its findings and requires more datasets. Besides, the number of samples is not so high, so the system has to work with small sample sizes. We can improve this by utilizing GAN architectures and providing higher-quality training videos.

6. CONCLUSION AND FUTURE WORK

This paper proposes a deep learning-based framework for automatically detecting and localizing video forgeries. Our framework proposes a hybrid deep learning model integrating Inception V3 and Gated Recurrent Units (GRU). Integrating InceptionV3, which can capture complex spatial features, and GRU, which can model temporal dependencies, results in a model that achieves an accuracy of 97.21%, more significant than other existing models. This is an important step forward in digital forensics, where ensuring the authenticity of video data is crucial. Outside digital forensics, the hybrid model has much promise in social media content moderation, legal evidence verification, and cyber security, where there is an ever-increasing need to identify multimedia that has been manipulated. The proposed framework meets this need by providing dynamic video forgery detection solutions as tampering techniques like deepfakes evolve. In our future work, we will employ generative adversarial networks along with some other datasets in the same model to improve the generalization of our model, making it applicable to a broader range of domains. This work constitutes a significant step towards detecting forgery in videos, setting the stage for future works to lead to practical adoption.

REFERENCES

[1] ESMA DİLEK AND MURAT DENER. (2024). Enhancement of Video Anomaly Detection Performance Using Transfer Learning and Fine-Tuning. *IEEE*. 12, pp.73304 - 73322. http://DOI:10.1109/ACCESS.2024.3404553

[2] Walid El Shafai, Mona A. Fouda, El Sayed M. El Rabaie, and Nariman Abd El Salam. (2024). A comprehensive taxonomy on multimedia video forgery detection techniques: challenges and novel trends. *Springer*. 83, p.4241–4307. https://doi.org/10.1007/s11042-023-15609-1

[3] P. Aberna and L. Agilandeeswari. (2024). Digital image and video watermarking: methodologies, attacks, applications, and future directions. *Springer*. 83, pp.1-61. https://doi.org/10.1007/s11042-023-15806-y

[4] Achhardeep Kaur, Azadeh Noori Hoshyar, Vidya Saikrishna, Selena Firmin and Feng. (2024). Deepfake video detection: challenges and opportunities. *Springer*. 59(159), pp.1-47. https://doi.org/10.1007/s10462-024-10810-6

[5] PRABODH KUMAR SAHOO, MANOJ KUMAR PANDA, UPASANA PANIGRAHI, GANAPATI PANDA, PRINCE JAIN, MD. SHABIUL ISLAM, AND MOHAMMAD TARIQUL ISLAM. (2024). An Improved VGG-19 Network Induced Enhanced Feature Pooling for Precise Moving Object Detection in Complex Video Scenes. *IEEE*. 12, pp.45847 - 45864. http://DOI:10.1109/ACCESS.2024.3381612

[6] Xia Zhao, Limin Wang, Yufei Zhang, Xuming Han, Muhammet Deveci, Milan Parmar. (2024). A review of convolutional neural networks in computer vision. *Springer*. 57(99), pp.1-43. https://doi.org/10.1007/s10462-024-10721-6

[7] Shobhit Tyagi, and Divakar Yadav. (2021). A detailed analysis of image and video forgery detection techniques. *Springer*. 39, pp.1-21. https://doi.org/10.1007/s00371-021-02347-4

[8] Yassine Himeur, Somaya Al-Maadeed, Hamza Kheddar, Noor Al-Maadeed, Khalid Abualsaud, Amr Mohamed, and Tamer Khattab. (2023). Video surveillance using deep transfer learning and deep domain adaptation: Towards better generalization. *Elsevier*. 119, pp.1-34. https://doi.org/10.1016/j.engappai.2022.105698

[9] Abhisek Ray, Maheshkumar H. Kolekar, R. Balasubramanian, and Adel Hafiane. (2023). Transfer Learning Enhanced Vision-based Human Activity Recognition: A Decade-long Analysis. *Elsevier*. 3(1), pp.1-15. https://doi.org/10.1016/j.jjimei.2022.100142

[10] Sanat Ramesh, Vinkle Srivastav, Deepak Alapatt, Tong Yu, Aditya Murali, Luca Sestini, Chinedu Innocent Nwoye, Idris Hamoud, Saurav Sharma, Antoine Fleurentin, Georgios Exarchakis, Alexandros Karargyris, and Nicolas Padoy. (2023). Dissecting self-supervised learning methods for surgical computer vision. *Elsevier*. 88, pp.1-19. https://doi.org/10.1016/j.media.2023.102844

