Borneo International Journal eISSN 2636-9826; Vol.9 (2); 2026; 47-52
Published by *Majmuah Enterprise*
www.majmuah.com

Adversarial Attacks on Biometric Systems: Vulnerabilities and Defense Mechanisms in Facial and Fingerprint Recognition

PAIWAND HADI HAMA SAEED and MOHAMAD FADLI BIN ZOLKIPLI

School of Computing, College of Arts and Sciences, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email : paiwandshekhhadi@gmail.com | Tel : +964 (773) 1522677

Received: May 21, 2026
Accepted: June 05, 2026
Online Published: July 19, 2026

Abstract

Biometric authentication systems are typically used for secure access to facilities, services or information through the use of physical characteristics (i.e., facial recognition and fingerprints). These types of systems are subject to being attacked through means of manipulating input data in order to gain unauthorized access. This paper explores several common attack techniques (e.g., spoofing, deepfakes and adversarial perturbations) and reviews existing defenses (such as liveness detection and multi-factor authentication) that have been created to counteract these attacks. In addition, the study will provide an overview of the current state of biometric systems regarding their effectiveness in preventing future attacks as well as identify gaps within the biometric security framework related to mitigating new threats.

Keywords: biometric authentication; adversarial attacks; facial recognition; fingerprint recognition; liveness detection.

1. Introduction

1.1 Background of Biometric Systems

Modern biometric systems are used widely in today's security applications to identify individuals based on their unique physiological traits (e.g., face and finger prints). The convenience, effectiveness and increased level of security provided by these types of systems compared to traditional authentication methods (e.g., password/PIN) has led to the increasing usage of biometric systems. With the rapid growth of artificial intelligence and deep learning technology, biometric systems have become more common and accurate for the verification of identity within the areas of mobile devices, banking/money transaction systems, surveillance equipment and access control devices.

1.2 Importance of Biometric Authentication

The increased use of biometric authentication provides significant benefits to security and user experience within various application areas. Biometric biometrics (e.g., fingerprint and facial recognition) are very difficult to replicate, making them a reliable means of confirming identity. Many biometric systems such as facial recognition and fingerprint readers, are both simple to use and provide quick processing times. The expansion of digital systems will lead to an increasing need for secure and reliable methods of authenticating users, creating a substantial reliance on biometric solutions within modern cyber security ecosystems.

1.3 Problem Statement

Although they present benefits, biometric systems are susceptible to adversarial attacks that take advantage of vulnerabilities in artificial intelligence models at an increasing rate. An attacker could present a hacked biometrics inputs (i.e., an image) in a way that misleads a biometric system into allowing an unauthorized individual to access resources. By employing methods such as generating deepfakes of biometric data, performing spoofing attacks against biometric systems and executing adversarial perturbations against biometric model inputs, an attacker also can bypass a biometric authentication system. These types of adversarial threats pose significant questions about the reliability and safety of biometric systems, particularly in situations where security is essential.

1.4 Research Objectives

The study has three specific aims:

1 Identify and analyze the diverse types of attacks that are adversarial to biometric systems.
2 Investigate the vulnerabilities associated with facial and fingerprint recognition systems.
3 Evaluate current countermeasures being implemented at the biometric authentication system level.

1.5 Scope of Study

This study examines adversarial attacks on facial recognition and fingerprint authentication systems. This study examines common methods of attack, including spoofing, manipulating biometric system outputs with deepfake technology and attacks against machine-learning models employed by biometric systems. Additionally, this study investigates available countermeasures against these types of attacks, including the use of liveness detection and multi-factor authentication techniques. Other forms of biometric modalities did not receive in-depth consideration because the scope of this study was limited to the biometric systems that are most commonly used.

2. Literature Review

2.1 Overview of Biometric Systems

Biometric authentication systems utilize biometrics to verify or identify individuals. Biometrics is based upon the unique biological and/or behavioral characteristics of the individual. Occasionally, biometric authentication systems use non-biometric data (i.e., driver's license, passport, social security number) to identify or verify an individual, however, the main objective of biometric authentication systems has been to provide an economically feasible, secure and accurate method for identifying individuals. The most common biometric modalities used today include facial recognition and fingerprint identification. Both of these modalities have been widely accepted because of the high accuracy of the systems and the ease of their application. In addition, many biometric authentication systems have improved significantly in their performance and security due to artificial intelligence and the use of multimodal data fusion techniques (Priesnitz et al., 2022). Various types of machine learning techniques have also greatly increased the performance of biometric authentication systems (Cui et al., n.d.; Ghilom & Latifi, 2024).

