

# People Identification Through Facial Recognition and Anti-Spoofing Using Deep Learning

Fathima Jameera. B, G. Suresh, S. Hemalatha, S. Vilma Veronica

Department of Computer Science and Engineering, Kings Engineering College, Irungattukottai  
Sriperumbudur, India

## ARTICLE INFO

### Article History :

Accepted: 01 Oct 2023

Published: 27 Oct 2023

### Publication Issue :

Volume 10, Issue 5

September-October-2023

### Page Number :

253-262

## ABSTRACT

This research effort uses cutting-edge anti-spoofing techniques in conjunction with deep learning approaches to address the issue of spoofing assaults on facial recognition systems. A diversified dataset containing real facial photos and several spoofing attack scenarios is compiled as the project's first step.

Then, data pretreatment methods are used to guarantee data consistency and the best model performance. The research makes use of MobileNet and VGG-16, two well-known deep-learning architectures, to build reliable facial recognition models. A thorough evaluation using well-established metrics including classification reports, accuracy scores, and confusion matrices is undertaken after thorough training and validation. It's significant because this research incorporates real-time anti-spoofing capabilities, which go beyond traditional facial recognition jobs. Webcam functionality is added to the deployed models to assess real-time images in comparison to reference passport-size photos. Dynamically shifting boundary box colors—blue for real faces and red for detected fake images—indicate the anti-spoofing technology. The project's conclusion contains a thorough comparison of the MobileNet and VGG-16 models that identifies and compares each model's advantages and disadvantages. Real-time demos also highlight the anti-spoofing methodology's effectiveness in practice.

Keywords : Anti-spoofing, MobileNet, Webcam Access, VGG-16.

## I. INTRODUCTION

Identity verification and access control have been transformed across a wide range of sectors by the

widespread use of facial recognition technology. However, a growing concern about face recognition systems' susceptibility to sophisticated spoofing assaults has arisen as a result of the technology's quick

adoption. The integrity of such systems is weakened by these attacks, which can take the form of static images or dynamic movies. They also pose serious risks to user trust and security. By fusing the strength of deep learning techniques with cutting-edge anti-spoofing algorithms, this research study sets out on a quest to increase the robustness and dependability of facial recognition systems.

The demand for reliable and accurate identity verification procedures has never been greater as digital interactions support modern lifestyles more and more. Even though they are effective, today's facial recognition systems are nevertheless vulnerable to phony attempts by enemies to impersonate them. Unauthorized access, fraudulent transactions, and data breaches can result from these subversions. Therefore, it becomes imperative to strengthen facial recognition with cutting-edge anti-spoofing techniques.

Meticulous preparation is the first step on the path to a facial recognition landscape that is safer. The creation comprehensive dataset with real facial photos and a variety of painstakingly generated spoofing scenarios is the first crucial step. The dataset is then rigorously pre-processed to standardize its quality and guarantee the best model performance. The foundation upon which the suggested solution is built is laid by this preliminary labor, which also sets the stage for the succeeding stages. The main goals of this research project are to increase the reliability of face recognition systems for identifying people and to develop a strong anti-spoofing system that can distinguish between real and fake facial data. The MobileNet and VGG-16 models, in particular, must be used to accomplish these aims, which demand the use of cutting-edge deep learning architectures. Our face recognition framework's foundation is made up of these architectures, which also make it possible to train models to recognize people based on complex facial traits.

The research process includes several stages, beginning with the creation of a varied and representative dataset that includes real facial photos and a range of spoofing scenarios. Data consistency is ensured and model performance is improved by later data pre-processing. The resulting models undergo thorough training, validation, and performance testing utilizing benchmark measures. This research also has a practical advantage because of the incorporation of a real-time anti-spoofing mechanism, which enables dynamic facial authenticity evaluation. The suggested framework's ability to foil complex spoofing efforts is strengthened by this method, which increases the robustness of the framework. This research project's breakthrough, the seamless integration of real-time anti-spoofing techniques into the facial recognition process, is one of its defining characteristics. The technology uses the capabilities of live webcam feeds and compares them to reference passport-size photographs to evaluate faces as real or fake on the fly. This revolutionary change raises the bar for adversarial assaults on facial recognition systems and improves the security of the identification process.