[11] Armin Danesh Pazho, Christopher Neff, Ghazal Alinezhad Noghre, Babak Rahimi Ardabili, Shanle Yao, Mohammadreza Baharani, and Hamed Tabkhi. (2023). Ancilia: Scalable Intelligent Video Surveillance for the Artificial Intelligence of Things. *IEEE*. 10(17), pp.14940 - 14951. http://DOI:10.1109/JIOT.2023.3263725

[12] Shraddha Suratkar, and Faruk Kazi. (2023). Deep Fake Video Detection Using Transfer Learning Approach. *Springer*. 48, p.9727–9737. https://doi.org/10.1007/s13369-022-07321-3

[13] YUNG-YAO CHEN, YU-HSIU LIN, YU-CHEN HU, CHIH-HSIEN HSIA, YI-AN LIAN, AND SIN-YE JHONG. (2022). Distributed Real-Time Object Detection Based on Edge-Cloud Collaboration for Smart Video Surveillance Applications. *IEEE*. 10, pp.93745 - 93759. http://DOI:10.1109/ACCESS.2022.3203053

[14] LORENZO DE DONATO, FRANCESCO FLAMMINI, STEFANO MARRONE, CLAUDIO MAZZARIELLO, ROBERTO NARDONE, CARLO SANSONE, AND VALERIA VITTORINI. (2022). A Survey on Audio-Video Based Defect Detection Through Deep Learning in Railway Maintenance. *IEEE*. 10, pp.65376 - 65400. http://DOI:10.1109/ACCESS.2022.3183102

[15] Tianfei Zhou, Fatih Porikli, David J. Crandall, Luc Van Gool, Wenguan Wang. (2022). A Survey on Deep Learning Technique for Video Segmentation. *IEEE*. 45(6), pp.7099 - 7122. http://DOI:10.1109/TPAMI.2022.3225573

[16] Feng Ding; Guopu Zhu; Mamoun Alazab; Xiangjun Li and Keping Yu;. (2022). Deep-Learning-Empowered Digital Forensics for Edge Consumer Electronics in 5G HetNets. IEEE Consumer Electronics Magazine, pp.1-6. http://doi:10.1109/mce.2020.3047606

[17] Verdoliva, Luisa. (2020). Media Forensics and DeepFakes: an overview. IEEE Journal of Selected Topics in Signal Processing, 14(5), pp.1-24. http://doi:10.1109/JSTSP.2020.3002101

[18] Stoyanova, Maria; Nikoloudakis, Yannis; Panagiotakis, Spyridon; Pallis, Evangelos and Markakis, Evangelos K. . (2020). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues. IEEE Communications Surveys & Tutorials, 22(2), 1–38. http://doi:10.1109/COMST.2019.2962586

[19] Parveen, Azra; Khan, Zishan Husain and Ahmad, Syed Naseem . (2019). Block-based copy–move image forgery detection using DCT. Iran Journal of Computer Science, 2, pp.1-11. http://doi:10.1007/s42044-019-00029-y

[20] Licheng Jiao; Ruohan Zhang; Fang Liu; Shuyuan Yang; Biao Hou; Lingling Li and Xu Tang;. (2021). New Generation Deep Learning for Video Object Detection: A Survey . IEEE Transactions on Neural Networks and Learning Systems, 33(8), pp.1-21. http://doi:10.1109/tnnls.2021.3053249

[21] Unlu, Eren; Zenou, Emmanuel; Riviere, Nicolas and Dupouy, Paul-Edouard . (2019). Deep learning-based strategies for the detection and tracking of drones using several cameras. IPSJ Transactions on Computer Vision and Applications, 11(1), pp.1-13. http://doi:10.1186/s41074-019-0059-x 4

[22] Rashmika Nawaratne, Damminda Alahakoon, Daswin De Silva, and Xinghuo Yu. (2019). Spatiotemporal Anomaly Detection Using Deep Learning for Real-Time Video Surveillance. *IEEE*. 16(1), pp.393 - 402. http://DOI:10.1109/TII.2019.2938527

