International Journal of Advanced Science and Computer Applications (2024); 3(1): 75-80
DOI: 10.47679/ijasca.v3i1.38
https://ijasca.org/index.php/ijasca

RESEARCH ARTICLE

E-passport security systems and attack implications

Kaznah Alshammari [1]

Published online: 20 November 2023

Abstract

Recent technological advances aim to recognise user data using biometrics such as the face, fingerprint, hand veins and iris. Currently, face prints are widely used to verify user data in e-passports. As a result, institutions face substantial difficulties in maintaining an appropriate level of security. Human error can introduce flaws that undermine security mechanisms. One potential solution to this problem is to install a facial recognition security system. Both hardware and software components make up this system, with the hardware being a camera and the software comprising face detection and identification algorithms. The purpose of this essay is to provide a thorough understanding of the Face Recognition Security System, including its application and deployment. Furthermore, the essay investigates the various weaknesses and methods of attack that could be used to target the system. The purpose of addressing these factors is to improve the effectiveness and robustness of system security, notably e-passport security.

Keyword: Face recognition system, e-passport processing, security system, face ID identification

Introduction

Facial recognition technology has attracted considerable interest and has been widely adopted in recent years due to its multiple benefits in a variety of sectors. It has developed as a potent biometric tool for identifying people based on their distinctive face traits. Facial recognition, as opposed to traditional authentication techniques which rely on physical tokens or passwords, is non-intrusive and contactless, thereby making it easier to use and more user-friendly.

As facial recognition technology becomes more prevalent in everyday life, it is critical to address the security problems that arise with its use (Bodepudi & Reddy, 2020). Malicious actors may try to exploit flaws in facial recognition systems in order to obtain unauthorised access, threaten privacy or commit identity theft (Telo, 2023). As a result, understanding potential attacks and developing effective security measures to ensure that facial recognition systems are reliable is critical (Syed et al., 2021).

Deep neural network innovation has substantially accelerated the field of automatic facial recognition. These systems have considerable generalisation capabilities, thereby enhancing face recognition performance in unconstrained situations with varied lighting conditions, stances, image quality or camera types (Sharma & Guleria, 2022). As a result, facial recognition technologies have been widely employed in a variety of scenarios such as video surveillance, mobile access control and automated border control (ABC) (Scherhag et al., 2019).

However, the growing use of facial recognition systems has prompted concerns about their vulnerability to assaults such as impersonation and attacks employing changed facial photos (Fang et al., 2022). The use of modified facial photographs to fool the recognition process is one specific attack vector for these systems' generalisation capabilities (Boutros et al., 2023). In the case of e-passport applications for example, criminals can use face shift assaults by replacing their own facial image with that of a lookalike accomplice. Using the altered photograph, the accomplice can then obtain a genuine e-passport with all of the accompanying document security measures (Ferrara & Franco, 2022). These altered facial photos have the potential to fool both human examiners and commercial facial recognition technologies. The offender and his accomplice can then use the e-passport supplied to the accomplice to pass through automatic border control gates or even human checks at border crossings (Masood et al., 2023). This kind of attack, known as a face transformation attack, is further supported by the availability of user-friendly face transformation software which can be obtained free of charge or purchased at a low cost (Butpheng et al., 2020).

To summarise, being aware of potential threats and weaknesses in facial recognition systems is critical to ensure their robustness and security. It is possible to develop effective countermeasures that safeguard against impersonation attacks, face transformation attacks and other

[1] Department of Information Technology, Faculty of Computing and Information Technology, Northern Border University, Rafha 91911, Saudi Arabia

*) corresponding author

Kaznah Alshammari

Email: Khaznah.alshammari2@nbu.edu.sa

Received 28 October 2023 | Received in revised form 18 December 2024 | Accepted 11 February 2024
Available online 10 March 2024

forms of malicious exploitation in the realm of facial recognition technology by tackling these difficulties (Scherhag, 2019).

The current essay takes an in-depth look at the components and procedures that go into a conventional face recognition system. Face identification, feature extraction and matching algorithms are among the topics covered. Understanding these fundamental principles is essential to detect potential security flaws and vulnerabilities.

