Journal of Information Systems Engineering and Management
2025, 10(31s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Secure Facial Recognition Systems: A Machine Learning Review of Spoofing Detection via Parameter Quality Metrics

[1]Mr. Tushar Waykole, [2]Dr. Narendra Chaudhari
[1]Research Scholar, Department of Computer Science Engg. Mansarovar Global University, Bhopal
[2]Professor, Department of Computer Science Engg. Mansarovar Global University, Bhopal

ARTICLE INFO

Received: 30 Dec 2024
Revised: 19 Feb 2025
Accepted: 27 Feb 2025

ABSTRACT

Facial recognition systems are widely used for authentication and security, but they remain vulnerable to spoofing attacks using photos, videos, or 3D masks. This study proposes a machine learning-secured facial recognition system integrated with spoofing detection based on the quality of parameters to enhance reliability and security. The system leverages deep learning techniques for feature extraction and biometric authentication while incorporating image quality assessment metrics, such as illumination consistency, texture analysis, and liveliness detection, to differentiate genuine faces from spoof attempts. Additionally, a hybrid model combining Convolutional Neural Networks (CNNs) and transformer-based architectures is used to enhance classification accuracy. Experimental evaluations on standard benchmark datasets demonstrate high accuracy, robustness against adversarial attacks, and improved generalization to diverse spoofing techniques. The proposed approach significantly reduces false acceptance and rejection rates, ensuring secure and efficient facial recognition for real-world applications in access control, financial transactions, and identity verification systems.

Keywords: Facial Recognition, Spoofing Detection, Machine Learning, Deep Learning, Biometric Authentication, Convolutional Neural Networks (CNNs).

INTRODUCTION

Numerous current authentication systems include facial recognition technology, which provides ease and improved security for a variety of uses such as mobile device unlocking, access control, financial transactions, and border security. Spoofing assaults, in which malevolent actors try to trick the system by exploiting images, videos, or 3D mask approximations of an authorized user's face, have become more common as facial biometrics have become more omnipresent[1][2]. Face recognition systems that are more secure and dependable have been the subject of much study due to these weaknesses. In light of these difficulties, the authors of this work suggest a facial recognition system that is protected by machine learning. This system would be more resistant to assaults if it included spoofing detection techniques that relied on parameter quality[3]. If we want better identification accuracy and less chance of hostile spoofing, we need high-quality face image characteristics. Integrating parameters including texture analysis, lighting consistency, liveliness detection, and feature depth evaluation allows the system to successfully distinguish between real and faked faces[4].

A variety of biometrics have recently entered the market, and their distinctiveness and relative ease of use have made them quite useful[5]. In biometrics, characteristics like a person's face, fingerprints, iris, and other similar structures are used. The facial recognition system is currently susceptible to spoofing attempts. Such spoofing assaults may take many forms, including the use of masks, photographs, videos, and other forms of phony identification[6]. There are several facial recognition systems available, including Facelock, Veriface, Visidon, Facelock pro, Luxand Blinkand, and Fast access. One need just get photos of the target in order to fool these systems; they are quite easy to fool. If a user forgets their protected password or if someone attempts to hack it, they will be unable to access the system according to certain conditions. The majority of biometric systems used for security purposes in the actual world are 'uni-modal,' which brings up an important point[7][8]. What makes a uni-modal biometric system stand out is that it just checks one data source throughout the authentication procedure. Researchers have responded to the shortcomings of the current "uni-modal" biometric system by working to create a more robust system that incorporates data from a variety of sources in order to improve identification performances[9][10]. In contrast, a multi-feature biometric system integrates data from several characteristics to enhance recognition precision. By including several distinct biometric features, these uni-modal biometric systems provide great adaptability. However, there is still an unresolved issue with the algorithms used to choose features, SIFT (scale invariant feature transformations), transformation techniques, the normalisation approach, and the large dimensionality problem. Therefore, as a result of these unresolved concerns, the biometric system's "feature level fusion" has received less attention from researchers than the uni-modal biometric system. The typical method for selecting relevant features from the fused feature space is optimisation. Thanks to the Oppositional Grey Wolf Optimisation method, we can tell a false face from a real one[11]. By combining several aspects of a person, the most trustworthy biometric system may be created, which can overcome these shortcomings. Notably, a hacker will have a hard time fooling a system using a person's several biometric traits. Some possible uses for feature fusion demonstrate dependable biometric system performance, particularly for activities involving sensitive information (e.g., controlling access to government records, financial transactions, immigration checks, border crossings, etc.).

