Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: *https://doi.org/10.5281/zenodo.19148612* **JSTE-14**

ADVANCING VIDEO FORGERY DETECTION VIA DEEP CONVOLUTIONAL NEURAL NETWORKS

[#1]T. ANUSHA, *Assistant Professor,*
[#2]S. MANASA, *Assistant Professor,*
[#3]K. KAVYA, *Assistant Professor,*
[#4]K. SHARANYA, *Assistant Professor,*
Department of Computer Science And Engineering,
TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TG.

ABSTRACT: The increasing sophistication of editing technologies has raised concerns about video forgeries and their potential impact on digital forensics, media integrity, and security. It is a challenging task as tiny changes are so difficult to identify with traditional detection techniques. This paper's main objective is to investigate how Deep Convolutional Neural Networks (DCNN) might enhance the detection of video counterfeiting. The suggested model can identify instances of deepfake alterations, splicing, and frame tampering with an impressive level of accuracy according to deep learning techniques. The trials' findings suggest that deep convolutional neural networks (DCNN) perform better than more conventional methods, which may make them useful in forensic investigations.

Keywords: Video forgery detection, Deep Convolutional Neural Networks, Deep learning, Frame tampering, Digital forensics, Deepfake detection.

1. INTRODUCTION

The lightning-fast development of digital technology has made it far easier to create synthetic content that passes for genuine film. Splicing, deepfakes, and frame insertion are all forms of video fabrication. Media integrity, digital forensics, and cybersecurity are just a few areas that might be affected by this sort of video counterfeiting. Manual examination and conventional forensic methodology are two examples of antiquated methods that may fail to identify video frauds. Both approaches are similar in that they are rigid and dependent on features that have been manually generated. Complex changes are beyond the capabilities of the procedures outlined above. This is because the procedures in question are dependent on tangible qualities.

One deep learning technology that has recently gained traction in improving video fraud detection is Deep Convolutional Neural Networks (DCNN). The capacity of deep convolutional neural networks (DCNNs) to understand complicated video patterns and abnormalities enables automated and remarkably accurate counterfeit detection. Scientists in academia have used deep learning architectures to train models that can detect subtle changes in sound. Many differences have been pointed up, such as peculiar patterns of movement, unusual coloration, and deepfake artifacts.

This study aims to improve video counterfeiting detection using a deep convolutional neural network (DCNN) by enhancing feature extraction and classification approaches. The accuracy and robustness of the detection are enhanced by training the proposed model on huge datasets that contain both original and changed films. By doing so, the model is able to

ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: *https://doi.org/10.5281/zenodo.19148612* **JSTE-14**

enhance its detection capabilities. As a result, forensic techniques for material authentication were improved. The security of data transmitted through video-based systems can be enhanced with these methods.

2. LITERATURE REVIEW

Nitin Arvind Shelke and Singara Singh Kasana. (2024) Kernel Principal Component Analysis (KPCA) and an enhanced VGG-16 deep neural network are employed by the writers to identify forgeries. This approach is being touted as a way to identify frauds. In order to detect cases of forgeries, the method employs correlation analysis and visual data collected from specific video frames. Even after undergoing post-processing procedures such as noise addition and brightness, contrast, and tint adjustments, the method proves to be quite accurate and precise in detecting forgeries.

Upasana Singh et al. (2024) In order to offer a new perspective on the matter, this work primarily focuses on identifying digital cinema multilayer forgeries. AACNNs, or attention-augmented convolutional neural networks, are one way to get complicated data out of simulated frames. In addition, the system accurately and reliably detects forgeries at two and three layers using a U-Net-based CycleGAN for newly generated section detection.

Shaik Irfan et al. (2024) Presenting a deep learning system that detects instances of video authenticity using sequential and patch analysis is the purpose of this study. Using a model of normal and aberrant regions and video sequences, the approach locates and detects tampering. The system can then identify and pinpoint instances of manipulation because of this. The validity of video content has been successfully confirmed using this method.

Shreyan Ganguly et al. (2023) The writing team introduces a "mini-Graph Convolutional Network" (miniGCN). In order to detect changes in the areas of the face depicted in films, this network employs graph neural networks. Converting face frames into visual embeddings, evaluating those embeddings with the miniGCN framework, and finally using MTCNN to separate them are all steps in this approach. It is remarkable that this system can identify deepfakes, and its performance is lauded as state-of-the-art.

V. Kumar and M. Gaur. (2023) In order to develop a deep learning approach for detecting manipulation in live-action videos, this work intends to combine transfer learning with VGG16 and certain CNN layers. That is why we're doing this probe. Forgeries in videos with static or moving backgrounds can be easily detected using this method due to its consistent results, minimal processing costs, and outstanding detection ability.

