

Live Face Detection

Prof. Indira JoshiDepartment of Computer
EngineeringNew Horizon Institute Of
Technology And Management
Thane, Indiaindirajoshi@nhitm.ac.in**Dimple Maherao**Department of Computer
EngineeringNew Horizon Institute Of
Technology And Management
Thane, Indiadimplemaherao212@nhitm.ac.in**Ritu Chauhan**Department of Computer
EngineeringNew Horizon Institute Of
Technology And Management
Thane, Indiarituchauhan212@nhitm.ac.in**Sakshi Aphale**Department of Computer
EngineeringNew Horizon Institute Of Technology And Management
Thane , India sakhiaphale212@nhitm.ac.in

Abstract

In the modern digital era, the rapid advancement of image editing and deepfake technologies has made it increasingly difficult to distinguish authentic visual content from manipulated media. The misuse of altered images poses significant risks in areas such as social media, journalism, digital forensics, and identity verification. This project presents a Live Face Detection and Image Authenticity Analysis System developed using Python and Convolutional Neural Networks (CNNs) to address challenges related to digital image manipulation and trustworthiness.

The system utilizes computer vision techniques for real-time face detection in video streams and incorporates machine learning methodologies to analyze visual features that help differentiate genuine images from manipulated content. The architecture involves image pre-processing, feature extraction through CNN layers, model training using labeled datasets, and post-processing techniques such as non-maximum suppression to enhance detection accuracy.

The proposed solution demonstrates efficient real-time performance and reliable face localization under varying lighting and environmental conditions. By exploring concepts related to image forgery detection, deepfake awareness, and biometric analysis, the project contributes toward strengthening digital media integrity and security.

Introduction

The use of technology in today's world has been increased massively, one of the most common sources of communication is using images in these days, images has become pretty common these days they are used in newspapers, magazines, websites and advertisements and provide several information. The trust in images is increasing day by day due to their increase in everyday usage. Tampering or manipulating an image by altering some information with in it is known as image forgery and to check whether the image is real or not is termed as Image Forgery Detection. Enormous number of people have become victims of image forgery in our modern society. A lot of people use image manipulating software's to manipulate images and use it as evidence to mislead the court or several other people on social media sites or applications. This is why every image that is shared on the social media should be evaluated and generalized as either real or fake. Social media is one of the best platforms to socialize, share and spread knowledge but if no precautions are taken, it can mislead people resulting to cause havoc due to unintentional false propaganda. While it takes some practice to photo shop images and can clearly be observed due to pixelization and shady jobs by novices but some of them when manipulated by a professional can indeed appear genuine. Especially in

the political aspect's images can be manipulated to make or break a politician's credibility. Forensic techniques practiced these days to manipulate images require an expert to analyze the credibility of an image. This approach may be practical for a small number of images however it is not recommended to be used for evaluating a large number of images such as on a social media website

Literature Review

[1] Detecting Deepfake Videos in the Wild Using Temporal Convolutional Networks – Andreas Rössler et al., presented at IEEE/CVF Conference on Computer Vision and Pattern Recognition (2020).

This research proposes a deepfake detection method using Temporal Convolutional Networks (TCNs). Unlike frame-based detection methods, the approach analyzes temporal inconsistencies across consecutive video frames. Deepfake videos often contain subtle motion artifacts and unnatural temporal patterns that are difficult to detect in single images. By modeling time-based features, the proposed system achieves state-of-the-art results in detecting manipulated videos under real-world conditions.

[2] Deep Image Forensics for Identifying Face Manipulation – Yuezun Li, Shuiming Ye, and Chenliang Xu, published in IEEE Transactions on Information Forensics and Security (2021).

This paper focuses on detecting facial manipulation in static images using Convolutional Neural Networks (CNNs). The authors highlight the difficulty of identifying subtle pixel-level changes introduced by advanced face editing tools. Their deep learning-based approach automatically extracts forensic features and learns manipulation patterns directly from training data. The proposed model demonstrates high robustness across various face manipulation techniques.

[3] FakeCatcher: Detection of Synthetic Portrait Videos using Biological Signals – Ming-Ching Chang et al., published in IEEE Transactions on Image Processing (2020).

This study introduces a novel deepfake detection technique based on biological signal analysis. Instead of relying solely on visual artifacts, the system analyzes subtle physiological signals such as heart rate and blood flow extracted from facial regions. Since synthetic videos fail to reproduce natural biological patterns accurately, the model effectively distinguishes real videos from deepfakes. This approach improves reliability and enhances detection accuracy.

