

Evaluating Deepfake Applications in Biometric Technology – A Review

Sameera Khan^{1&2}, B. M. Praveen³

¹ Post-Doctoral Fellow, Srinivas University, Mangalore, India,

² Assistant Professor, Vardhaman College of Engineering, Hyderabad
ORCID-ID: 0000-0002-8724-6817; E-mail: isameerakhan11@gmail.com

³ Professor, Institute of Engineering and Technology, Srinivas University,
Mangaluru, India,
ORCID-ID: 0000-0003-2895-5952; E-mail: bm.praveen@yahoo.co.in

Subject Area: Engineering and technology.

Type of the Paper: Review Paper.

Type of Review: Peer Reviewed as per [C|O|P|E|](#) guidance.

Indexed In: OpenAIRE.

DOI: <https://doi.org/10.5281/zenodo.15023220>

Google Scholar Citation: [IJAEML](#)

How to Cite this Paper:

Khan, S., & Praveen, B. M. (2025). Evaluating Deepfake Applications in Biometric Technology – A Review. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 9(1), 1-10. DOI: <https://doi.org/10.5281/zenodo.15023220>

International Journal of Applied Engineering and Management Letters (IJAEML)

A Refereed International Journal of Srinivas University, India.

Crossref DOI: <https://doi.org/10.47992/IJAEML.2581.7000.0231>

Received on: 26/02/2025

Published on: 14/03/2025

© With Authors.



This work is licensed under a [Creative Commons Attribution-Non-Commercial 4.0 International License](#) subject to proper citation to the publication source of the work.

Disclaimer: The scholarly papers as reviewed and published by Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the S.P. The S.P. disclaims of any harm or loss caused due to the published content to any party.

Evaluating Deepfake Applications in Biometric Technology – A Review

Sameera Khan^{1&2}, B. M. Praveen³

¹ Post-Doctoral Fellow, Srinivas University, Mangalore, India,

² Assistant Professor, Vardhaman College of Engineering, Hyderabad
ORCID-ID: 0000-0002-8724-6817; E-mail: isameerakhan11@gmail.com

³ Professor, Institute of Engineering and Technology, Srinivas University,
Mangaluru, India,
ORCID-ID: 0000-0003-2895-5952; E-mail: bm.praveen@yahoo.co.in

ABSTRACT

Purpose: This paper aims to comprehensively evaluate the impact of deepfake applications on biometric technologies by utilizing the Theories, Contexts, Characteristics, and Methodologies (TCCM) framework. The objective is to identify and analyze the vulnerabilities, threats, and opportunities posed by deepfake technologies to enhance the understanding and security of biometric systems.

Methodology: The research follows a systematic review of literature with the TCCM framework. Various academic sources through scopus database are analysed to obtain data regarding the intersection of deepfake technologies and biometric systems. The research focuses on analyzing the theoretical underpinnings, contextual applications, distinctive characteristics, and methodologies for detection and prevention.

Findings/Results: The review reveals that deepfake technologies pose significant threats to the integrity and reliability of biometric systems. Key findings highlight the potential of deepfakes to manipulate biometric data, leading to privacy breaches and security vulnerabilities. The study also identifies advancements in detection and prevention technologies, emphasizing the necessity for reliable security measures and ethical guidelines to mitigate risks.

Originality/Value: This review provides a novel application of the TCCM framework in regard to deepfake and biometric technologies, offering a complete analysis of current challenges and future directions. The study's findings are vital for researchers, practitioners, and policymakers seeking to understand and address the implications of deepfake technologies on biometric systems, ensuring the development of more secure and reliable biometric applications.

Paper Type: Review Paper.

Keywords: biometric, deepfake, deep learning, synthetic signature, TCCM framework

1. INTRODUCTION TO DEEPPFAKE TECHNOLOGY :

Deepfake technology is the application of artificial intelligence (AI) algorithms, specifically deep learning processes, to produce or alter digital content, generally images or videos, in a format that is hard to separate from original content. "Deepfake" is short for "deep learning" and "fake." Deep learning is part of machine learning, which is training neural networks on large data sets in order to identify patterns and produce outputs. In the case of deepfake videos, these neural networks learn to transfer the facial expressions, movements, and speech patterns of a target subject onto someone else's face in a video. This enables highly realistic videos to be created in which people are made to appear as if they said or did something they never actually did. Deepfake technology has developed very quickly over the past few years, thanks to the presence of huge amounts of data, high-performance computing resources, and ever-improving algorithms.