## II. LITERATURE REVIEW

In Lin, H. Y. S., & Su, Y. W. (2019, November). The development of biometric identification techniques, such as fingerprint, iris, finger vein, and so on, has become relatively mature over the past few decades, and related applications have become quite popular. The development of GPU acceleration techniques and the influence of deep neural networks boost the popularity of face recognition systems while also improving their accuracy. Face spoofing and presentation attacks are a new difficult tasks that face recognition systems' applications would disclose, even though they solve the problem of person identification. Face spoofing assaults, whether they take the form of images, videos, or 3D masks, not only limit the use of face recognition systems but also make them more security-vulnerable. Therefore, a

deep neural network technique for face anti-spoofing and liveness detection is suggested in this paper to guard against common face spoofing assaults on the existing face recognition systems. The experimental findings have shown that the suggested approach is resistant to print, cut, and replay attacks.

In A. K., Castiglione, A., ... & Baik, S. W. (2019). There are numerous hybrid and multimodal biometric recognition strategies that use both soft and hard biometric schemes to create secure and authentic systems. This article suggests a brand-new hybrid technique that verifies a user's identity to the system and checks to see if they authenticated themselves or used a fake biometric. The suggested system consists of two parts: Tier I integrates face, palm vein, and fingerprint identification to match with relevant databases, and Tier II uses a convolutional neural network (CNN)-based models for face, palm vein, and fingerprint anti-spoofing to detect spoofing. A fingerprint's hash is first matched to a database of fingerprints. The fingerprint is evaluated against a CNN-based fingerprint model after a successful match to determine if it is fake or not. The process is repeated for the face and palm, and after considering all the evidence, the system allows the user to log in. The usefulness of the suggested approach in providing efficient and reliable verification, overcoming the constraints in customary authentication and spoofing practices, was confirmed by experimental findings over five benchmark datasets.

In Anthony, P., Ay, B., & Aydin, G. (2021, August). Face recognition systems are becoming more widely used, popularized, and applicable due to their advantages of being very convenient, contactless, and non-intrusive when compared to other biometric systems like voice recognition and fingerprint. It is, regrettably, the most susceptible to spoofing assaults because registered users' photos and videos may easily be obtained online or by simply

taking a photo of their face with a camera, even without their knowledge or permission. Therefore, the requirement for anti-spoofing defenses against such assaults. The development of face anti-spoofing techniques has been the subject of numerous research initiatives. When compared to other biometric systems like voice recognition and fingerprint, face recognition systems have the advantages of being extremely convenient, contactless, and non-intrusive. As a result, they are becoming more and more commonplace. Regrettably, it is the most open to spoofing attacks because registered users' photographs and videos may be easily obtained online or by simply taking a photo of someone's face with a camera, even without that person's knowledge or consent. As a result, anti-spoofing measures are necessary against such attacks. Numerous research endeavors have been devoted to the development of face anti-spoofing systems.

In Bezas, K., & Filippidou, F. (2023). People's lifestyles must adapt to a number of adjustments and difficulties as Covid-19 spreads over the globe. Additionally, this causes additional issues and demands for automation facilities. Masks, for instance, are nearly always worn by people in public these days. To handle the increasingly acute epidemic pressure, the majority of access control systems (ACS) are unable to identify people who are wearing masks and validate their identities. As a result, many public entries now operate in an attendant mode, which has a low efficiency, a high risk of infection, and a tiny margin for error. In this study, a brand-new face-based security classification paradigm is being forth. This framework makes use of a face authentication method with anti-spoofing capabilities and a mask detection technique. This research uses the Reply-Attack datasets and the Chinese Academy of Science Institute of Automation-Face Anti-spoofing Datasets (CASIA-FASD) as benchmarks to assess the performance of the framework. According to performance

evaluation, the Equal Error Rate (EER) is 5.5%, and the Half Total Error Rate (HTER) is 9.7%. A single frame processes in 0.12 seconds on average. The outcomes show that this framework may be used on an embedded system to carry out the task of mask recognition and face authentication in real time and has a high anti-spoofing capability.

In Wang, D., Ma, G., & Liu, X. (2022). Technology is advancing our capacity to automatically detect people and secure access in the emerging field of biometrics. Due to the fact that the majority of devices can be fitted with a camera, the face is a fantastic alternative for an authentication application. Fraudsters can alter biometric data by, for instance, utilizing photographs of faces rather than the real thing. Therefore, it is crucial to verify that the biometric belongs to an actual, live individual. One approach to stopping this kind of fraud is to face anti-spoofing. The goal of this work is to compare five potent deep learning architectures for anti-spoofing, namely DenseNet201, DenseNet169, VGG16, MiniVGG, InceptionV3, and ResNet50. The ROSE-Youtu Face Liveness Detection dataset was used in this investigation. According to experimental findings, using deep learning and particularly the MiniVGG architecture is effective in terms of both maximum accuracy and conventional performance evaluation metrics.