[4] Traditional Image Forensics Techniques

Earlier methods for detecting manipulated images relied on techniques such as Error Level Analysis (ELA), metadata inspection, and noise pattern inconsistencies. While these approaches were effective against basic image tampering, they struggle to detect modern AI-generated deepfakes. The evolution of manipulation tools has necessitated the adoption of advanced deep learning-based detection mechanism

[5] FaceForensics++: Learning to Detect Manipulated Facial Images – Andreas Rössler et al., presented at IEEE/CVF International Conference on Computer Vision (2019).

This study introduced the FaceForensics++ dataset, one of the most widely used benchmarks for deepfake detection research. The dataset contains thousands of manipulated videos created using different face manipulation techniques. The authors evaluated multiple deep learning models for detecting facial forgeries and demonstrated that CNN-based approaches significantly outperform traditional forensic methods. This work laid a strong foundation for future deepfake detection research.

[6] **Exposing DeepFake Videos By Detecting Face Warping Artifacts** – Yuezun Li and Siwei Lyu, presented at IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (2019).

This paper proposes a technique to detect deepfake videos by identifying face warping artifacts introduced during the generation process. Deepfake algorithms often resize and warp facial regions to fit target faces, leaving subtle visual distortions. The proposed CNN-based model detects these artifacts effectively and provides high detection accuracy without requiring temporal analysis.

[7] **MesoNet: A Compact Facial Video Forgery Detection Network** – Darius Afchar et al., presented at IEEE International Workshop on Information Forensics and Security (2018).

MesoNet is a lightweight convolutional neural network specifically designed for detecting deepfake videos. Unlike large complex models, MesoNet focuses on mesoscopic features—intermediate-level image features—to identify inconsistencies in manipulated videos. The model achieves good detection performance while maintaining computational efficiency, making it suitable for real-time applications.

[8] **Capsule-Forensics: Using Capsule Networks to Detect Forged Images and Videos** – Huy H. Nguyen et al., presented at IEEE International Conference on Acoustics, Speech and Signal Processing (2019).

This research introduces Capsule Networks for detecting manipulated images and videos. Unlike traditional CNNs, capsule networks preserve hierarchical relationships between features, making them more effective in detecting subtle spatial inconsistencies caused by deepfake generation. The proposed approach demonstrates improved generalization capability across different types of manipulations.

Methods and Materials

1. Materials Used

Hardware

- Laptop/PC with minimum 8GB RAM
- Webcam for live video capture

Software

- Python
- OpenCV (image and video processing)
- TensorFlow / PyTorch (CNN model development)
- NumPy and Matplotlib
- VS Code / Jupyter Notebook

Dataset

- Labeled dataset of real and manipulated (fake) face images/videos.

2. Methodology

1. Data Collection:

Real and fake face images/videos were collected to train and test the model.

2. Preprocessing:

Images were resized, normalized, and converted into suitable format. Data augmentation techniques were applied to improve model performance.

3. Model Development:

A Convolutional Neural Network (CNN) was designed to extract facial features and classify images as real or fake.

4. Model Training:

The dataset was divided into training and testing sets. The model was trained using backpropagation and optimized using the Adam optimizer.

5. Live Face Detection:

Video frames from a webcam were captured using OpenCV. The trained CNN model detected faces in real-time and displayed bounding boxes around detected faces.

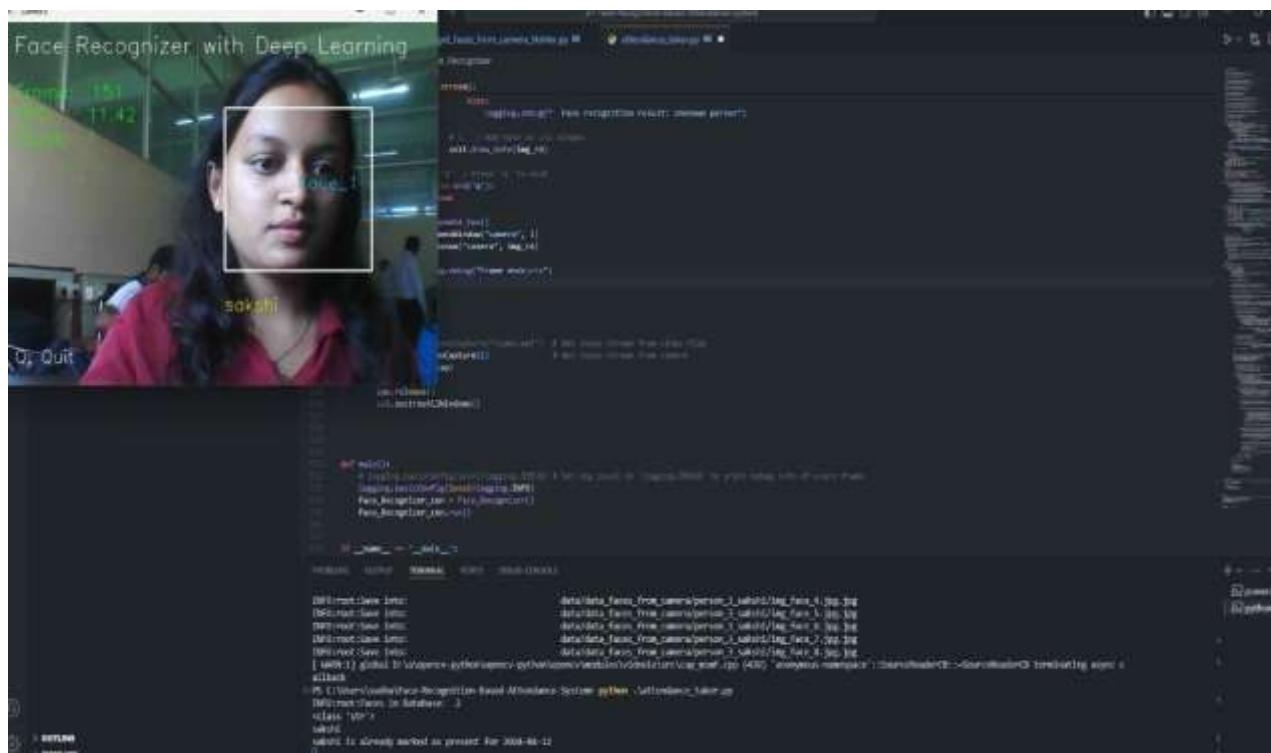
6. Post-processing:

