Society for Multidisciplinary & Advanced Research Techniques (SMART)
West Midlands Open University – Projects, Research, Innovations, Strategies & Multimedia (PRISM) Centre
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA
Harmath Global Educational Services

38th International Science Technology Education Arts Management
& Social Sciences (iSTEAMS) Bespoke Conference - Accra Ghana 2024

Anti-Spoofing Detection Model Using Transfer Learning Techniques for Smart Door Security Systems

[1]Shamsudeen Hussaini, [2]Isiaq Oludare Alabi[2] & [3]Oluwaseun Adeniyi Ojerinde
[1]Department of Computer Science, Federal University of Technology, Minna, Nigeria.
[2]Department of Information Technology, Federal University of Technology, Minna, Nigeria.

ABSTRACT

This study introduces a robust anti-spoofing detection model specifically designed for smart door security systems, targeting critical vulnerabilities present in current facial recognition technologies. Utilising transfer learning-based architectures, particularly VGG16 and MobileNet, the proposed approach integrates pre-trained weights alongside advanced image augmentation techniques to improve the model's capability to identify various spoofing attacks, including print, replay, and 3D mask attacks. The VGG16-based model achieved an impressive accuracy of 98.75%, while the MobileNet-based model recorded an accuracy of 97.82%, showcasing exceptional performance in differentiating between genuine and spoofed images. Evaluations using metrics such as precision, recall, and F1-score further confirmed the robustness and efficiency of the models. With its real-time applicability and computational efficiency, this system is well-suited for deployment in smart homes and IoT-enabled security frameworks. By addressing limitations related to dataset generalisation, robustness, and scalability, this research significantly enhances the reliability and security of biometric-based authentication systems, offering a scalable framework for future smart security applications.

Keywords: Anti-Spoofing, Detection Model, Transfer Learning, Techniques, Smart Door Security Systems

Proceedings Citation Format
Shamsudeen Hussaini, Isiaq Oludare Alabi & Oluwaseun Adeniyi Ojerinde (2024): Anti-Spoofing Detection Model Using Transfer Learning Techniques for Smart Door Security Systems. Proceedings of the 38th iSTEAMS Multidisciplinary Bespoke Conference. 17th – 19th July, 2024. University of Ghana, Accra, Ghana. Pp 211-220.
dx.doi.org/10.22624/AIMS/ACCRABESPOKE2024P22

1. INTRODUCTION

Spoofing is the act of impersonating an individual or system to gain unauthorized access or perform malicious actions, particularly in the context of biometric authentication systems like facial recognition.

This can involve techniques such as using a printed photo or a video of a person's face to deceive the system into granting access, which poses significant risks for identity theft and fraud. Anti-spoofing refers to the methods and technologies developed to detect and prevent such fraudulent attempts, ensuring that only legitimate users can access secured systems. These measures often analyze various indicators of liveness, such as eye movement or facial expressions, to differentiate between real users and spoofed representations, thereby enhancing the security of biometric systems against exploitation.

Based on existing technology, it is anticipated that by the end of 2023, there will be 478.2 million smart homes worldwide (Ali, 2022). Intriguingly, internet-connected devices can be used to secure smart home technology remotely. Smart home devices have the potential to reduce personal data security in addition to making it easier to safeguard the house from theft, damage, or accidents. According to research, while different smart homes make residents' lives easier, they also have several vulnerabilities that make them vulnerable to attacks by unauthorized users (Ali & Awed, 2018). Attackers may attempt to remotely operate smart appliances, use spoofing or masking techniques to unlock IOT-enabled smart door locks, or obtain video footage from smart cameras as examples of common smart home attacks (Ali & Awad, 2018).