[23] Kuntai Du; Ahsan Pervaiz; Xin Yuan; Aakanksha Chowdhery; Qizheng Zhang; Henry Hoffmann; and Junchen Jiang;. (2020). Server-Driven Video Streaming for Deep Learning Inference . Proceedings of the Annual conference of the ACM Special Interest Group on Data Communication on the applications, technologies, architectures, and protocols for computer communication, pp. 557 - 570. http://doi:10.1145/3387514.3405887

[24] Song, Huansheng; Liang, Haoxiang; Li, Huaiyu; Dai, Zhe; Yun, Xu . (2019). Vision-based vehicle detection and counting system using deep learning in highway scenes. European Transport Research Review, 11(51), pp.1-16. http://doi:10.1186/s12544-019-0390-4

[25] Sharma, Vipul and Mir, Roohie Naaz. (2020). A comprehensive and systematic look up into deep learning based object detection techniques: A review. Computer Science Review, 38, pp. 1-29. http://doi:10.1016/j.cosrev.2020.100301

[26] Sergiu Oprea; Pablo Martinez-Gonzalez; Alberto Garcia-Garcia; John Alejandro Castro-Vargas; Sergio Orts-Escolano; Jose Garcia-Rodriguez and Antonis Argyros;. (2020). A Review on Deep Learning Techniques for Video Prediction . IEEE Transactions on Pattern Analysis and Machine Intelligence, 44(6), pp.1-20. Http://doi:10.1109/tpami.2020.3045007

[27] Weixin Luo, Wen Liu, Dongze Lian, Jinhui Tang, Lixin Duan, Xi Peng, and Shenghua Gao. (2019). Video Anomaly Detection with Sparse Coding Inspired Deep Neural Networks. *IEEE*. 43(3), pp.1070 - 1084. http://DOI:10.1109/TPAMI.2019.2944377

[28] Chen, Zhihao; Khemmar, Redouane; Decoux, Benoit; Atahouet, Amphani and Ertaud, Jean-Yves . (2019). Real Time Object Detection, Tracking, and Distance and Motion Estimation based on Deep Learning: Application to Smart Mobility, pp.1–6. http://doi:10.1109/EST.2019.8806222

[29] Sankar K. Pal; Anima Pramanik; J. Maiti and Pabitra Mitra;. (2021). Deep learning in multi-object detection and tracking: state of the art. Applied Intelligence, 51, pp.1-30. http://doi:10.1007/s10489-021-02293-7

[30] Mittal, Payal; Sharma, Akashdeep and Singh, Raman. (2020). Deep learning-based object detection in low-altitude UAV datasets: A survey. Image and Vision Computing, 104, pp.1-24. http://doi:10.1016/j.imavis.2020.104046

[31] Wu, Xiongwei; Sahoo, Doyen and Hoi, Steven C.H. . (2020). Recent Advances in Deep Learning for Object Detection. Neurocomputing, 396, pp.39-64. http://doi:10.1016/j.neucom.2020.01.085

[32] Johnston, Pamela; Elyan, Eyad and Jayne, Chrisina . (2019). Video tampering localisation using features learned from authentic content. Neural Computing and Applications, 32, pp.1-15. http://doi:10.1007/s00521-019-04272-z

[33] Kompatsiaris, Ioannis; Huet, Benoit; Mezaris, Vasileios; Gurrin, Cathal; Cheng, Wen-Huang and Vrochidis, Stefanos . (2019). Detecting Tampered Videos with Multimedia Forensics and Deep Learning. ,pp.374–386. http://doi:10.1007/978-3-030-05710-7_31

[34] Johnston, Pamela and Elyan, Eyad. (2019). A review of digital video tampering: From simple editing to full synthesis. Digital Investigation, 29, pp.67–81. http://doi:10.1016/j.diin.2019.03.006

[35] Quanxin Yang; Dongjin Yu; Zhuxi Zhang; Ye Yao and Linqiang Chen;. (2021). Spatiotemporal Trident Networks: Detection and Localization of Object Removal Tampering in Video Passive Forensics . IEEE Transactions on Circuits and Systems for Video Technology, 31(10). Pp.1-14 http://doi:10.1109/tcsvt.2020.3046240

[36] Yang, Tongfeng; Wu, Jian; Liu, Lihua; Chang, Xu and Feng, Guorui . (2020). VTD-Net: Depth Face Forgery Oriented Video Tampering Detection based on Convolutional Neural Network. pp.7247–7251. http://doi:10.23919/CCC50068.2020.9188580