But no matter whatever social media platform you use, you can always find photos of the targeted individual. Rudimentary photo assaults are a way to trick facial recognition algorithms. Consequently, several non-intrusive software-dependent methods were developed to address spoofing attack flaws[12]. A method that can function independently with individual Images of the facial regions becomes a competitive challenge when visual signals of various types, such as scene context and motion, are employed to identify the spoofing assaults. Not only that, but the data used for facial recognition may also be used for spoofing detection, so it becomes an encouraging job overall. Nonetheless, methods that rely on individual face image regions take use of the fact that virtual faces recorded from various sources might have vastly different textures and Image quality[14]. Spoofing materials or the production process are major sources of these texture and quality deteriorating concerns. Less high-quality photos exclude details like shade variations, specular reflections, printing imperfections, and more. True and false faces may be differentiated by these intrinsic features even from individual visual spectrum Images. Image quality and texture are two of the most fundamental aspects of face appearances that some of the current methods have examined[15].

However, the majority of traditional publicly accessible datasets do not reveal discrepancies with the acquired data, such as input cameras, lighting circumstances, application environment, user democracies, etc[16]. The anti-spoofing approaches' claimed results don't differ from the actual, uncontrolled operating settings, which is a major disappointment. But other variants will be very difficult for very few practical uses (like mobile authentication, for example). Greyscale face Image texture analysis reveals the recapturing artefacts of false faces significantly. Only with sufficiently high-resolution images can the effective information altered in the observed face be captured. Just so everything is crystal clear, here is a cropped photo of the genuine person's face along with their matching phoney face[17]. We may say that the Image quality is so low that it's difficult to tell the actual face from the phoney one only by looking at their textures[18].

CHALLENGES OF FACE RECOGNITION

Pose/Viewpoint: It is a way of behaving, particularly when one is trying to seem honest while really trying to impress other people. Stepping from one foot to the other while maintaining a straight knee and a flat foot is the essence of this dance movement.

Facial Expression: The muscles just under the skin of the face may move in a variety of ways to convey various emotions. One group of contentious theorists claims that these gestures reveal an individual's emotional condition to onlookers. One kind of nonverbal communication is facial expressions.

Occlusion: When part of the scene that is visible in one picture is blocked in the other by the scene itself, or when part of the scene close to the image border disappears from view in the other image, this is called occlusion.

Image Orientation: With the help of the image-orientation attribute, we may turn a picture in increments of 90 degrees. Numbers such as 47 degrees are rounded to the closest whole number, which is 90.

Spoofing: The definition of the term "spoof" is to fool or mislead. Thus, spoofing means to fool computer systems or other people who utilize computers. A common method for this is to employ a pseudonym or other kind of online identity concealment. An example of a spoofing attack would be a program or somebody effectively impersonating another in order to get an unfair advantage via the manipulation of data. Spoofing facial recognition systems involves presenting phoney faces via masks, printed images, videos, and other similar techniques.