Studies have indicated that the most straightforward method of identifying an individual is through their facial characteristic or features. Nonetheless, the human brain begins to recognize images from the faces of their parents and relatives. Smart locks are modern and innovative devices that provide enhanced security features compared to traditional locks. They offer benefits such as keyless entry, remote access, real-time alerts, monitoring and tracking capabilities, customizable user permissions, and integration with smart home systems. However, smart locks are not immune to vulnerabilities, such as hacking, physical tampering, and software bugs or glitches (Berglöf & Brunzell, 2023).

Anti-spoofing detection models can help prevent hackers from exploiting vulnerabilities in smart locks by detecting and blocking attempts to bypass the lock's authentication system. By using multiple factors for authentication, such as a combination of a passcode and fingerprint or facial recognition, anti-spoofing detection models can make it more difficult for hackers to gain unauthorized access to smart locks. Additionally, anti-spoofing detection models can help prevent physical tampering by detecting and blocking attempts to manipulate the lock mechanism or intercept wireless signals (Berglöf & Brunzell, 2023).

Since facial images are used on so many important documents worldwide, including passports, identity cards, driver's licenses, and students' identity cards, the value of facial image recognition technology cannot be understated, especially in light of the current generation (Zahra et al., 2023). Furthermore, the development of smart technology has led to a rise in the use of automated techniques for facial recognition tasks. Modern, highly capable processors can complete billions of computational or complex tasks in less than a second, including biometric detection, tracking-based applications, disease diagnosis, and various authentication computations. Face recognition technology is now widely used in devices and applications for daily tasks, and its adoption has become the norm. Adoption is widespread in applications like sophisticated security systems that monitor specific sensitive areas, identity, and verification in airports, businesses, and other service providers. Smartphone facial recognition and laptop facial login security are two other common uses of facial recognition that give users more freedom to experiment.

Spoofing, or impersonating someone else to carry out illicit actions, is the use of that person's identity without authorization. According to an evaluation of a recent study, facial spoofing attacks pose a seriously concerning risk to society in situations like bank fraud and social media account hijacking. Numerous tactics have been used recently to prevent spoofing attacks on facial recognition systems (Zahra et al., 2023). These attacks are known to take many different forms, such as 3-dimensional mask attacks, print attacks, and video assaults. On the other hand, in a print attack, the attacker tricks the camera by using a printed picture of the victim's face. In contrast, a video attack, which is thought to be slightly more sophisticated than a print attack, uses the victim's brief video clip to gain access to the victim's system.

1.1 Statement of the Problem

Increased security features and ease of use, facial recognition-based smart door lock systems have become more and more common in smart homes (Ajao et al., 2018). Despite the advantages, spoofing attacks have increased as a result of the widespread use of these systems, especially in places like Nigeria where there is a high prevalence of theft, corruption, and cybercrime (Umezinwa, 2013; Verissimo et al., 2023). To combat this increasing danger, scientists have investigated several AI-based anti-spoofing strategies, ranging from machine learning to deep learning approaches (Birnbach et al. 2019). When facial security locks are breached, it can lead to unauthorized access to restricted areas, loss of privacy, and potential identity theft. The implications of a breach can be significant, including financial losses, damage to reputation, and legal consequences (Berglöf & Brunzell, 2023). This is to ensure a great reduction in the risks associated with spoofing attacks and improve the security of smart door systems by utilizing cutting-edge machine-learning techniques like Transfer learning-based Architecture.

2. REVIEW OF RELATED STUDIES

Reviewing the research work of (Yang et al., 2020) titled FVRAS-Net: An Embedded Finger-Vein Recognition and Anti-Spoofing System Using a Unified Convolution Neural Network (CNN). The researchers talked about how the current finger-vein biometric systems can be vulnerable to spoofing attacks, where forged vein patterns printed on distinctive paper can fool the systems, leading to concerns regarding identification authenticity. They proposed a solution using a lightweight convolutional neural network (CNN) called the Finger-Vein Recognition and Anti-Spoofing Network (FVRAS-Net). FVRAS-Net integrates the recognition task and the anti-spoofing task into a unified CNN model using multitask learning (MTL) approach. The proposed solution shows that the Finger Vain Recognition system and anti-spoofing FVRAS-Net achieves excellent performance in both the recognition and anti-spoofing tasks.

