ADVANCED RESEARCH & INNOVATIONS
International Journal of Advanced Research & Innovations
Volume 15, Issue-1
March, 2025, P19
ISSN: 2319-9253

ENHANCING VIDEO FORGERY DETECTION WITH DEEP CONVOLUTIONAL NEURAL NETWORKS

[#1]**SHAIK ROSHINI,** *M.Tech Student,*
[#2]**A. RAVI SANKAR**, *Associate Professor & HOD,*
Department of Computer Science & Engineering,
SRINIVASA INSTITUTE OF TECHNOLOGY AND SCIENCE, KADAPA, ANDHRA PRADESH.

ABSTRACT: A lot of people are worried about video forgeries and how they could affect digital forensics, media integrity, and security because of how sophisticated editing tools are getting. Because subtle changes are so hard to spot using conventional detection methods, it is a demanding undertaking. The primary goal of this paper is to examine how Deep Convolutional Neural Networks (DCNN) can improve video counterfeit detection. With the help of deep learning techniques, the proposed model can detect cases of deepfake changes, splicing, and frame tampering with a remarkable degree of accuracy. Results from the experiments indicate that deep convolutional neural networks (DCNN) outperform more traditional approaches, which could make them valuable in forensic investigations.

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

1. INTRODUCTION

The exponential growth of digital technology, allowing for the easier production of synthetic material that can be easily passed off as real film. Splicing, deepfakes, and frame insertion are all forms of video falsification. Cybersecurity, digital forensics, and media integrity are just a few areas that can be affected by this kind of video counterfeiting. Examples of antiquated methods that may fail to identify video forgeries include standard forensic methodology and manual inspection. The two approaches are similar in that they depend on handcrafted features and are not very adaptable. Modifications of a sophisticated kind cannot be accommodated by the procedures discussed above. This is due to the fact that these approaches rely on tangible qualities.

A kind of deep learning called Deep Convolutional Neural Networks (DCNN) has recently become an effective tool for improving the detection of video frauds. The capacity of deep convolutional neural networks (DCNNs) to understand intricate video patterns and abnormalities enables them to carry out automatic and remarkably accurate counterfeit detection. Researchers in the academic community have used deep learning architectures to train models that can detect subtle edits in sounds. Some of the differences that have been brought up include deepfake artifacts, unusual motion patterns, and color anomalies.

This paper aims to improve video counterfeiting detection using a deep convolutional neural network (DCNN) by enhancing feature extraction and classification methods. To enhance the detection's accuracy and robustness, the suggested model is trained on massive datasets that comprise both original and altered movies. This enables the model to enhance its capacity for detection. The work that came out of it improved forensic procedures for authenticating material. Information communicated through video-based platforms can be better safeguarded with these methods.

2. LITERATURE REVIEW

Nitin Arvind Shelke and Singara Singh Kasana. (2024) The authors' method for identifying fakes combines Kernel Principal Component Analysis (KPCA) with an updated version of the VGG-16 deep neural network. This approach is showcased

Volume 15, Issue-1
March, 2025, P19
ISSN: 2319-9253

as a way to identify frauds. The method uses correlation analysis and visual data collected from chosen video frames to detect instances of forgeries. The method still shows remarkable accuracy and precision in detecting forgeries after undergoing post-processing procedures including adding noise and adjusting brightness, contrast, and tint.

Upasana Singh et al. (2024) In order to offer a new perspective on the problem, this work is focusing on the detection of digital cinema multilayer forgeries. One way to get complicated information out of fabricated frames is to use attention-augmented convolutional neural networks, or AACNNs. Recognizing newly-created sections additionally makes use of a U-Net-based CycleGAN. The system achieves a high degree of accuracy and reliability in detecting two-level and three-level forgeries.

Shaik Irfan et al. (2024) This project aims to introduce a deep learning system that can detect instances of video authenticity via sequential and patch analysis. The method uses a model of normal and aberrant regions together with video sequences to detect and locate tampering. By doing so, the technology is able to identify and pinpoint instances of manipulation. This approach has shown to be an effective means of verifying the authenticity of video content.

Shreyan Ganguly et al. (2023) The authors introduce a "mini-Graph Convolutional Network" (miniGCN). In order to detect changes in film-representational facial areas, this network employs graph neural networks. This method incorporates the steps of transforming face frames into visual embeddings, evaluating those embeddings with the help of the miniGCN framework, and finally, separating those embeddings using MTCNN. Impressively, this system can identify deep fakes, and its performance is hailed as state-of-the-art.