Overview of Biometric Authentication:

Biometric authentication makes use of distinctive physical or behavioral attributes of individuals to confirm their identity. Some common biometric modalities are fingerprints, facial recognition, iris scanning, voice verification, and even behavioral biometrics like typing rhythms or gait recognition. Biometric authentication systems collect biometric data from people, extract characteristic features, and match them with stored templates in order to authenticate or confirm their identity. Biometric

authentication has various benefits compared to conventional techniques like passwords or PINs. Biometric characteristics are inherently one-of-a-kind for the individual and challenging to impersonate, hence safer and easier for users. Also, biometric verification disbands the user's need to keep track of and remember passwords, thereby reducing unauthorized access based on weak or lost credentials.

Significance of the Intersection between Deepfake and Biometric Technology:

The intersection between deepfake and biometric technology has profound implications for security, privacy, and trust in digital systems. While biometric authentication is designed to enhance security by providing robust identity verification, deepfake technology can undermine these systems by generating highly realistic spoofing attacks.

Security Risks: Deepfake technology can be utilized to generate realistic fake biometric information, including synthetic fingerprints or facial photos, that can deceive biometric authentication systems. This can be exploited by attackers to circumvent security controls and access sensitive systems or data without authorization.

Privacy Concerns: The proliferation of deepfake technology raises serious privacy concerns, particularly regarding the manipulation of personal data. Deepfake videos can be used to generate compromising or false evidence, leading to defamation, blackmail, or other forms of exploitation. The misuse of biometric data in deepfake applications further exacerbates these privacy risks, as individuals may have limited control over how their biometric information is used or manipulated.

Trust and Reliability: The advent of deepfake technology erodes trust and credibility in digital content and authentication systems. With deepfake videos becoming more realistic and hard to identify, there is an increased threat of misinformation, social engineering attacks, and loss of trust in online interactions. In biometric authentication, the existence of deepfake attacks erodes confidence in the security and integrity of these systems, which can result in hesitation or skepticism towards their use.

Countermeasures and Mitigation Strategies: Addressing the challenges modelled by the intersection of deepfake and biometric technology requires a multi-faceted approach. This includes the development of robust authentication techniques that are resilient to spoofing attacks, such as liveness detection mechanisms and multi-modal biometric systems that combine multiple biometric modalities for enhanced security. Additionally, advancements in deepfake detection and forensic study tools are vital for identifying and mitigating the spread of manipulated content.

Research Questions-

RQ1- How do current deepfake technologies exploit vulnerabilities in biometric systems, and what theoretical frameworks can be applied to understand these security threats?

RQ2- What are the specific characteristics of deepfake applications that pose significant risks to biometric technology, and how do different contexts influence these characteristics?

RQ3- What methodologies are currently employed to detect and prevent deepfake intrusions in biometric systems, and how effective are these methods in different scenarios?

2. LITERATURE REVIEW :

In [1], the authors address the vulnerability of current face anti-spoofing (FAS) and forgery detection methods to sophisticated attacks like deepfakes. They propose a fresh approach that mixes both visual appearance and physiological cues, such as remote photoplethysmography (rPPG), to create a robust multi-modal fusion mechanism. By jointly considering FAS and forgery detection tasks, they establish a benchmark dataset and explore various deep learning models and fusion strategies. Their findings demonstrate improved generalization capabilities for both unimodal and multi-modal models, highlighting the potential of multi-task learning in improving the security of face biometric systems against presentation attacks and digital manipulation.

[2] explores the escalating threat of deepfakes in cyberspace, fueled by advancements in machine learning that blur the line between reality and fabrication. Both human and machine identification systems struggle to discern deepfakes, making them particularly insidious. Contrasting previous surveys, this paper focuses on deepfake risks to biometric systems, including facial and speech recognition. It categorizes deepfakes within each domain and outlines creation tools, datasets, and detection methods. The research's significant contribution lies in defining attack vectors across

deepfake categories and evaluating their real-world implications on various biometric systems, enhancing understanding and preparedness against such threats.