According to the research work of (Czajka et al., 2017) titled Recognition of image-orientation-based iris spoofing. The researchers present a solution for automatically recognizing the correct orientation (left/right and upright/upside-down) of iris images by comparing two approaches: feature engineering using hand-crafted features classified by a Support Vector Machine (SVM), and feature learning using data-driven features learned and classified by a Convolutional Neural Network (CNN). The result of the experiment shows that the Support Vector Machine (SVM) approach achieves a classification rate of 99% for both orientations.

On the other hand, the Convolution Neural Network (CNN) based approach performs better for same-sensor experiments but exhibits slightly worse generalization capabilities to unknown sensors compared to the SVM. (Sajjad et al., 2019) This paper, titled Convolution Neural Network (CNN) based Anti-Spoofing Two-Tier Multi-Factor Authentication System. The researchers present a new hybrid technique for biometric recognition. There aims to provide a secure and authentic system while detecting spoofing attempts. The proposed scheme consists of two tiers: Tier I incorporates fingerprint, palm vein print, and face recognition to match with corresponding databases, while Tier II employs fingerprint, palm vein print, and face anti-spoofing convolutional neural networks (CNN) based models to detect spoofing. It has been stated in the article that the experimental results over five benchmark datasets verified the effectiveness of the proposed system in providing efficient and robust verification, overcoming the limitations in normal authentication and spoofing practices.

Reviewing the research work (Ganjoo & Purohit, 2021) titled Anti-Spoofing Door Lock Using Face Recognition and Blink Detection. The researchers discuss a computer vision approach for human face recognition and anti-spoofing mechanism using texture analysis, specifically the Histogram of Gradients (HOG) method and Support Vector Machines (SVMs) to recognize a face. According to the researchers, the proposed system aims to enhance security levels by detecting and preventing malicious attempts to deceive the face recognition system. The result in this article shows that the maximum accuracy achieved by this model is 92.68%, and it performs best in the afternoon. The total time required for both face recognition and blink detection is 9.89 seconds.

In this Article, the researchers proposed a methodology using a convolutional neural network (CNN) with handcrafted techniques such as LBP-TOP for feature extraction and training of the classifier. According to the authors (Asim et al., 2017). The researcher further stated that the CASIA and REPLAY-ATTACK which is publically available and achieved high competitive scores compared with state-of-art techniques results.

According to the research work of (Li et al., 2018) titled Unsupervised Domain Adaptation for Face Anti-Spoofing. This article highlights the limitations of existing face spoofing detection methods that assume training and testing samples belong to the same domain in terms of feature space and marginal probability distribution. These single-domain methods often lack generalization capability, limiting their practical application in real-world scenarios characterized by diverse conditions such as illumination, facial appearance, and camera quality. To address this issue, the authors propose an unsupervised domain adaptation face anti-spoofing scheme. The authors perform extensive experiments on existing benchmark databases and the new database verifies that the proposed approach can gain significantly better generalization capability in cross-domain scenarios by providing consistently better anti-spoofing performance

Based on the research work of (O. Lucena et al., 2017), the researchers revel that as a result of recent advancements in computer vision, face recognition systems are becoming more popular. As methods for fooling these systems get more sophisticated, countermeasure strategies are required. The researchers proposed transfer learning using a pre-trained Convolution Neural Network (CNN) model applying only static features to detect pictures, video, and mask attacks. The proposed method was tested on the REPLAY-ATTACK and 3DMAD public databases.

The experimental result indicates that on the REPLAY-ATTACK database, achieved an accuracy of 99.04% and a half total error rate (HTER) of 1.20%. For the 3DMAD achieved an accuracy of 100.00% and HTER 0.00%. In this paper, the researchers discuss that face recognition biometrics is quick employed. Based on the fast development of computer vision technology. The drawback of face recognition systems lies in their ability to differentiate between real and fake face images, which makes them prone to impersonation and spoofing. The authors (B & Chakkarwar, 2023) introduce a novel approach to face live detection, with a combination of a Convolution Neural Network (CNN). The experimentation and testing of face liveliness detection provide promising results accuracy, with an accuracy of 98%.

