EasyChair Preprint

№ 10033

Deep Learning Based Facial Obfuscation Using MobileNet

Madhumitha Peruboina, M Ramesh, Venkatesh Jinka, Likitha Machapalli, Sravan Venkata Ganesh Badveli and V P M B Aarthi

May 9, 2023

Deep Learning Based Facial Obfuscation Using MobileNet

P.Madhumitha
Department Of ECE
Kalasalingam Academy of Research and Education
Krishnankoil
madhumitha9802@gmail.com

M.Ramesh
Department of ECE
Kalasalingam Academy of Research and Education
Krishnankoil
mrameshme@gmail.com

J.Venkatesh
Department of ECE
KalasalingamAcademy of Research and Education
Krishnankoil
venkateshjinka189@gmail.com

M.Likitha
Department of ECE
Kalasalingam Academy of Research and Education
Krishnankoil
likithamachapalli36@gmail.com

B.Sravan Venkata Ganesh
Department of ECE
Kalasalingam Academy of Research and Education
Krishnankoil
badvelisravan@gmail.com

Aarthi V P M B
Department of ECE
Kalasalingam Academy of Research and Education
Krishnankoil
vpmb2aarthi@gmail.com

***Abstract*—More and more daily tasks are being completed electronically rather than with pen and paper or in person. This method is more secure since spoofing techniques may be used to identify unauthorized users, and once someone has been authenticated, only they can access the system. Because it provides greater segmentation than other techniques, the ability of LBPH to capture these distinctions between genuine and spoofed faces has been employed as a method for separating features, although LBPH may not be adequate to identify all face spoofing attempts, this is why MobilenetV2 model is used to detect faces. Overall, MobileNetV2 is a promising deep-learning model for face spoofing detection due to its efficiency and effectiveness. However, to increase its accuracy and resilience in identifying various sorts of face spoofing attempts, it might need to be integrated with additional techniques like LBPH, texture analysis, or depth analysis. This architecture will be used for classification, and people may be categorized based on their student ID or employee ID. Even with a large dataset, this architecture can provide superior accuracy. Therefore, other techniques such as the MobileNetV2 model may also be used in combination with LBPH to improve the accuracy of face spoofing detection.**

Keywords - Convolutional Neural Network (CNN), Facial Obfuscation, Image recognition, Enrollment Process, Biometrics, MobileNet Version2, Local Binary Pattern Histogram.

I. INTRODUCTION

The security of vital applications like border control, monitoring, and access control can be jeopardized by face spoofing or facial obfuscation, a significant weakness in biometric systems. To mislead the facial recognition system into providing illegal access, attackers might generate fictitious or counterfeit faces. To stop such assaults, it is crucial to create effective face spoofing detection systems. When someone tries to impersonate another person by fabricating data to gain unauthorized access and advantages, this is known as a spoofing attack. For instance, by placing a fake target in front of the camera in a photo, video, mask, or 3D model, one might fool a facial recognition system. Although one can also spoof using makeup or plastic surgery since it's so simple to acquire and capture facial images, the most frequent source of spoofing attacks is undoubtedly photos.

In recent years, deep learning has emerged as a promising solution for face spoofing detection due to its ability to learn discriminative features from large datasets. However, traditional deep learning models are computationally expensive and require high-end hardware to operate effectively. In less than a second, the face identification software recognizes a person's face and logs their attendance in the system. No physical touch is made. To avoid fraudsters from using other people's identities as fake to detour facial recognition systems. This technology is widely used in many companies allied when a person opens a new account on an online platform, businesses utilize face recognition to identify them specifically. In the event of risky or suspect account behavior**,** facial recognition technology can be utilized to confirm the identity of the real person using the account once this is completed.

To improve cybersecurity, businesses utilize facial recognition technology in place of passwords. Since your face cannot be altered, acquiring unwanted access to facial recognition systems is difficult. Another practical and extremely reliable security method for unlocking cell phones and other personal electronics is face recognition software. A lot of airports use biometric information as passports, letting travelers bypass lengthy lineups and move quickly via an automated terminal to their gate. The use of e-Passports using face recognition technology decreases wait times and enhances.