2.2 Facial Recognition Systems

Systems using facial recognition work by examining the distinct characteristics of a person's face, thus enabling them to determine who they are. Today, facial recognition technology is used in many applications, including smartphones, video surveillance and access-control systems in several different industries. Many facial recognition systems utilize deep-learning methods to extract the features of a face from an image and compare these features to an image of the same person that was previously captured and stored in a database. Several researchers (Tremoço et al., n.d.) have discovered vulnerabilities in the design of facial recognition systems which can be exploited by adversarial attacks. (Carletti et al., 2024) demonstrated that adversarial attacks can alter observable facial features so that once modified, the altered faces would go undetected by the recognition system but still be recognizable to a typical observer. (Kaur & Kant, 2025) noted that having a liveness detection system is important to prevent spoofing attacks.

2.3 Fingerprint Recognition Systems

Since fingerprint recognition is a unique biometrics form and has an established history of durability, it can be considered to be the most common method of biometrics authentication. Many of today's modern fingerprint identification systems utilize deep learning-based approaches to improve their performance with regard to feature extraction and matching within the system. There is a comprehensive summary of fingerprint authentication systems, including their advantages and disadvantages in a review by(Sumalatha et al., 2024). There are several methods by which a fingerprint identification system can be compromised by spoofing (the use of a fictitious fingerprint created from materials like gel or silicone). Advancements in contactless fingerprint identification technologies have been addressed by (Priesnitz et al., 2022; Sumalatha et al., 2024).

2.4 Adversarial Attacks in Machine Learning

Adversarial attacks are designed to attack a machine learning model through perturbing its input data with small, sometimes imperceptible, changes. The output from an adversarial attack could cause the machine learning model to produce incorrect results, which would then create a severe security risk. Model inversion attacks, in which someone tries to reclaim the private data associated with the model, have been investigated by(Bangoy Pacheco et al., 2025; Dionysiou et al., 2023) examined how an adversary could utilize the vulnerabilities in biometric systems based on deep learning to manipulate them. These studies indicate that there is an increased focus on securing adopted machine learning models in biometric applications through new research and development (Khairnar et al., 2023).

2.5 Adversarial Attacks on Biometric Systems

Biometric systems have suffered from increasingly advanced attacks by adversaries, such as spoofing, deepfake creation and the introduction of adversarial perturbations meant to circumvent the use of a biometric match for authentication. (Park et al., 2024)created a framework for performing risk analysis and assessing the identification risk of a biometric system when attacked by adversarial means. (Rabhi et al., 2024)investigated the potential of deepfake technology to deceive biometric authentication technology, thus providing insight into how synthetic media may be used to mislead identification/recognition technologies.(Minaee et al., 2021) explored the role that deep learning plays in both improving the performance of biometric systems and creating new and additional points of attack against biometric identification/recognition technology.

3. Discussion

3.1 Types of Adversarial Attacks on Facial Recognition

Facial recognition technology can be easily manipulated by adversaries who intend to deceive that system by adding or modifying input photos or video images in order to appear as though they are a legitimate party or individual. A common example of how this occurs is through a presentation attack, where photos, videos or masks are used during the act of impersonation. More sophisticated attacks use "deepfake" technology, which generates real-looking face-image/photo/video via artificial intelligence in order to gain access to authenticating systems. Adversarial perturbation involves taking an image and adding a very small artificial perturbation that is invisible to the naked eye but is capable of having an enormous impact on how the facial/visual recognition model will predict things based on the input data. Adversarial attacks will take advantage of the inadequacies found within deep learning models, and the vulnerability of facial recognition systems to compromise by unauthorized persons is a potential existential threat (Rabhi et al., 2024; Salko et al., 2024).