(Larbi et al., 2019) adopt a novel face anti-spoofing approach based on the multi-color Convolution Neural Network (CNN) architecture label DeepColorFASD. To address the problem of face recognition, which is vulnerable to spoofing attacks. The researchers evaluate the proposed system through experimental research using CASIA FASD. Results using this difficult database show that our method outperforms more current solutions as judged by the ROC curve and half total error rate (HTER).

Reviewing the research work of (Lin & Su, 2019), stated that the building of identification technology, such as iris, fingerprint, and finger vein, has become very popular. Attacks that can use face spoofing can limit a face recognition system's use while also making it more susceptible to security risks. The researchers proposed a deep neural network scheme for face anti-spoofing and liveliness detection. The experimental results have indicated the robustness of the proposed methodology against cut, print and replay attacks.

(Hamza et al., 2022) introduce the issue of potential failures in facial detection, recognition and authentication systems, additionally, the research identifies certain vulnerabilities that are common to many systems in terms of biometric attacks, such as morphing attacks. However, to address this issue the researcher proposed morphing detection techniques that his highly robust enough to detect variation in facial features such as eyes, age, headgear and the like. The researcher utilizes a comprehensive approach to evaluate the performance of the proposed system by using versatile datasets, thus Morph-2 and Morph-3 images. Based on the experimental analysis conducted the researcher achieved a promising and efficient performance.

(Almghraby & Elnady, 2021) in recent times Face mask detection has witnessed significant advancements in the domain of computer vision since the occurrence of the Covid-19 pandemic. However, various attempts have been made to develop software that is capable of detecting whether an individual is wearing masks or not. This researcher explains in detail the creation of a face mask detection model using "deep learning," "Tensor-Flow," "Keras," and "OpenCV." The basic technology used by the researcher for real-time mask detection is built on the MobilenetV2 architecture. 80% of the dataset is allocated for training the model training while 20% is used for testing. Furthermore, the dataset is further split into 80% training and 20% validation, resulting in a model trained on 65% of the dataset, validated on 15%, and tested on 20%. The optimization technique employed is "stochastic gradient descent" with SGD optimizer, using a learning rate of 0.001. Training and validation accuracy continually improved, reaching an epoch of 12 with 99% training accuracy and 98% validation accuracy.

Concurrently, training and validation losses steadily decreased, reaching their final stage at the 12th epoch, with a validation loss of 0.050% and a training loss of less than 0.025%. This system is efficient in a real-time detection environment, for detecting an individual without appropriate face masks and is also efficient for deployment, making it suitable for safety applications. It can be integrated with embedded systems in public places, such as airports, train stations, workplaces, and schools, to enforce public safety guidelines. This model is developed in such a way that it is compatible with both IP and non-IP cameras and can be utilized by web and desktop applications for live video feed detection. Moreover, it can be linked to entrance gates, granting access only to mask-wearing individuals, and applied in settings like shopping malls and universities.

(Iyer et al., 2021) In today's word, the utilization of deep learning is demonstrating its full potential across various ranges of applications and is pivotal in various technological domains. It reveals that one of the most prominent applications of deep learning is object recognition and tracking, and recent advancements have yielded promising outcomes in this regard. In this study the researcher drive tries to compare different systematic approaches for analyzing images in other to determine whether an individual is wearing a face mask correctly, not correctly, or not at all. Mask detection is applied to images, videos, and real-time surveillance using the three most widely adopted machine learning techniques which include You Only Look Once version 3 (YOLOv3), You Only Look Once version 5 (YOLOv5), and MobileNet-SSD V2. Based on the experimental analysis conducted it is identify the model can efficiently identify the presence of a face mask on a person's face, and their performance is assessed based on the accuracy and the efficiency of video processing. The study evaluates the real-time performance of the three algorithms in terms of Frames per Second (FPS) for detecting the present of face masks in the individual phase.