Facial recognition system

Theoretically, facial recognition systems are able to make comparisons between digital images of a human face and a stored database (Srinivas et al., 2022). A system like this is often utilised to confirm people's identities by means of ID verification services and it involves the system measuring and locating facial features in an image such as an e-passport in airports and border control, tracking student or worker attendance, and healthcare (Fubara-Manuel, 2020). Principal component analysis (PCA), linear discriminant analysis (LDA) and deep learning-based techniques are used in facial recognition systems (Natsheh & Said-Ahmed, 2022). Figure 1 depicts the steps of the facial recognition system. Many individuals are familiar with facial recognition technology due to its widespread usage. Typically, facial recognition does not rely on a vast database of images to determine an individual's identification; rather, it recognises and distinguishes one person as the self-person while restricting access to others (Mandal & Bhattacharya, 2020).

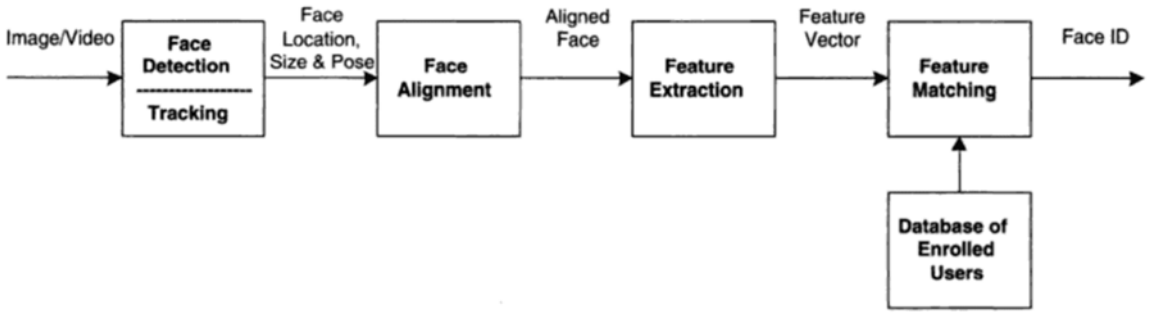

Figure 1: Facial recognition system (Mandal & Bhattacharya, 2020)

Facial recognition works by matching photographs of people on a watch list to the faces of those passing specific cameras (Roussi, 2020). The images on the watch lists can be of anyone, even persons who are not suspected of any wrongdoing and they can come from anywhere including accounts on social media. Facial technology systems differ but, in general, they work as follows:

Step 1: Detecting faces

The camera recognises and locates a facial picture, whether of a single person or a mass of people. The person captured in the picture can be either in profile or looking directly ahead (Afra & Alhajj, 2020).

Step 2: Examining a face

The image of the face is then collected and evaluated. The majority of facial recognition systems operate using 2D instead of 3D images because matching with photos in databases is more convenient in the 2D format (Ming et al., 2020). Your face's geometry is read by the software. The factors taken into consideration include your eyes' distance from one another, how deep your eye sockets are, how far your forehead extends below your chin, the contours of the chin, ears and lips, as well as how pronounced the cheekbones are. The aim is to identify the features of the face that enable people to be identified reliably (More et al., 2022).

Step 3: Image to data conversion

The face capture procedure effectively takes a series of analogue details from the image of the face and turns this into a series of digital data. As such, this entails the depiction of a human face in the form of a mathematical formula (Hasnine et al., 2021). The numerical code is referred to as a faceprint. Each person has their own faceprint, just as each person has their own thumbprint (Sharma et al., 2021).

Step 4: Check for a match

Subsequently, the faceprint is compared to a database of recognised faces. For example, the US FBI has access to a series of databases which collectively feature as many as 650 million images (JameerModi et al., 2022). Facebook has a facial recognition feature which utilises a database containing all of the images that have ever been tagged on the platform. In the event that your faceprint tallies with an image in a facial recognition database, a decision will be determined (Hanley, 2021).

In terms of biometric measurements, facial recognition is thought to be the most natural. Given that we typically recognise ourselves and other individuals by looking at their faces rather than their thumbprints or irises, this makes obvious sense. More than half of the world's population is believed to frequently interact with facial recognition technology (Fourati et al., 2020).

