Synthetic Biometrics for Next-Generation Identity Systems: A Comprehensive Review

Sameera Khan[1], Eugenio Vocaturo[2]
[1] Lincoln University College, Petaling Jaya, Malaysia ; [2] University of Calabria, Italy;
Email ID -isameerakhan11@gmail.com

Abstract: The accelerated development of the generative AI has greatly changed the environment of the biometric identity systems. In the last ten years, Generative Adversarial Networks (GANs), Recurrent Neural Networks (RNNs), diffusion models, and transformers have made it possible to synthesize very realistic biometric identifiers, such as face, fingerprint, voice, and handwritten signatures. The developments present effective ways to address the long-term issues of the lack of data, demographic disequilibrium, and the weak regulation around sensitive identity data. Meanwhile, they also present new threats, such as deep fake-based spoofing, template inversion, adversarial manipulation, and systemic amplification of bias. This general survey discusses the history of synthetic biometric generation, threat models, forensic detection tools, as well as privacy-sensitive models. It brings together the insights of biometric security, forensic analysis and privacy-conscious AI systems, mentioning methods to perform reversible de-identification, detect deepfakes in the frequency domain, multimodal authentication, and optimisation-based model improvement. The review also compares new methods such as fairness-conscious evaluation procedures, decentralized identity systems, and machine unlearning in identity revocation and regulatory adherence. On the basis of this synthesis, an enhanced research agenda has been stated to inform the safe, fair, and confidential creation of the next-generation synthetic biometric identity systems.

Keywords: Deepfakes; GAN; Synthetic Signatures; Biometrics; Cybersecurity;

Introduction

The rapid advancement of artificial intelligence has fundamentally transformed digital media creation and manipulation. The recent deep learning models including Generative Adversarial Networks (GANs), diffusion models, and transformer-based models, are now capable of generating highly realistic synthetic images, audio and video that are progressively indistinguishable to the original data. Although early applications of generative models were limited to the domain of creativity and entertainment, their integration into security-critical systems has introduced significant implications for digital identity.

Biometric authentication involves the use of unique physiological and behavioral characteristics like facial features, fingerprints, irises, voice patterns and handwritten signatures to identify the identity with high level of certainty [1][2]. These modalities form the basis of authentication in financial transactions, border control, healthcare systems, and online governance platforms. However, with the advent of synthetic biometric generation, biometric permanence and uniqueness assumptions have been challenged. Deepfake-enabled manipulation introduces new challenges related to trust, authenticity, and system resilience, particularly in adversarial and high-stakes environments. [3], [4]

Growing body of literature has delved into the application of generative models in the synthesis of biometric features across modalities. These studies shows a significant enhancement in the realism, the controllability and data augmentation capabilities. Meanwhile, synthetic biometrics represent a complicated set of vulnerabilities, such as the presentation attacks, morphing, template inversion, adversarial manipulation, and the amplification of bias. Through the accelerated verge of technical advancement, research is still divided among modalities and mostly focused on the quality of generative results rather than systemic issues like fairness auditing, privacy concerns, lifecycle management, and the unitary benchmarking [5].

The current paper is a synthesis of the up-to-date research in synthetic biometrics, which includes but is not limited to generative architectures, security threat model, forensic detection, fairness-conscious evaluation, privacy-conscious identity mechanisms, and newer methods, like machine unlearning in identity revocation. The paper aims to establish a systematic basis to the secure, fair, and responsible development of next-generation biometric identity systems by connecting these dimensions.

Related work

The intersection of biometric technology and deepfakes is an emerging research area, as it represents a double-edged sword. GANs are capable of creating highly realistic artificial biometric data, and they also pose severe threats to security and privacy. Conventionally, authentication and verification are highly reliant on biometrics for their uniqueness and permanence of human traits such as fingerprints, facial features, voice, or handwritten signatures. The recent advances in GANs have disturbed this perception heavily by generating synthetic biometric traits that are indistinguishable from the real ones. Due to this, new possibilities of data manipulation, training, and testing are available. Especially where large and diverse datasets cannot be collected, a synthetic dataset can be a savior. Although it is proving to be threatening to the security systems, too, through deepfake-based spoofing attacks.[6], [7].