[3] introduces a deepfake detection method targeting subtly altered video segments, an under-explored area in current detection methods. Using a new benchmark dataset, the proposed method employs Vision and Timeseries Transformers to predict deepfakes at frame and video levels effectively, promising improved moderation capabilities. The experimental results demonstrate high performance.

[4] It explores the feasibility of using deepfake faces for gender classification tasks, aiming to overcome data collection challenges and privacy concerns. Through deep learning-based approaches, convolutional neural networks trained on artificial faces achieve high accuracy rates comparable to those using real faces. The research culminates in a gender-labeled deepfake facial dataset of over 200k corpora, available for research purposes, promising significant advancements in gender classification research.

[5] introduces a novel approach termed "timbre-reserved adversarial attack" for speaker identification systems. By integrating an adversarial constraint during voice conversion model training, the proposed method preserves the target speaker's timbre while exploiting vulnerabilities in the speaker identification model. The experimental results demonstrate significant improvements in attack success rate without introducing additional noise, with evaluations confirming the superior quality of generated fake audio compared to traditional adversarial perturbation methods.

Touch-based fingerprint biometrics, while widely used, faces challenges like latent prints and hygiene concerns. This spurred interest in non-contact solutions, leading to the rise of contactless fingerprint systems. However, concerns persist, including resilience against presentation attacks and limited datasets. This study addresses these by developing a comprehensive Presentation Attack Detection (PAD) dataset. Using DenseNet-121 and NasNetMobile models, the suggested algorithms achieve high accuracy rates, with tests replicating real-world scenarios against unseen spoof types [6].

[7] addresses ethical concerns in face recognition by introducing three access models in a social network, where users control their photo appearances. It replaces unapproved faces with dissimilar deepfakes and proposes new metrics. Evaluations on real and synthetic datasets show significant accuracy reduction in face recognition, supporting the efficacy of the approach.

[8] addresses the challenges faced by facial recognition systems due to COVID-19, proposing a hybrid methodology to enhance reliability. By employing a Source Camera Identification (SCI) technique based on Pixel Non-Uniformity (PNU), the system analyzes video stream integrity and detects fake frames. A prototype demonstrates high accuracy even with face masks and the ability to identify deepfake alterations, showcasing improved robustness against occlusions and forgery attacks in real-life scenarios.

[9] (Javed et al., 2022) addresses vulnerabilities in voice-controlled systems (VCS) and voice-based biometrics due to various spoofing attacks, including deepfakes with artificially generated audio. Existing countermeasures often fail to generalize across different attack types. To address this, a unified anti-spoofing framework utilizing novel acoustic-ternary co-occurrence patterns (ATCoP) is proposed. The experimental results demonstrate the effectiveness of the framework in detecting multiple spoofing attacks, including multi-order replay and cloned-replay attacks, across diverse datasets.

[10] addresses the pressing need for synthetic voice detection in light of potential malicious uses of deep learning-generated speech. A new detection approach is proposed, leveraging speaker biometric characteristics without reference to specific attacks, ensuring automatic generalization. Tested on three popular datasets, the approach demonstrates good performance, high generalization ability, and robustness to audio impairment, offering a promising solution for real-world scenarios.

[11] addresses the rising threat of deep fakes, particularly face-swapped images and videos used maliciously to discredit key figures. Current detection methods based on pixel-level artifacts lack interpretability and robustness. The proposed method leverages biometric information to exploit appearance and shape features for face-swap detection, focusing on inconsistencies in 3D facial shape and appearance. Experimental results demonstrate superior robustness across diverse data, validating the effectiveness of the approach.

[12] (Colbois & Marcel, 2022) examines GAN-based morphing attacks, exploring simple detection methods like spectral features, LBP histograms, and CNN models. While LBP-based systems show accuracy within datasets, they struggle with generalization. Pretrained ResNet proves most effective,

nearing perfect accuracy. However, LBP-based systems remain relevant due to lower computational needs and potential performance improvements in fusion with ResNet.

[13] addresses the need for precise detection of forged images and videos, focusing on expression swap detection, an area not extensively explored. A novel framework leverages facial expression recognition models to identify manipulated features, effectively localizing alterations. Demonstrated on Face2Face and Neural-Textures datasets, the method achieves higher accuracy in classification and localization compared to existing methods. Additionally, it performs comparably in detecting identity swaps, offering a generalized approach for facial manipulation detection.