Facial recognition technology is now used by commercial organisations and governments throughout the world. Its efficacy varies, however, and some methods have already been abandoned due to their failure to work (Rowe, 2020). The use of facial recognition systems has generated criticism as well, with concerns that the technology violates individuals'

privacy, frequently identifies the wrong people, and fails to safeguard crucial biometric data. Deep fakes and other synthetic media have also prompted questions regarding the security of that media (Skeba & Baumer, 2020).

The current essay intends to contribute to the development of secure and reliable e-passports which rely on a type of facial recognition system by analysing vulnerabilities and suggesting appropriate security measures. It offers useful insight for researchers, developers and companies wishing to adopt facial recognition technology while protecting sensitive data and retaining user confidence.

E-passport system

Biometric passports (otherwise referred to as digital passports or e-passports) look like traditional passports but they have a small microprocessor chip embedded in them which can be used to confirm the identity of the person in possession of the passport (Choudhury, 2022). They make use of contactless smart card technology which includes an antenna and a microprocessor chip (a computer chip) inserted in the passport's front or rear cover or on its centre page. The crucial details of the passport are printed on the data sheet, reproduced on lines that can be read by a machine and saved on a chip (Gupta & Quamara, 2019). When the various security measures have been implemented as intended, public key infrastructure (PKI) is able to verify the details saved to the chip embedded in the passport, thereby reducing the likelihood of being able to use a forged passport (bin Suhaimi, 2020).

These types of identification systems currently use iris, fingerprint and face recognition as their standard biometrics. These were adopted following evaluation of various biometrics, including retinal scans. The ICAO Doc 9303 (ICAO 9303) of the International Civil Aviation Organization describes and documents chip features (Moolla, 2021). It is the ICAO that specifies the communication protocols and biometric file formats utilised in passports. The only thing that is actually recorded in the chip is the digital image of each biometric feature (often in JPEG or JPEG 2000 format). Electronic border control systems (e-borders) make comparisons between biometric features beyond the chip in the passport. The contactless chip has an interface that complies with the ISO/IEC 14443 international standard and has at least 32 kilobytes of EEPROM storage capacity to record biometric data. These specifications aim to facilitate communication between various nations and passport book producers (Moolla, 2021).

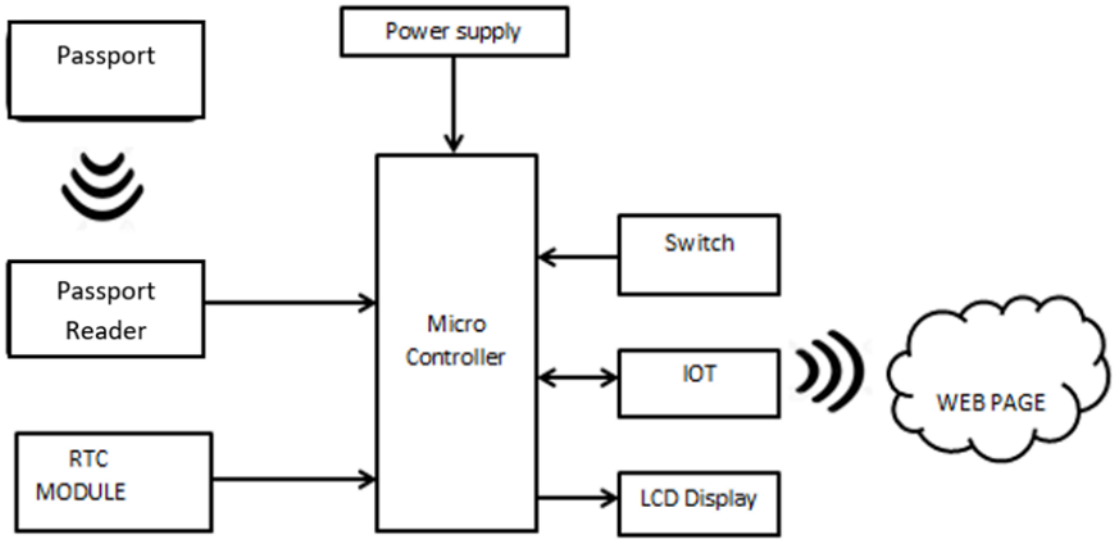

Figure 2: Architecture diagram of the proposed passport system (Vignesh et al., 2022)

Face recording system attacks

The security concerns relating to the deployment of facial recognition technologies will become apparent as it becomes increasingly ingrained in daily life. Malicious actors may try to exploit flaws in facial recognition systems to access restricted areas, violate users' privacy or commit identity theft (Alshammari, 2023). Numerous strategies for face presentation assault detection have been put forth to address the problem (Fang et al., 2023). These methods may be categorised as follows: hand-crafted feature-based methods and deep learning-based methods. The discussion that follows offers further details.