Table 1. Summary of Literature review

Reference	Modality	Generative Approach / Model	Objective of Study	Dataset Type / Scale	Evaluation Metrics	Security Analysis Conducted?	Fairness / Bias Consideration	Privacy / Regulatory Alignment	Key Findings / Limitations
[8]	Face / Video	GAN (SimSwap, GHOST, FSGAN)	De-identify driver videos for data sharing in driving studies.	Naturalistic Driving Study (NDS); 9 participants.	Head pose error, EAR, LAR, SSIM, PSNR.	**Yes** (Re-identification risks).	Gender combinations evaluated for swapping.	HIPAA/Common Rule alignment.	SimSwap best preserved behavior; automated thresholds needed.
[9]	Face	BiGAN (Bidirectional GAN)	Compact face representation to reduce bandwidth in online meetings.	813 frames of an individual's face.	SSIM, PSNR, Data Compression Ratio (DCR).	**No** (Focus on operational efficiency).	Model ability to generalize to unseen data.	Bandwidth optimization for remote interaction.	Outperformed MPEG-2; 16-dim vector provides expressiveness.

[10]	Face & Hair	Controllable GAN (SimSwap backbone)	Real-time face/hair swapping to conceal identity in interviews.	CelebA-HQ, LFW; Internet videos.	Attribute preservation score, User study.	**Yes** (Identity security/witness protection).	Preservation of age and gender of original subject.	Witness safety and anonymous conferencing.	Successfully disconnected real identity from exchanged traits.
[11]	Face (Medical)	StyleGAN2-ADA	Generate high-fidelity rosacea images from limited medical data.	"Irish Dataset"; 300 full-face images.	KID, FID, MOS (Expert rating).	**No** (Focus on clinical diagnosis utility).	Standardized full-face approach across races.	GDPR adherence; Anonymization confirmed.	R1 regularization crucial for convergence on small data.
[12]	Face	GaFaR (GAN + GNeRF)	Evaluate vulnerability to template inversion (TI) attacks using 3D.	MOBIO, LFW, FFHQ (70k images).	Success Attack Rate (SAR), Cosine Similarity.	**Yes** (Whitebox/ Blackbox TI attacks).	Identification of demographic leakage (age, gender).	High privacy threat from leaked templates.	3D reconstruction is more dangerous for recognition systems than 2D.
[13]	Fingerprint	pix2pix (cGAN)	Create privacy-friendly mated synthetic fingerprint impressions.	FVC2002/2004; 40,000 samples (AMSL SynFP).	NFIQ2, Verifinger SDK (Matching score).	**No** (Focus on algorithm evaluation).	Basic pattern distribution (UL, RL, WH, AR, TA).	GDPR (Article 9) harmonization.	Mated impressions viable via minutiae map modification.
[14]	Face	GAN (Multiple subnetworks)	Gender-preserving face aging for imbalanced data.	Age_FR (181,824 images); CACD.	Verification accuracy, Age balance loss.	**No** (Focus on image translation).	High emphasis on maintaining gender attributes.	Missing child location and fugitive identification.	Relative 3.75% improvement in gender accuracy over baselines.
[15]	Fingerprint	SpoofGAN (Multi-stage GAN)	Generate synthetic spoof fingerprints to boost detection models.	LivDet, GCT; 38,164 live/3,366 spoof images.	TDR @ FDR, NFIQ2, Minutiae quality.	**Yes** (Presentation Attack Detection).	Minority class (thumb) imbalance noted.	Identity leakage checked (low risk found).	Only 25% real data needed when augmented by synthetic spoofs.
[16]	Face	StyleGAN2 (Inversion)	Discriminate between real and GAN-generated faces.	FFHQ, CelebA, LFW, Caltech.	Global Accuracy, AUC, ROC.	**Yes** (Forensic forgery detection).	Demographics (age, gender) included in corpora.	Robustness to social network sharing.	Landmark-based SVM yields >88% detection accuracy.
[17]	Iris	StyleGAN3	Comparative analysis of Cartesian vs.	CASIAv3, Warsaw-	FID, Hamming	**No** (Focus on data	Multi-dataset diversity.	GDPR compliance; banned	Polar representation carries lower