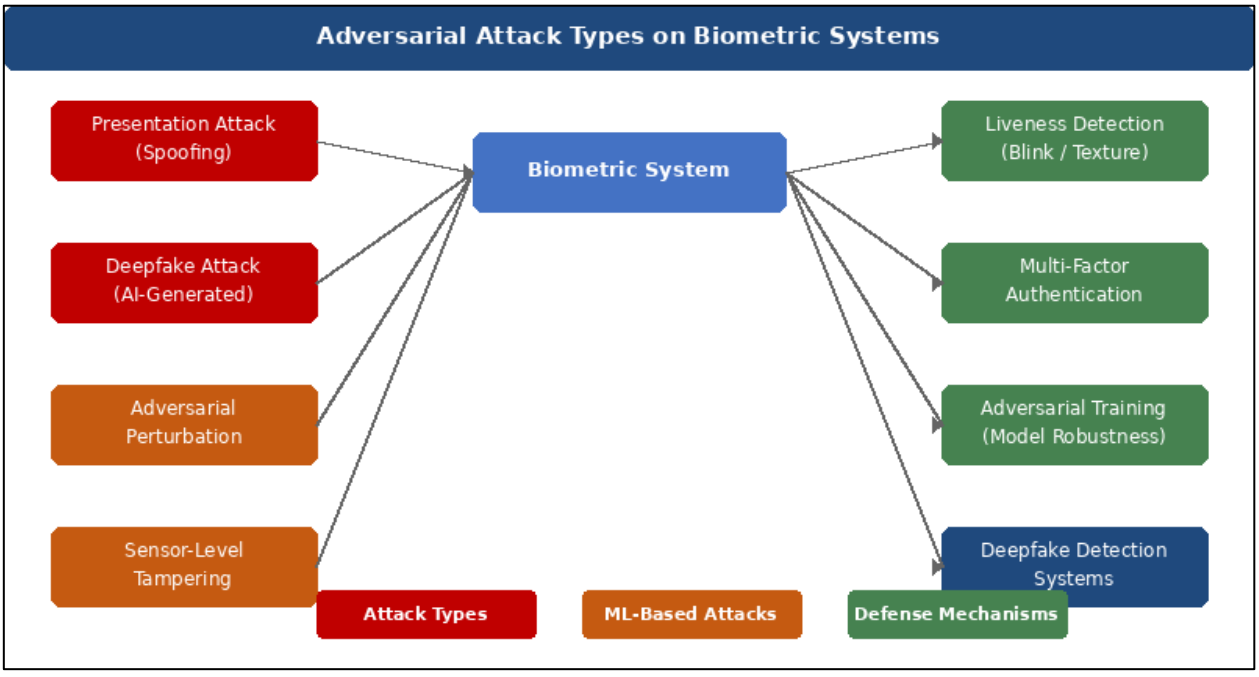

Figure 1. Overview of adversarial attack types and corresponding defense mechanisms in biometric systems.

3.2 Types of Adversarial Attacks on Fingerprint Recognition

There are many different types of adversarial attacks against fingerprint recognition systems but the most common type is spoofing (or using fake fingerprints). Spoofing involves a user creating fake fingerprints out of materials like silicone, gelatin or latex to resemble the fingerprint of an actual user. If the proper detection method is not in place, a fake fingerprint can fool a sensor. Another form of attack against fingerprint recognition systems is sensor-level tampering, where an adversary tampers with the data collected by the fingerprint scanner. Machine learning-based fingerprint recognition systems could also be vulnerable to adversarial input that is designed to confuse the recognition model. The identified vulnerabilities in the fingerprint recognition systems indicate a need for stronger protective measures (Bangoy Pacheco et al., 2025; Park et al., 2024).

3.3 Deepfakes and AI-Generated Spoofing

Deepfake technology has greatly increased the potential for adversarial attacks against biometric systems. Attackers use deep learning models to produce very realistic synthetic images or videos that closely resemble actual people. This method allows for possible creation of fraudulent identities that could allow bypassing facial recognition systems, particularly in remote authentication methods. Additionally, deepfake-based attacks can potentially be very difficult to identify using traditional security methods. The continued evolution of artificial intelligence not only enhances the quality and accessibility of the tools required for the creation of deepfakes but also represents an increasing danger to biometric authentication systems (Dionysiou et al., 2023; Patnaik et al., 2023).

3.4 Security Impacts of Adversarial Attacks

Adversarial attacks hold a very possible risk to security of biometric systems. They can allow attackers to gain unauthorized access, commit identity theft and breach data, especially in sensitive environments (such as banking, government systems and secure facilities). They are likely to affect the degree to which users trust biometric systems, which will ultimately limit their adoption. The ability to bypass the authentication systems of AI security solutions raises further questions about their reliability. To create a more secure biometric system, it is crucial to understand potential risks and adversarial attack effects.