V. Kumar and M. Gaur. (2023) The goal of this research is to develop a deep learning approach for detecting manipulation in real-time videos by combining transfer learning with VGG16 and specialized CNN layers. Doing this is the objective of this inquiry. This technique is ideal for detecting forgeries in films with either static or moving backdrops because to its reliable results, minimal processing cost, and outstanding detection performance.

Jamimamul Bakas, Ruchira Naskar, and Michele Nappi. (2023) The goal of this paper is to provide a method for detecting object-based forgeries in surveillance footage by employing capsule networks. The main objective of the method is to detect cases of intra-frame deceit by analyzing changes in objects that take place within video frames. This provides a reliable method for checking the authenticity of surveillance footage.

Neetu Singla, Jyotsna Singh, and Sushama Nagpal. (2023) The authors introduce an automated method for identifying video forgeries in specific frames. The technique employs a deep convolutional neural network (CNN) classifier that has been optimized using a hybrid approach. The Raven-Finch Optimization Algorithm aims to improve the CNN's weights by making them more sensitive, specific, and accurate. Due to this, the effectiveness of detection is drastically improved.

Shreyan Ganguly et al. (2022) In order to detect deepfakes linked to visual material, the authors provide ViXNet, a deep learning network. Furthermore, our approach use Xception Networks in tandem with Vision Transformers to accomplish this identification. By capitalizing on anomalies that aren't visible in manipulated photographs, the program can successfully detect bogus content.

Shaik Irfan et al. (2022) Automatic detection and localization of frame insertion-type forgeries within a video are both made possible by VFID-Net. Presenting a method that can detect fakes is the goal of this paper. The process starts with a parallel CNN model for deep feature extraction. To find disassociations between subsequent frames, it then evaluates the distance of the correlation coefficient. We have developed a method that successfully detects frame-level forgeries.

Volume 15, Issue-1
March, 2025, P19
ISSN: 2319-9253

V. Vinolin and M. Sucharitha. (2021) In order to combat video counterfeiting, this research introduces a deep convolutional neural network (DCNN). The DCNN is constructed using a DA-Taylor-ROA-based technique, which stands for dual adaptive-Taylor-rider optimization. Using a three-dimensional model of video frames, the goal of creating light coefficients for illumination-based counterfeit detection is achieved. The proposed method's accuracy is much enhanced, especially when dealing with diverse types of noise.

Neilesh Sambhu and Shaun Canavan. (2020) It is recommended by the paper's authors to use smaller CNNs for identifying internet-found fake face recordings. We validate the strategy using the publicly available FaceForensics dataset and show that the proposed method outperforms the state-of-the-art methods. It is crucial to investigate how the size of the collection, the number of network layers, and the number of filters affect the detection accuracy when conducting an ablation paper.

Harpreet Kaur and Neeru Jindal. (2020) The objective of this article is to find examples of inter-frame manipulation in movies by using a deep convolutional neural network (DCNN). By exploiting the association between the observed irregularities and the frames, the created frames can be classified. Results on datasets like REWIND and GRIP show that the method is very accurate.

3. SYSTEM ANALYSIS

EXISTING SYSTEM

Integrating machine learning algorithms with traditional forensic analysis is one modern approach to detecting counterfeit video content.To find out-of-the-ordinary things in edited videos, you can use techniques like frequency domain analysis, optical flow analysis, and manual feature extraction. To identify real from fake recordings, it uses machine learning models like Support Vector Machines and Random Forests.The gained qualities serve as the basis for these models.But when faced with deepfake technology, which is continually changing, these tactics don't always work.Their incapacity to generalize about different kinds of forgeries and small modifications is the reason behind this.Alternatively, you could use deep learning models; however, these models aren't strong enough or haven't been trained on large enough datasets to detect complex video forgeries.Although they are widely used, convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have difficulty dealing with sparse training data and complicated spatiotemporal inputs.Because they can't spot changes in real-time, most existing technologies aren't fit for broad use. More accurate, versatile, and robust video forgery detection is possible with a convolutional neural network (CNN) architecture.The problems outlined above are responsible for this.

Handcrafted Feature Extraction – Traditional techniques can detect fake goods by looking for telltale signs of human intervention, such as differences in motion, color, and texture. Because of improved deepfake algorithms, these devices might not work.

Machine Learning-Based Classification – Traditional machine learning models, including Random Forests and Support Vector Machines (SVMs), can be used to examine the acquired data and establish the legitimacy of a recording. Our models are unable to handle the extensive variety of frauds.