This work proposes lightweight deep learning-based face spoofing detection method using the MobileNetV2 architecture and the Local Binary Patterns Histograms (LBPH) method. MobileNetV2 is a computationally efficient deep learning model that is designed for mobile and embedded devices such as Digital cameras, Laptops,

Computers, etc. Here the proposed method extracts feature from the input face image using MobileNetV2 and apply a classification algorithm to detect face spoofing attacks. It has several advantages over traditional face spoofing detection methods suitable for real-time applications such as access control systems and this method does not require any pre-processing steps such as face alignment or normalization, increasing its resistance to changes in illumination, posture, and expression.

It tests the effectiveness of the suggested strategy using publicly accessible face spoofing datasets and contrasts it with current state-of-the-art techniques. The statistics show that the suggested technique provides great accuracy, resilience, and generalization while requiring significantly fewer computational resources compared to existing methods. This paper, endeavors to set up software that is mainly helpful in the attendance system of an organization. Implementing this technique, can confirm the authorized person and deny the fraud admittance. As a result, data from a corporation cannot be accessed by others or those outside your organization, and fake attendance cannot be entered. Using the suggested technology, face recognition systems' security and dependability should be greatly enhanced in practical applications.

II. RELATED WORK

Several research papers that discuss various techniques of facial obfuscation were cited. Maatta et al.,[1] used micro-texture analysis in face spoofing detection works in places like offices, colleges, and universities. These techniques are used to identify a Person's identity and secure it. But in some areas the research is going in some, In biometrics the main mission is to secure the identity of a person and spoof the faces, for this they use the parameters to steal the identity like spoofing faces, printed images, and lighting faces. How vulnerabilities will happen means due to lack of anti-spoofing. In biometrics, they are fooling trust by keeping a hard copy of a particular person. Using techniques like spoofing detection utilizing Micro-Texture analysis, picture quality evaluation, characterization of printing defects, and variations in light reflection, these vulnerabilities may be closed. this methodology will act as anti-spoofing to clarify whether the identity is real or fake.

L. Li et al.,[2] Convolutional neural network (CNN) data has been retrieved in this study to distinguish between real and fake faces. They used the Principal Component Analysis (PCA) method to reduce the number of attributes that might lead to overfitting problems. Ultimately, a Support Vector Machine (SVM) is employed to distinguish between actual and fake faces. They preferred DPCNN to pull out the division attributes from Convolutional Neural Networks (CNN). They preferred the DPCNN to pull out the division attributes from convolutional layers. Because of this, it is challenging to train a deep model that can achieve superior results with only a few available data. To get over this obstacle, they use a pre-trained VGG-face model for Anti-Spoofing. There are 11 blocks in it. beginning with 8 convolutional blocks, followed by multiple blocks carrying one or more convolutional layers that are subordinated by one or more chaotic layers (either Relu or max pooling layers). To extract deep part characteristics, some of the equations and calculations are done in the final three fully linked blocks.

A. da S. Pinto et al.,[3] This works explains how recent advancements in biometrics, information forensics, and security have increased the accuracy of biometric systems, particularly those that depend on facial information. An enormous problem with such systems is their susceptibility to imposter attacks, in which users try to log in as legitimate users even though they have no access credentials. In this work, they provide a fix for video-based face faking to biometric devices. This kind of attack presents an actual user's footage to the biometric system. The first attempt to address face spoofing in videos using an analysis of global data that is independent of video content. To distinguish between authentic and false access, the method uses noise fingerprints produced by the recovered video. They first compute the visual rhythm, then extract the matrices of gray-level co-occurrence, which are then employed as feature descriptors, in order to create a little depiction while capturing the noise. Results show that the proposed technique can distinguish between legitimate and fraudulent users for video-based spoofing with almost perfect classification accuracy.