### III. RESEARCH METHODOLOGY

Our research's central idea is around a complex yet user-friendly architecture that not only improves face recognition's accuracy but also fortifies the system against spoofing attempts. Our suggested approach combines a cutting-edge real-time anti-spoofing mechanism with the benefits of deep learning architectures, particularly MobileNet and VGG-16. For reliable and accurate facial recognition, we use deep learning architectures. The MobileNet and VGG-16 models were chosen due to their success

in image classification challenges in the past. These models are able to accurately discriminate between people because they can learn complex facial patterns and features from huge datasets.

Our suggested method entails training these models on a variety of datasets made up of real face image data. The models acquire the ability to separate distinguishing characteristics from facial data and encode them into small representations. The trained models then function as potent classifiers, able to link input photographs with appropriate people. The seamless incorporation of real-time anti-spoofing methods into the facial recognition process is what distinguishes our research from others. By effectively preventing adversaries from tricking the system with fake pictures or videos, this method offers an extra degree of protection. The system uses a webcam to record live video while our model is running in real-time. Following that, the anti-spoofing method is applied to these live photos. The mechanism operates by dynamically assessing the facial image that is displayed and contrasting it with a reference passport-size photo of the person. When using facial recognition to identify a person, the system checks to see if the facial image is real. If it is, it marks the identification with a distinctive blue boundary box. On the other hand, if the system notices potential spoofing through anomalies like uneven depth, bizarre texture patterns, or a lack of motion cues, it raises an alert and indicates this with a conspicuous red boundary box.

By continuously evaluating the veracity of displayed facial photos in real time, our anti-spoofing technology serves as a watchful guardian. The method greatly increases the bar for spoofing attacks by dynamically assessing the liveliness and consistency of the images, hence improving the overall security of the identification procedure. Innovative deep learning methods and in-the-moment anti-spoofing safeguards come together in

the suggested model. Our framework seeks to transform the field of safe people identification by combining the strength of MobileNet and VGG-16 for facial recognition with a vigilant anti-spoofing mechanism. We provide a thorough examination of the efficiency and potential of our model in the parts that follow by delving into the technical design, training approaches, and experimental findings.

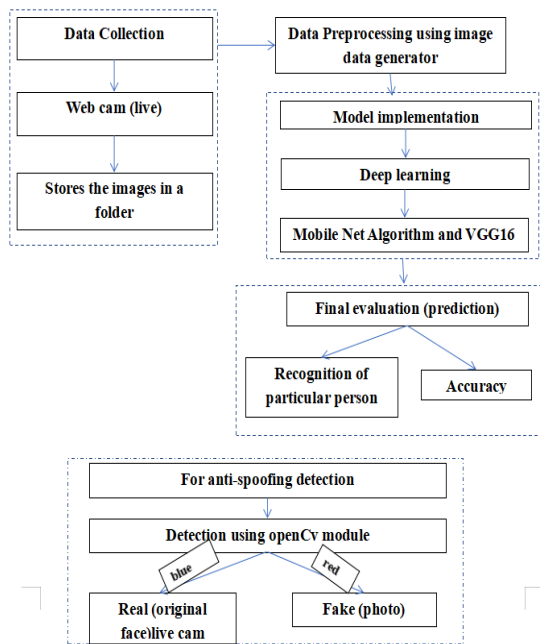


Figure 1. Methodology

### 1) Dataset Collection:

A diversified and comprehensive dataset including a wide range of facial photos is first gathered as the first step in the procedure. This dataset contains both real facial photos and different spoofing techniques, such as printed images, digital screens, and 3D masks. In order to verify that the model can effectively distinguish between authentic and fake photos, a number of spoofing scenarios must be included.

Images from a variety of repositories, including those that are open to the public, controlled settings, and real-world situations, may be included in the collection. To ensure that the data gathering procedure respects privacy and adheres to legal requirements, ethical issues are taken into account.

### 2) Data-preprocessing:

Data pre-processing is a crucial step in the machine learning pipeline that converts raw data into a format that is suitable for efficient model training. The performance and generalization of your deep learning models are greatly improved by data pre-processing, which is a key component of your research article on "People Identification Through Facial Recognition And Anti Spoofing Method Using Deep Learning."