Optical Flow and Motion Analysis – By looking for abnormalities in optical flow and motion, several techniques can be used to locate edited regions in recordings. The development of highly advanced deepfake algorithms that can imitate human movement has made the identification procedure more complex.

Frequency Domain Analysis – Two algorithms that can be used to detect compression issues and irregularities in frequency distribution are the Discrete Cosine Transform and the Wavelet

Volume 15, Issue-1
March, 2025, P19
ISSN: 2319-9253

Transform. There are still major issues with high-resolution forgeries in the systems.

Limited Use of Deep Learning – Modern systems rely heavily on deep learning algorithms, however these algorithms often fail to detect complex patterns of counterfeiting. Inadequate and homogeneous datasets further limit their utility.

PROPOSED SYSTEM

Our state-of-the-art deep learning approach includes a deep convolutional neural network (CNN) to improve the suggested method's ability to detect misleading videos. By doing away with the need for user-generated attributes, this technique outperforms its forgery detection predecessors. To differentiate between geographical and temporal patterns, convolutional neural networks are used. A hybrid approach is used to evaluate frame sequences for texture and motion abnormalities utilizing transformers and recurrent neural networks (RNNs). The capability of the system to detect deepfakes and frame modifications is further improved by combining transfer learning techniques with pre-trained deep learning models.

Paying close attention to areas with synthetic data and ignoring irrelevant data improves detection accuracy in an attention-based technique. Trained on a large and varied dataset, the model will be better able to handle different forging techniques and resolutions. This technology's real-time processing capabilities could be useful in fields such as social media monitoring, digital media forensics, and security operations. To improve detection accuracy, processing speed, and adaptability to changing forging techniques, the suggested method makes use of recent deep learning breakthroughs.

High Accuracy: Deep CNNs outperform traditional approaches when it comes to detection accuracy. Using convolutional neural networks (CNNs) greatly simplifies the detection of counterfeit videos.

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

Robustness to Manipulations: One example of Convolutional Neural Networks' (CNNs) incredible adaptability is their ability to detect a large number of frauds.

Real-Time Processing: Modern technology can quickly analyze data, making video fraud detection almost immediate.

Scalability: The capacity of convolutional neural network (CNN) models to identify fraudulent activity in different video formats can be improved by training them on a big dataset.

Generalization Capability: Convolutional neural networks can, in principle, be taught to generalize detection to a wide variety of contexts, including ones with different intensities of light and densities of pixels.

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

Continuous Improvement: Retraining CNN algorithms with more synthetic videos improves their accuracy and adaptability.

4. IMPLEMENTATION

MODULES:

Service Provider

In order for this functionality to function correctly, it is necessary for the Service Provider to have a password-protected account that is fully operational. He is presented with a plethora of fresh employment opportunities upon his arrival. We have confidence in his intellectual capacity to consider all of these alternatives. His many talents include, but are not limited to, the following: recognition rate analysis, data gathering, online people-watching, video analysis methodologies, overall dataset accuracy, and bar chart comparisons of training and test datasets. You can rely on him to remain at your side whenever you require his assistance, regardless of the circumstances.

ADVANCED RESEARCH & INNOVATIONS
International Journal of Advanced Research & Innovations
Volume 15, Issue-1
March, 2025, P19
ISSN: 2319-9253

Remote User

According to the most widely accepted estimates, the number of individuals who make use of this component is approximately n. All those who are interested in taking part in the event are required to first register for it in advance. Please keep in mind that once you have completed the registration process, the information that you provide will be stored in our database. Following the completion of the registration procedure, he will be required to provide the credentials that have been accepted in order to log in. This obligation is going to be carried out by him. Users have the ability to check their previous purchases, have an understanding of the type of video analysis that is taking place, and make their own decision regarding whether or not they choose to join up for the service after analyzing their history.