To detect face spoofing, J. Tekli et al., [4] suggested a dual-channel neural architecture. The deep channel makes use of a CNN architecture to extract discriminative spoofing patterns from the data. The purpose of the proposed architecture is to extract small distortions of images that a demonstration assaults. To equip the model with domain-specific features that are well-known to specialists, the wide channel, in contrast, uses handcrafted features with a shallow network. The collected features from each channel are then combined into a low-dimensional latent space for classification.

From the perspective of color texture analysis, Z. Boulkenafet et.al.,[5] described an approaching issue of face anti-spoofing. They examined how effective the various color picture representations (RGB, HSV, and YCbCr) are at characterizing objects. The inherent differences in color and texture between real faces and synthetic ones, as well as whether they offer complementary representations. The effectiveness of the various face color texture representations was examined by deleting various local descriptors from the individual picture channels in the various color spaces.

III. EXISTING SYSTEM

Biometric technology that recognizes faces is now commonly used. Face recognition software ought to be able to spot spoofing attempts that use printed faces or digital presentations in addition to real people's faces. Attackers can quickly disable a face recognition system by presenting a fake image of a consumer to the camera. A mask or a facial picture projected on a digital or printed image can be a spoofing face. Thus, effective Face Anti-Spoofing (FAS) techniques are required for the development of safe face recognition systems. The FAS issue has made significant progress during the last few years. Several methods have historically been presented to extract handcrafted features using picture descriptors as spatial or Fourier space representations. These characteristics are often used to train a Support Vector Machine (SVM) to differentiate between actual and fraudulent examples. Nevertheless, since many descriptors were not initially intended for the FAS problem, these features are not adequately discriminative.

IV. PROPOSED SYSTEM

This work suggested a brand-new convolutional neural network (CNN)-based framework for the face obfuscation problem that is inspired by the method people use to determine whether a presented face example is real or not, namely, to first carefully observe the local regions to gain more discriminative information. Everything in modern life is automated. Automation is a technique for reducing manual labor that makes use of information technology. In several industries, a biometric system is utilized to identify individuals. Facial recognition is a technique for identifying someone or confirming their identity by using their face. Facial recognition technology can identify people in real time, in still photos, and in movies. Face recognition software is one form of a biometric system. Using biometric software, the ability to recognize voices, fingerprints and the retina or iris of the eye are further options. In biometrics, face detection is frequently used in conjunction with or as an addition to facial recognition systems. Moreover, it is utilized in picture database administration, human-computer interface, and video surveillance. In this work, the recommended model is instantly updated with the images as input. The dataset that was utilized is the CelebA Spoof dataset from Kaggle.

