A research study of 3D attacks on facial recognition systems

Punam Dawgotra
Mehr Chand Mahajan DAV College for Women, Chandigarh, India

Abstract— Facial recognition systems are predominant in the fields of identification and authentication of persons. With rapid development in creating robust facial recognition systems there is a rapid proliferation of attacks on such systems to break them for impersonation attacks and forgery. This survey paper explores the landscape of 3D attacks on facial recognition systems, delving into the underlying methodologies, potential vulnerabilities, and face recognition algorithms that are compromised using such attacks. Understanding these threats is crucial for developers, security experts, and policymakers bearing the responsibility of fortifying facial recognition technologies against emerging attacks on them. This analysis provides comprehensive insights into different types of 3D attacks and the most common techniques used in such attacks. Through this survey, researchers and academicians may gain valuable insights into the field of 3D face recognition attacks, facilitating informed decision-making and advancements in the field of face recognition systems' threat and vulnerability prevention.

Keywords—Face Recognition Systems, FR Attacks, FR 3D Attack.

I. INTRODUCTION

Authentication of people is the most crucial aspect of security systems all over the world. Authentication is a prerequisite to authorization of people over the responsibilities and assignments within organizations. Authentication can be done through physical verification of ID proofs issued by competent authorities according to the law of land. With advancement in technologies like Artificial Vision, AI, Deep learning, and hardware, authentication process has been made more reliable, efficient and robust with the help of Facial Recognition Systems. Facial recognition systems have emerged as indispensible tools used in authentication, security, and identification in biometric systems using local, holistic or hybrid approaches [1]. These systems are extremely beneficial but are susceptible to sophisticated attacks like 3D attacks. The traditional facial recognition systems involve 2D images captured from various angles but they are vulnerable to manipulation through the introduction of 3D perturbations.

There is a tremendous growth in 3D modeling techniques, rightly supported by the availability of economical and advanced accessible hardware such as 3D printers and depth-sensing cameras. These advanced technologies have enabled attackers to exploit the intrinsic limitations of conventional facial recognition systems [2]. Face Recognition system attacks can be incorporated by physical modifications of ID documents or digital alterations like swapping, morphing, and presentation in facial images that permits the attackers to deceive these systems, leading to unauthorized access, identity theft, or privacy breaches [3].

The Facial recognition Systems are prone to be affected by a multitude of 3D attacks that are used by attackers to deceive and obstruct the efficient operations. These attacks can be categorized as under.

- **Structured-Light Attacks**: This kind of attack is incorporated by manipulating structured-light patterns that are mapped onto a face by distorting 3D facial features of a person to fool the recognition system.

- **3D Mask Attacks**: These attacks involve generating physical masks to imitate an authorized person's face to deceive the system. These attacks are enforced by exploiting the depth information captured by 3D sensors from the image of the target face.

- **Texture Manipulation**: Many facial recognition systems authenticate facial images by the texture variations of the face due to lighting and environmental conditions. The texture manipulation attack is executed by changing the texture or appearance of facial surface using adversarial perturbations. This is one of the most commonly used methods of falsely identifying faces.

- **Geometry Alteration**: This attack is executed by modifying the geometric structure of facial features like eyes, nose, and shape to create subtle changes that may not be caught by human eye but can dodge a face recognition system to misclassify faces.

- **Pose Manipulation**: An alteration in facial pose or orientation is also a very common technique to exploit vulnerabilities in the facial recognition system's ability to handle variations in facial alignment.

- **Lighting and Reflectance Manipulation**: This attack is executed by adjusting lighting or reflectance of the facial image to produce adversarial perturbations on the captured 3D data, leading to false classification.

- **Physical Object Interference**: This kind of attack involves introducing physical objects such as glasses, mask, hat, a piece of jewelry or scarf to cover, hide or alter facial features in face images, thereby leading to inaccurate recognition.