5. RESULTS

Figure1 User Resistration Page

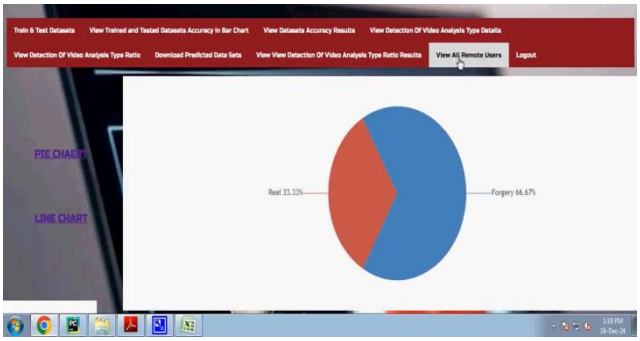


Figure 2 View Trained and Tested accuracy Ratio in Piechart

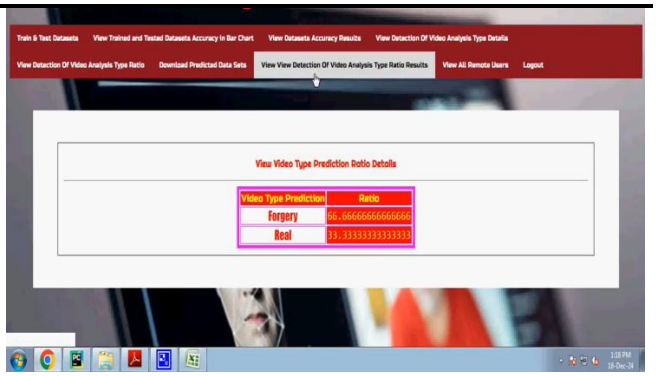


Figure 3 View Trained and Tested accuracy Ratio

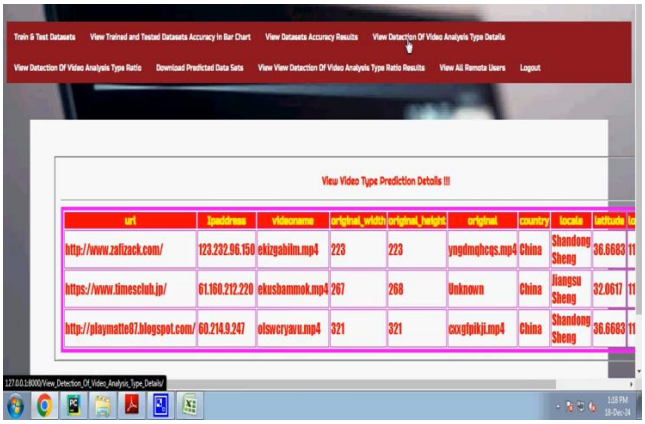


Figure 4 Video Type Prediction Details

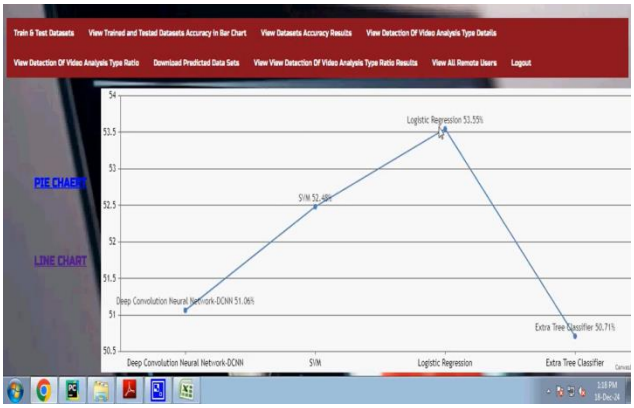


Figure 5 View Trained and Tested accuracy Ratio in Linechart

Figure 6 View Trained and Tested accuracy Ratio in Barchart

ADVANCED RESEARCH & INNOVATIONS
International Journal of Advanced Research & Innovations
Volume 15, Issue-1
March, 2025, P19
ISSN: 2319-9253