			Polar iris generation.	BioBase; 1327 unique irises.	Distance (OSIRIS).	augmentation).		real datasets alternative.	"identity leak" risk.
[18]	Face (Medical)	3DG-GA (GAN + Genetic Algorithm)	Generate facial drug abuse images for sensitive research.	IDAD (120 people) upscaled to 3000 synthetic.	Accuracy, Facial Asymmetry, Forgery Detect.	**Yes** (Forgery detection check).	Ethnic plurality and both genders.	Anonymity guaranteed to avoid legal restrictions.	Achieved 97.2% accuracy on unseen real-world validation data.
[19]	Face	StyleGAN3, ProGAN, InterfaceGAN	Forensic detection of static deepfakes via frequency artifacts.	CelebA + Multi-GAN Mixed Dataset (15k images).	Accuracy, F1-score, Precision, Recall.	**Yes** (Deepfake detection/Taxonomy).	Mixed dataset for cross-model generalization.	Combating misinformation/digital fraud.	SVM with RBF kernel achieved 100% detection accuracy.
[20]	Face	PPSA-GAN (Self-Attention) + Blockchain	Secure storage and generation of synthetic faces.	CelebA (202,599 images).	Inception Score (IS), FID, Accuracy.	**Yes** (Blockchain-based immutability).	Demographic bias (age/gender) noted as limitation.	Decentralized ledger for auditing/privacy.	Synergy of GAN and Blockchain ensures verifiable storage.
[21]	Face	IPCGAN-Alexnet (Optimal variant)	Speed up face aging while preserving identity.	CACD; 100 identities (500 generated).	k-NN/SVM accuracy, Training speed.	**No** (Focus on computational efficiency).	Balanced age group distribution.	Cross-aging recognition enhancement.	17% faster training by reducing residual layers.
[22]	Face	CycleGAN	Generate synthetic disguised faces (beards, makeup, glasses).	Sejong Face Database (SFD); 12,600 images.	Rank-1 recognition rate, FID, KID.	**Yes** (Spoofing/Disguise robustness).	Gender-specific add-ons (wigs/beards).	Privacy concerns of real disguised subjects.	Training on synthetic data improved recognition by 68.3%.

The literature review shows that the field of generative modeling towards biometric systems as a use of GANs, diffusion-based models, and hybrid deep learning has made significant evolutionary strides on facial, fingerprint, signature, iris, and voice data representations. In spite of the considerable achievements in the context of the improvement of perceptual realism and diversity, the majority of the studies are specific to the modality and limited by the datasets. There is limited cross-domain generalizability and integrated multimodal synthesis frameworks that exudes the need to have more systematic integration in architecture and evaluation.

Synthetic biometric Security assessments in the literature verify that synthetic biometric systems create severe vulnerabilities, such as presentation attacks, morphing, deep fake-based spoofing, template inversion, and adversarial manipulation. Though detection techniques including liveness detection, GAN-conscious classifiers and multi-modal fusion approaches have been presented, there is still fragmentation

in terms of comprehensive threat modelling and adversarial stress-testing procedures. Also, fairness issues are not represented to a great extent. Seldom are such factors as demographic imbalance, accessibility limitations, and amplification of bias in generative models evaluated based on structured evaluation metrics. Privacy-preserving statements are often talked about but rarely implemented in regulatory standards like identity ecosystems in accordance with GDPR. Equally, identity lifecycle management, especially the revocation and the right-to-be-forgotten compliance, has been given little consideration in biometric pipelines. Lastly, the unavailability of standardized benchmarking suites, harmonized datasets, and single evaluation protocols restricts reproducibility and comparability of studies. In light of these identified gaps, the companion study will focus on the following objectives:

1. To develop and evaluate advanced generative models for high-fidelity synthesis of multimodal biometric traits (e.g., signatures, fingerprints, face, voice) with emphasis on realism, diversity, and cross-domain generalizability.
2. To analyse the security vulnerabilities of synthetic biometric systems by designing and testing adversarial, spoofing, and deepfake-based attack scenarios, and by proposing robust countermeasures for secure authentication.
3. To design fairness-aware evaluation metrics and protocols that identify and mitigate demographic, accessibility, and dataset imbalance biases in synthetic biometric generation and verification.
4. To develop privacy-preserving frameworks for biometric authentication using synthetic identities in centralized and decentralized digital ecosystems, ensuring compliance with data-protection mandates.
5. To integrate machine unlearning into biometric pipelines for dynamic identity control, enabling revocation, right-to-be-forgotten compliance, and removal of user influence from trained models without full retraining.
6. To build a comprehensive benchmarking suite—including datasets, threat models, evaluation metrics, and protocols—to guide the secure, fair, and ethical deployment of next-generation synthetic biometric identity systems.