3.5 Detection and Defense Mechanisms

To mitigate adversarial attacks, various defense techniques have been developed. Perhaps most effective are techniques for determining whether the biometric input is from a living human rather than a nonliving representation, also known as liveness detection. Techniques such as blink detection, texture analysis and thermal detection are used in facial recognition systems. In fingerprint identification systems, liveness detection is based on measuring characteristics of skin (e.g. moisture, elasticity). Additionally, multi-factor authentication, which involves the combining of biometric verification and other verification means (e.g. passwords and tokens) can provide another layer of security. Similarly, model robustness and adversarial training can improve the resistance of machine learning models to adversarial attacks(Asmitha et al., 2024; Kaur & Kant, 2025).

Table 1. Comparison of adversarial attack types and defense mechanisms for biometric systems.

Attack Type	Target Modality	Defense Mechanism	Effectiveness
Spoofing / Presentation Attack	Face & Fingerprint	Liveness Detection	High
Deepfake Attack	Facial Recognition	Deepfake Detection Systems	Moderate
Adversarial Perturbation	Face & Fingerprint (ML models)	Adversarial Training	Moderate
Sensor-Level Tampering	Fingerprint Recognition	Hardware-Level Security	Variable
Model Inversion Attack	ML-based Biometric Models	Multi-Factor Authentication	High

3.6 Current Challenges and Future Directions

While there have been advancements in defense mechanisms against threats such as adversarial attacks, challenges still exist. Adversarial attacks are ever-changing and this presents difficulties for currently available methods to detect them. There exists a balancing act between offering sufficient security and providing ease of use with the knowledge that an increase in security could lead to increased computational resources being required or more user interaction. Future

research should be focused on the development of improved, more resilient and adaptable defense mechanisms. Additionally, there will need to be an increased focus on improving the ability to explain how biometric systems work and ensuring that they comply with ethical standards for the use of biometric data while protecting individuals' privacy (Minaee et al., 2021; Wu, 2025).

4. Conclusion

Biometric authentication systems (e.g., facial recognition, fingerprint identification) play a major role in delivering convenience and efficiency as part of contemporary security infrastructure. This research has shown that the use of these technologies leaves them vulnerable to a variety of adversarial attacks (e.g., spoofing, modifying through deepfake-based means, introducing variances through adversarial perturbations) that threaten to undermine their effectiveness and reliability (Rabhi et al., 2024; Tremoço et al., n.d.). According to the analysis, although biometric systems have greater security than conventional methods, there is an associated risk of exploitation through the use of machine learning models(Bangoy Pacheco et al., 2025). The development of various techniques such as liveness detection, multi-factor authentication and adequate training of machine learning models provides partial protection from these threats, they may be insufficient to address the evolving methodologies used to conduct attacks (Kaur & Kant, 2025; Tremoço et al., n.d.). To adequately protect the integrity of biometric systems against adversary attacks, continuous efforts to conduct research and make improvements are required. Future efforts should focus on developing stronger, more adaptable and secure defence mechanisms while maintaining usability and privacy(Asmitha et al., 2024; Wagner, n.d.).

Acknowledgments

The author wishes to extend his sincere appreciation to the lecturer Prof. Madya Ts. Dr. Mohamad Fadli Bin Zolkipli, for granting him the opportunity to work on this project and for his assistance and encouragement during the course of this project. The author would also like to acknowledge and thank the many researchers whose work has supported the advancement of knowledge in the area of adversarial attacks and developing protection against them, to increase security in the field of biometric systems.

References

Asmitha, P., Rupa, C., Nikitha, S., Hemalatha, J., & Sahu, A. K. (2024). Improved multiview biometric object detection for anti spoofing frauds. *Multimedia Tools and Applications*, *83*(33), 80161–80177. https://doi.org/10.1007/s11042-024-18458-8

Bangoy Pacheco, S. A., Estrada, J. E., & Goyani, M. M. (2025). Hidden adversarial attack on facial biometrics - A comprehensive survey. *Procedia Computer Science*, *258*, 1383–1390. https://doi.org/10.1016/j.procs.2025.04.371

Carletti, V., Foggia, P., Greco, A., Saggese, A., & Vento, M. (2024). Facial Soft-biometrics Obfuscation through Adversarial Attacks. *ACM Transactions on Multimedia Computing, Communications and Applications*, *20*(11). https://doi.org/10.1145/3656474