#### 2.1. Image DataGenerator:

A tool used for real-time data augmentation during training is called ImageDataGenerator and is used in deep learning frameworks like Keras. In order to improve the model's capacity to generalize, it creates augmented pictures as the model is being trained. This exposes the model to a wide range of data variances. The training pictures are subjected to augmentations such as rotations, flips, shifts, and zooms in order to increase the dataset's diversity and aid the model's ability to learn robust features.

### 3) Model Architecture Selection:

In your research paper on "People Identification Through Facial Recognition And Anti Spoofing Method Using Deep Learning," choosing the right neural network architecture is essential to getting the best performance and accuracy. Data processing, feature extraction, and pattern learning are all governed by the architecture that is selected. The model architecture in your situation should be capable of handling facial recognition tasks and include real-time anti-spoofing techniques.

#### 3.1. Convolutional Neural Networks (CNNs):

Convolutional Neural Networks (CNNs) make sense as the foundation of your model because your goal

requires picture processing. CNNs are made to analyse data that is organized in a grid, like photographs, and they are particularly good at identifying hierarchical structures. They are made up of pooling layers that downsample the data and lower spatial dimensions, followed by convolutional layers that extract features from the input data by applying filters.

### 3.2. MobileNet:

MobileNet is made for embedded and mobile applications and is well-known for its effectiveness. While preserving excellent feature extraction skills, it uses depth-wise separable convolutions to simplify the computing process. If real-time processing on limited resource devices is what you're after, this architecture is very well suited.

### 3.3. VGG-16:

VGG-16, on the other hand, has a deeper and more intricate construction. Small 3x3 convolutional filters are used consistently across the network, giving it a uniform structure. VGG-16 has shown good performance on several picture classification tasks and excels in capturing complex features.

### 4) Model Evaluation:

Model evaluation evaluates how well a deep learning or machine learning model performs on new data. It entails measuring how effectively the model generalizes to new cases using a variety of metrics and methodologies. We are able to comprehend the model's strengths and weaknesses and make wise judgments regarding its deployment or potential enhancements thanks to model assessment, which provides us with insights into its accuracy, precision, recall, F1-score, and other pertinent indicators.

### 5) Comparative Analysis between VGG-16 and MobileNet:

A comparison investigation of the two well-known architectures VGG-16 and MobileNet was performed as part of the evaluation of our deep learning models for persons identification using face recognition and anti-spoofing. The impressive accuracy score of 0.989 that VGG-16 attained demonstrates its outstanding capacity to recognize people accurately and thwart spoofing efforts. This high level of precision highlights VGG-16's ability to capture complex face patterns and characteristics, allowing for accurate identification.

As opposed to VGG-16, MobileNet demonstrated a good accuracy score of 0.919, proving its capacity for persons identification and anti-spoofing, but with a little lower level of precision.

According to the comparison investigation, VGG-16 surpasses MobileNet in terms of accuracy. When deciding which option is best for a certain application setting, it's crucial to take into account other aspects including computing efficiency, model complexity, and real-time responsiveness. Although VGG-16 displays improved accuracy, its additional complexity may result in more computational work. Even while MobileNet's accuracy is a little bit lower, its lightweight architecture may be advantageous in situations where resource efficiency is important. The decision between VGG-16 and MobileNet ultimately comes down to carefully weighing the costs and benefits of accuracy vs computational demands, led by the application's unique needs and limits.

### 6) Real-Time Anti-Spoofing Integration:

A further degree of protection and resistance to spoofing efforts is provided by the real-time anti-spoofing technology included into our persons identification system. This ground-breaking



innovation improves the precision and dependability of our facial recognition method by studying and distinguishing between real and fake facial photos in real time.

### 6.1. Dynamic Boundary Box Color Indicators:

To visually communicate the outcome of the anti-spoofing analysis, the system employs dynamic boundary box color indicators. These indicators are superimposed around the detected face in the image.

#### 6.1.1. Blue Boundary Box:

When the deep learning model determines that the presented facial image corresponds to a genuine face, a blue boundary box surrounds the face. This blue indicator signifies the authenticity of the identification, instilling confidence that the individual is indeed who they claim to be.

