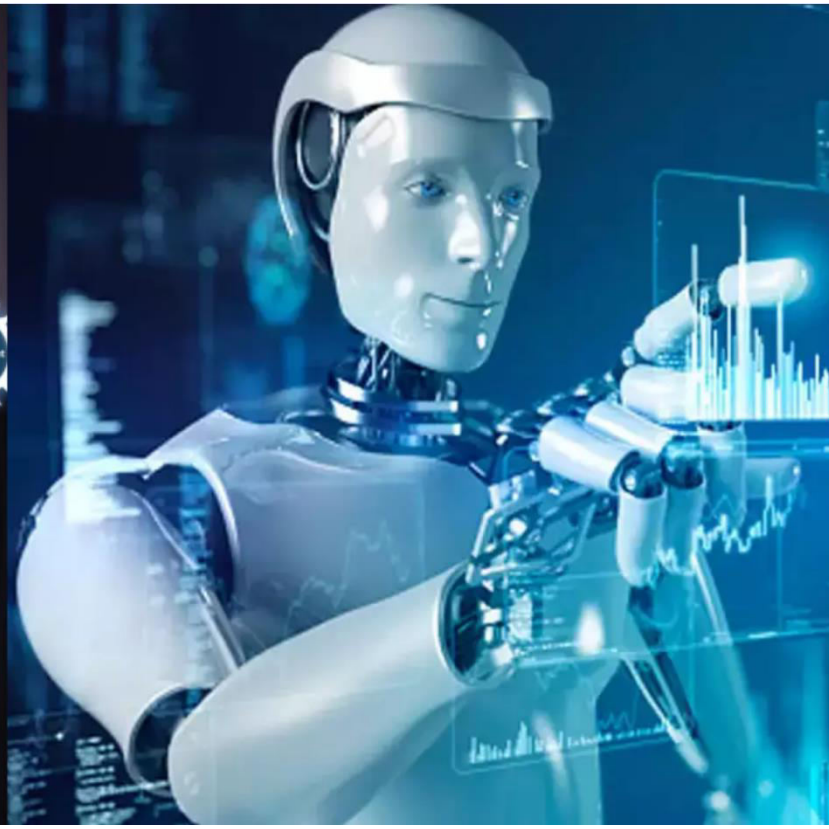
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 11, November 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411091|

Enhancing Deepfake Detection using Deep Learning Framework: A Review

Dr.Deepti Varshney[1], Pund Komal Satish[1]

Department of Computer Engineering, Ajeenkya D.Y.Patil School of Engineering, Pune, India[1]

ABSTRACT: Deepfakes threaten information security, yet existing detection models struggle against advanced forgeries because they primarily rely on spatial analysis within single frames and overlook temporal inconsistencies. We propose BMNet (BiLSTM), a novel architecture to enhance deepfake detection robustness. BMNet integrates a Bidirectional Long Short-Term Memory (BiLSTM) layer to effectively capture crucial sequential dependencies across video frames. Additionally, a Multi-Head Self-Attention Mechanism (MHSAM) is used to intelligently weigh and focus on the most discriminative, forgery-indicative feature regions.

KEYWORDS: Deepfake, deepfake image/video detection, bi-directional long short-term memory network, deep learning.

I. INTRODUCTION

Deepfakes seriously threaten digital trust, necessitating robust detection. Current CNN-based methods fail by ignoring vital temporal inconsistencies across video frames, focusing only on visual artifacts. Our BMNetarchitecture solves this by integrating temporal and spatial analysis.

Conventional deepfake detectors primarily rely on Convolutional Neural Networks (CNNs) for spatial analysis, focusing on finding visual irregularities and subtle artifacts within single frames. While effective for basic manipulation, these models falter against advanced forgeries because they treat frames independently, ignoring the sequential relationship inherent in video. This results in a critical inability to model temporal coherence across video sequences, leaving the systems vulnerable to sophisticated deepfakes that strategically employ inconsistent movements or flicker artifacts across time to bypass static detection methods. The current reliance on solely spatial cues creates a generalization gap that modern countermeasures must urgently address.

BMNetis designed to overcome these current system limitations. It uses a CNN base for initial feature extraction, feeding those features into a Bidirectional Long Short-Term Memory (BiLSTM) layer to capture comprehensive sequential dynamics and long-range dependencies. Crucially, a Multi-Head Self-Attention Mechanism (MHSAM) is then employed to intelligently weigh and focus on the most forgery-indicative features and regions, maximizing the model's discriminative power. This novel integration of BiLSTM and MHSAM ensures superior, robust detection by effectively modeling subtle spatio-temporal artifacts.