[37] Kaur, Harpreet; Jindal, Neeru . (2020). Deep Convolutional Neural Network for Graphics Forgery Detection in Video. Wireless Personal Communications, 112, pp.1-19. http://doi:10.1007/s11277-020-07126-3

[38] Bui, Tu; Thereaux, Olivier; Cooper, Daniel; Collomosse, John; Bell, Mark; Green, Alex; Sheridan, John; Higgins, Jez; Das, Arindra and Keller, Jared Robert . (2020). Tamper-proofing Video with Hierarchical Attention Autoencoder Hashing on Blockchain. IEEE Transactions on Multimedia, 22(11), 1–11. http://doi:10.1109/TMM.2020.2967640

[39] da Costa, Kelton A.P.; Papa, JoÃ£o P.; Passos, Leandro A.; Colombo, Danilo; Ser, Javier Del; Muhammad, Khan and de Albuquerque, Victor Hugo C. . (2020). A critical literature survey and prospects on tampering and anomaly detection in image data. Applied Soft Computing, 97, pp.1-15. http://doi:10.1016/j.asoc.2020.106727

[40] Feng Ding; Guopu Zhu; Yingcan Li; Xinpeng Zhang; Pradeep K Atrey and Siwei Lyu;. (2021). Anti-Forensics for Face Swapping Videos via Adversarial Training. IEEE Transactions on Multimedia, 24, pp.1-13. http://doi:10.1109/tmm.2021.3098422

[41] Deepfake Detection Challenge Dataset. Retrieved from https://www.kaggle.com/code/kuldeepprasadds321/fake-video-image-detection/input

BIOGRAPHY OF AUTHORS

Dr. K. Bhargavi, Associate Professor at Keshav Memorial Institute of Technology(KMIT), Hyderabad, Telangana. She has done her doctorate in Soft Computing Techniques from Sri Padmavathi Mahila Viswa Vidyalayam (SPMVV), WOMEN'S UNIVERSITY, TIRUPATI and M.Tech from *Acharya Nagarjuna University. She* is having 23 years of teaching experience. Her areas of interest are Soft Computing, Image Processing, Artificial Intelligence and Computer Vision. She has published more than 15 research papers in reputed International and National Journals. She has presented papers at various National and International Conferences.

Dr M JAHIR PASHA is the Associate professor of Computer Science and Engineering (Data Science) at Rajeev Gandhi Memorial College of Engineering & Technology. He is a researcher in software Engineering and an educator specializing in Computer Science and Engineering. He is also interested in Machine learning in interdisciplinary research. Dr M Jahir Pasha received his Ph.D. degree in Computer Science and Engineering from JAIN University, Bangalore, India. He has a total of 15 years of experience in academics. He published over 35 research papers and he is the member of IEEE.

Dr. Rajitha Kotoju possesses over 15+ years of teaching experience. She obtained her Ph.D. in Computer Science and Engineering from JNTUH, Hyderabad, in 2022, and her M. Tech in the same discipline from JNTUH, Hyderabad, in 2009. Dr. Rajitha Kotoju has disseminated her research through numerous publications in high-impact national and international journals. Additionally, she has engaged in a multitude of workshops and symposia, presenting her research findings at various prestigious conferences globally.

Her instructional expertise encompasses a broad spectrum of subjects, including Computer Networks, Unix Programming, Network Programming, Operating Systems, Data Warehousing and Data Mining, Programming for Problem Solving, Python Programming, Web Technologies, and Database Security. Dr. Rajitha Kotoju's research interests are multifaceted, with a focus on Machine Learning, Data Mining, Big Data Analytics, Computer Networks, Information Retrieval Systems, and Database Management Systems.

Dr. M. Sree Vani, Professor, Dept of CSE, BVRITH, Hyderabad. An academician with 20 years of extensive teaching and demonstration experience with excellent communication skills Implementing creative teaching methodologies using available audio/video tools, subjective blogs, email threads, web boards, formula cards, e-calendars and discussion forums Practising research and innovation, reaping the benefits from internet communications tools and open source tools/technologies. Distinction of handling AICTE sponsoring project(s) and various management activities (encompassing project proposals, proof of concept implementation, pilot releases, resource planning, time scheduling, task allocation and technology management) Exposure in setting up CSE/CSIT Department infrastructure development, operations, processes and support activities. Supervised major BTech/MTech projects, Key reviewer of Cognitive science research initiative (CSRI) proposals Guiding one Ph.D Student at present.