[14] addresses the rising threat of deepfake technology by proposing a unified Gabor function for generating adaptive filters in convolutional neural networks (CNNs). It introduces a dual-scale large receptive field network for deepfake image recognition and evaluates its performance on four benchmark datasets. Experimental results demonstrate that the proposed adaptive Gabor filters significantly decrease model size while upholding performance, offering a promising solution for deepfake detection.

[15] evaluates deep face recognition's effectiveness in identifying deepfakes, surpassing traditional two-class CNNs. Using various loss functions and deepfake generation techniques, it achieves an AUC of 0.98 and EER of 7.1% on Celeb-DF, and an AUC of 0.99 and EER of 2.04% on FaceForensics++, bypassing the need for large fake datasets

[16] addresses the growing concern around voice authentication vulnerabilities due to advances in voice recognition technology and the proliferation of sound editing tools and deep-fake concepts. It outlines an approach for penetration testing of voice recognition solutions and dispels common misconceptions regarding voice pattern characteristics, aiming to enhance security measures in voice authentication systems.

[17] proposes a method to detect DeepFakes with minimal computational power by enhancing MesoNet with new activation functions. Replacing original activations yields over 1% improvement and enhances result consistency. Additionally, a new activation function, "Pish," is introduced and verified to offer even higher accuracy with slight time overhead on specific datasets.

[18] presents a biometric-based forensic method for detecting face-swap deepfakes, crucial in combatting their potential for widespread misinformation and harm. The technique integrates static facial recognition with a temporal, behavioral biometric utilizing facial expressions and head movements, learned through a CNN with a metric-learning objective. Demonstrated across various large-scale video datasets and real-world scenarios, the approach proves effective in detecting deepfakes and mitigating their harmful impacts.

[19] addresses the growing threat of photorealistic deep fakes by proposing an approach to not only differentiate them from real videos but also identify the specific generative model used. By leveraging biological signals, particularly spatiotemporal patterns in photoplethysmogram (PPG) data, the method disentangles manipulation artifacts from the generator's residuals. The experimental results demonstrate appropriate accuracy in detecting fake videos (97.29%) and identifying the source model (93.39%), highlighting the effectiveness of the proposed approach.

[20] introduces a dataset of Deepfake videos created from the VidTIMIT database, emphasizing the impact of training and blending parameters on video quality. Results reveal vulnerabilities of state-of-the-art face recognition systems to Deepfake videos, with false acceptance rates of 85.62% and 95.00%. Baseline approaches show a promising equal error rate of 8.97% on high-quality Deepfakes. The study underscores the challenges posed by GAN-generated Deepfake videos for recognition systems and detection methods, highlighting the need for further research.

Table 1: Summary of Literature Review

| S. no | Title | Year | Technology used | Modality |
|-------|---|------|---|----------|
| 1 | “Benchmarking Joint Face Spoofing and Forgery Detection with Visual and Physiological Cues” | 2024 | Deep learning, visual appearance, physiological cues, CNN | Face |

