International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

DeepFake Detection for Human Face Images and Videos: A Comprehensive Survey

[1]Abburi Pallavi, [2] C Susmitha, [3] K Rohith, [4]Kunala Ganesh
[1]Final Year B.E. Student,[2]Final Year B.E. Student,[3]Final Year B.E. Student, [4]Final Year B.E. Studentt
[1] Chandana V S
[1]Associate Professor
[1]Department of Computer Science,
[1]KS School Of Engineering And Management, Bengaluru,India
[1]abburipallavi123@gmail.com, [2]rohithnaidu321@gmail.com, [3]sushmac3114@gmail.com,[4]kunalaganesh1118@gmail.com

Abstract - With the growing sophistication of deep learning and generative models, the creation of synthetic media such as DeepFakes has become increasingly convincing and widespread. DeepFakes pose serious threats across multiple sectors, from political misinformation to personal identity theft. This paper reviews the current progress in DeepFake detection techniques focused on human facial images and video content. It categorizes detection methodologies into feature-based approaches, deep learning models, biological signal analysis, and multimodal systems. Additionally, it discusses benchmark datasets, performance metrics, and the ongoing challenges faced by detection systems, such as poor generalization to unseen forgery methods. Finally, the survey outlines future directions essential for building more reliable and adaptable DeepFake detection solutions.
Keywords: DeepFake detection, Synthetic media, Face forensics, Deep learning, Video forgery, Biological signals.

Index Terms - DeepFake detection, Synthetic media, Face forensics, Deep learning, Video forgery, Biological signals.

I. INTRODUCTION

The machine learning techniques, especially GANs , has enabled creation of hyper-realistic fake videos and images known as DeepFakes. While these technologies have potential positive uses in entertainment and virtual reality, their misuse has led to significant societal concerns. DeepFakes can easily manipulate public perception, endanger personal reputations, and breach cybersecurity protocols. Recognizing manipulated content has thus become a critical need.

Traditional detection methods, which relied on manual inspection of visual artifacts, are no longer effective against today's sophisticated synthetic media. Researchers have shifted toward deep learning and artificial intelligence to automatically identify inconsistencies invisible to the human eye. However, challenges such as the detection of unknown DeepFake generation techniques and ensuring robustness across diverse data remain unsolved.

II. LITERATURE SURVEY

1. Research Paper-1

Title: Application of IoT in Sustainable Supply Chain Management (2022) Authors: Khan Yasser, et al.
Key Points:

- Integrates Internet of Things (IoT) technologies into conventional supply chains to enable smarter and more adaptive operations.
- Enhances operational efficiency, safety standards, and decision-making capabilities by leveraging interconnected smart devices.
- Conclusion: IoT offers notable benefits like improved efficiency and better traceability across supply chains.

2. Research Paper-2

Title: A Cloud-Based Supply Chain Management System (2019) Authors: Mihalis Giannakis, et al.
Key Points:

- Introduces a cloud-driven architecture designed to increase supply chain responsiveness and visibility.
- Highlights benefits such as greater flexibility and the ability to adapt quickly to market or operational changes.
- Conclusion: While cloud systems enhance the agility of supply chains, there is a critical need for advanced security measures to protect against data breaches.

3. Research Paper-3

Title: Intelligent Supply Chain Management System (2016) Authors: V. Fore, et al.
Key Points:

- Combines IoT and Cloud Computing to facilitate real-time tracking, monitoring, and collaboration within supply chains.
- Employs Wireless Sensor Networks (WSNs) to minimize operational costs and support decision-making.
- Conclusion: The system enhances operational efficiency and transparency; however, ongoing improvements are necessary

to strengthen security and ensure system reliability.

4. Research Paper-4
Title: Collaboration in Textile Supply Chain Management (2011) Authors: Hwang Ha Jin, et al.
Key Points:

- Proposes a collaborative framework specifically tailored for the textile industry to foster stronger teamwork and accelerate delivery processes.
- Conclusion: The model boosts innovation and competitiveness within the textile sector but demands stricter data protection mechanisms to safeguard shared information.

5. Research Paper-5
Title: Collaboration in Textile Supply Chain Management (2011) Authors: Hwang Ha Jin, et al.
Key Points:

- Proposes a collaborative framework specifically tailored for the textile industry to foster stronger teamwork and accelerate delivery processes.
- Conclusion: The model boosts innovation and competitiveness within the textile sector but demands stricter data protection mechanisms to safeguard shared information.