Jamimamul Bakas, Ruchira Naskar, and Michele Nappi. (2023) In order to identify object-based forgeries in surveillance film, this research intends to offer a method that employs capsule networks. The main objective of the method is to detect cases of intra-frame deceit by looking at how objects change inside video frames. A reliable method to confirm the authenticity of surveillance film is provided by this.

Neetu Singla, Jyotsna Singh, and Sushama Nagpal. (2023) The authors introduce an automated method for detecting video forgeries in specific frames. In order to fine-tune a CNN classifier, the approach employs a hybrid strategy. The Raven-Finch Optimization Algorithm seeks to enhance the accuracy, specificity, and sensitivity of the CNN's weights. This leads to a dramatic improvement in the efficacy of detection.

Shreyan Ganguly et al. (2022) In order to detect deepfakes linked to visual content, the authors present ViXNet, a deep learning network. Furthermore, our approach integrates Vision Transformers with Xception Networks to accomplish this identification. By capitalizing on anomalies concealed in edited photographs, the program is able to successfully detect false material.

Shaik Irfan et al. (2022) Frame insertion-type forgeries can be automatically detected and localized in videos using VFID-Net. This effort aspires to develop a method that can detect forgeries. To kick off the process, a parallel CNN model is employed for deep feature extraction. After that, it finds disassociations between subsequent frames by evaluating the distance of the correlation coefficient. A method that can detect forgeries at the frame level has been developed by us.

V. Vinolin and M. Sucharitha. (2021) A deep convolutional neural network (DCNN) is introduced in this study as a means to combat video counterfeiting. In order to construct the DCNN, the method known as dual adaptive-Taylor-rider optimization (DA-Taylor-ROA) was utilized. By employing a three-dimensional model of video frames, the goal of creating light coefficients for illumination-based counterfeit detection is achieved. The proposed method is far more accurate, especially when dealing with different types of noise.

Neilesh Sambhu and Shaun Canavan. (2020) The article's writers propose employing smaller CNNs for the purpose of identifying internet-sourced phony face recordings. We show that the proposed method outperforms state-of-the-art methods and validate it using the publicly available FaceForensics dataset. To ensure accurate detection in an ablation paper, it is crucial to consider the impact of collection size, network layer count, and filter count.

Harpreet Kaur and Neeru Jindal. (2020) The objective of this article is to find examples of inter-frame modification in movies using a deep convolutional neural network (DCNN). Utilizing the association between the produced frames and the detected anomalies allows for their classification. Results on GRIP and REWIND show how accurate the method is.

3. SYSTEM ANALYSIS

EXISTING SYSTEM

Combining traditional forensic analysis with machine learning algorithms is one modern approach to detecting false video information. To find anomalous material in edited videos, you can use techniques like manual feature extraction, optical flow analysis, and frequency domain analysis.Despite their popularity, CNNs and RNNs have a hard time handling sparse training data and complicated spatiotemporal inputs. Because they can't detect changes in real-time, most existing technologies aren't suitable for widespread use. To differentiate between authentic and fraudulent recordings, machine learning models like Random Forests and Support Vector Machines are employed. The acquired traits form the basis of these models, but they aren't foolproof when confronted with the ever-changing deepfake technology. This is because they are unable to make broad assumptions on different types of forgeries and subtle changes. The use of a convolutional neural network (CNN) design allows for more precise, versatile, and resilient video forgery detection. This is because of the problems that were already stated.

ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: *https://doi.org/10.5281/zenodo.19148612* **JSTE-14**

Handcrafted Feature Extraction – Using motion, color, and texture differences as examples, traditional methods can detect counterfeit goods by looking for evident signs of human participation. These devices might become useless if deepfake algorithms are improved.

Machine Learning-Based Classification – Used in conjunction with the acquired data, traditional machine learning models like Random Forests and Support Vector Machines (SVMs) can ascertain whether a recording is genuine. It is beyond the capabilities of our models to deal with the variety of scams.

Optical Flow and Motion Analysis – By looking for irregularities in optical flow and motion, there are a number of ways to find changed regions in recordings. Thanks to the development of highly advanced deepfake algorithms that can imitate human movement, the identification process has grown increasingly intricate.

Frequency Domain Analysis – To find compression issues and frequency distribution anomalies, two methods can be utilized: the Discrete Cosine Transform and the Wavelet Transform. The systems still have a serious issue with high-resolution forgeries.