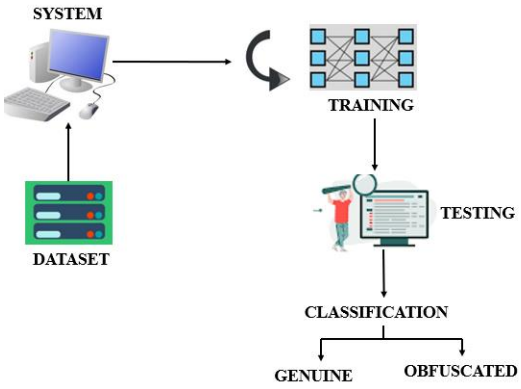


Fig 1. Architecture

There are 53 convolutional neural network layers in MobileNet-v2. The ImageNet database contains a pre-trained version of the network that has been trained on more than a million images. [1]. A number of animals, a keyboard, a mouse, and a pencil are among the 1000 distinct object categories that the pre-trained network can classify images into. A shallow neural network with fewer parameters and improved classification accuracy is Mobile Net. MobileNetV2 makes use of dense blocks from Dense Nets to significantly reduce the number of network parameters and increase classification accuracy. Local binary pattern histograms, or LBPH, are feature extraction techniques extensively employed in face recognition and identification systems. A binary pattern is generated for each small cell in LBPH by comparing the pixel values of the center pixel with those of its surrounding pixels. An image is segmented into tiny cells for LBPH. The decimal representation of this binary pattern, which indicates a feature for that specific cell, is then achieved. The occurrences of each feature value in the whole picture are counted to create a histogram after computing the LBPH features for each cell. For the purpose of categorization or recognition, this histogram represents the texture of the image and is employed as a feature vector. It has been demonstrated that LBPH is useful for recognizing faces, particularly when there may be differences in lighting, expression, and stance. It is a popular option for real-time facial recognition applications since it is also somewhat computationally efficient.

V.FLOW OF THE PROJECT

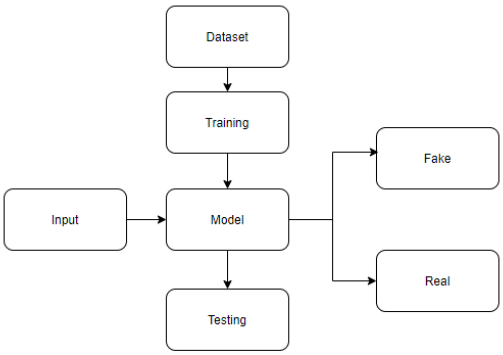


Fig 2. The Flow of the proposed system

Firstly, train the algorithm. For this, two datasets were utilized: CelebA dataset containing 2,02,599 face images with a size of 178×218. The next is a custom dataset which can include more images that contain the facial photographs of the persons to identify to accomplish this. For this algorithm to identify an input image and provide an output, and also need to assign each image an ID (which may be an employee/student ID). The same ID must appear on all images of the same person. A MobileNetV2 deep neural network architecture with weights regarded as 'ImageNet' weights that have already been pre-trained. LBPH was utilized in the past to identify the faces. The trained model determines if the facial landmarks in the Area of Interest (ROI) are real or fake by using the real-time video from the camera as an input. When the authorized person tries to access the system, the respective ID will be displayed.

VI. IMPLEMENTATIONS

The following are the implements for this work:

i. **Data gathering:** Needs to gather the information or data from the open source, this will be used in the training of the models.
ii. **Pre-processing:** Data must be pre-processed in accordance with the models in order to improve model accuracy and provide greater information about the data.
iii. **Feature Engineering:** This stage involves choosing characteristics depending on the importance of the column data, which can cut down on the time spent on multiple columns.
iv. **Model Building:** To get the final result model building for the dataset is an important step. Based on the dataset let's build the model for classification and regression.

v. **View Results:** The user views the generated results from the model**.**

vi. **Model Checking:** The system checks model accuracy and it takes off the necessary for the model building

vii. **Generate Results:** The system takes the input data from the users and produces the output.

VII.RESULTS AND DISCUSSION

The project is separated into two sections; the first portion is about actions taken within a system, and the second half is about actions taken by the user.

1)Tasks are done by the System:

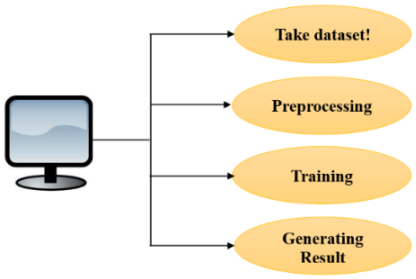


Fig 3. Tasks done by the System.

2)Tasks done by the User:

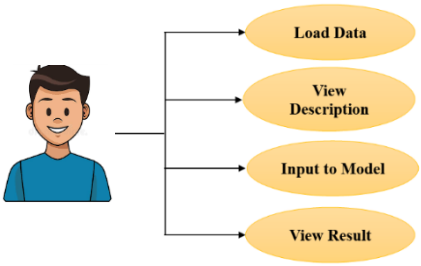


Fig 4. Tasks done by the User.

Step 1: **Capture Images-** A person must register with their face and unique ID in order to access the system, and for this OpenCV platform[5] is used to capture photos.