| | | | | |
|----|---|------|--|--------------|
| 2 | “Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors” | 2023 | Machine learning, deep learning, datasets, detection methods | Face, Speech |
| 3 | “Undercover Deepfakes: Detecting Fake Segments in Videos” | 2023 | Vision Transformer, Timeseries Transformer, benchmark dataset | Face, Video |
| 4 | “Deep Learning-Based Gender Classification by Training With Fake Data’ | 2023 | Deep learning, convolutional neural networks, benchmark dataset | Face |
| 5 | “Timbre-Reserved Adversarial Attack in Speaker Identification” | 2023 | Adversarial attack, voice conversion model, speaker identification | Voice |
| 6 | “Presentation Attack Detection with Advanced CNN Models for Noncontact-based Fingerprint Systems” | 2023 | Deep learning, DenseNet-121, NasNetMobile, benchmark dataset | Fingerprint |
| 7 | “My Face My Choice: Privacy Enhancing Deepfakes for Social Media Anonymization” | 2023 | Deep learning, convolutional neural networks, access models | Face |
| 8 | “A PNU-Based Methodology to Improve the Reliability of Biometric Systems” | 2022 | Source Camera Identification (SCI) technique, Pixel Non-Uniformity (PNU) | Face |
| 9 | “Voice spoofing detector: A unified anti-spoofing framework” | 2022 | Acoustic-ternary co-occurrence patterns (ATCoP), unified anti-spoofing framework | Voice |
| 10 | “Deepfake audio detection by speaker verification” | 2022 | Speaker biometric characteristics, voice recognition tools | Voice |
| 11 | “Robust Face-Swap Detection Based on 3D Facial Shape Information” | 2022 | Deep learning, biometric information, 3D facial shape, appearance | Face |
| 12 | “On the detection of morphing attacks generated by GANs” | 2022 | Spectral features, LBP histograms, CNN, ResNet | Face |
| 13 | “Detection and Localization of Facial Expression Manipulations” | 2022 | Facial expression recognition models, video datasets | Face |
| 14 | “Convolutional Neural Network Based on Diverse Gabor Filters for Deepfake Recognition” | 2022 | Gabor function, convolutional neural networks | Face |
| 15 | ‘An Experimental Evaluation on Deepfake Detection using Deep Face Recognition” | 2021 | Deep learning, face recognition systems, Celeb-DF, FaceForensics++ | Face |
| 16 | “Breaking voice authentication - Security testing approach” | 2021 | Voice recognition solutions, penetration testing | Voice |
| 17 | “Verify it yourself: A note on activation functions’ influence on fast deepfake detection” | 2021 | MesoNet, activation functions, "Pish" | Face |
| 18 | “Detecting Deep-Fake Videos from Appearance and Behaviour” | 2020 | Facial recognition, behavioural biometric, CNN | Face |
| 19 | “How do the hearts of deep fakes beat? deep fake source detection via interpreting residuals with biological signals” | 2020 | Biological signals, photoplethysmogram (PPG) data | Face |
| 20 | “Vulnerability assessment and detection of Deepfake videos” | 2019 | Deep learning, VidTIMIT database | Face |

3. RESULTS AND DISCUSSION :

This study presents an extensive examination of the current landscape of synthetic biometrics, particularly focusing on deepfakes and their implications for biometric security systems. The findings reveal several key insights based on the TCCM framework proposed by [21] for systematic literature reviews. The TCCM framework is designed to deliver a structured approach to writing literature reviews, particularly within the field of Information Systems (IS) research. It helps organize the review of literature based on:

- Theory:** Identifying the theories that underpin the research in the reviewed studies.
- Context:** Outlining the situational or environmental factors where the research is applied.
- Characteristics:** Detailing the specific features, properties, or attributes studied.
- Methodology:** Describing the research methods used in the studies, such as qualitative, quantitative, or mixed-method approaches.

Theories

Theoretical exploration within the domain of synthetic biometrics has primarily centered on the detection of deepfake and synthetic attacks. This includes exploring the vulnerabilities inherent in face and audio biometric systems. The use of synthetic data to enhance the training of biometric classification systems, such as gender recognition, demonstrates the innovative approaches being considered to improve accuracy and reliability. Furthermore, theories surrounding adversarial attacks on biometric systems provide critical insights into the potential methods attackers might use to bypass security measures. These theoretical frameworks lay the groundwork for developing more robust and resilient biometric authentication systems.

Contexts

The context of this study spans a wide array of applications in biometric security, with a particular focus on facial recognition and voice authentication systems. The increasing prevalence of deepfakes in the public domain has significant implications for personal privacy and security. The research points to the importance of better measures in preserving video integrity and secure authentication. This is especially so in social media environments where privacy is of utmost importance. As biometric authentication becomes more widespread, the significance of secure and dependable systems grows even more critical, highlighting the need for continuous research and development on this matter.