II. LITERATURE SURVEY

Rue Marconi [1], In recent years, multi-channel methods have been proposed to improve the robustness of PADsystems. Often, only a limited amount of data is avail able for additional channels, which limits the effectiveness of these methods. In this work, we present a new framework for PAD that uses RGB and depth channels together with a novel loss function.

Mathilde Caron [2], In this paper, we question if self-supervised learning pro vides new properties to Vision Transformer (ViT) [19] that stand out compared to convolutional networks (convnets). Beyond the fact that adapting self-supervised methods to this architecture works particularly well, we make the follow ing observations: first, self-supervised ViT features contain explicit information about the semantic segmentation of an image, which does not emerge as clearly with supervised ViTs, nor with convnets.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411091|

AnukulMuley [3], RFID technology, fingerprint, facial recognition, iris scan, OTP, reference number, random keypad, and other technologies are all utilized to ensure the security of ATM machines. In a standard ATM system, card and PIN numbers are required for authentication, which causes security issues like lost cards, stolen pin numbers, card cloning, shoulder surfing, fake keyboard, skimming, etc. This paper mainly focuses on the implementation of Anti spoofing based facial recognition for ATM system using liveness detection.

Jianyu Xiao [4], The Face Anti-Spoofing (FAS) methods plays a very important role in ensuring the security of face recognition systems. The existing FAS methods perform well in short-distance scenarios, e.g., phone unlocking, face payment, etc. However, it is still challenging to improve the generalization of FAS in long-distance scenarios (e.g., surveillance) due to the varying image quality.

Raghavendra Mudgalgundurao [5], This study proposes a pixel-wise supervision on DenseNet to detect presentation attacks of printed and digitally replayed attacks. The authors encourage the use of pixel-wise supervision to take use of minute hints on a variety of artifacts, including moiré patterns and artifacts left by the printers. A newly built in-house database from an operational system comprising 886 users with 433 genuine, 67 print, and 366 display attacks is utilized to show the baseline benchmark using several handcrafted and deep learning models.

Akshay Kumar [6], This research paper proposes a system for smart transaction through ATM machines using face recognition. To proceed transactions user, need to enter their registered mobile number on which an OTP will be generated subsequently the camera mounted on top of the ATM will capture user's face which will then be compared with the picture associated by the contact number using custom trained YOLO algorithm.

Siddhika Pokharkar [7], This paper presents a dual-factor authentication system that integrates face recognition and Personal Identification Number (PIN) verification to improve ATM transaction security. Utilizing a Convolutional Neural Network (CNN) for real-time face recognition, the proposed system significantly reduces the risk of unauthorized access.

Sangeetha S [8], The review also analyses research gaps and future directions in areas like multimodal fusion, explainable AI, collaborative learning, online adaptation etc. Overall, this review provides useful insights into the capabilities and limitations of existing literature which can guide future research on secure face recognition systems for attendance marking.

II. GAP ANALYSIS

Current deepfake detection systems are heavily reliant on Convolutional Neural Networks (CNNs). These models operate primarily on the spatial domain, analyzing individual video frames for visual anomalies like warped edges, pixelated regions, or artifacts in facial texture. Their strength lies in feature extraction at the frame level, quickly identifying patterns established during the fake generation process.

However, this frame-by-frame analysis treats the video stream as a series of isolated images, effectively ignoring the continuous nature of real-world video. The critical flaw is the failure to model temporal consistency. Since the system cannot compare features across time, it is highly susceptible to advanced deepfake techniques that introduce subtle, time-based noise or simply smooth out spatial artifacts between frames, thereby masking the forgery and allowing it to bypass detection.

III. PROPOSED SYSTEM

The BMNet architecture addresses the temporal limitations of CNNs by using a hybrid approach. It first extracts spatial features via a CNN backbone, and then passes these features to a Bidirectional Long Short-Term Memory (BiLSTM)network, which is designed to capture comprehensive sequential dependencies across the video timeline. This temporal modeling is further enhanced by a Multi-Head Self-Attention Mechanism (MHSAM), which intelligently weighs the most critical spatio-temporal cues, significantly enhancing the model's discriminative power and robustness against subtle, time-based forgeries.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411091|