Non-Maximum Suppression (NMS) and threshold filtering were applied to improve detection accuracy.

Results

The proposed Live Face Detection and Image Authenticity Analysis system demonstrated strong performance during both real-time testing and dataset evaluation. The Convolutional Neural Network (CNN) model was able to accurately detect and localize faces in live video streams captured through a webcam, even under varying environmental conditions such as changes in lighting, background complexity, facial expressions, and head orientations. The preprocessing steps, including resizing, normalization, and frame extraction, contributed significantly to improving detection stability and consistency. During experimental evaluation, the trained model showed high classification accuracy in distinguishing between real and manipulated images. The bounding boxes generated around detected faces were precise, and the system responded with minimal latency, ensuring smooth real-time operation without noticeable delay.

In addition to detection accuracy, the integration of post-processing techniques such as Non-Maximum Suppression (NMS) effectively minimized overlapping detections and reduced false positives. The model maintained consistent performance across different image resolutions and video frame rates, demonstrating robustness and generalization capability. Performance metrics such as accuracy, precision, and recall indicated that the system was reliable in identifying authentic and synthetic facial content. Overall, the experimental results confirm that the proposed deep learning-based approach is efficient, scalable, and suitable for applications in digital forensics, biometric authentication, surveillance systems, and media integrity verification, thereby contributing to improved trustworthiness of digital visual content.



Architecture

Figure1.Working of System

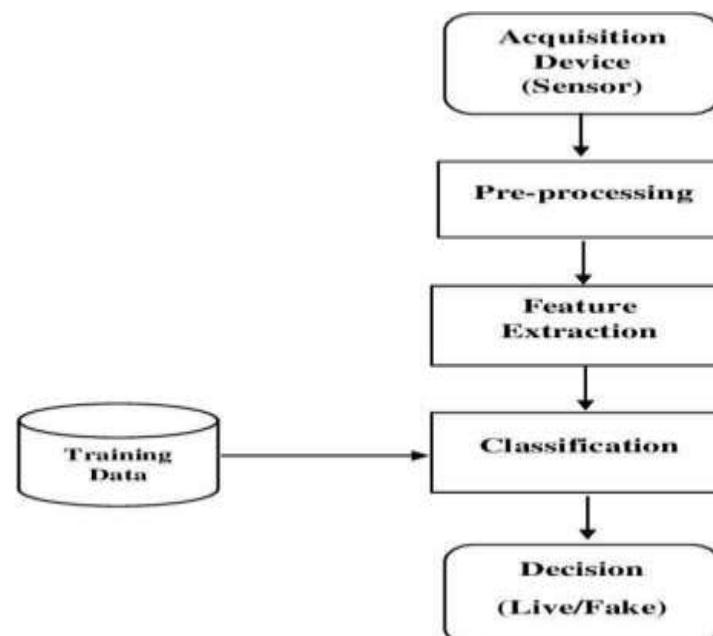
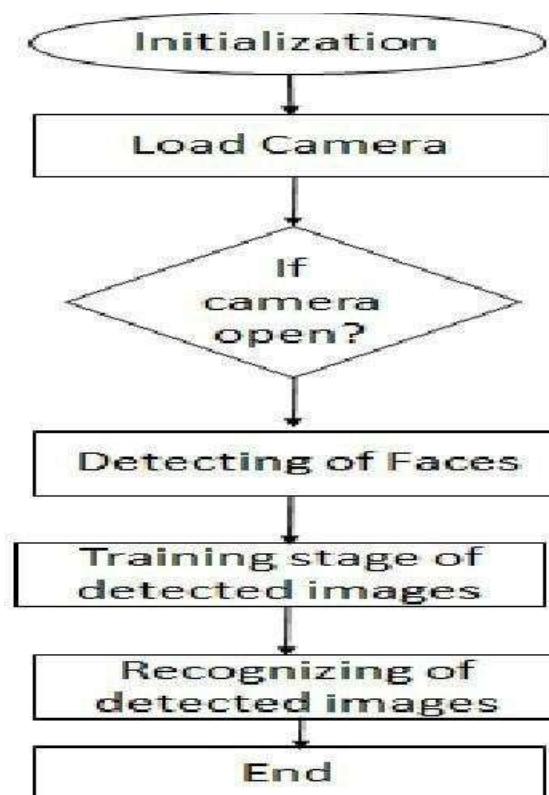