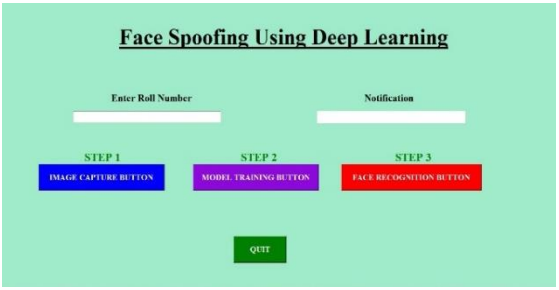
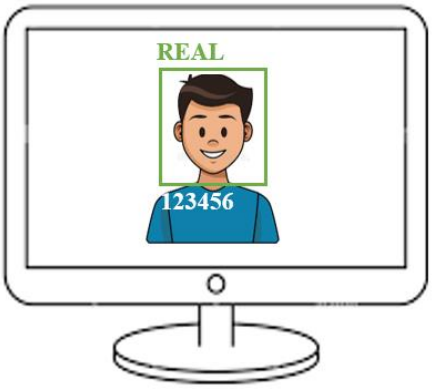


Fig 5. Admin page for registering.

Step 2: The ID that was provided by the designated individual in the previous stage is now trained on the taken image. To implement this MobileNetV2 was employed.



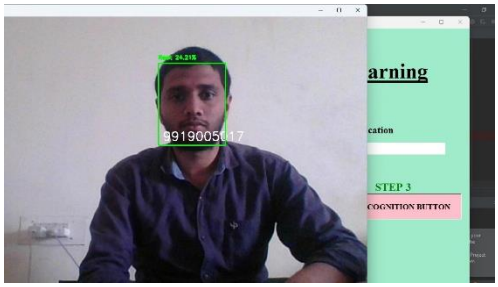


Fig 6. Real image of the user.

Step 3: Now that the image has been trained, LBPH is utilized to identify faces. And the appropriate ID will be shown on the screen when the authorized individual tries to access the system[6].

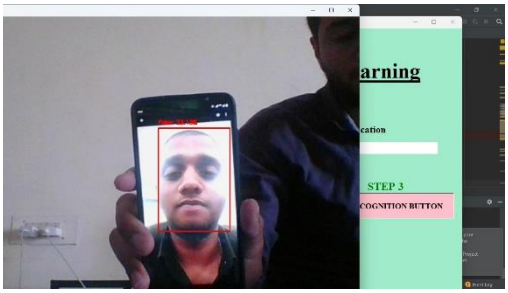


Fig 7. Obfuscated image recognized.

When an unauthorized user tries to enter the system, a popup message with the word "Fake" will appear on the screen [7].

VIII. CONCLUSION

The research on Deep Learning-Based Facial Spoofing Using MobileNet V2 and LBPH provides a comprehensive solution for both detecting fake or real faces and identifying individual faces. Facial recognition systems are more accurate and dependable when these two techniques are combined. An effective method for identifying facial spoofing assaults is provided by the MobileNet V2-based deep learning technology, which is essential for maintaining the security of facial recognition systems. The model's capacity to recognise various spoofing assaults is improved by the usage of a sizable dataset of both genuine and fake face photos during training.

The Local Binary Patterns Histograms (LBPH) technique, on the other hand, offers a reliable method for recognizing certain faces. It works by extracting features from facial images and using these features to match them with existing faces in a database. This method is highly effective in scenarios where facial recognition is required for access control, attendance management, or personal identification. Combining these two methods provides a comprehensive solution for facial recognition, ensuring that the system is secure and accurate in identifying both fake and real faces while maintaining a high level of identification accuracy for individual faces. The Deep Learning-Based Facial Spoofing Using MobileNet V2 and LBPH presents a promising solution for facial recognition systems, providing both security against spoofing attacks and accurate identification of individual faces. It is argued that video-based spoofing attacks are more realistic than photo-based spoofing attacks since algorithms based on eye movements may not be effective in identifying such assaults.