Cui, X., Aparcedo, A., Jang, Y. K., & Lim, S.-N. (n.d.). *On the Robustness of Large Multimodal Models Against Image Adversarial Attacks.*

Dionysiou, A., Vassiliades, V., & Athanasopoulos, E. (2023). Exploring Model Inversion Attacks in the Black-box Setting. *Proceedings on Privacy Enhancing Technologies*, *2023*(1), 190–206. https://doi.org/10.56553/popets-2023-0012

Ghilom, M., & Latifi, S. (2024). The Role of Machine Learning in Advanced Biometric Systems. *Electronics (Switzerland)*, *13*(13). https://doi.org/10.3390/electronics13132667

Kaur, P., & Kant, C. (2025). 2-Phase Multi-trait Biometric Authentication Model Against Spoofing Attack Using Deep Hash Model. *SN Computer Science*, *6*(1). https://doi.org/10.1007/s42979-024-03513-w

Khairnar, S., Gite, S., Kotecha, K., & Thepade, S. D. (2023). Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions. In *Big Data and Cognitive Computing* (Vol. 7, Number 1). MDPI. https://doi.org/10.3390/bdcc7010037

Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., & Zhang, D. (2021). *Biometrics Recognition Using Deep Learning: A Survey*. http://arxiv.org/abs/1912.00271

Park, S. H., Lee, S. H., Lim, M. Y., Hong, P. M., & Lee, Y. K. (2024). A Comprehensive Risk Analysis Method for Adversarial Attacks on Biometric Authentication Systems. *IEEE Access*, *12*, 116693–116710. https://doi.org/10.1109/ACCESS.2024.3439741

Patnaik, S. A., Chansoriya, S., Jain, A. K., & Namboodiri, A. M. (2023). *AdvGen: Physical Adversarial Attack on Face Presentation Attack Detection Systems*. http://arxiv.org/abs/2311.11753

Priesnitz, J., Huesmann, R., Rathgeb, C., Buchmann, N., & Busch, C. (2022). Mobile Contactless Fingerprint Recognition: Implementation, Performance and Usability Aspects. *Sensors*, *22*(3). https://doi.org/10.3390/s22030792

Rabhi, M., Bakiras, S., & Di Pietro, R. (2024). Audio-deepfake detection: Adversarial attacks and countermeasures. *Expert Systems with Applications*, *250*. https://doi.org/10.1016/j.eswa.2024.123941

Salko, M., Firc, A., & Malinka, K. (2024). Security Implications of Deepfakes in Face Authentication. *Proceedings of the ACM Symposium on Applied Computing*, 1376–1384. https://doi.org/10.1145/3605098.3635953

Sumalatha, U., Prakasha, K. K., Prabhu, S., & Nayak, V. C. (2024). A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection. *IEEE Access*, *12*, 64300–64334. https://doi.org/10.1109/ACCESS.2024.3395417

Tremoço, J., Medvedev, I., Freitas, N., Costa, A., Nunes, D., Bunzel, N., Graner, L., Göller, N., Pellegrini, L., Di Domenico, N., Borghi, G., Verghese, M., Bhilare, S., Hati, A., Lourenço, M., & Gonçalves, N. (n.d.). *Adversarial Attack Challenge for Secure Face Recognition 2025*.

Wagner, F. (n.d.). Deep Learning-Based Liveness Detection to Prevent Biometric Payment Fraud. In *International Journal of Research in Mulidisciplinary Technology* (Vol. 1). Retrieved https://ijrmt.com/https://ijrmt.com/

Wu, H. (2025). A Research on Deepfake Face Detection Techniques Based on Multimodal Biometric Cross – Verification. *ITM Web of Conferences*, *78*, 02017. https://doi.org/10.1051/itmconf/20257802017

Nguyen, T. T., Nguyen, T. T., Nguyen, Q. V. H., Nguyen, D. T., Nguyen, D. T., Huynh-The, T., Nahavandi, S., Nguyen, T. T., Nguyen, T. T., Pham, Q., & Nguyen, C. M. (2022b). Deep learning for deepfakes creation and detection: A survey. *Computer Vision and Image Understanding*, *223*, 103525. https://doi.org/10.1016/j.cviu.2022.103525

Kaur, A., Hoshyar, A. N., Saikrishna, V., Firmin, S., & Xia, F. (2024). Deepfake video detection: challenges and opportunities. *Artificial Intelligence Review*, *57*(6). https://doi.org/10.1007/s10462-024-10810-6