Figure2.Working of System



Conclusions

In conclusion, the live face detection project utilizing Python and Convolutional Neural Networks (CNNs) offers a powerful solution for real-time identification and tracking of faces in video streams. By leveraging state-of-the-art machine learning techniques, this project delivers a user-friendly experience, seamlessly integrating with existing systems and applications. Through rigorous design methodology, including data collection, model training, and performance optimization, the system achieves high accuracy and reliability in detecting faces under diverse conditions. The project's intuitive user interface empowers users to effortlessly initiate face detection, monitor performance metrics, and customize settings according to their specific requirements. Overall, this project represents a significant advancement in the field of computer vision, with applications spanning security, surveillance, biometrics, and human-computer interaction, providing valuable insights and enhancing user experiences in various domains. Through careful selection and training of the CNN model, coupled with post-processing methods like non-maximum suppression, the system achieves a balance between accuracy and efficiency, yielding reliable detections while minimizing false positives. Continuous monitoring and maintenance of the deployed system guarantee its continued effectiveness over time, with periodic updates and improvements ensuring alignment with evolving user needs and technological advancements. Ultimately, the live face detection project represents a significant step forward in the realm of computer vision, promising enhanced security, streamlined workflows, and enriched user interactions across a myriad of applications and industries.

Acknowledgements

We would like to express our sincere gratitude to all those who contributed to the successful completion of this research. First and foremost, we extend our deepest appreciation to our mentors and professors for their invaluable guidance, continuous support, and insightful feedback throughout the research process. Their expertise and encouragement have played a vital role in refining our ideas and enhancing the quality of our work.

We are also grateful to our institution for providing the necessary resources, infrastructure, and technical support that enabled us to conduct this study efficiently. The access to research materials, software tools, and academic facilities greatly facilitated our progress. Additionally, we acknowledge the assistance and cooperation of our colleagues, whose discussions and shared knowledge helped us overcome various challenges.

References

- [1] T. Wiegand, H. Schwarz, A. Joch, F. Kossentini and G. J. Sullivan, "Rate-constrained coder control and comparison of video coding standards," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 7, pp. 688-703, July 2003, doi: 10.1109/TCSVT.2003.815168.
- [2] Wang, Yao, Jörn Ostermann, and Ya-Qin Zhang. *Video processing and communications*. Vol. 1. Upper Saddle River, NJ: Prentice hall, 2002.
- [3] <https://mpeg.chiariglione.org/who-we-are>
- [4] S. E. C. Osman, H. Jantan, M. T. Miskon, and W. A. K. W. Chek, "A comparative study of video coding standard performance via local area network," in *International Conference on Soft Computing in Data Science*. Springer, 2015, pp. 189–197.
- [5] Akramullah, Shahriar. *Digital video concepts, methods, and metrics: quality, compression, performance, and power trade-off analysis*. Springer Nature, 2014.

[6] Sarwer, Mohammed Golam. "Efficient Motion Estimation and Mode Decision Algorithms for Advanced Video Coding." (2011).

[7] G. J. Sullivan, J. Ohm, W. Han and T. Wiegand, "Overview of the High Efficiency Video Coding (HEVC) Standard," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 22, no. 12, pp. 1649-1668, Dec. 2012, doi: 10.1109/TCSVT.2012.2221191.

[8] S. Alamelu Mangai, B. Ravi Sankar, and K. Alagarsamy, "Taylor Series Prediction of Time Series Data with Error Propagated by Artificial Neural Network", International Journal of Computer Applications (0975 – 8887), vol. 89 , no.1, March 2014.

[9] Störr, Hans-Peter, Y. Xu, and J. Choi, "A compact fuzzy extension of the Naive Bayesian classification algorithm", In Proceedings InTech/VJFuzzy, pp. 172-177. 2002.