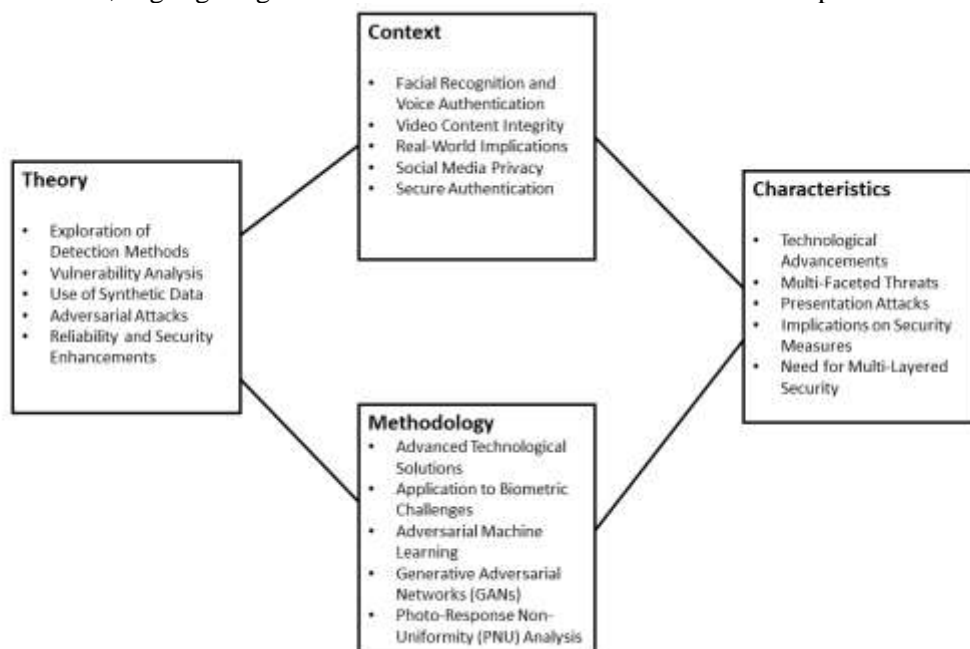


Figure 1- Review of Deepfake Applications in Biometric Technology through TCCM framework Characteristics

The characteristics of synthetic biometric threats are diverse and complex, reflecting the rapid advancements in technology. The study identifies the specific types of attacks, such as presentation attacks that preserve timbre in audio or physiological cues in facial recognition, which pose significant challenges to existing security measures. These multi-faceted threats require a comprehensive

approach to security, integrating multiple layers of defense to effectively counteract potential breaches. The implications of these characteristics on current security protocols are profound, necessitating a shift towards more adaptive and dynamic security solutions.

Methodologies

A range of advanced technological solutions has been employed to address the challenges posed by synthetic biometrics. The study highlights the use of deep learning models and convolutional neural networks (CNNs) for the detection of fake video segments and the improvement of gender classification accuracy. Adversarial machine learning techniques have also been utilized to test the robustness of biometric systems, highlighting areas for potential enhancement. The use of generative adversarial networks (GANs) in detecting morphing attacks and photo-response non-uniformity (PNU) analysis to bolster system reliability are indicative of the innovative methodologies being explored. These approaches represent a significant step forward in the development of more secure and reliable biometric systems.

4. FUTURE SCOPE :

The future researches can be guided towards more robust detection algorithms, ethical frameworks and multimodal biometric detection. **Advanced Detection Algorithms:** Develop and refine algorithms capable of identifying and adapting to new and evolving deepfake techniques, ensuring continuous protection of biometric systems against sophisticated attacks. **Multi-Modal Biometric Systems:** Explore the integration of multi-modal biometric systems that combine multiple biometric traits, such as facial recognition, voice recognition, and fingerprinting, to enhance security and reduce vulnerabilities to deepfake manipulations. **Ethical and Legal Frameworks:** Conduct in-depth studies on the ethical and legal implications of using deepfake technology in biometrics, focusing on establishing guidelines and regulations to govern the responsible use of this technology. **Collaborative Research and Development:** Encourage partnerships between academia, industry, and governmental organizations to accelerate innovation in creating more secure and reliable biometric systems that can withstand deepfake attacks. **Real-World Application Testing:** Implement pilot projects and real-world testing of new deepfake detection methods and biometric system integrations to evaluate their effectiveness and practicality in diverse environments and scenarios.













5. CONCLUSION :

This review aimed to evaluate the applications of deepfake technology in biometric systems using the TCCM (Theories, Contexts, Characteristics, and Methodologies) framework. Through this evaluation, several insights have been gathered concerning the interaction between deepfakes and biometric technologies, addressing the research questions posed.