Discussion

The literature portrays that synthetic biometrics are both a technological breakthrough and a structural vulnerability of the contemporary identity structures. Recent innovations in generative models and especially GANs, diffusion models, and hybrid ones have enabled a greater level of realism, diversity, and controllability of synthetic biometric features in a variety of modalities, including face, fingerprint, iris, voice, and signature. These advancements are actual advantages. Synthetic data has the ability to overcome scarcity of datasets, minimize demographic imbalance, allow controlled experimentation, and facilitate privacy-sensitive model development without necessarily exposing personal biometric data. Synthetic generation offers a possible route of research and system-development in regulated areas where data gathering is limited.

Nonetheless, systemic risk is enhanced by the same characteristics that make synthetic biometrics useful. The high-fidelity generative models reduce the identity spoofing, attack presentation, morphing, and template reconstruction barriers. Identity-specific forgeries are made possible by controllable

architectures and gradually more stable models contain fewer artifacts that can be detected and used by traditional verification systems. The attack area grows along with the biometric authentication in the financial, legal, healthcare, and governmental systems. It is no longer a question of whether synthetic biometrics can be used to fool automated systems, but the key issue is how robust those systems are in the face of adaptive adversarial pressure.

The other vital observation that comes out of the review is the lack of balance between the generative innovation and responsible deployment. The majority of research emphasizes realism and performance indicators like FID, EER, or accuracy but relatively less study adds information on fairness auditing, mitigation of demographic biases, and inclusion of accessibility and compliance with regulations. The amplification of bias due to synthetic-based datasets is not well studied, especially in non-Western culture and biometric situations. In the same manner, preservation of privacy is usually presented as an advantage of synthetic data, but its formal implementation with decentralized identity architectures, data minimization principles, as well as right-to-be-forgotten mechanisms is not underdeveloped.

Lack of standardized benchmarking protocols also makes evaluation more difficult. There is difference in demographic composition of datasets, imprecise definition of threat models and inconsistency in attack simulations of varying sophistication. The lack of harmonized assessment systems limits the comparability of cross studies. This fragmentation highlights the importance of holistic suites of benchmarking that combine generative quality, adversarial robustness, fairness measures, and privacy assurances into one evaluative framework. Technical constraints of the existing body of research exist as well. Most research is centered on individual modalities in controlled conditions and cannot be generalized. Video-based biometrics temporal consistency, multimodal systems cross-modal coherence, and resistance against the changing generative architecture are open problems. In addition, biometric pipelines have not systematically been embedded with lifecycle management, specifically identity revocation and machine unlearning.

Finally, biometrics created artificially challenge the line between true and false identity. Their long-term feasibility will be based not only on the sophistication in models, but also on the concerted progress in security engineering, fairness auditing, privacy preserving design, regulation compliance, and interdisciplinary governance. The field is at a transitional point: now it is no longer about proving what generative models can create, but how these systems can be implemented in a responsible manner in adversarial and socially sensitive settings.

Conclusion & Future Scope

Discuss The article has discussed the dynamic nature of synthetic biometrics in the future of identity systems that use next-generation methods, but it has also summarized the progress in generative modelling, security assessment, fairness assessment, privacy preservation, and identity lifecycle management. It has been shown in the literature that generative architectures, such as GANs, diffusion models, and hybrid frameworks, have attained significant progress in realism, controllability, and scalability across a variety of biometric modalities. Such abilities make synthetic data a useful resource in solving the problem of data sets being scarce, allowing controlled experimentation, and facilitating

privacy-conscious development in controlled settings. Synthetic biometrics have high-fidelity that makes them more prone to spoofing, morphing, template reconstruction, and adversarial manipulation. The blistering development of generative models remains to put the traditional authentication pipelines under the challenge, which highlights the necessity of adaptable defensive measures. Of the same importance is unresolved issues on demographic bias, exclusion in access to services, regulatory compliance and no standard benchmarking protocols.

Future studies should not concentrate on the performance of the isolated models but on the system design. It should focus on multimodal generative models based on cross-domain generalizability, cross-domain adversarial stress testing, fairness-conscience evaluation measures and privacy-preserving authentication systems in accordance with the emerging data-protection requirements. The incorporation of machine unlearning into biometric pipelines presents a positive trend to dynamic identity revocation and the right-to-be-forgotten compliance. Also, the creation of full benchmarking suites through which datasets, threat models and evaluation metrics are in harmony will be essential to reproducibility and responsible deployment. Synthetic biometrics is transforming the digital identity architecture. Their long-term sustainability will not only rely on the generative sophistication, but also the intentional convergence between the security engineering, fairness auditing, privacy directing and interdisciplinary control.