#### 6.1.2. Red Boundary Box:

On the other hand, if the deep learning model recognizes traits indicative of spoofing, such as flatness, a lack of motion signals, or abnormal texture patterns, a red border box is shown around the face. This red signal acts as a quick warning sign of possible fraud or spoofing, requiring closer examination and providing protection against unauthorized access.

#### 6.1.3. Enhancing Security and Trustworthiness:

A proactive protection method against increasingly complex spoofing attempts is the real-time anti-spoofing integration. Individuals and system operators obtain immediate actionable information by graphically expressing the authenticity or probable fraud nature of provided face photos. This feature increases the reliability of face recognition

while also fostering a greater sense of security and confidence in the system.

The dynamic boundary box color indications are an essential part of our real-time anti-spoofing mechanism and enable our system to effectively differentiate between actual and fake face photos. With its unique integration, facial recognition technology has advanced significantly, enhancing security and guaranteeing the reliability of people identification procedures.

## IV. RESULTS AND DISCUSSIONS

Insightful findings that highlight the robustness and security advancements made in the field of persons identification using face recognition have been obtained through the evaluation of the deep learning models MobileNet and VGG-16 in conjunction with the real-time anti-spoofing mechanism.

The algorithms were put through rigorous testing on a dataset that was kept secret and had both real facial photos and various spoofing scenarios. The excellent capacity of VGG-16 to correctly identify people was demonstrated by its impressive accuracy score of 0.989. MobileNet showed remarkable competence in persons identification, albeit getting a slightly lower accuracy score of 0.919. The better accuracy of VGG-16 is highlighted by this comparison analysis, highlighting its potential as the main model for applications that prioritize precision.

Notable results were obtained through the incorporation of the real-time anti-spoofing system. To indicate the veracity of supplied face photographs during real-time assessments, the system dynamically added border box color markers. Genuine faces were always surrounded by a unique blue border box, confirming their authenticity. On the other hand, potential spoofing attempts resulted in the appearance of an alert red border box, warning consumers of possible fraudulent activity. With its

high level of sensitivity, the real-time anti-spoofing system was able to identify different spoofing efforts, including printed images and digital screen presentations. The mechanism's effectiveness in defending against hostile attacks is demonstrated by the speed and accuracy with which authentic and fake pictures can be distinguished.

The outcomes highlight how the suggested architecture may be used to improve the security and dependability of facial recognition systems. While MobileNet shown resource efficiency and outperformed VGG-16 in accuracy, this suggests that MobileNet is a good choice for situations where computing demands are a problem. The capacity of the real-time anti-spoofing system to dynamically evaluate and alert on picture authenticity is a significant breakthrough that reduces the hazards brought on by ever-more advanced spoofing tactics. From security access control to financial transactions, these results have ramifications for a wide range of businesses. The actual use of our suggested approach will also be heavily influenced by the ethical issues of data privacy, prejudice, and responsible deployment.

The combination of effective deep learning models and a real-time anti-spoofing mechanism offers a thorough strategy to strengthen face recognition for the identification of persons. In addition to advancing biometric security, the study's findings have the potential to increase public confidence in digital identity verification procedures.

## V. CONCLUSION

Our research article sought to make a substantial contribution to this paradigm change in the identity verification environment, which is now experiencing a disruptive development. We have provided a complete framework that not only improves face recognition accuracy but also fortifies the system against adversarial assaults. This

framework makes use of deep learning techniques and cutting-edge anti-spoofing technologies. We showed that two well-known architectures, VGG-16 and MobileNet, are effective at identifying persons through careful data collecting, pre-processing, and model training. MobileNet demonstrates efficiency, particularly in situations where resource limits are critical, while VGG-16 emerges as the leader in correct recognition with a phenomenal accuracy of 0.989.

A dynamic layer of security is added to the identifying process by the real-time anti-spoofing system, the pinnacle of our study. It represents a significant leap in defeating complex spoofing efforts since it can distinguish between actual and fake pictures in real time, as seen by the contrasting blue and red border box signs. Our discoveries have consequences that go beyond new technological developments. There are significant societal and moral implications to the combination of deep learning with anti-spoofing. It's crucial to strike a balance between security and privacy as we get closer to a digital future. For the advantages of our solution to be realized fairly and ethically, responsible deployment, openness, and constant improvement are necessary.

Our study is a testament to the power of convergent technologies to transform the field of secure people identification. We contribute to a future where face recognition is not simply a technology but a guarantee of trust and integrity in an increasingly linked world by improving accuracy, strengthening against spoofing, and promoting ethical concerns.