IX. FUTURE WORK

Further research and development in deep learning-based face spoofing or obfuscation utilizing MobileNetV2 and LBPH may be possible. It may focus on establishing a system that is resistant to adversarial assaults, combining several modalities for feature extraction, investigating other data augmentation approaches to increase the system's resilience, and developing a real-time detection system for video streams. Moreover, creating an explainable AI system might offer insights into the model's decision-making process and raise the system's credibility and transparency. The accuracy, effectiveness, and security of face recognition systems may be further improved by pursuing these directions, ensuring that continue to be dependable and trustworthy tools for identity verification across a variety of applications.

REFERENCES

[1] J. Maatta, A. Hadid, and M. Pietikainen, “Face spoofing detection from single images using micro-texture analysis,” in *2011 International Joint Conference on Biometrics (IJCB)*, Oct. 2011, pp. 1–7. doi: 10.1109/IJCB.2011.6117510.

[2] L. Li, X. Feng, Z. Boulkenafet, Z. Xia, M. Li, and A. Hadid, “An original face anti-spoofing approach using partial convolutional neural network,” in *2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA)*, Dec. 2016, pp. 1–6. doi: 10.1109/IPTA.2016.7821013.

[3] A. da S. Pinto, H. Pedrini, W. Schwartz, and A. Rocha, “Video-Based Face Spoofing Detection through Visual Rhythm Analysis,” in *2012 25th SIBGRAPI Conference on Graphics, Patterns and Images*, Aug. 2012, pp. 221–228. doi: 10.1109/SIBGRAPI.2012.38.

[4] J. Tekli, B. al Bouna, R. Couturier, G. Tekli, Z. al Zein, and M. Kamradt, “A Framework for Evaluating Image Obfuscation under Deep Learning-Assisted Privacy Attacks,” in *2019 17th International Conference on Privacy, Security and Trust (PST)*, Aug. 2019, pp. 1–10. doi: 10.1109/PST47121.2019.8949040.

[5] Z. Boulkenafet, J. Komulainen, and A. Hadid, “Face Spoofing Detection Using Colour Texture Analysis,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1818–1830, Aug. 2016, doi: 10.1109/TIFS.2016.2555286.

[6] Di Wen, Hu Han, and A. K. Jain, “Face Spoof Detection With Image Distortion Analysis,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 746–761, Apr. 2015, doi: 10.1109/TIFS.2015.2400395.

[7] S. R. Arashloo, J. Kittler, and W. Christmas, “An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol,” *IEEE Access*, vol. 5, pp. 13868–13882, 2017, doi: 10.1109/ACCESS.2017.2729161.

[8] K. Patel, H. Han, and A. K. Jain, “Secure Face Unlock: Spoof Detection on Smartphones,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 10, pp. 2268–2283, Oct. 2016, doi: 10.1109/TIFS.2016.2578288.

[9] W. R. Schwartz, A. Rocha, and H. Pedrini, “Face spoofing detection through partial least squares and low-level descriptors,” in *2011 International Joint Conference on Biometrics (IJCB)*, Oct. 2011, pp. 1–8. doi: 10.1109/IJCB.2011.6117592.

[10] T. I. Dhamecha, A. Nigam, R. Singh, and M. Vatsa, “Disguise detection and face recognition in visible and thermal spectrums,” in *2013 International Conference on Biometrics (ICB)*, Jun. 2013, pp. 1–8. doi: 10.1109/ICB.2013.6613019.

[11] A. George, Z. Mostaani, D. Geissenbuhler, O. Nikisins, A. Anjos, and S. Marcel, “Biometric Face Presentation Attack Detection With Multi-Channel Convolutional Neural Network,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 42–55, 2020, doi: 10.1109/TIFS.2019.2916652.