First, deepfake technologies exploit specific vulnerabilities in biometric systems by manipulating visual and audio data. Theoretical frameworks such as adversarial machine learning and generative adversarial networks (GANs) illustrate the ease with which deepfakes can imitate biometric traits. This theoretical understanding is crucial for developing more robust biometric security systems that can withstand such sophisticated attacks. Second, the study highlights the characteristics of deepfake applications that pose significant risks to biometric systems. These include high levels of realism and adaptability to different biometric modalities, such as facial recognition and voice authentication. The influence of various contexts, such as the type of biometric modality and the environment in which it is deployed, affects the effectiveness of deepfake attacks. Understanding these characteristics is vital for creating targeted solutions that address specific vulnerabilities in different contexts. Finally, the methodologies currently employed to detect and prevent deepfake intrusions in biometric systems vary in their effectiveness. Techniques such as deep learning-based detection, adversarial training, and physiological signal analysis have shown promise in identifying and mitigating deepfake threats. However, their effectiveness can be context-dependent, with variations in performance based on the type of biometric system and the nature of the deepfake. Continued research and development in these methodologies are essential to enhance the resilience of biometric technologies against deepfake attacks.

The intersection of deepfake technology and biometric systems presents both challenges and opportunities. By understanding the theoretical foundations, contextual influences, and characteristic threats posed by deepfakes, as well as the effectiveness of current methodologies, a more robust biometric security solutions can be developed .

REFERENCES :

- [1] Yu, Z., Cai, R., Li, Z., Yang, W., Shi, J., & Kot, A. C. (2024). Benchmarking Joint Face Spoofing and Forgery Detection with Visual and Physiological Cues. *IEEE Transactions on Dependable and Secure Computing*, 1–15. <https://doi.org/10.1109/TDSC.2024.3352049> [Google Scholar](#) 
- [2] Firc, A., Malinka, K., & Hanáček, P. (2023). Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors, e15090. *Heliyon*, 9(4). <https://doi.org/10.1016/j.heliyon.2023.e15090> [Google Scholar](#) 
- [3] Saha, S., Perera, R., Seneviratne, S., Malepathirana, T., Rasnayaka, S., Geethika, D., Sim, T., & Halgamuge, S. (2023). Undercover Deepfakes: Detecting Fake Segments in Videos. *Proceedings - 2023 IEEE/CVF International Conference on Computer Vision Workshops, ICCVW 2023*, 415–425. <https://doi.org/10.1109/ICCVW60793.2023.00048> [Google Scholar](#) 
- [4] Oulad-Kaddour, M., Haddadou, H., Vilda, C. C., Palacios-Alonso, D., Benatchba, K., & Cabello, E. (2023). Deep Learning-Based Gender Classification by Training With Fake Data. *IEEE Access*, 11, 120766–120779. <https://doi.org/10.1109/ACCESS.2023.3328210> [Google Scholar](#) 
- [5] Wang, Q., Yao, J., Zhang, L., Guo, P., & Xie, L. (2023). Timbre-Reserved Adversarial Attack in Speaker Identification. *IEEE/ACM Transactions on Audio Speech and Language Processing*, 31, 3848–3858. <https://doi.org/10.1109/TASLP.2023.3306714> [Google Scholar](#) 
- [6] Purnapatra, S., Miller-Lynch, C., Miner, S., Liu, Y., Bahmani, K., Dey, S., & Schuckers, S. (2023). Presentation Attack Detection with Advanced CNN Models for Noncontact-based Fingerprint Systems. *2023 11th International Workshop on Biometrics and Forensics, IWBF 2023*, 1-6. <https://doi.org/10.1109/IWBF57495.2023.10157605> [Google Scholar](#) 
- [7] Ciftci, U. A., Yuksek, G., & Demir, I. (2023). My Face My Choice: Privacy Enhancing Deepfakes for Social Media Anonymization. *Proceedings - 2023 IEEE Winter Conference on Applications of Computer Vision, WACV 2023*, 1369–1379. <https://doi.org/10.1109/WACV56688.2023.00142> [Google Scholar](#) 
- [8] Capasso, P., Cimmino, L., Abate, A. F., Bruno, A., & Cattaneo, G. (2022). A PNU-Based Methodology to Improve the Reliability of Biometric Systems. *Sensors*, 22(16), 1-15. <https://doi.org/10.3390/s22166074> [Google Scholar](#) 
- [9] Javed, A., Malik, K. M., Malik, H., & Irtaza, A. (2022). Voice spoofing detector: A unified anti-spoofing framework. *Expert Systems with Applications*, 198, 1-15. <https://doi.org/10.1016/j.eswa.2022.116770> [Google Scholar](#) 
- [10] Pianese, A., Cozzolino, D., Poggi, G., & Verdoliva, L. (2022). Deepfake audio detection by speaker verification. *2022 IEEE International Workshop on Information Forensics and Security, WIFS 2022*, 1-6. <https://doi.org/10.1109/WIFS55849.2022.9975428> [Google Scholar](#) 
- [11] Guan, W., Wang, W., Dong, J., Peng, B., & Tan, T. (2022). Robust Face-Swap Detection Based on 3D Facial Shape Information. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 13604 LNAI, 404–415. https://doi.org/10.1007/978-3-031-20497-5_33 [Google Scholar](#) 
- [12] Colbois, L., & Marcel, S. (2022). On the detection of morphing attacks generated by GANs. *BIOSIG 2022 - Proceedings of the 21st International Conference of the Biometrics Special Interest Group*, 1-5. <https://doi.org/10.1109/BIOSIG55365.2022.9897046> [Google Scholar](#) 
- [13] Mazaheri, G., & Roy-Chowdhury, A. K. (2022). Detection and Localization of Facial Expression Manipulations. *Proceedings - 2022 IEEE/CVF Winter Conference on Applications of Computer Vision, WACV 2022*, 2773–2783. <https://doi.org/10.1109/WACV51458.2022.00283> [Google Scholar](#) 
- [14] Khalifa, A. H., Zaher, N. A., Abdallah, A. S., & Fakhr, M. W. (2022). Convolutional Neural Network Based on Diverse Gabor Filters for Deepfake Recognition. *IEEE Access*, 10, 22678–22686. <https://doi.org/10.1109/ACCESS.2022.3152029> [Google Scholar](#) 