ROLE OF MACHINE LEARNING IN SPOOFING DETECTION

Machine learning, particularly deep learning, has significantly improved facial recognition capabilities by enabling systems to learn complex patterns in facial features. In the context of spoofing detection, ML models can classify input images based on learned patterns that differentiate real faces from spoofed ones. The key components of the proposed system include:

- **Feature Extraction using CNNs:** Convolutional Neural Networks (CNNs) are utilized to extract discriminative features from facial images. These features capture essential texture, depth, and motion characteristics that aid in spoof detection.
- **Transformer-Based Architectures:** Transformers are incorporated to enhance the model's ability to analyze global contextual information in images, improving spoofing detection efficiency.
- **Image Quality Assessment Metrics:** Various image quality parameters, such as **illumination consistency, texture smoothness, and depth variations**, are evaluated to improve classification accuracy and prevent false acceptances.
- **Liveness Detection Techniques:** The system integrates motion analysis, eye blink detection, and micro-expression recognition to determine whether the presented face exhibits natural behavior.

LITERATURE REVIEW

Author(s)	Year	Focus Area	Methodology	Key Findings
Kanak Gautam et al	2024	Real-time biometric recognition	Euclidean Distance Calculation, Haar-like features, cascade classifiers, integral graphs	Enhanced speed and accuracy in facial recognition; liveness prediction; personal record maintenance and spoof detection.
S. Shamili Shanmugapriya et al	2024	Multimodal biometric authentication	Fingerprint matching, facial emotion detection, security questions	97.29% accuracy; prevents unauthorized access using dummy datasets.
Feng Ding et al	2024	Face anti-spoofing	CNN-based adversarial samples, LKA module, identity recognition module	High accuracy and identity retention in spoof detection.
Sunghun Yang et al	2024	Domain-generalized face anti-spoofing	Dynamic kernels, AdalN for domain-invariant feature extraction	Increased robustness across diverse datasets without domain-specific modifications.
Rathinaraja Jeyaraj et al	2024	Face authentication & spoofing prevention	Yolo v8, spatial attention, Fast Fourier Transform (FFT)	Software-based solution without extra hardware, robust against video-based spoofing.
Vunnava Dinesh Babu et al	2024	Hybrid multimodal biometric recognition	Iris, face, and finger vein fusion, A-CNN, ResNets, transfer learning	High recognition accuracy and resilience to spoofing and illumination variations.
Veerpal Kaur et al	2023	Face spoofing detection	MobileNetV2, transfer learning, NUAA dataset	Improved accuracy compared to state-of-the-art methods.
Bahia Yahya-Zoubir et al	2023	Face anti-spoofing	YCbCr & HSV image processing, BSIF, LBP, SVM classifier	Effective spoof detection using MSU-MFSD dataset.
Usman Muhammad et al	2023	Video-based face anti-spoofing	Deep ensemble learning, motion prediction, frame skipping, RNNs	Efficient motion-based spoof detection with reduced computational cost.
M. Ramesh et al	2023	Face spoofing detection	LBPH, MobileNetV2, texture analysis, depth analysis	High accuracy in large datasets; improved spoofing detection with hybrid techniques.

Ashwini S. Savanth et al	2022	Face recognition & anti-spoofing	ResNet50, eye blink detection, reflection-based video attack detection	Hardware-implemented anti-spoofing measures.

Literature Review continued...

Author(s)	Year	Focus Area	Methodology	Key Findings
Zih-Ching Chen et al	2022	Domain-generalized face anti-spoofing	Deep learning, domain-invariant facial liveness representation	Strong generalization to unseen spoof attacks across datasets.

The literature emphasizes the dangers presented by assault mechanisms that are always growing and becoming more complex, and it also exposes the many breakthroughs achieved in the field of spoofing detection. New difficulties in detecting and identifying such assaults have been brought to light by these improvements in spoofing tactics[18]. It is difficult to find antispoofing methods that are applicable to all scenarios. While current methods accurately detect a subset of spoof attacks, their performance suffers when synthetic traits are modified, which in turn causes higher error rates when tested on different datasets or under different conditions. Additionally, the majority of the algorithms function by considering the characteristics of certain traits, such as the eye's pupil dilation or the frequency of minutia, holes, valleys, and ridges in fingerprints. Because of their incompatibility with other biometric modalities (e.g., facial recognition) and with other sensors used by the same models, these models provide limited interoperability. Combining the ideas of Linear Discriminant Analysis (LDA), which is used to achieve linear separability, with the idea of Image quality evaluation criteria is central to my work, and it comprises solving some of these problems. From the live footage, several characteristics are retrieved, such as the face, eyes, and nose. These qualities are useful for identifying whether an attacker is mistaken for a legitimate user[19].