II. LITERATURE REVIEW

Recent research and advancement in artificial intelligence and deep learning have led to generation of numerous FR algorithms and development of Face Recognition Systems. At the other end attackers also utilize this knowledge to use various deep learning techniques to deceive or fool the face recognition system. This is a detailed survey of work undergoing in creating attacks on face recognition systems that help in understanding and identifying the possible vulnerabilities and shortcomings of FR systems so that the Facial recognition systems can be made robust, effective and reliable .

Below is a comprehensive list of commonly used face recognition algorithms before the discussion of research work done in the field of generating 3D attacks on Facial Recognition Systems .

Algorithm Name	Implementation Technique
DeepFace [25]	Uses deep neural networks to learn facial representations by mapping face images to a low-dimensional space.
FaceNet [26]	Uses a deep convolutional network to learn a mapping from face images to a compact Euclidean space where distances directly correspond to a measure of face similarity.
ArcFace [27]	Uses an additive angular margin loss to enhance the discriminative power of the face recognition model.
CosFace [28]	Introduces a large margin into the cosine similarity measure for better separation of different identities by focusing on angular distance, leading to improved accuracy in recognizing faces under varied conditions.
MagFace [29]	Employs feature discrimination by learning magnitude-aware embeddings, enhancing robustness and accuracy for identity verification across varied conditions.
ElasticFace [30]	Employs elastic regularization techniques to improve the discriminative power and generalization capability of face recognition models, particularly under challenging conditions such as variations in pose, expression, and occlusion.
LightCNN[31]	High accuracy with reduced computational complexity, making it suitable for resource-constrained environments.
ResNet-50 [32]	Tackle the vanishing gradient problem, achieving high accuracy in image recognition tasks through residual learning.

Table 1 Commonly Used Face Recognition Algorithms

A structured-light attack on 3D face recognition was proposed by [4], integrating 3D reconstruction and skin reflectance in optimization which proves to be resilient to head movements, achieves imperceptible perturbations, with adaptable adversarial point placement. It has proven efficacy against point-cloud and depth-image systems, it outperforms prior physical 3D adversarial methods with fewer perturbations.

A physical attack method, termed as PadvFace is proposed by [5]. The proposed model recognizes the complicated physical-world condition variations that are used in attacking face recognition. They implement sticker-based attack to generate a wearable adversarial sticker that can be physically worn to fool the face recognition system against correct recognition. Similar concept is used by FaceAdv, proposed by [6], which is a physical-world attack utilizing adversarial stickers to deceive FR systems using sticker generator and converter. The authors conducted extensive experiments targeting on algorithms like ArcFace, CosFace, and FaceNet to reliably commit impersonate attacks.

A geometry-aware generator network using generative neural radiance fields (GNeRF) was proposed by [7]. Their proposed model maps facial templates to the generator's latent space. It is semi-supervised trained with real and synthetic images to optimize camera parameters during inference. Their method is evaluated on whitebox and blackbox attacks on LFW and MOBIO datasets and displayed attack success rates by up to 17.14%. Geometrically Adaptive Dictionary Attack (GADA) proposed by [9] is a generalized black-box attack on face recognition experimentally executed on LFW ad CPLFW that incorporates adversarial perturbation in the UV texture map of the face and added to the facial image for face recognition forgery.

Presentation attacks can be carried out with the help of custom silicone masks [8]. The proposers of this research used a dataset based on six customized silicone masks to demonstrate the high efficacy of attacking the FR system of the rate of 10 times higher than its false match rate. Adversarial Mask is proposed by [10] as a physical adversarial universal perturbation (UAP) created as face masks with a crafted pattern. The researchers conducted experiments to check transferability of adversarial mask with multiple Face Recognition models and datasets. A very interesting experiment was conducted by[11] by printing facial images on T-shirts to bluff face recognition systems. The used the T-shirt Presentation Attack Database (TFPA) and an extensive benchmark to evaluate attack feasibility, FR vulnerability, and detecting presentation attack.