Deep learning method

Deep learning has demonstrated its effectiveness with regards to computer vision and has successfully tackled challenges including face presentation attack detection. Lei (2017) utilised a CNN to extract deep features and SVM was utilised for classification purposes rather than fully linked layers. Atoum (2017) proposed a two-stream network architecture which is able to learn depth- as well as patch-based features; the fusion scores from the two streams determine the classification outcome. In order to overcome the limits of only spatial information being extracted, Li (2018) presented a 3D-CNN structure. By utilising additional visual signals, this method effectively detects face presentation attacks. To improve the model's generalisability, a domain generalisation regularisation technique was included. The subject of face presentation attack detection using deep learning has hitherto been predominantly framed as a binary

classification problem. The importance of auxiliary supervision was emphasised by Liu et al. (2019) who developed a CNN-RNN architecture which makes use of remote photoplethysmography (rPPG) signals and depth map data. This method efficiently uses spoof patterns in both the spatial and temporal domains. Meanwhile, Yang (2019) constructed an expanded dataset is utilising particular picture synthesis techniques which improved the model's robustness yet further.

In the event that test and training samples derive from similar settings, deep learning-based approaches often outperform them in terms of classification accuracy. However, because these methods primarily rely on large-scale, well-designed datasets, they perform significantly worse when confronted with testing and training samples that are mismatched. Poor generalisability was especially common in previous deep learning-based approaches (Yang, 2014). However, recent work (Jia, 2020) has made significant progress in resolving this constraint.

Hand-crafted feature-based methods

To extract distinguishing traits, the approaches in this area generally rely on established patterns. Because it is typically the case that static face presentation attack samples are used, motion analysis-based methods including mouth movement, eye blinking (Kollreider, 2017) and holistic facial area movement analysis have been developed. Typically, it is possible to analyse optical flows in certain parts of images to collect biometric information. While motion-based approaches are able to successfully identify print assaults, they may struggle to detect replay attacks when motion cues for presentation attacks are readily apparent. Furthermore, image quality is critical in detecting face presentation attacks. Marcel (2017) provided a strategy for addressing presentation attacks which calculates prominent factors from 25 picture quality measures.

Although it has been demonstrated that colour space features and texture descriptors are effective at countering face presentation attacks, it is typically the case that discriminative features are extracted from the original pixels in the spatial domain and these can be harmed by annoyance noise added during image capture. Additionally, it is still challenging to investigate how to combine different colour spaces' various texture features to achieve the optimal colour texture characteristics. Furthermore, compared to strong ensemble classifiers, a single classifier may not always produce the best prediction results (Marcel, 2017).

The current essay delves into the components and techniques that comprise a traditional facial recognition system. Among the subjects discussed are facial recognition, feature extraction and matching algorithms. Understanding these basic principles is critical to identify potential security flaws and vulnerabilities. The following methods have been suggested for present attack detection:

Presentation attacks

Biometrics can provide convenience in applications requiring identity authentication such as access control, payments or travel. Biometric systems have become considerably more accurate, quicker and resilient to environmental and user variables thanks to recent advances in AI and computer vision (Moolla et al., 2021). However, without the appropriate technology, even biometric systems can be exploited and bypassed.

These direct attacks, often known as "spoofs" or presentation attacks (PAs), can disrupt a biometric system by employing presentation attack instruments (PAIs) (Micheletto, 2023). Photographs, masks, phony silicone fingerprints and even video replays are examples of such instruments. Presentation assaults pose significant problems to all main real-time biometric modalities (including face, fingerprint, hand vein, and iris recognition). Recognition-based presentation assaults are on the rise, as face recognition has emerged as the dominant biometric in many applications due to its low cost, precision and usefulness (Micheletto, 2023).