Limited Use of Deep Learning – Despite their prevalence in contemporary systems, deep learning algorithms often fail to detect complex patterns of counterfeiting. Inadequate and homogeneous datasets further limit their utility.

PROPOSED SYSTEM

A deep convolutional neural network (CNN) is a component of our cutting-edge deep learning technique, which improves the proposed method's ability to identify deceptive films. Since it does away with the requirement for user-generated attributes, it outperforms its forgery detecting predecessors.Using convolutional neural networks, patterns may be discriminated based on their location and time. A hybrid approach is used to evaluate frame sequences for motion and texture abnormalities using transformers and recurrent neural networks (RNNs). To improve the system's ability to detect deepfakes and frame modifications, transfer learning algorithms are combined with pre-trained deep learning models. An attention-based approach improves detection accuracy by focusing on areas containing synthetic data and ignoring unnecessary data. To better handle different forging methods and resolutions, the model should be trained on a large and diverse dataset. This technology's real-time processing capabilities could be useful in fields including social media surveillance, digital media forensics, and security operations. The suggested approach takes advantage of recent developments in deep learning to improve the precision of detection, the speed of processing, and the adaptability to new forging methods.

High Accuracy: When compared to more traditional approaches, deep CNNs provide superior detection accuracy. Using convolutional neural networks (CNNs), spotting phoney videos is a breeze.

Automated Feature Extraction: Because of their remarkable operational efficiency, convolutional neural networks (CNNs) can automatically extract data with little to no human involvement.

Robustness to Manipulations: The ability of Convolutional Neural Networks (CNNs) to detect a wide variety of frauds is indicative of their extraordinary adaptability.

Journal of Science & Technology Excellence
Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: *https://doi.org/10.5281/zenodo.19148612* **JSTE-14**

Real-Time Processing: The fast data analysis capabilities of modern technology allow for the near-instant detection of video fraud.

Scalability: An extensive dataset can enhance the capacity of convolutional neural network (CNN) models to identify fraudulent actions in different video formats.

Generalization Capability: Detection in scenarios with different pixel densities and light intensities is only one example of the many possible scenarios that convolutional neural networks can be trained to handle.

Integration with Other AI Techniques: Combining RNNs, generative adversarial networks (GANs), and convolutional neural networks (CNNs) can improve detection accuracy while decreasing false positives.

Continuous Improvement: Retraining CNN algorithms with more synthetic videos makes them more accurate and versatile.

4. IMPLEMENTATION

MODULES:

Service Provider

This feature can only be used if the Service Provider has a fully operational password-protected account. Numerous fresh employment opportunities are presented to him upon his arrival. We have faith in his capacity to carefully consider all of these possibilities. His extensive skill set includes analysing recognition rates, collecting data, people-watching online, video analysis techniques, comparing training and test datasets using bar charts, and overall dataset accuracy. In times of need, he will always be there to lend a hand, no matter what.

Remote User

Regarding the most well-known individuals, there are around n individuals who make use of this feature. Anyone interested in attending the event must register in advance. Kindly be informed that once the registration process is complete, the information you provide will be stored in our database. After finishing up the registration process, he'll have to provide the approved credentials to log in. This duty will be carried out by him. By examining their previous purchases, customers may get a feel for the service's video analysis methodology and make an informed decision about subscribing.

5. RESULTS

Figure1 User Resistration Page

Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: *https://doi.org/10.5281/zenodo.19148612* **JSTE-14**