A method of FR system attack is proposed by [12] through images generated with adversarial networks using facial structure detected with landmark detection algorithm (from facial features) and superpixel segmentation to pick pixel values from neighborhood of the extracted facial landmarks having matching pixel values. These segmented regions implemented as masks with existing FR attack methods to attach adversarial noise in masked areas.

Adversarial relighting attack termed as albedo-quotient-based adversarial relighting attack (AQ-ARA) proposed by [13] generates natural adversarial lighting to generate versatile attack face images. It is an auto-predictive adversarial relighting attack (AP-ARA) incorporated by training adversarial relighting network (ARNet). The digitally created attack is transferred with precise relighting device. Researchers validated these methods on two public datasets. [14] Proposed template inversion (TI) attacks against face recognition systems using synthetic data using reconstruction model to generate high-resolution face images from facial templates. Their method supports both whitebox and blackbox TI attacks. Experimental results on MOBIO, LFW, AgeDB, and IJB-C datasets show that their approach outperforms previous methods in high-resolution 2D face reconstruction, demonstrating the vulnerability of face recognition systems to the proposed TI attacks with synthetic training data.

[15] propose Sibling-Attack, a multi-task perspective based FR attack. The proposed attack chooses tasks associated with FR and Attribute Recognition based on theoretical and quantitative analysis. An optimization framework is developed to combine adversarial gradient information in the course of limiting cross-task features within same space, and a joint-task meta optimization framework to increase gradient compatibility in tasks, and cross-task gradient stabilization technique to moderate the oscillation effect while attack.

DepthFake attack is proposed by [16] to fraudulently ditch a 3D face authentication system with a single 2D photo. DepthFake estimates the 3D depth of a victim's face from a 2D photo and projects scatter patterns with this depth information, giving the photo 3D properties. This research addresses challenges such as depth estimation errors, depth image forgery, and alignment of RGB and depth images. DepthFake achieve a 79.4% depth attack success rate and a 59.4% RGB-D attack success rate on three commercial systems and one access control device. [18] Investigate a 3D-face custom silicone mask for attacking face recognition system. A new dataset constructed from eight custom 3D silicone face masks and from facial images captured with three smartphones. Mask morphing and subsequent experiments to perform the attacks.

[17] Assessed the vulnerability of the Legendre moments invariants (LMI)-based face recognition method to 3D mask attacks using the 3DMAD database, which includes real and masked faces. The spoof false acceptance rate (SFAR) was a good 65%, indicating significant vulnerability. They propose a new method combining LMI with linear discriminant analysis for feature extraction and maximum likelihood for classification. This method achieves a 97.6% recognition rate and an SFAR of 0.83%.

These results, obtained with lower computational time, outperform state-of-the-art methods using the same 3DMAD database. VLA is proposed by [19], a novel attack to dodge black-box face recognition systems using light. Visible light-based adversarial perturbations are projected onto the faces for targeted or untargeted attacks. VLA uses a perturbation frame to modify images and a concealing frame to hide modifications. Experiments confirm VLA's effectiveness and inconspicuousness.

Researchers [20] created real-world attacks on face recognition systems, focusing on the LResNet100E-IR model with ArcFace loss. They propose an attack that generates physically adversarial patch creation on a facial image. This patch, printed and added as a face attribute, alters the classifier's recognized class when photographed. Their method allows projecting adversarial patches on various facial areas, like the nose or forehead, as well as on wearable accessories, such as eyeglasses. [21] Studied and evaluated various Face recognition systems to check their vulnerability when the target face images are modified with adversarial geometrical-perturbations. They proposed a landmark manipulation method to achieve speedier attacks with a 99.86% success rate. The proposed semantic structure-constrained attack demonstrated 99.96% success rate. Their experimented methods promised robustness against well known defense mechanisms, at success rates over 53.59%.

Actual mated morph presentation match rate (AMPMR) by [22] successfully evaluates the performance of morphing attacks on the actual FR systems. The target faces for Morph attacks are tempered by modifying the geometrical features of eyes and nose. They have experimented with different datasets to evaluate attack types, target image quality, and modification parameters. Their morphed attacks outperformed in anti-detectability. The target morphs generated displayed low visual distortion and an optimal balance for facial biometrics verification, anti-detectability, and visual differences.