References

[1] S. Khan, M. Mishra, and V. K. Mishra, “Autogenic, prognostic, and collective signature affirmation framework based on diverse set of features,” *Int. J. Biom.*, vol. 15, no. 5, pp. 539–559, 2023, doi: 10.1504/IJBM.2023.133124.

[2] S. Khan, M. Mishra, and V. K. Mishra, “Use of synthetic signature images for biometric authentication and forensic investigation,” *Int. J. Biom.*, vol. 15, no. 6, pp. 685–704, 2023, doi: 10.1504/IJBM.2023.133957.

[3] D. T. Toledano, R. Fernández Pozo, A. Hernández Trapote, and L. Hernández Gómez, “Usability evaluation of multi-modal biometric verification systems,” *Interact. Comput.*, vol. 18, no. 5, pp. 1101–1122, 2006, doi: 10.1016/j.intcom.2006.01.004.

[4] S. Purnapatra *et al.*, “Presentation Attack Detection with Advanced CNN Models for Noncontact-based Fingerprint Systems,” in *2023 11th International Workshop on Biometrics and Forensics, IWBF 2023*, 2023. doi: 10.1109/IWBF57495.2023.10157605.

[5] L. Colbois and S. Marcel, “On the detection of morphing attacks generated by GANs,” in *BIOSIG 2022 - Proceedings of the 21st International Conference of the Biometrics Special Interest Group*, 2022. doi: 10.1109/BIOSIG55365.2022.9897046.

[6] S. Saha *et al.*, “Undercover Deepfakes: Detecting Fake Segments in Videos,” in *Proceedings - 2023 IEEE/CVF International Conference on Computer Vision Workshops, ICCVW 2023*, 2023, pp. 415–425. doi: 10.1109/ICCVW60793.2023.00048.

[7] A. Firc, K. Malinka, and P. Hanáček, “Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors,” *Heliyon*, vol. 9, no. 4, 2023, doi: 10.1016/j.heliyon.2023.e15090.

[8] S. Thapa and A. Sarkar, “A deep dive into enhancing sharing of naturalistic driving data through face deidentification,” *Vis. Comput.*, vol. 41, no. 4, pp. 2563–2594, 2025, doi: 10.1007/s00371-024-03552-7.

[9] K. Eyglys Araujo Dos Santos, A. Dória Neto, and A. Medeiros Martins, “Face Representation for Online Interactions Using Bidirectional Generative Adversarial Networks (BiGANs),” *IEEE Access*,