Spoofing attacks

Spoofing attacks seek to circumvent the facial recognition system by exploiting its flaws. This section concerns techniques including facial makeup, 3D mask spoofing and morphing faces (Bodepudi & Reddy, 2020). 3D mask attacks: In this kind of assault, the perpetrator reconstructs the face of the victim in a 3D form and presents this model to the camera/sensor (Bodepudi & Reddy, 2020).

Adversarial attacks

Adversarial assaults offer ways to create adversarial instances which are purposely created inputs that lead a machine learning model to make a mistake or incorrect categorisation. These inputs can be very minute and invisible to human eyes but they can influence the model's forecast. Adversarial attacks can degrade machine learning performance, induce model deviance or steal sensitive data. That witch made an error on the passport image (Devabhakthini et al., 2023).

What follows is a description of the procedures and experimental setups employed to determine how effective the proposed countermeasures are. It addresses measures for performance, dataset selection and evaluation criteria. The findings of these tests provide vital information regarding the countermeasures' strengths and limitations.

This section discusses various countermeasures and mitigation approaches for the vulnerabilities and attacks described in the preceding sections. It considers advances including liveness detection methods, anti-spoofing algorithms and adversarial resilience training.

Countermeasures can be taken to address these vulnerabilities and improve system security:

1. Liveness detection: Using liveness detection techniques can assist in the identification of presentation and spoofing attacks. The system can distinguish between live and artificial presentations by assessing dynamic indicators such as eye blinking or facial movement (Sharma & Selwal, 2023).

2. Anti-spoofing algorithms: By recognising anomalous face traits or characteristics that suggest counterfeit samples, robust anti-spoofing algorithms can detect spoofing attempts (Hajare & Ambhaikar, 2023).
3. Adversarial robustness: Including adversarial robustness strategies can help to protect the system against adversarial attacks. This includes training the system on adversarial examples or employing defensive techniques to identify and mitigate hostile perturbations (Bai et al., 2021).
4. Multi-factor authentication: Using face recognition alongside the other available authentication factors or biometric modalities (e.g., iris or fingerprint recognition) offers an additional layer of protection and minimises the risk of attacks proving successful.

To ensure the integrity and reliability of these systems, researchers, system developers and security professionals must continually explore and evaluate potential attack vectors, devise robust countermeasures and be aware of the latest advances in facial recognition security (Das et al., 2019).

Conclusion

The current essay has discussed the vulnerabilities and assaults that the e-passport facial recognition systems may encounter. Researchers and practitioners can create powerful remedies to ensure the security and reliability of facial recognition technology by recognising these vulnerabilities. In this rapidly changing industry, ongoing research and collaboration are critical to staying ahead of emerging dangers.

The facial recognition security system provides a quick and easy way to identify people based on their distinctive facial traits. Various sectors can improve access control, monitoring and authentication processes by implementing this technology. The system detects faces, extracts facial traits and compares them to a reference database. However, it is critical to recognise the potential weaknesses and threats that could jeopardise the system's security.

Presentation assaults entail deceiving the system by using modified or counterfeit facial samples. Spoofing assaults attempt to circumvent the system by using disguises or phony facial features. By modifying facial photos, adversarial attacks take advantage of flaws in the system's decision-making process. These attack vectors represent serious threats to the dependability of facial recognition systems.

Several interventions can be implemented to mitigate these hazards. To distinguish between real and false presentations, liveness detection algorithms might be used. Meanwhile, anti-spoofing algorithms can detect and reject fake samples. By training the system on adversarial cases or incorporating defensive measures, adversarial robustness strategies can reinforce the system against adversarial attacks. Furthermore, incorporating multi-factor authentication, which combines facial recognition with other biometric modalities or authentication factors, can further improve security.

To keep ahead of developing risks and ensure the resilience of facial recognition security systems, continuous research, development and collaboration are required. Organisations can improve the security and dependability of these systems by recognising the vulnerabilities and implementing effective countermeasures, resulting in a more secure environment for access control, surveillance and identity verification applications.

Acknowledgments: The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA, for funding this research work through project number " ".

References

Afra, S., & Alhajj, R. (2020) Early warning system: From face recognition by surveillance cameras to social media analysis to detecting suspicious people. *Physica A: Statistical Mechanics and its Applications*, *540*, 123151.