- [15] Ramachandran, S., Nadimpalli, A. V., & Rattani, A. (2021). An Experimental Evaluation on Deepfake Detection using Deep Face Recognition. *Proceedings - International Carnahan Conference on Security Technology, 2021-October*, 1-6. <https://doi.org/10.1109/ICCST49569.2021.9717407> [Google Scholar ↗](#)
- [16] Dziegielewska, O. (2021). Breaking voice authentication - Security testing approach. *IBIMA Business Review, 2021.1-11*, <https://doi.org/10.5171/2021.198312> [Google Scholar ↗](#)
- [17] Kawa, P., & Syga, P. (2021). Verify it yourself: A note on activation functions' influence on fast deepfake detection. *Proceedings of the 18th International Conference on Security and Cryptography, SECRYPT 2021*, 779–784. <https://doi.org/10.5220/0010581707790784> [Google Scholar ↗](#)
- [18] Agarwal, S., Farid, H., El-Gaaly, T., & Lim, S.-N. (2020). Detecting Deep-Fake Videos from Appearance and Behavior. *2020 IEEE International Workshop on Information Forensics and Security, WIFS 2020*. 1-6, <https://doi.org/10.1109/WIFS49906.2020.9360904> [Google Scholar ↗](#)
- [19] Ciftci, U. A., Demir, I., & Yin, L. (2020). How do the hearts of deep fakes beat? deep fake source detection via interpreting residuals with biological signals. *IJCB 2020 - IEEE/IAPR International Joint Conference on Biometrics, 1-10*. <https://doi.org/10.1109/IJCB48548.2020.9304909> [Google Scholar ↗](#)
- [20] Korshunov, P., & Marcel, S. (2019). Vulnerability assessment and detection of Deepfake videos. *2019 International Conference on Biometrics, ICB 2019*, 1-6. <https://doi.org/10.1109/ICB45273.2019.8987375> [Google Scholar ↗](#)
- [21] Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly, 26(2)*, xiii–xxiii. <http://www.jstor.org/stable/4132319> [Google Scholar ↗](#)