III. METHODOLOGY

The prime objective of this paper is to offer insights into latest attacks on Face Recognition Systems for impersonation and forgery. With this objective, systematic collection and analysis of literature is the main focus to create a relevant comparison study. The methodology for this systematic study is meant to define the scope of exploring available works, literature exploration, defining inclusion and exclusion criteria of existing research works, data collection and its analysis.

The first step was to define and limit the scope of the survey in presence of a vast range of available studies. The following aspects were taken care of :

- Focus topic: 3D attacks on face recognition systems, impersonation attacks, masked attacks, spoofing attacks, adversarial attacks, and defense mechanisms.
- Time Frame: Advancements, trends and research work after 2014 were chosen.
- Types of Publications: Peer-reviewed journal articles, conference papers, technical reports, and patents.

The databases explored are IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink and Google Scholar. The Search terms and keywords used include: 3D face recognition attacks, 3D spoofing face recognition, adversarial attacks 3D face recognition, defense mechanisms 3D face recognition, threats and vulnerabilities in face recognition systems

For the chosen publications, the following key data points were identified and documented:

- Authors and Year of Publication
- Title and Source
- Type of Attack
- Methodology Used
- Key Findings
- Datasets

The collected data is analyzed on follwoing dimensions:

- Types of 3D Attacks: Categorizing the different methods and techniques used for 3D attacks.
- Attack methodologies: Evaluating the effectiveness of various attack methodologies.
- Future Directions: Identifying promising areas for future research and development.

By following this systematic methodology, the survey aims to provide a comprehensive and critical overview of 3D attacks on face recognition systems, contributing valuable insights to the field and guiding future research efforts.

IV. FINDINGS

The table given in this section summarizes the work of researchers who created Facial Recognition attack models, methods or framework. Some researchers have experimented with more than one type of attack in their work as can be seen from the table.

Researcher/ Author	**3D Attack Type**	**Face Recognition Algorithm attacked**	**Datasets Used**	**Key Findings**
Y. Li, et al [4]	Structured-Light Attacks, Lighting and Reflectance	Pointnet, Pointnet++ , DGCNN, CurveNet and FR3DNet.	Bosphorus , Eurecom and SIAT-3DFE	Face recognition system can be easily dodged by adding small, visible adversarial perturbations using a structured light systems.
X. Zheng, et al [5]	Physical Object Interference	ArcFace	MS1MV2 and LFW	Successfully dodged and impersonated ArcFace Face recognition System
M. Shen, et al [6]	Physical Object Interference	ArcFace, CosFace and FaceNet	MS-Celeb	FaceAdv successfully dodged and impersonated on the mentioned face recognition systems
H. O. Shahreza et al [7]	Geometry Alteration	ArcFace , ElasticFace. FR models with FaceX-Zoo, AttentionNet, HRNet, RepVGG and Swin as backbone	LFW and MOBIO	It is possible to befool a facial recognition system by creating 3D face image from templates. Another important conclusion is that skin complexion and age of

				faces may fail to break an FR system
S. Bhattacharjee et al [8]	Structured-Light Attacks	FaceNet, LightCNN	Custom Silicone Mask Attack Dataset (CS-MAD)	The CNN-FR methods are significantly vulnerable to custom-mask based Personation Attacks. Thermal images of live face images are hugely distinct from those of PAs and silicone mask attacks. Basic PAD can be utilized for Personation Attacks Detection with thermal imagery for robust FR system
J. Byun, et al [9]	Texture Manipulation	ArcFace, ResNet-50, FaceNet	LFW and CPLFW	Available successful perturbations are used for efficient dodging or impersonation attacks
A. Zolfi, et al [10]	3D Mask Attacks	ArcFace, CosFace, MagFace	CASIA-WebFace, CelebA, MS-Celeb	The method proves robustness of adversarial mask in digital simulations and real conditions.
M. Ibsen et al [11]	Texture Manipulation	ArcFace , COTS	HQ-WMCA d	Exposes vulnerability of the state-of-the-art face recognition systems
C.-Y. Lin, et al [12]	3D Mask Attacks, Texture Manipulation	Facenet, ArcFace	CASIA-WebFace	Bypassing digital-world and physical-world recognition of common FR systems is possible
Q. Zhang, et al [13]	Lighting and Reflectance	FaceNet, ArcFace, CosFace	VGGFace2, CelebA	lighting of a natural looking face image can be used to deceive face recognition models
H. O. Shahreza et al [14]	Texture Manipulation	ArcFace, FaceNet, DeepFace	MOBIO, LFW, AgeDB, and IJB-C	Trained model with synthetic data used to reconstruct face images from templates to fool FR.