Alshammari, K., Beach, T., Rezgui, Y., & Alelwani, R. (2023) Built environment cybersecurity: development and validation of a semantically defined access management framework on a university case study. *Applied Sciences*, *13*(13), p.7518.

Atoum, Y. Y. L. (2017) Face anti-spoofing using patch and depth-based cnns. USA: Proceedings of the IEEE International Joint Conference on Biometrics, Denver.

Bai, T., Luo, J., Zhao, J., Wen, B., & Wang, Q. (2021) Recent advances in adversarial training for adversarial robustness. *arXiv preprint arXiv:2102.01356*.

bin Suhaimi, A. I. H., Noordin, N., & bin Ya'kub, M. F. (2020) Assessment of Malaysian e-passport PKI based on ISO 27000 series international standards. In *Journal of Physics: Conference Series,* 1551(1), p. 012003. IOP Publishing.

Bodepudi, A., & Reddy, M. (2020) Spoofing Attacks and Mitigation Strategies in Biometrics-as-a-Service Systems. *Eigenpub Review of Science and Technology*, *4*(1), pp. 1-14.

Boutros, F., Struc, V., Fierrez, J., & Damer, N. (2023) Synthetic data for face recognition: Current state and future prospects. *Image and Vision Computing*, 104688.

Butpheng, C., Yeh, K. H., & Xiong, H. (2020) Security and privacy in IoT-cloud-based e-health systems—A comprehensive review. *Symmetry*, *12*(7), pp. 1191.

Choudhury, Z. H. (2022) Encryption and encoding of facial images into quick response and high capacity color 2d code for biometric passport security system. *arXiv preprint arXiv:2203.15738*.

Das, S., Wang, B., Tingle, Z., & Camp, L. J. (2019) Evaluating user perception of multi-factor authentication: A systematic review. *arXiv preprint arXiv:1908.05901*.

Devabhakthini, P., Parida, S., Shukla, R. M., & Nayak, S. C. (2023) Analyzing the Impact of Adversarial Examples on Explainable Machine Learning. *arXiv preprint arXiv:2307.08327*.

Fang, M., Damer, N., Kirchbuchner, F., & Kuijper, A. (2022) Real masks and spoof faces: On the masked face presentation attack detection. *Pattern Recognition*, *123*, 108398.

Fang, M., Boutros, F., & Damer, N. (2023) Intra and Cross-spectrum Iris Presentation Attack Detection in the NIR and Visible Domains. In *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment* (pp. 171-199) Singapore: Springer Nature Singapore.

Ferrara, M., & Franco, A. (2022) Morph Creation and Vulnerability of Face Recognition Systems to Morphing. In *Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks* (pp. 117-137) Cham: Springer International Publishing.

Fourati, E., Elloumi, W., & Chetouani, A. (2020) Anti-spoofing in face recognition-based biometric authentication using image quality assessment. *Multimedia Tools and Applications*, *79*(1-2), pp. 865-889.

Fubara-Manuel, I. (2020) Biometric capture: disrupting the digital codification of black migrants in the UK. *African Diaspora*, *12*(1-2), pp. 117-141.

Gupta, B. B., & Quamara, M. (2019) *Smart Card Security: Applications, Attacks, and Countermeasures*. CRC Press.

Hajare, H. R., & Ambhaikar, A. (2023) Face Anti-Spoofing Techniques and Challenges: A short survey. In *2023 11th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing (ICETET-SIP),* pp. 1-6. IEEE.

Hanley, M., Barocas, S., Levy, K., Azenkot, S., & Nissenbaum, H. (2021) Computer vision and conflicting values: Describing people with automated alt text. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society,* pp. 543-554.

Hasnine, M. N., Bui, H. T., Tran, T. T. T., Nguyen, H. T., Akçapınar, G., & Ueda, H. (2021) Students' emotion extraction and visualization for engagement detection in online learning. *Procedia Computer Science*, *192*, pp.3423-3431.

JameerModi, S., Shaikh, T. R., & Mane, S. V. (2022) Automatic Door Opening with Face Recognition and Temperature Detecting Device. *NeuroQuantology*, *20*(12), p. 3272.

Jia, Y. J. Z. (2020) Single-side domain generalization for face anti-spoofing. USA: Proceedings of the 2020 IEEE.