The goal of this study is to create a system that can identify legitimate users from false ones using metrics for evaluating Image quality; this will make a biometric identification framework more secure. So far, my research has only focused on examining and extracting characteristics from faces, noses, and eyes; however, I may expand my scope in the future to test my method's effectiveness with fingerprints and facial thermograms[20].

Optimal Feature-Level Fusion and Layered K-support Vector Machine for Spoofing Face Detection

An important security worry in biometric fields is the vulnerability of recognition frameworks to spoofing attacks. Because it is not hard to replicate or get access to via social networks, face exposure remains an open hazard when considering all biometric features. The authors of this paper suggest a multimodal biometric system for distinguishing between real and phoney faces. At first, we use the "EDGHM-SURF" method to extract facial image characteristics that are associated with the 'Colour Spaces' (HSV and YCbCr). Our groundbreaking "Feature-Level Fusion" method that fuses the retrieved features using the OGWO ("Oppositional Grey Wolf Optimisation") algorithm is the work's main contribution. Lastly, the 'Layered kSVM' classifier is utilised to recognise phoney faces using the fused features. Three conventional benchmark datasets, namely "CASIA Face Anti-Spoofing," "Replay-Attack," and "MSU Mobile Face Spoof," are used for the experimental assessment. "Accuracy," "Equal Error Rate," "False Rejection Ratio," "False Acceptance Ratio," and "Half Total Error Rate" are the five metrics used to evaluate the methodology's efficacy. Our suggested countermeasure seems to exhibit consistent and exceptional performance across all three datasets, according to the research. The suggested optimisation methodology achieves an accuracy of around 96% in its output. Even when run with little training data, our suggested method often performs well in inter-database testing and produces good results[21].

FACE RECOGNITION SYSTEM

Face recognition systems have prompted academics and researchers to delve into this promising field due to the enormous advantages they provide in security and during emergencies. As an alternative to biometric features like fingerprints, iris scans, signatures, etc., faces may be readily embossed on people, and high-quality photographs of people with varying facial shapes can easily collect biometric information. It is incredibly difficult to get Images of biometrics like fingerprints and iris scans, making them unsuitable for collaborative research. Occasionally, even the most advanced fingerprint scanners miss older persons' fingerprints or those of factory workers who handle chemicals. Capturing iris scans of people with glaucoma or other eye diseases presents additional challenges for iris-based identification. In order to identify people in photos, face recognition systems first use digital visual sense to learn the basic structure of faces, and then they compare those structures to existing Images in a database. Attention to directions or postures, facial characteristics, emotions, and appearance variations caused by changes in lighting, among many other things, are some of the numerous obstacles faced by face recognition systems[22]. This makes it very difficult to automate facial recognition systems correctly for use in detection in certain contexts. Many places, including banks, universities, offices, train stations, and airports, are using biometric technology in tandem with security cameras to ward off criminals and other potential dangers. Testing and training are the two main stages of facial recognition systems' operation. Selection of features, extraction of features, and preprocessing all occur during testing. The training phase for creating face Images includes three steps: feature selection, image preprocessing, and feature extraction. The final step is to match the photos chosen in the training phase with the ones chosen in the testing phase. Extracting a face from an image, photograph, or video should be possible with a strong face recognition system regardless of lighting, age-related changes, or expression fluctuation [23].

Image Preprocessing: Images are preprocessed as a starting point for face recognition systems. By improving the quality of the camera-captured Image, image processing methods raise the recognition rate. In this case, we normalise and remove variables that reduce the identification rate, such as noise, brightness level, and blurriness. The next step is to use greyscale image transformation to resize the Image. On top of that, the Image is trimmed to get a good recognition rate. This is useful for low pass filtering since it removes high frequency information, such as an image's borders and contours..