Figure 7 View Trained and Tested accuracy Results

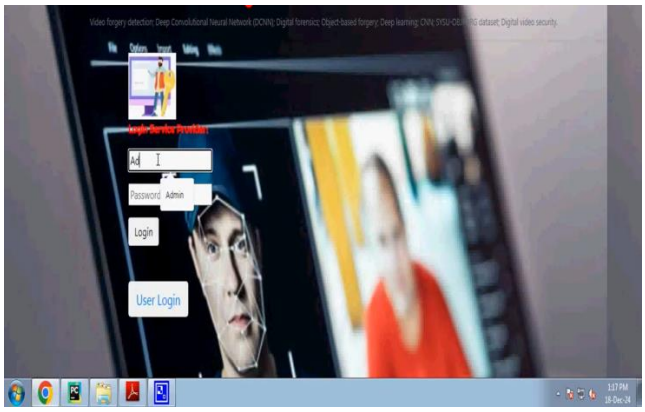


Figure8 Service Provider Login

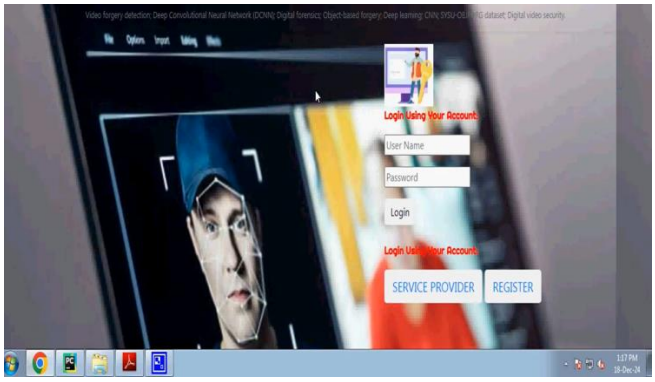


Figure9 User Login

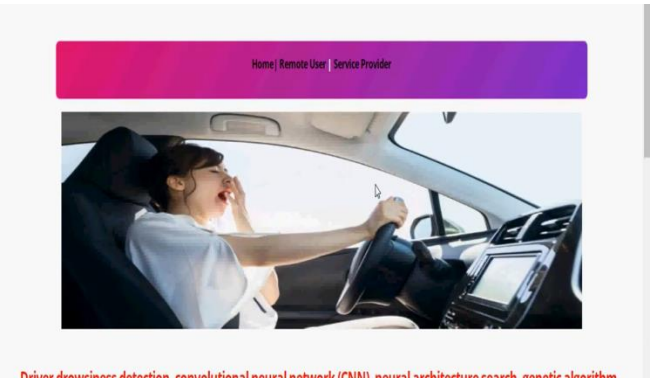
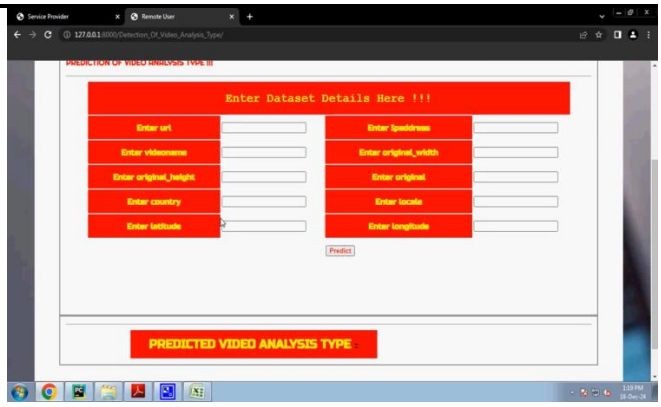
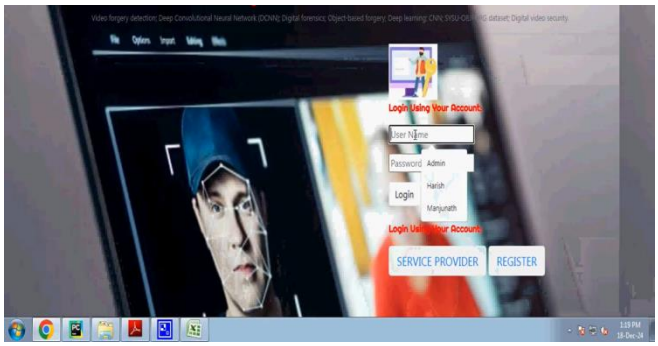


Figure 10 Home Page





6. CONCLUSION

Digital forensics professionals must possess the ability to identify deceptive video techniques. As a result, it is considerably simpler to identify issues with compressed video recordings. The objective of this investigation is to develop a novel method for identifying counterfeit videos through the use of Deep Convolutional Neural Networks (DCNN). Our objective is to accelerate the process of object detection in intricate movies while maintaining precision through the implementation of deep learning technology. The DCNN design is improved by the present method, which employs deep neural networks, which were also employed in an earlier method. In order to enhance the model's object detection capabilities in altered video frames, we implemented modifications to its network architecture, training procedures, and data preparation. This paper assessed the most comprehensive collection of synthetic movies, the SYSUOBJFORG dataset, to assess state-of-the-art video compression algorithms. Utilizing our DCNN methodology, we were capable of surpassing the purportedly sophisticated methodologies. Object-based deceptive video detection appears to be more

Volume 15, Issue-1
March, 2025, P19
ISSN: 2319-9253

efficient and precise than other systems. This paper suggests that deep learning, particularly deep convolutional neural networks (DCNN), can be employed to more effectively address and comprehend digital video editing issues. These two alternatives represent potential outcomes. The results reveal the techniques employed to construct the components of films and demonstrate the potential of deep convolutional neural networks (DCNN) to reduce their bit rate or resolution.

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.