vol. 12, pp. 132701–132713, 2024, doi: 10.1109/ACCESS.2024.3443643.
[10] D. Tran, D. Tung Phung, D. Manh Duong, K. Inoue, J.-H. Lee, and A. Q. Nguyen, “Privacy-Preserving Face and Hair Swapping in Real-Time with a GAN-Generated Face Image,” *IEEE Access*, vol. 12, pp. 179265–179280, 2024, doi: 10.1109/ACCESS.2024.3420452.
[11] A. Mohanty, A. Sutherland, M. Bezbradica, and H. Javidnia, “High-Fidelity Synthetic Face Generation for Rosacea Skin Condition from Limited Data,” *Electron.*, vol. 13, no. 2, 2024, doi: 10.3390/electronics13020395.
[12] H. O. Otroshi-Shahreza and S. Marcel, “Comprehensive Vulnerability Evaluation of Face Recognition Systems to Template Inversion Attacks via 3D Face Reconstruction,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 12, pp. 14248–14265, 2023, doi: 10.1109/TPAMI.2023.3312123.
[13] A. Makrushin, V. S. Mannam, and J. Dittmann, “Privacy-Friendly Datasets of Synthetic Fingerprints for Evaluation of Biometric Algorithms,” *Appl. Sci.*, vol. 13, no. 18, 2023, doi: 10.3390/app131810000.
[14] S. Li and H. J. Lee, “GFAM: A Gender-Preserving Face Aging Model for Age Imbalance Data,” *Electron.*, vol. 12, no. 11, 2023, doi: 10.3390/electronics12112369.
[15] S. A. Grosz and A. K. Jain, “SpoofGAN: Synthetic Fingerprint Spoof Images,” *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 730–743, 2023, doi: 10.1109/TIFS.2022.3227762.
[16] C. Pasquini, F. Laiti, D. Lobba, G. Ambrosi, G. Boato, and F. G. B. De Natale, “Identifying Synthetic Faces through GAN Inversion and Biometric Traits Analysis,” *Appl. Sci.*, vol. 13, no. 2, 2023, doi: 10.3390/app13020816.
[17] A. Kordas, E. Bartuzi-Trokielewicz, M. Ołowski, and M. Trokielewicz, “Synthetic Iris Images: A Comparative Analysis between Cartesian and Polar Representation,” *Sensors*, vol. 24, no. 7, 2024, doi: 10.3390/s24072269.
[18] H. Zein, L. Laurent, R. Fournier, and A. Naït-Ali, “Generation of artificial facial drug abuse images using deep de-identified anonymous dataset augmentation through genetics algorithm (3DG-GA),” *Multimed. Tools Appl.*, vol. 84, no. 28, pp. 34629–34643, 2025, doi: 10.1007/s11042-025-20639-y.
[19] T. Say, M. Alkan, and A. Kocak, “Advancing GAN Deepfake Detection: Mixed Datasets and Comprehensive Artifact Analysis,” *Appl. Sci.*, vol. 15, no. 2, 2025, doi: 10.3390/app15020923.
[20] M. A. N. Ul Ghani, K. She, M. A. Rauf, M. Alajmi, Y. Y. Yasin, and A. Algarni, “Securing synthetic faces: A GAN-blockchain approach to privacy-enhanced facial recognition,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 36, no. 4, 2024, doi: 10.1016/j.jksuci.2024.102036.
[21] H. Pranoto, Y. Heryadi, H. L. H. Warnars, and W. Budiharto, “Enhanced IPCGAN-Alexnet model for new face image generating on age target,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 9, pp. 7236–7246, 2022, doi: 10.1016/j.jksuci.2021.09.002.
[22] M. Ahmad, U. Cheema, M. Abdullah, S. Moon, and D. Han, “Generating synthetic disguised faces with cycle-consistency loss and an automated filtering algorithm,” *Mathematics*, vol. 10, no. 1, 2022, doi: 10.3390/math10010004.
[1] S. Khan, M. Mishra, and V. K. Mishra, “Autogenic, prognostic, and collective signature affirmation framework based on diverse set of features,” *Int. J. Biom.*, vol. 15, no. 5, pp. 539–559, 2023, doi: 10.1504/IJBM.2023.133124.
[2] S. Khan, M. Mishra, and V. K. Mishra, “Use of synthetic signature images for biometric authentication and forensic investigation,” *Int. J. Biom.*, vol. 15, no. 6, pp. 685–704, 2023, doi: 10.1504/IJBM.2023.133957.
[3] D. T. Toledano, R. Fernández Pozo, A. Hernández Trapote, and L. Hernández Gómez, “Usability evaluation of multi-modal biometric verification systems,” *Interact. Comput.*, vol. 18, no. 5, pp. 1101–1122, 2006, doi: 10.1016/j.intcom.2006.01.004.