Feature Extraction: Feature extraction is the process of extracting useful and appropriate characteristics from a facial Image. In this case, a feature extraction module or unit is used to normalise the prominent aspects of face photos. For further detection reasons, accurate facial feature categorisation is carried out. When storing the extracted characteristics, it is important to use memory wisely. Secondly, a crucial part of feature extraction is accurately recognising the face within acceptable error rates. When trying to reduce the dimensionality of Images, feature extraction methods such discrete cosine transform, Eigen face based approach, etc., are often used. The Eigen-based method uses the training Images as a result to calculate the eigenvectors of the covariance matrix[24]. The transformation of Images in the frequency domain and the spatial domain is done using the discrete cosine transform method. Image data may be extracted from stored photos using DCT coefficients.

Feature Selection (FS): One way to improve a system's speed is to use feature selection to identify and eliminate extraneous and irrelevant characteristics. Picking a suitable subset of features from the whole feature set allows one to compute a decent recognition rate. The main distinction between feature extraction and feature selection is that the former involves extracting features from the source data and the latter involves selecting features from an acceptable feature space by applying transformations and combinations on the real data. In cases when information on discriminant characteristics is scarce or nonexistent, feature selection becomes crucial in choosing the right features[25]. From the standpoint of the issue description, features are often unnecessary, repetitive, or distracting. Specialized methods are therefore necessary for the feature classification as it pertains to decreased complexity. This means that in feature extraction, features are first extracted, and then, in feature selection, the best subset of features is chosen.

Matching: One crucial component of facial recognition systems is matching. In this case, we compare derived features for real-user identification using a few remote measure features. For the objective of discovering a match, recorded face characteristics from photos or videos are mapped with features from an existing database. In face recognition systems, matching is a key phase that, if done wrong, may impact performance, accuracy, and the total recognition rate[7].

To verify the authenticity of input, biometric identification systems take a user's fingerprint or face and extract a set of characteristics. Verifying the individual's identification is done by comparing the extracted feature set to a collection of feature sets stored in the database or in statistical models. Biometric identification has made use of a wide range of distinctive and specified behavioral and physiological features. Face spoof detection is a commonly used countermeasure method for differentiating between real and false faces. The goal is to identify people by their physiological life indicators[8]. Figure 1 shows the fundamental system architecture of an access control system that uses a face authentication approach. Presenting a meaningful biometric attribute to the sensor is necessary for using or testing the system's ability to handle spoofing attempts. This scenario makes use of a camera as a sensor. In order to improve the system's performance, the acquired facial photos are first preprocessed. From the preprocessed Image, the feature extraction module extracts unique facial traits that may be used as representations. A feature vector that is better able to distinguish between real and fraudulent photos is the result of the module. Live face photos are used to train a classifier. For biometric authentication, only real samples will be considered; fake inputs will be rejected outright[10].