3. RESEARCH METHODOLOGY

This section introduces the scientific research methodology adopted for developing the proposed transfer learning-based anti-spoofing detection model. Additionally, it covers the requirement gathering methods, data sources, data collection methods, collection tools, resources, modules, Application Programming Interface (API), and Integrated Development Environment (IDE). The performance evaluation metrics and the transfer learning methodology will also be discussed.

Transfer Learning Anti-Spoofing model

The transfer learning is a concept of using pre-trained models on larger image dataset and down task the model prediction capability to a more streamline problem. This study will be using the ImageNet pre-trained weight by downloading them on VGG16 and MobileNet Architecture for Training the anti-spoofing detection model. This approach will provide a more robust, and highly accurate anti-spoofing detection model.

Transfer Learning Research Approach (Methodology)

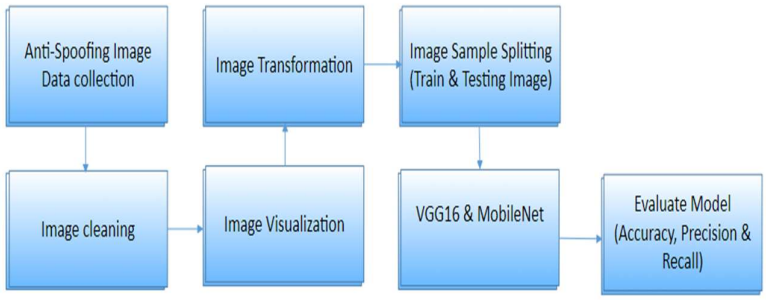

Figure 1: Research Methodology

In this section, we would be explaining the scientific step needed to be followed to achieve the proposed ant-spoofing detection model. The research methodological concept adopted is the transfer learning approach. This method involves loading pre-trained weights that was trained on a very large dataset, such text, video and images to leverage the performance of a smaller model. This transfer learning process reduce the computation cost of training large model and improve performance of a weak model or smaller model. The pre-trained model or weights been considered in this study is the VGG16, and the MobileNet pre-train weight. Finally, the transfer learning layer will now be connected to the Convolutional Neural Network (CNN) layers.

In respect to figure 3.4 it is shown that the Anti-Spoofing Image dataset is downloaded from and online space (Google drive) into the developer local system and imported into the Kaggle or jupyter lab notebook Integrated development environment for further processing. However, it's essential to upload the spoof/real image dataset on Kaggle repository to carry out exploratory data analysis and visualization on the image downloaded dataset. This step is essential to get an insight on what the images contain and other essential properties of the images such as image size, channel, and the life. Then the images are clean by extracting essential features and removing noisy content from the images. Furthermore, some transformation is carried out on the dataset to achieve a cleaned image for Anti-spoofing model training. Based on the figure the VGG16 and MobileNet Architecture weight is loaded which is later integrated which the CNN Architecture to enhance or leverage the training understanding of the model using the training image dataset. The testing data is used to test the model performance and evaluating the Accuracy, precision, and recall. Finally, a simulation web system interface is built to interact and evaluate the model in a real time environment.

4. CONCLUSION

The experimental analysis was conducted using an anti-spoofing image dataset sourced from publicly available Google Drive repositories, employing deep convolutional neural network (CNN) architectures, specifically VGG16 and MobileNet, to train the anti-spoofing detection model. MobileNet, characterized by its deeper layers compared to VGG16, demonstrated superior performance in the experiments, achieving an impressive accuracy of 99.9% with ImageNet weights, while VGG16 reached 97% accuracy.

Additionally the performance of the model was compared with the traditional method and outstanding performance was observed in the proposed method. In conclusion, the model's robustness indicates its potential for deployment in smart door systems as an effective anti-spoofing security solution.