## VI. REFERENCES

- [1]. Lin, H. Y. S., & Su, Y. W. (2019, November). Convolutional neural networks for face anti-spoofing and liveness detection. In 2019 6th



- International Conference on Systems and Informatics (ICSAI) (pp. 1233-1237). IEEE.
- [2]. Sajjad, M., Khan, S., Hussain, T., Muhammad, K., Sangaiah, A. K., Castiglione, A., ... & Baik, S. W. (2019). CNN-based anti-spoofing two-tier multi-factor authentication system. *Pattern Recognition Letters*, 126, 123-131.
- [3]. Anthony, P., Ay, B., & Aydin, G. (2021, August). A review of face anti-spoofing methods for face recognition systems. In *2021 International Conference on INnovations in Intelligent SysTems and Applications (INISTA)* (pp. 1-9). IEEE.
- [4]. Bezas, K., & Filippidou, F. (2023). Anti-spoofing methods in face recognition. *Indonesian Journal of Computer Science*, 12(3).
- [5]. Wang, D., Ma, G., & Liu, X. (2022). An intelligent recognition framework of access control system with anti-spoofing function. *Aims Mathematics*, 7(6), 10495-10512.
- [6]. Abdelouahed, S. M., Assia, E., & Abdellah, A. (2023, May). A Comparative Study of Anti-Spoofing Detection Based on Deep Learning. In *2023 3rd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)* (pp. 1-6). IEEE.
- [7]. Das, P. K., Hu, B., Liu, C., Cui, K., Ranjan, P., & Xiong, G. (2019, November). A new approach for face anti-spoofing using handcrafted and deep network features. In *2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)* (pp. 33-38). IEEE.
- [8]. 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), 865-889
- [9]. 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), 139.
- [10]. Toprak, I., & Toygar, Ö. (2021). Detection of spoofing attacks for ear biometrics through image quality assessment and deep learning. *Expert Systems with Applications*, 172, 114600.
- [11]. Tu, X., Ma, Z., Zhao, J., Du, G., Xie, M., & Feng, J. (2020). Learning generalizable and identity-discriminative representations for face anti-spoofing. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 11(5), 1-19.
- [12]. Jing, B. Z., Chan, P. P., Ng, W. W., & Yeung, D. S. (2010, July). Anti-spoofing system for RFID access control combining with face recognition. In *2010 International Conference on Machine Learning and Cybernetics (Vol. 2, pp. 698-703)*. IEEE.
- [13]. Fegade, V., Chodankar, A., Bhingle, A., & Mhatre, S. (2022, April). Residential security system based on facial recognition. In *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 01-09). IEEE.
- [14]. Li, H., Li, W., Cao, H., Wang, S., Huang, F., & Kot, A. C. (2018). Unsupervised domain adaptation for face anti-spoofing. *IEEE Transactions on Information Forensics and Security*, 13(7), 1794-1809.
- [15]. Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric antispoofing methods: A survey in face recognition. *IEEE Access*, 2, 1530-1552.
- [16]. Hosen, M. A., Moz, S. H., Khalid, M. M. H., Kabir, S. S., & Galib, S. M. (2023). Face recognition-based attendance system with anti-spoofing, system alert, and email automation. *Radioelectronic and Computer Systems*, (2), 119-128.
- [17]. Xu, Y., Wu, L., Jian, M., Zheng, W. S., Ma, Y., & Wang, Z. (2021). Identity-constrained noise modeling with metric learning for face anti-spoofing. *Neurocomputing*, 434, 149-164.

- [18]. Pei, M., Yan, B., Hao, H., & Zhao, M. (2023). Person-specific face spoofing detection based on a siamese network. *Pattern Recognition*, 135, 109148.
- [19]. Hadiprakoso, R. B., & Setiawan, H. (2020, November). Face anti-spoofing using CNN classifier & face liveness detection. In *2020 3rd International Conference on Information and Communications Technology (ICOIACT)* (pp. 143-147). IEEE.

**Cite this article as :**

Fathima Jameera. B, G. Suresh, S. Hemalatha, S. Vilma Veronica, "People Identification Through Facial Recognition and Anti-Spoofing Using Deep Learning", *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET)*, Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 5, pp. 253-262, September-October 2023. Available at doi : <https://doi.org/10.32628/IJSRSET2310539>  
Journal URL : <https://ijsrset.com/IJSRSET2310539>