[4] S. Purnapatra *et al.*, “Presentation Attack Detection with Advanced CNN Models for Noncontact-based Fingerprint Systems,” in *2023 11th International Workshop on Biometrics and Forensics, IWBF 2023*, 2023. doi: 10.1109/IWBF57495.2023.10157605.
[5] L. Colbois and S. Marcel, “On the detection of morphing attacks generated by GANs,” in *BIOSIG 2022 - Proceedings of the 21st International Conference of the Biometrics Special Interest Group*, 2022. doi: 10.1109/BIOSIG55365.2022.9897046.
[6] S. Saha *et al.*, “Undercover Deepfakes: Detecting Fake Segments in Videos,” in *Proceedings - 2023 IEEE/CVF International Conference on Computer Vision Workshops, ICCVW 2023*, 2023, pp. 415–425. doi: 10.1109/ICCVW60793.2023.00048.
[7] A. Firc, K. Malinka, and P. Hanáček, “Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors,” *Heliyon*, vol. 9, no. 4, 2023, doi: 10.1016/j.heliyon.2023.e15090.
[8] S. Thapa and A. Sarkar, “A deep dive into enhancing sharing of naturalistic driving data through face deidentification,” *Vis. Comput.*, vol. 41, no. 4, pp. 2563–2594, 2025, doi: 10.1007/s00371-024-03552-7.
[9] K. Eyglys Araujo Dos Santos, A. Dória Neto, and A. Medeiros Martins, “Face Representation for Online Interactions Using Bidirectional Generative Adversarial Networks (BiGANs),” *IEEE Access*, vol. 12, pp. 132701–132713, 2024, doi: 10.1109/ACCESS.2024.3443643.
[10] D. Tran, D. Tung Phung, D. Manh Duong, K. Inoue, J.-H. Lee, and A. Q. Nguyen, “Privacy-Preserving Face and Hair Swapping in Real-Time with a GAN-Generated Face Image,” *IEEE Access*, vol. 12, pp. 179265–179280, 2024, doi: 10.1109/ACCESS.2024.3420452.
[11] A. Mohanty, A. Sutherland, M. Bezbradica, and H. Javidnia, “High-Fidelity Synthetic Face Generation for Rosacea Skin Condition from Limited Data,” *Electron.*, vol. 13, no. 2, 2024, doi: 10.3390/electronics13020395.
[12] H. O. Otroshi-Shahreza and S. Marcel, “Comprehensive Vulnerability Evaluation of Face Recognition Systems to Template Inversion Attacks via 3D Face Reconstruction,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 12, pp. 14248–14265, 2023, doi: 10.1109/TPAMI.2023.3312123.
[13] A. Makrushin, V. S. Mannam, and J. Dittmann, “Privacy-Friendly Datasets of Synthetic Fingerprints for Evaluation of Biometric Algorithms,” *Appl. Sci.*, vol. 13, no. 18, 2023, doi: 10.3390/app131810000.
[14] S. Li and H. J. Lee, “GFAM: A Gender-Preserving Face Aging Model for Age Imbalance Data,” *Electron.*, vol. 12, no. 11, 2023, doi: 10.3390/electronics12112369.
[15] S. A. Grosz and A. K. Jain, “SpoofGAN: Synthetic Fingerprint Spoof Images,” *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 730–743, 2023, doi: 10.1109/TIFS.2022.3227762.
[16] C. Pasquini, F. Laiti, D. Lobba, G. Ambrosi, G. Boato, and F. G. B. De Natale, “Identifying Synthetic Faces through GAN Inversion and Biometric Traits Analysis,” *Appl. Sci.*, vol. 13, no. 2, 2023, doi: 10.3390/app13020816.
[17] A. Kordas, E. Bartuzi-Trokielewicz, M. Ołowski, and M. Trokielewicz, “Synthetic Iris Images: A Comparative Analysis between Cartesian and Polar Representation,” *Sensors*, vol. 24, no. 7, 2024, doi: 10.3390/s24072269.
[18] H. Zein, L. Laurent, R. Fournier, and A. Naït-Ali, “Generation of artificial facial drug abuse images using deep de-identified anonymous dataset augmentation through genetics algorithm (3DG-GA),” *Multimed. Tools Appl.*, vol. 84, no. 28, pp. 34629–34643, 2025, doi: 10.1007/s11042-025-20639-y.
[19] T. Say, M. Alkan, and A. Kocak, “Advancing GAN Deepfake Detection: Mixed Datasets and Comprehensive Artifact Analysis,” *Appl. Sci.*, vol. 15, no. 2, 2025, doi: 10.3390/app15020923.
[20] M. A. N. Ul Ghani, K. She, M. A. Rauf, M. Alajmi, Y. Y. Yasin, and A. Algarni, “Securing synthetic

faces: A GAN-blockchain approach to privacy-enhanced facial recognition," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 36, no. 4, 2024, doi: 10.1016/j.jksuci.2024.102036.

[21] H. Pranoto, Y. Heryadi, H. L. H. Warnars, and W. Budiharto, "Enhanced IPCGAN-Alexnet model for new face image generating on age target," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 9, pp. 7236–7246, 2022, doi: 10.1016/j.jksuci.2021.09.002.

[22] M. Ahmad, U. Cheema, M. Abdullah, S. Moon, and D. Han, "Generating synthetic disguised faces with cycle-consistency loss and an automated filtering algorithm," *Mathematics*, vol. 10, no. 1, 2022, doi: 10.3390/math10010004.