REFERENCE

Abu-, T. N., Samy, J., & Abu-Naser, S. (2022). Classification of Sign-language Using VGG16. International Journal of Academic Engineering Research, 6(6), 36–46.

Afridi, T. H., Alam, A., Khan, M. N., Khan, J., & Lee, Y.-K. (2021). A Multimodal Memes Classification: A Survey and Open Research Issues. In M. Ben Ahmed, İ. Rakıp Karaş, D. Santos, O. Sergeyeva, & A. A. Boudhir (Eds.), Innovations in Smart Cities Applications Volume 4 (Vol. 183, pp. 1451–1466). Springer International Publishing. https://doi.org/10.1007/978-3-030-66840-2_109

Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., & Benjamins, R. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82–115.

B, R. Z., & Chakkarwar, V. (2023). Real-Time Face Liveness Detection and Face Anti-spoofing Using Deep Learning. Atlantis Press International BV. https://doi.org/10.2991/978-94-6463-196-8

Bendjillali, R. I., Beladgham, M., Merit, K., & Taleb-Ahmed, A. (2020). Illumination-robust face recognition based on deep convolutional neural networks architectures. Indonesian Journal of Electrical Engineering and Computer Science, 18(2), 1015. https://doi.org/10.11591/ijeecs.v18.i2.pp1015-1027

Berglöf—Smart locks User perception on security vs conven.pdf. (n.d.).

Bhangale, K., Ingle, P., Kanase, R., & Desale, D. (2022). Multi-view Multi-pose Robust Face Recognition Based on VGGNet (pp. 414–421). https://doi.org/10.1007/978-3-030-84760-9_36

Boulkenafet, Z., Komulainen, J., & Hadid, A. (2015). Face anti-spoofing based on color texture analysis. 2015 IEEE International Conference on Image Processing (ICIP), 2636–2640. https://ieeexplore.ieee.org/abstract/document/7351280/

Chen, H., Chen, Y., Tian, X., & Jiang, R. (2019). A Cascade Face Spoofing Detector Based on Face Anti-Spoofing R-CNN and Improved Retinex LBP. IEEE Access, 7, 170116–170133. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2955383

Czajka, A., Bowyer, K., Krumdick, M., & Vidal Mata, R. (2017). Recognition of Image-Orientation-Based Iris Spoofing. IEEE Transactions on Information Forensics and Security, PP, 1–1. https://doi.org/10.1109/TIFS.2017.2701332

De Marsico, M., Nappi, M., Riccio, D., & Dugelay, J.-L. (2012). Moving face spoofing detection via 3D projective invariants. 2012 5th IAPR International Conference on Biometrics (ICB), 73–78. https://ieeexplore.ieee.org/abstract/document/6199761/

Fei, Z., Li, Q., Ren, Y., Xu, H., Song, Y., & Liu, S. (2019). An Expression Recognition Method on Robots Based on Mobilenet V2-SSD (p. 122). https://doi.org/10.1109/ICSAI48974.2019.9010173

Ganjoo, R., & Purohit, A. (2021). Anti-spoofing door lock using face recognition and blink detection. 2021 6th International Conference on Inventive Computation Technologies (ICICT), 1090–1096.

George, A., Ecabert, C., Shahreza, H. O., Kotwal, K., & Marcel, S. (2023). EdgeFace: Efficient Face Recognition Model for Edge Devices (No. arXiv:2307.01838). arXiv. http://arxiv.org/abs/2307.01838

Ghosh, M., Mohsin Sarker Raihan, Md., Raihan, M., Akter, L., Kumar Bairagi, A., S. Alshamrani, S., & Masud, M. (2021). A Comparative Analysis of Machine Learning Algorithms to Predict Liver Disease. Intelligent Automation & Soft Computing, 30(3), 917–928. https://doi.org/10.32604/iasc.2021.017989