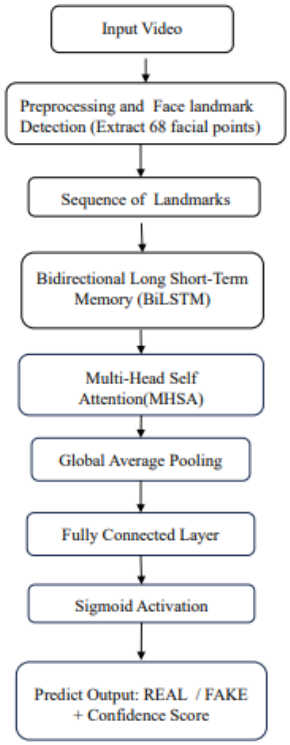


Figure 1. System Architecture

IV. CONCLUSION

In summary, the BMNet framework represents a significant advancement in deepfake detection technology by successfully integrating essential spatio-temporal analysis. The synergy between the robust BiLSTM for sequence modeling and the MHSAM for intelligent feature discrimination allows BMNet to overcome the critical weakness of prior, spatially-constrained CNN models. This novel hybrid approach confirms that it yields superior performance and improved resilience against increasingly sophisticated media manipulation, providing a more reliable foundation for identifying and combating deepfake technology.

REFERENCES

[1] Rue Marconi 19, CH- 1920, Martigny, Switzerlan" Cross Modal Focal Loss for RGBD Face Anti-Spoofing", published year arXiv:2103.00948v1 [cs.CV] 1 Mar 2021.

[2] Mathilde Caron12 Julien Mairal2 Hugo Touvron13 Ishan Misra1 Piotr Bojanowski1 Herv´e Jegou1 Armand Joulin" Emerging Properties in Self-Supervised Vision Transformers", published year arXiv:2104.14294v2 [cs.CV] 24 May 2021.

[3] Anukul Muley1, Akash Bendre2, Priti Maheshwari3, Shanmukh Kumbhar4, Prof.BhagyashreeDhakulkar," Anti-Spoofing Based Secured Transaction Using Facial Recognition And 2FA", 2022.

[4] Jianyu Xiao 1, Wei Wang 2, Lei Zhang 1 and Huanhua Liu," AMobileFaceNet-Based Face Anti-Spoofing Algorithm for Low-Quality Images", published year Electronics 2024, 13, 2801. https://doi.org/10.3390/ electronics13142801.

[5] Raghavendra Mudgal gundurao, Patrick Schuch, KiranRaja, Raghavendra Ramachandra Naser Damer "Pixel-wises upervision for presentation attack detectionon identity document cards", Accepted:7June2022.

[6] Akshay Kumar1, Pooja Joshi2, Anju Bala3, PravinkumarSudhakar Patil4, Dilip Kumar Jang Bahadur Saini5 and Kapil Joshi," Smart Transaction through an ATM Machine using Face Recognition", Accepted 30 October 2023.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411091|

[7] Siddhika Pokharkar1, Bhagyashri Bhalerao2, Pratiksha Dolas3, Dr.Anand Khatri," A Real Time Face Detection & Security System for ATM Machine." 2025.

[8] Sudha V, Sangeetha S, Ganesh Shankar S," FACE RECOGNITION-BASED ATTENDANCE SYSTEMS USING ANTI-SPOOFING METHODS", 2024.

[9] Deepti Varshney, Birendra Kumar Sharma, Mamta Bansal "Secure Watermarking to Protect Colour Images on Social Media from Misuse", Electronic Systems and Intelligent Computing. Lecture Notes in Electrical Engineering, vol 860, June 2022, Springer, Singapore, ISBN: 978-981- 16-9487-5.

[10] Deepti Varshney "Secure Watermarking Technique for Color Images using Aadhar Number, DWT and SVD" Turkish Journal of Computer and Mathematics Education,Vol.12 No.6 (2021), 4252-4268.

[11] "Robust Watermarking Technique for Sharing Family Photos on Social Media using Aadhar Number and DCT", International Journal of Recent Technology and Engineering, ISSN: 2277-3878 , Volume-9 Issue-3, September 2020. Page No.:381-387.

[12] "Watermarking for images using Alphanumeric Technique", International Journal of Recent Technology and Engineering, ISSN: 2277-3878 , Volume-8 Issue-6, March 2020. Page No.: 2639- 2645.

[13] "A Singular Value Decomposition Based Robust Image Watermarking Scheme" International Journal of Computer Science & Communication, Vol. 7,Sep 2015 - March 2016, pp 89-94, ISSN: 0973-739.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details