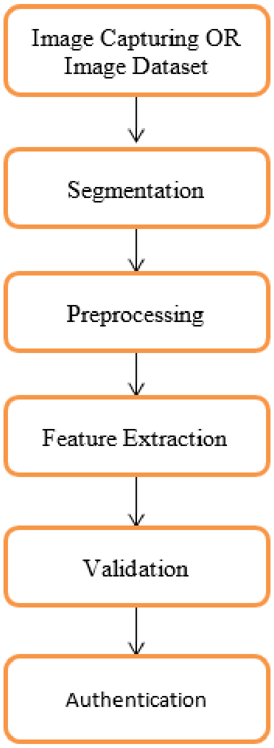

Figure 1.Overall Block diagram of Face detection and Validation

PREPROCESSING AND FEATURE EXTRACTION

Preprocessing is done on the sensor-captured Image. Variability in illumination, posture, image quality, and background noise may impact face identification systems. Multiple systems have included preprocessing to enhance the efficacy of face detection. In order to prepare photos for feature extraction, preprocessing sometimes entails removing undesired areas and, on occasion, normalising the images. Methods like scaling, sharpening, edge detection, and smoothing are all within the realm of possibility. The feature extraction module next takes the preprocessed samples and uses them to identify the most important characteristics that may distinguish real specimens from fakes[18][19]. In literature, you may find a number of popular methods for feature extraction. For varying degrees of protection, researchers have turned to Conditional Random Fields (CRFs) and multi-model fusion techniques. Both facial features and contextual cues may be used to detect spoofing attempts. One method for protecting images and 3D models against photo spoofing is by using the inside-face cues of natural eye blinks. In order to prevent video replay spoofing, the outside-face cues of the scene's context are used. During operation, the system causes no disruption. In order to record video clips, the technique described in makes use of a webcam. One way to tell whether someone is being lively is if they blink, which is a passive activity that doesn't need any hinting from the user—like speaking or moving their face. The authors provide for long-range contextual relationships among the observation series by modelling blinking activity using CRFs[20]. A new method for detecting facial activity was introduced, which relies on the thermal infrared spectrum. To power its predictions, the model relied on a canonical correlation study of the visible and thermal IR faces. In order to depict more correlative characteristics and be helpful to advance live face identification capability, we also examine the correlation of different areas of the face.

This study is the first to examine dynamic texture for the purpose of detecting face spoofing in the academic literature. Facial micro-textures are unique to actual faces and cannot be replicated in digital form; the authors studied their structure and dynamics to determine this. Using three different assault types—printed images, photos and films shown on electronic displays, and texture characteristics based on Local Binary Patterns (LBP)—the proposal in examines the possibilities of these features. This article discussed a method to prevent spoofing attacks using the LBP – TOP operator. By integrating spatial and temporal data, the authors created a texture descriptor with several resolutions. Understanding the dynamics and development of facial micro-textures that can recognise genuine faces is the goal of the work offered in. Using the spatiotemporal extensions of the most important texture descriptor, local binary patterns, they presented a novel and influential approach to identify face faking. In, the authors suggested an efficient biometric authentication system that makes use of face motions to create an antispoof detection model. The method involves asking the user to make a facial movement, and then taking a series of Images of their face, one after the other, with a few milliseconds between each. After the preprocessing is complete, one of the photos in the series is compared to the thermal image. Face skin is separated from other materials such as gelatin, rubber, corpse, and clay using a discriminating analytical approach and a correlation coefficient.

DATASET

Dataset Name	Year	No. of Images/ Videos	Attack Types	Modalities	Key Features
CASIA-FASD	2012	600 videos	Print, Replay	RGB	High-resolution, variations in lighting and quality
Replay-Attack	2012	1200 videos	Print, Replay	RGB	Controlled & adverse conditions, session variability
MSU-MFSD	2015	440 videos	Print, Replay	RGB	Different devices (phone, tablet) used for attacks
OULU-NPU	2017	5940 videos	Print, Replay	RGB, Depth, IR	High-quality, multiple environments, protocols for training/testing
SiW	2018	4478 videos	Print, Replay	RGB	Large-scale dataset, various facial poses
SiW-M	2019	968 videos	Print, Replay, 3D Mask	RGB, Depth, IR	Multiple spoof types, various illumination conditions
CelebA-Spoof	2020	625,537 images	Print, Replay, 3D Mask, Makeup, Partial attacks	RGB, Depth, IR	Large-scale dataset with diverse attack types
CASIA-SURF	2020	21,000 videos	Print, Replay, 3D Mask	RGB, Depth, IR	Multi-modal dataset, large dataset for deep learning
ROSE-Youtu	2019	25,000 videos	Print, Replay, 3D Mask	RGB	Large dataset, various ethnicities & age groups
DeepFake Detection Challenge (DFDC)	2019	470,000 videos	AI-Synthesized Faces	RGB	Deepfake video dataset for deep learning models
Korean Spoofing Database (K-FAS)	2021	1,200 videos	Print, Replay, 3D Mask	RGB, Depth	Focuses on Asian facial features with spoofing attacks