[12] G. Heusch, A. George, D. Geissbuhler, Z. Mostaani, and S. Marcel, “Deep Models and Shortwave Infrared Information to Detect Face Presentation Attacks,” *IEEE Trans Biom Behav Identity Sci*, vol. 2, no. 4, pp. 399–409, Oct. 2020, doi: 10.1109/TBIOM.2020.3010312.

[13] L. Fan, “Practical Image Obfuscation with Provable Privacy,” in *2019 IEEE International Conference on Multimedia and Expo (ICME)*, Jul. 2019, pp. 784–789. doi: 10.1109/ICME.2019.00140.

[14] Q. Hong, Z. Wang, Z. He, N. Wang, X. Tian, and T. Lu, “Masked Face Recognition with Identification Association,” in *2020 IEEE 32nd International Conference on Tools with Artificial Intelligence (ICTAI)*, Nov. 2020, pp. 731–735. doi: 10.1109/ICTAI50040.2020.00116.

[15] S. R. Arashloo, J. Kittler, and W. Christmas, “Face Spoofing Detection Based on Multiple Descriptor Fusion Using Multiscale Dynamic Binarized Statistical Image Features,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2396–2407, Nov. 2015, doi: 10.1109/TIFS.2015.2458700.

[16] S. Kumar, S. Singh, and J. Kumar, “A comparative study on face spoofing attacks,” in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, May 2017, pp. 1104–1108. doi: 10.1109/CCAA.2017.8229961.

[17] X. Zhao, Y. Lin, and J. Heikkila, “Dynamic Texture Recognition Using Volume Local Binary Count Patterns With an Application to 2D Face Spoofing Detection,” *IEEE Trans Multimedia*, vol. 20, no. 3, pp. 552–566, Mar. 2018, doi: 10.1109/TMM.2017.2750415.

[18] X. Sun, L. Huang, and C. Liu, “Multispectral face spoofing detection using VIS–NIR imaging correlation,” *Int J Wavelets Multiresolut Inf Process*, vol. 16, no. 02, p. 1840003, Mar. 2018, doi: 10.1142/S0219691318400039.

[19] Xudong Sun, Lei Huang, and Changping Liu, “Context based face spoofing detection using active near-infrared images,” in *2016 23rd International Conference on Pattern Recognition (ICPR)*, Dec. 2016, pp. 4262–4267. doi: 10.1109/ICPR.2016.7900303.

[20] S. Chen, A. Pande, and P. Mohapatra, “Sensor-assisted facial recognition,” in *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*, Jun. 2014, pp. 109–122. doi: 10.1145/2594368.2594373.

[21] C. Benegui and R. T. Ionescu, “Convolutional Neural Networks for User Identification Based on Motion Sensors Represented as Images,” *IEEE Access*, vol. 8, pp. 61255–61266, 2020, doi: 10.1109/ACCESS.2020.2984214.

[22] H. Chen, W. Wang, J. Zhang, and Q. Zhang, “EchoFace: Acoustic Sensor-Based Media Attack Detection for Face Authentication,” *IEEE Internet Things J*, vol. 7, no. 3, pp. 2152–2159, Mar. 2020, doi: 10.1109/JIOT.2019.2959203.

[23] E. M. Nowara, A. Sabharwal, and A. Veeraraghavan, “PPGSecure: Biometric Presentation Attack Detection Using Photopletysmograms,” in *2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017)*, May 2017, pp. 56–62. doi: 10.1109/FG.2017.16.

[24] S. Ait Chellouche, J. Arnaud, and D. Negru, “Flexible User Profile Management for Context-Aware Ubiquitous Environments,” in *2010 7th IEEE Consumer Communications and Networking Conference*, Jan. 2010, pp. 1–5. doi: 10.1109/CCNC.2010.5421640.

[25] Muthukumar, S., & Kavi Priya A, “A biometric system based on Gabor feature extraction with SVM classifier for Finger-Knuckle-Print”, in 2017 *IEEE Access*, 5, 14138-14147. doi: 10.1109/ACCESS.2017.2717320