Goel, R., Mehmood, I., & Ugail, H. (2021). A Study of Deep Learning-Based Face Recognition Models for Sibling Identification. Sensors, 21(15), 5068. https://doi.org/10.3390/s21155068

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT press. https://books.google.com/books?hl=en&lr=&id=omivDQAAQBAJ&oi=fnd&pg=PR5&dq=Goodfellow,+I.,+Bengio,+Y.,+%26+Courville,+A.+(2016).+Deep+learning.+MIT+press.&ots=MOO_hprFPQ&sig=ndYbY8j43GVZu3stlYbnvbpuGNY

Hamza, M., Tehsin, S., Karamti, H., & Alghamdi, N. S. (2022). Generation and Detection of Face Morphing Attacks. IEEE Access, 10, 72557–72576. https://doi.org/10.1109/ACCESS.2022.3188668

Iyer, R., Bhensdadiya, K., & Ringe, P. (2021). Comparison of YOLOv3, YOLOv5s and MobileNet-SSD V2 for Real-Time Mask Detection. International Journal of Research in Engineering and Technology, 2395–0056.

Javadian Kootanaee, A., Poor Aghajan, A. ali, & Hosseini Shirvani, M. (2021). A hybrid model based on machine learning and genetic algorithm for detecting fraud in financial statements. Journal of Optimization in Industrial Engineering, 14(2). https://doi.org/10.22094/joie.2020.1877455.1685

Larbi, K., Ouarda, W., Drira, H., Ben Amor, B., & Ben Amar, C. (2019). DeepColorFASD: Face Anti Spoofing Solution Using a Multi Channeled Color Spaces CNN. Proceedings - 2018 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2018, 4011–4016. https://doi.org/10.1109/SMC.2018.00680

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436–444. https://doi.org/10.1038/nature14539

Lin, H. Y. S., & Su, Y. W. (2019). Convolutional neural networks for face anti-spoofing and liveness detection. 2019 6th International Conference on Systems and Informatics, ICSAI 2019, Icsai, 1233–1237. https://doi.org/10.1109/ICSAI48974.2019.9010495

Liu, H., Huang, S., Wang, P., Li, Z., Business School of Hunan Institute of Technology, Hengyang 421002, Hunan, China, & College of Computer Science and Engineering, Hunan Institute of Technology, Hengyang 421002, Hunan, China. (2021). A review of data mining methods in financial markets. Data Science in Finance and Economics, 1(4), 362–392. https://doi.org/10.3934/DSFE.2021020

Lucena, O., Junior, A., Moia, V., Souza, R., Valle, E., & Lotufo, R. (2017). Transfer learning using convolutional neural networks for face anti-spoofing. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10317 LNCS(1), 27–34. https://doi.org/10.1007/978-3-319-59876-5_4

Lucena, P., Braz, A., Chicoria, A., & Tizzei, L. (2016). IBM Design Thinking Software Development Framework. https://doi.org/10.1007/978-3-319-55907-0_9

Malik, M. A., Mazhar, T., Haq, I., Shahzad, T., Ghadi, Y. Y., Mallek, F., & Hamam, H. (2023). A Novel Deep Learning-Based Method for Real-Time Face Spoof Detection. https://www.researchsquare.com/article/rs-3371756/latest

Meenpal, T., Balakrishnan, A., & Verma, A. (2019). Facial Mask Detection using Semantic Segmentation (p. 5). https://doi.org/10.1109/CCCS.2019.8888092

Muhammadasim2017.pdf. (n.d.).

Pan, S. J., & Yang, Q. (2009). A survey on transfer learning. IEEE Transactions on Knowledge and Data Engineering, 22(10), 1345–1359.