Z. Li et al [15]	Geometry Alteration	FaceNet, IRSE50	CelebA-HQ & LFW	Dodges real-world commercial platforms with black-box attacks
Z. Wu ,et al [16]	Texture Manipulation	commercial face authentication systems namley Tencent Cloud, Baidu Cloud, and 3DiVi	300W-3D, Texas-3DFR	Higher security implementation exploiting depth-sensing capabilities in FR are vulnerable
Hamdan, B.et al [17]	3D Mask Attacks	DeepFaceLiveness	3DMAD	Vulnerability of face recognition systems to 3D mask attacks was demonstrated
R. Ramachandra et al [18]	3D Mask Attacks	ArcFace	On generated dataset of 635 bona fide, 1034 face masks and 613 mask morphing face images	Advanced mask manipulation methods can pose potential vulnerabilities on FRs
M. Shen,et al [19]	Structured-Light Attacks	Facenet	CusFace & LFW	VLA displayed effective and robust technique to break SOTA FaceNet
M. Pautov, et al [20]	Physical Object Interference	ArcFace	CASIA WebFace	Use of adversarial stickers in form of eyeglasses or forehead are effective to attack ArcFace. Position of the sticker, its size, dramatically contributes to success of attack
L. Qin, et al [22]	Geometry Alteration	ArcFace	LFW	Low-visibility and robust morphing attacks pose threats to face recognition systems

Table 2 3D attacks experiments on Face Recognition Systems conducted by researchers

It is observed from the above summarization of previous researches that the most common face recognition system attacks created by the researchers are 3D Mask Attacks., Texture Manipulation and Geometry Alteration. Most of the attacks are executed by digitally altering the victim face images. A few researchers have demonstrated work using other ways like silicone masks, stickers and faces printed on T-Shirt. The existing SOTA FR algorithms and systems are prone to attacks for impersonation and miss-classification. The insights presented here can give a direction to improve the robustness of FR systems.

V. CONCLUSION

In conclusion, this research study on 3D attacks on facial recognition systems highlights and identifies the significant research being done in creating sophisticated spoofing techniques on the Face Recognition Systems. It was observed through various research works that by leveraging 3D models, attackers can effectively deceive facial recognition algorithms, highlighting the need for robust countermeasures in security applications. The study illustrates that while 2D spoofing methods have been widely studied and mitigated to an extent, 3D attacks introduce a higher level of complexity that current systems are not fully equipped to handle.

This investigation also reveals that existing facial recognition technologies often lack the necessary depth perception and live detection capabilities to distinguish between a real face and a high-quality 3D copy of a face. Consequently, researchers and scientists must focus on the development and integration of advanced anti-spoofing techniques, such as multi-modal biometrics, 3D sensing technologies, and enhanced machine learning algorithms capable of detecting subtle discrepancies indicative of a 3D attack.

Moreover, the study emphasizes the importance of ongoing research and collaboration between academic, industry, and regulatory bodies to stay ahead of potential threats. By continuously evolving and improving facial recognition systems, it is possible to maintain their efficacy and reliability in security-critical environments. This research not only identifies the current FR vulnerability due to sophisticated 3D dodging but also paves the way for future innovations to safeguard biometric authentication methods against increasingly sophisticated attacks.