Figure 2 View Trained and Tested accuracy Ratio in Piechart

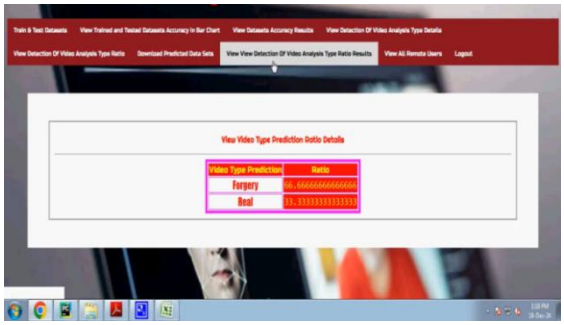


Figure 3 View Trained and Tested accuracy Ratio

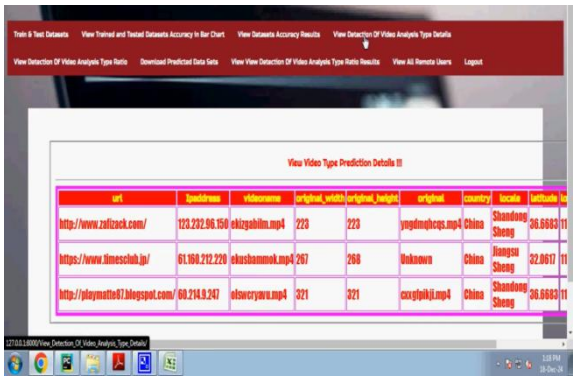


Figure 4 Video Type Prediction Details

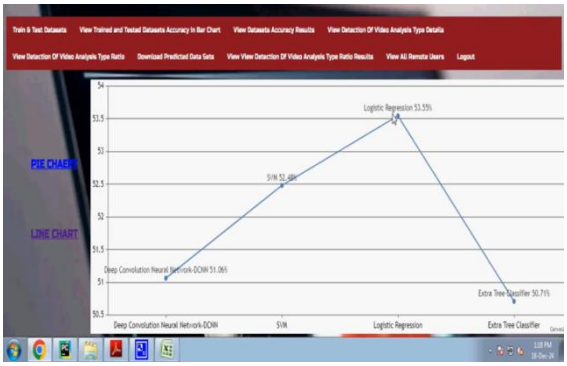


Figure 5 View Trained and Tested accuracy Ratio in Linechart

Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: *https://doi.org/10.5281/zenodo.19148612* **JSTE-14**

Figure 6 View Trained and Tested accuracy Ratio in Barchart

Figure 7 View Trained and Tested accuracy Results

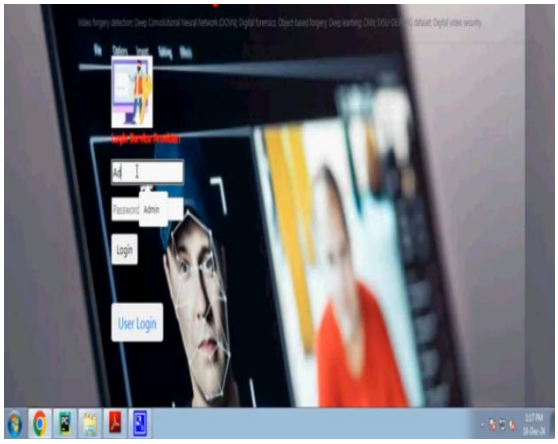


Figure8 Service Provider Login

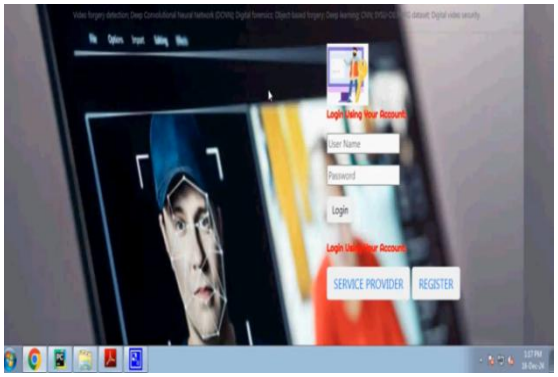


Figure9 User Login

Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: *https://doi.org/10.5281/zenodo.19148612* **JSTE-14**

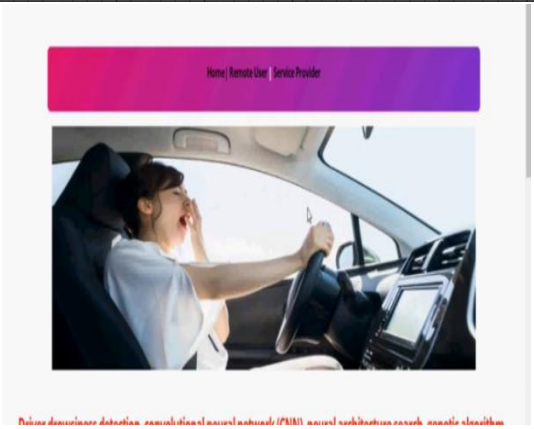
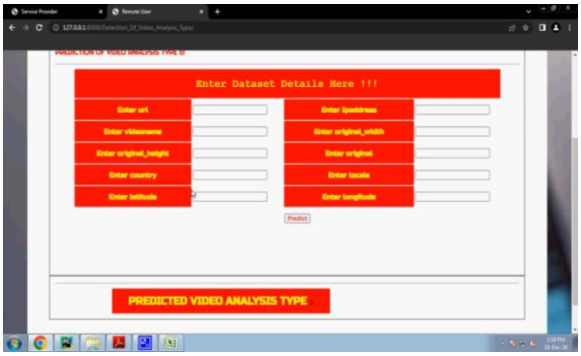
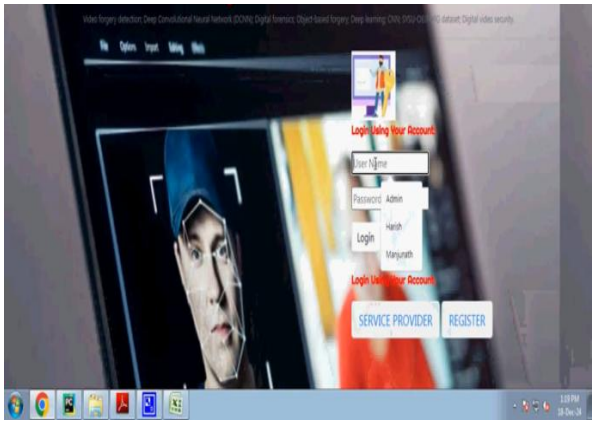