Sajjad, M., Khan, S., Hussain, T., Muhammad, K., Sangaiah, A. K., Castiglione, A., Esposito, C., & Baik, S. W. (2019). CNN-based anti-spoofing two-tier multi-factor authentication system. Pattern Recognition Letters, 126, 123–131. https://doi.org/10.1016/j.patrec.2018.02.015

Santoso, A. J., & Saragih, R. E. (2022). Automatic Face Mask Detection Based on MobileNet V2 and DenseNet 121 Models (No. 04). ICIC International 学会. https://doi.org/10.24507/icicel.16.04.433

Savchenko, A. V. (2021). Facial expression and attributes recognition based on multi-task learning of lightweight neural networks. 2021 IEEE 19th International Symposium on Intelligent Systems and Informatics (SISY), 119–124. https://doi.org/10.1109/SISY52375.2021.9582508

Smart Home Security Solutions using Facial Authentication and Speaker Recognition through Artificial Neural Networks—ScienceDirect. (n.d.). Retrieved August 26, 2023, from https://www.sciencedirect.com/science/article/pii/S266630742100019X

Tu, X., Zhang, H., Xie, M., Luo, Y., Zhang, Y., & Ma, Z. (2019). Enhance the Motion Cues for Face Anti-Spoofing using CNN-LSTM Architecture (No. arXiv:1901.05635). arXiv. http://arxiv.org/abs/1901.05635

UG Student, Department of Mechatronics, Faculty of Engineering October 6 University, Egypt, Almghraby, M., Elnady*, A. O., & Head, Department of Mechatronics, Faculty of Engineering October 6 University, Egypt. (2021). Face Mask Detection in Real-Time using MobileNetv2. International Journal of Engineering and Advanced Technology, 10(6), 104–108. https://doi.org/10.35940/ijeat.F3050.0810621

Venkateswarlu, I. B., Kakarla, J., & Prakash, S. (2020). Face mask detection using MobileNet and Global Pooling Block. 2020 IEEE 4th Conference on Information & Communication Technology (CICT), 1–5. https://doi.org/10.1109/CICT51604.2020.9312083

Wang, T., Yang, J., Lei, Z., Liao, S., & Li, S. Z. (2013). Face liveness detection using 3D structure recovered from a single camera. 2013 International Conference on Biometrics (ICB), 1–6. https://ieeexplore.ieee.org/abstract/document/6612957/

Wang, Y., Yan, J., Sun, Q., Li, J., & Yang, Z. (2019). A MobileNets Convolutional Neural Network for GIS Partial Discharge Pattern Recognition in the Ubiquitous Power Internet of Things Context: Optimization, Comparison, and Application. IEEE Access, 7, 1–1. https://doi.org/10.1109/ACCESS.2019.2946662

Yacouby, R., & Axman, D. (2020). Probabilistic Extension of Precision, Recall, and F1 Score for More Thorough Evaluation of Classification Models. Proceedings of the First Workshop on Evaluation and Comparison of NLP Systems, 79–91. https://doi.org/10.18653/v1/2020.eval4nlp-1.9

Yang et al. - 2020—FVRAS-Net An Embedded Finger-Vein Recognition and.pdf. (n.d.). Retrieved August 27, 2023, from https://www.researchgate.net/profile/Yang-Weili/publication/342085897_FVRAS-Net_An_Embedded_Finger-Vein_Recognition_and_AntiSpoofing_System_Using_a_Unified_CNN/links/6086ce6c907dcf667bc6f157/FVRAS-Net-An-Embedded-Finger-Vein-Recognition-and-AntiSpoofing-System-Using-a-Unified-CNN.pdf

Yang, Y., Gupta, A., Feng, J., Singhal, P., Yadav, V., Wu, Y., Natarajan, P., Hedau, V., & Joo, J. (2022). Enhancing Fairness in Face Detection in Computer Vision Systems by Demographic Bias Mitigation. Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society, 813–822. https://doi.org/10.1145/3514094.3534153

Zhou, Y. (2022). The Efficient Implementation of Face Mask Detection Using MobileNet. Journal of Physics: Conference Series, 2181(1), 012022. https://doi.org/10.1088/1742-6596/2181/1/012022