VI. FUTURE WORK

The future scope of research on 3D attacks on facial recognition systems is vast and critical for enhancing security measures of these systems responsible for authentication of users. Future studies can be focused on developing advanced anti-spoofing technologies, including multi-modal biometric systems that integrate facial recognition with other biometric data like voice or fingerprint recognition. Additionally, incorporating 3D sensing technologies, such as LiDAR [23] and structured light [24], can improve depth perception and detect three-dimensional anomalies indicative of spoofing attempts.

Another promising direction is the use of machine learning algorithms trained on large datasets of 3D attack scenarios to recognize subtle differences between genuine and spoofed inputs. Collaborating with interdisciplinary fields, such as computer vision, artificial intelligence, and cybersecurity, can lead to innovative solutions and robust defense mechanisms. Furthermore, continuous evaluation and updating of facial recognition systems in real-world environments will ensure they can adapt to evolving threats. Implementing rigorous testing protocols and standardizing security benchmarks globally will also contribute to the development of more secure and reliable facial recognition systems.

References

[1] Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, ‘Face Recognition Systems: A Survey’, Sensors, vol. 20, no. 2, 2020.

[2] N. Erdogmus and S. Marcel, "Spoofing Face Recognition With 3D Masks," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 7, pp. 1084-1097, July 2014, doi: 10.1109/TIFS.2014.2322255.

[3] N. Sadman, K. A. Hasan, E. Rashno, F. Alaca, Y. Tian and F. Zulkernine, "Vulnerability of Open-Source Face Recognition Systems to Blackbox Attacks: A Case Study with InsightFace," 2023 IEEE Symposium Series on Computational Intelligence (SSCI), Mexico City, Mexico, 2023, pp. 1164-1169, doi: 10.1109/SSCI52147.2023.10371801.

[4] Y. Li, Y. Li, X. Dai, S. Guo, and B. Xiao, 'Physical-World Optical Adversarial Attacks on 3D Face Recognition', in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2023, pp. 24699–24708.

[5] X. Zheng, Y. Fan, B. Wu, Y. Zhang, J. Wang, and S. Pan, 'Robust Physical-World Attacks on Face Recognition', Pattern Recognition, vol. 133, p. 109009, 2023.

[6] M. Shen, H. Yu, L. Zhu, K. Xu, Q. Li and J. Hu, "Effective and Robust Physical-World Attacks on Deep Learning Face Recognition Systems," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4063-4077, 2021, doi: 10.1109/TIFS.2021.3102492.

[7] H. O. Shahreza and S. Marcel, 'Template inversion attack against face recognition systems using 3d face reconstruction', in Proceedings of the IEEE/CVF International Conference on Computer Vision, 2023, pp. 19662–19672.

[8] S. Bhattacharjee, A. Mohammadi, and S. Marcel, 'Spoofing Deep Face Recognition with Custom Silicone Masks', in 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2018, pp. 1–7.

[9] J. Byun, H. Go, and C. Kim, 'Geometrically Adaptive Dictionary Attack on Face Recognition', in Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), 2022, pp. 3021–3030.

[10] A. Zolfi, S. Avidan, Y. Elovici, and A. Shabtai, 'Adversarial mask: Real-world adversarial attack against face recognition models', arXiv preprint arXiv:2111. 10759, vol. 2, no. 3, 2021.

[11] M. Ibsen et al., 'Attacking Face Recognition With T-Shirts: Database, Vulnerability Assessment, and Detection', IEEE Access, vol. 11, pp. 57867–57879, 2023.

[12] C.-Y. Lin, F.-J. Chen, H.-F. Ng, and W.-Y. Lin, 'Invisible Adversarial Attacks on Deep Learning-Based Face Recognition Models', IEEE Access, vol. 11, pp. 51567–51577, 2023.

[13] Q. Zhang, Q. Guo, R. Gao, F. Juefei-Xu, H. Yu, and W. Feng, 'Adversarial Relighting Against Face Recognition', IEEE Transactions on Information Forensics and Security, pp. 1–1, 2024.