Kollreider, K. H. F. (2017) Real-time face detection and motion analysis with application in "liveness. USA: IEEE Transactions on Information Forensics and Security.

Lei, L. X. F. (2017) An original face anti-spoofing approach using partial convolutional neural network. USA: in Proceedings of the International Conference on Image Processing Theory Tools & Applications.

Li, H. P. H. (2018) Learning generalized deep feature representation for face anti-spoofing. IEEE Transactions on Information Forensics and Security.

Liu, Y. A. J. (2019) Learning deep models for face anti-spoofing: binary or auxiliary supervision. USA: Proceedings of the IEEE International Conference on Computer Vision and Pattern Recognition.

Mandal, J. K., & Bhattacharya, D. (2020) *Emerging technology in modelling and graphics*. Springer Singapore.

Marcel, J. G. (2017) Face anti-spoofing based on general image quality assessment. Sweden: Proceedings of the International Conference on Pattern Recognition IEEE Computer Society.

Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2023) Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward. *Applied Intelligence*, *53*(4), pp. 3974-4026.

Micheletto, M. (2023) Fusion of fingerprint presentation attacks detection and matching: a real approach from the LivDet perspective.

Ming, Z., Visani, M., Luqman, M. M., & Burie, J. C. (2020) A survey on anti-spoofing methods for facial recognition with RGB cameras of generic consumer devices. *Journal of Imaging*, *6*(12), p. 139.

Moolla, Y., De Kock, A., Mabuza-Hocquet, G., Ntshangase, C. S., Nelufule, N., & Khanyile, P. (2021) Biometric recognition of infants using fingerprint, iris, and ear biometrics. *IEEE Access*, *9*, pp. 38269-38286.

More, C. S., Kumar, S. R. N., Chatterji, S., & Prawal, P. (2022) Detection of Face and Location of Driver for Vehicle Theft using RaspberryPi.

Natsheh, E., & Said-Ahmed, H. (2022) Authentication System by Facial Recognition with Principal Component Analysis and Deep Neural Networks. *International Journal of Intelligent Systems and Applications in Engineering*, *10*(4), pp. 179-183.

Roussi, A. (2020) Resisting the rise of facial recognition. *Nature*, *587*(7834), pp. 350-354.

Rowe, E. A. (2020) Regulating facial recognition technology in the private sector. *Stan. Tech. L. Rev.*, *24*, 1.

Scherhag, U., Rathgeb, C., Merkle, J., Breithaupt, R., & Busch, C. (2019) Face recognition systems under morphing attacks: A survey. *IEEE Access*, *7*, pp. 23012-23026.

Sharma, D., & Selwal, A. (2023) A survey on face presentation attack detection mechanisms: hitherto and future perspectives. *Multimedia Systems*, *29*(3), pp. 1527-1577.

Sharma, G., Patidar, G., Vishwakarma, H., & Shringi, D. (2021) Future of cybersecurity: a study on biometric scans.

Sharma, S., & Guleria, K. (2022) Deep learning models for image classification: comparison and applications. In *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE),* pp. 1733-1738, IEEE.

Skeba, P., & Baumer, E. P. (2020) Informational friction as a lens for studying algorithmic aspects of privacy. *Proceedings of the ACM on Human-Computer Interaction*, *4*(CSCW2), pp. 1-22.

Srinivas, T. S., Goutham, T., & Kumaran, M. S. (2022) Face Recognition based Smart Attendance System Using IoT.

Syed, F., Gupta, S. K., Hamood Alsamhi, S., Rashid, M., & Liu, X. (2021) A survey on recent optimal techniques for securing unmanned aerial vehicles applications. *Transactions on Emerging Telecommunications Technologies*, *32*(7), e4133.

Telo, J. (2023) Smart City Security Threats and Countermeasures in the Context of Emerging Technologies. *International Journal of Intelligent Automation and Computing*, *6*(1), pp. 31-45.

Vignesh, T., Thyagharajan, K. K., & Jeyavathana, R. B. (2022) An improved E-passport system with secured IoT and wireless communication technology. In *AIP Conference Proceedings,* 2452(1) AIP Publishing

Yang, X. W. L. (2019) Face anti-spoofing: model matters, so does data. USA: IEEE.

Yang, J. Z. L. (2014) Learn convolutional neural network for face anti-spoofing. Computer Science.