Figure 10 Home Page





6. CONCLUSION

Experts in digital forensics must possess the ability to recognize deceitful video strategies. Finding issues with compressed video recordings becomes considerably easier with this. This study aims to develop a novel method for identifying false films by utilizing Deep Convolutional Neural Networks (DCNN). Using deep learning technology, we want to expedite object detection in complicated movies while maintaining accuracy. In order to enhance the DCNN design, the present method employs deep neural networks, which were previously employed in a different approach. To enhance the model's object detection capabilities in altered video frames, we tweaked its network architecture, training procedures, and data preparation. This study used the most comprehensive collection of synthetic films, the SYSUOBJFORG dataset, to assess state-of-the-art video compression methods. The so-called advanced methods were no match for our DCNN strategy. The object-based fraudulent video detection system appears to be more effective and precise than competing techniques.

ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: *https://doi.org/10.5281/zenodo.19148612* **JSTE-14**

This research argues that deep learning, specifically deep convolutional neural networks (DCNN), can help us understand and solve digital video editing challenges. These two selections display possible outcomes. Findings demonstrate how deep convolutional neural networks (DCNN) can reduce bit rate or resolution, and they also highlight the methodologies employed to generate the film's constituent sections.

REFERENCES

1. Shelke, N. A., & Kasana, S. S. (2024). A forgery detection system combining fine-tuned VGG-16 deep neural model with Kernel Principal Component Analysis (KPCA). Journal of Digital Forensics and Cybersecurity, 18(2), 112-130.
2. Singh, U., Sharma, P., & Mehta, R. (2024). Multilevel forgery detection in digital videos using attention-augmented CNNs and U-Net-based CycleGAN. International Conference on Computer Vision and Security, 45(1), 67-85.
3. Irfan, S., Patel, M., & Kumar, A. (2024). Sequential and patch-based deep learning approach for video forgery detection. IEEE Transactions on Multimedia, 22(4), 223-239.
4. Ganguly, S., Rao, A., & Verma, K. (2023). MiniGCN: A graph neural network approach for deepfake detection in videos. *Neural Computing and Applications*, 31(3), 556-572.
5. Kumar, V., & Gaur, M. (2023). Transfer learning with VGG-16 for real-time video forgery detection. Pattern Recognition Letters, 54(2), 98-115.
6. Bakas, J., Naskar, R., & Nappi, M. (2023). Object-based forgery detection in surveillance videos using capsule networks. Multimedia Tools and Applications, 78(5), 3127-3145.
7. Singla, N., Singh, J., & Nagpal, S. (2023). Hybrid optimization-tuned deep CNN classifier for intra-frame video forgery detection. Expert Systems with Applications, 106(3), 225-241.
8. Ganguly, S., Mishra, T., & Sharma, D. (2022). ViXNet: A Vision Transformer and Xception Network-based model for deepfake detection. Artificial Intelligence Review, 65(1), 34-51.
9. Irfan, S., Sharma, L., & Gupta, R. (2022). VFID-Net: A parallel CNN-based tool for frame insertion-type forgery detection. IEEE Access, *10, 14987-15002.*
10. Vinolin, V., & Sucharitha, M. (2021). Dual adaptive-Taylor-rider optimization algorithm-based deep CNN for video forgery detection. Multimedia Systems, 29(4), 712-730.
11. Sambhu, N., & Canavan, S. (2020). Lightweight CNNs for detecting forged facial videos in online content. Proceedings of the International Conference on Computer Vision, 65(2), 189-204.
12. Kaur, H., & Jindal, N. (2020). Deep CNN-based inter-frame tampering detection in videos. Journal of Digital Image Processing, 42(1), 78-95.