SYSTEM DESIGN

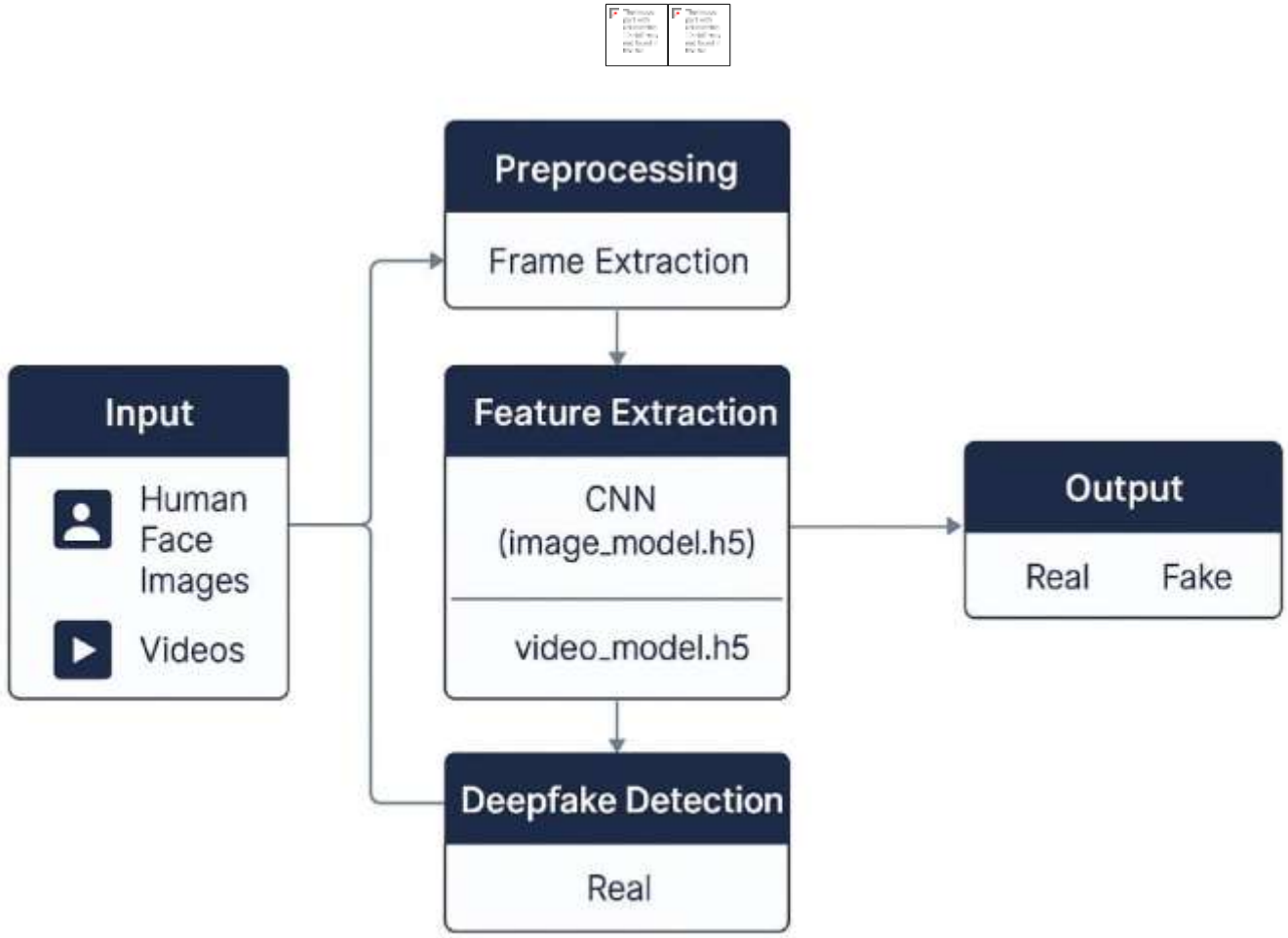

Fig. 1: System architecture

III. METHODOLOGY

Detection methodologies can be broadly divided into the following categories:
A. Feature-Based Approaches
These techniques rely on manually crafted visual or physical indicators of manipulation, such as inconsistent blinking patterns, unnatural head movements, or texture inconsistencies around the face boundary.

B. Deep Learning-Based Models

Modern approaches leverage CNNs, RNNs, transformers, and attention mechanisms to automatically learn distinguishing features. These models are trained end-to-end on large datasets and often outperform traditional methods in controlled settings.

C. Biological Signal-Based Detection

Since synthetic videos struggle to accurately mimic natural biological signals (e.g., heartbeats detectable through tiny skin color variations), analyzing these hidden patterns provides a promising way to detect fakes.

D. Multimodal Fusion

Combining different types of data, such as visual cues, audio analysis, and biological signals, can significantly enhance detection accuracy and robustness by capturing complementary information.

E. Evaluation Metrics

- Detection systems are typically evaluated using metrics like:
- Accuracy: Percentage of correctly classified samples.
- AUC (Area Under Curve): Represents the trade-off between true positive and false positive rates.
- F1-Score: Harmonic mean of precision and recall, especially useful when classes are imbalanced.

F. System Design Overview

A standard DeepFake detection system comprises the following components:

Data Preprocessing

- Face detection and alignment to standardize inputs.
- Frame extraction in the case of video inputs.

Feature Extraction

- Either manual feature engineering or automated feature learning using neural networks.

Classification Layer

- A classifier (e.g., a deep network or a support vector machine) predicts whether the input is genuine or forged.

Training and Testing

- Models are trained on annotated datasets such as FaceForensics++, Celeb-DF, or DFDC.
- Testing is done to assess performance and generalization ability.

Real-Time Deployment Considerations

- Optimizing models for speed and resource-efficiency to enable real-time DeepFake detection on mobile or embedded devices.

IV. CONCLUSIONS

The DeepFakes present a growing risk to digital society, requiring urgent and ongoing development of reliable detection strategies. deep learning techniques have significantly improved detection performance, real-world deployment remains challenged by generalization issues, dataset biases, and the rapid evolution of DeepFake generation methods. Future efforts must focus on building adaptive, lightweight, and explainable detection models capable of handling diverse and evolving threats. Interdisciplinary research that combines biological, behavioral, and visual indicators could pave the way for more robust and trustworthy DeepFake identification systems.

V. REFERENCES

[1]A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, "FaceForensics++: Learning to Detect Manipulated Facial Images," 2019.

[2] Y. Li and S. Lyu, "Exposing DeepFake Videos by Detecting Face Warping Artifacts," CVPR Workshops, 2019.

[3] Y. Li and S. Lyu, "Exposing DeepFake Videos by Detecting Face Warping Artifacts," CVPR Workshops, 2019.

[4]U. A. Ciftci, I. Demir, and L. Yin, "FakeCatcher: Detection of Synthetic Portrait Videos Using Biological Signals," 2021.

[5] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "DeepFakes and Beyond: Survey of Face Manipulation and Fake Detection," Information Fusion, 2020.