[14] H. O. Shahreza and S. Marcel, 'Template Inversion Attack Using Synthetic Face Images Against Real Face Recognition Systems', IEEE Transactions on Biometrics, Behavior, and Identity Science, 2024.

[15] Z. Li et al., 'Sibling-Attack: Rethinking Transferable Adversarial Attacks Against Face Recognition', in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2023, pp. 24626–24637.

[16] Z. Wu, Y. Cheng, J. Yang, X. Ji, and W. Xu, 'DepthFake: Spoofing 3D Face Authentication with a 2D Photo', in 2023 IEEE Symposium on Security and Privacy (SP), 2023, pp. 917–933.

[17] Hamdan, B., Mokhtar, K. A self-immune to 3D masks attacks face recognition system. SIViP 12, 1053–1060 (2018). https://doi.org/10.1007/s11760-018-1253-5.

[18] R. Ramachandra and S. Marcel, 'MASK-MORPH: Does morphing of custom 3D face masks threatens the face recognition systems?', in 2022 18th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Madrid, Spain, 2022.

[19] M. Shen, Z. Liao, L. Zhu, K. Xu, and X. Du. VLA: A practical visible light-based attack on face recognition systems in physical world. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol., 3(3):103:1–103:19, 2019.

[20] M. Pautov, G. Melnikov, E. Kaziakhmedov, K. Kireev, and A. Petiushko, 'On Adversarial Patches: Real-World Attack on ArcFace-100 Face Recognition System', in 2019 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON), 2019.

[21] A. Dabouei, S. Soleymani, J. Dawson, and N. M. Nasrabadi, 'Fast Geometrically-Perturbed Adversarial Faces', arXiv [cs.LG]. 2018.

[22] L. Qin, F. Peng, S. Venkatesh, R. Ramachandra, M. Long, and C. Busch, 'Low Visual Distortion and Robust Morphing Attacks Based on Partial Face Image Manipulation', IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 3, no. 1, pp. 72–88, 2021.

[23] T. Raj, F. H. Hashim, A. B. Huddin, M. F. Ibrahim, and A. Hussain, 'A Survey on LiDAR Scanning Mechanisms', Electronics, vol. 9, no. 5, 2020.

[24] B. Cui, W. Tao, and H. Zhao, 'High-precision 3D reconstruction for small-to-medium-sized objects utilizing line-structured light scanning: A review', Remote Sensing, vol. 13, no. 21, p. 4457, 2021.

[25] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, 'DeepFace: Closing the Gap to Human-Level Performance in Face Verification', in 2014 IEEE Conference on Computer Vision and Pattern Recognition, 2014, pp. 1701–1708.

[26] F. Schroff, D. Kalenichenko, and J. Philbin, 'FaceNet: A unified embedding for face recognition and clustering', in 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015, pp. 815–823.

[27] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, 'ArcFace: Additive Angular Margin Loss for Deep Face Recognition', in 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2019, pp. 4685–4694.

[28] Wang, H., Wang, Y., Zhou, Z., Ji, X., Gong, D., Zhou, J., ... & Liu, W. (2018). "CosFace: Large Margin Cosine Loss for Deep Face Recognition." IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 5265-5274.

[29] Meng, Q., Zhao, S., Huang, Z., Zhou, F.: Magface: A universal representation for face recognition and quality assessment. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. pp. 14225–14234 (2021).

[30] Boutros, F., Damer, N., Kuijper, A., & Kirchbuchner, F. (2022). "ElasticFace: Elastic Margin Loss for Deep Face Recognition." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 1578-1587.

[31] X. Wu, R. He, Z. Sun, and T. Tan, 'A Light CNN for Deep Face Representation with Noisy Labels', arXiv [cs.CV]. 2018.

[32] He, K., Zhang, X., Ren, S., & Sun, J. (2016). "Deep Residual Learning for Image Recognition." IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 770-778.