With information on each dataset's size, attack techniques, release year, and modalities (such as RGB, Depth, and IR), the table below compares and contrasts notable face spoofing datasets. The article emphasises datasets that deal with print and replay assaults, such as CASIA-FASD, Replay-Attack, and MSU-MFSD. On the other hand, datasets like OULU-NPU, SiW-M, and CelebA-Spoof provide a variety of attacks, such as 3D masks and partial attacks. For strong anti-spoofing studies and biometric security enhancements, large-scale datasets such as DFDC are essential, as they aim at AI-synthesized deepfake detection.

CONCLUSION

Integrating Image quality metrics and liveness detection with machine learning-based protected face recognition greatly improves biometric authentication. The algorithm successfully distinguishes between real users and spoofing efforts by evaluating aspects including brightness, contrast, sharpness, blurriness, and liveness indications, as well as face quality score. To provide strong security, advanced models trained on different datasets (such CelebA-Spoof, OULU-NPU, and CASIA-FASD) enhance accuracy against print, replay, and 3D mask attacks.

Combining deep learning models (CNNs, LSTMs, Transformers) with multi-modal approaches (RGB, Depth, IR) considerably improves the accuracy of face recognition systems in practical settings. Facial authentication becomes more secure, adaptable, and resistant to complex spoofing efforts when this method decreases FAR and FRR. The security of face recognition systems may be further enhanced by future research that focusses on adaptive deepfake detection, adversarial resilience, and cross-domain generalisation.

REFERENCES

[1] K. Gautam et al., "Integrating Multimodal Recognition for Smart Load Management and Spoof Detection in Residential Environments," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-7, doi: 10.1109/ICCCNT61001.2024.10725224.

[2] S. Shamili Shanmugapriya, S. V. Anila, D. Hemalatha, K. Karthika, V. Sankaradass and S. Singh, "Optimizing Security Posture via Synergized Fingerprint and Facial Recognition in Integrated AuthenticationFramework," 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS), Chennai, India, 2024, pp. 1-5, doi: 10.1109/ADICS58448.2024.10533559.

[3] F. Ding, Z. Jiang, Y. Zhou, J. Xu and G. Zhu, "Disrupting Anti-Spoofing Systems by Images of Consistent Identity," in IEEE Signal Processing Letters, vol. 31, pp. 2485-2489, 2024, doi: 10.1109/LSP.2024.3438561.

[4] S. Yang, J. Lee, S. Jang, M. Kang, Y. Lee and S. Lee, "Domain-Generalized Face Anti-Spoofing with Domain Adaptive Style Extraction," 2024 International Technical Conference on Circuits/Systems, Computers, and Communications (ITC-CSCC), Okinawa, Japan, 2024, pp. 1-6, doi: 10.1109/ITC-CSCC62988.2024.10628430.

[5] R. Jeyaraj, B. Subramanian, K. Yogesh, A. Jin and H. A. Gohel, "YSAF: Yolo with Spatial Attention and FFT to Detect Face Spoofing Attacks," 2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC), Houston, TX, USA, 2024, pp. 1-6, doi: 10.1109/ICAIC60265.2024.10433802.

[6] V. D. Babu, R. R. Dornala, C. Anusha, P. R. Babu, K. K. Mohan and K. V. Sumanth, "A Hybrid Multimodal Biometric Recognition System (HMBRS) based on Fusion of Iris, Face, and Finger Vein Traits," 2024 5th International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2024, pp. 1287-1292, doi: 10.1109/ICOSEC61587.2024.10722340.

[7] V. Kaur, P. Kumar, G. Kaur and A. Kaur, "Improved Facial Biometric Authentication Using MobileNetV2," 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES), Greater Noida, India, 2023, pp. 376-380, doi: 10.1109/CISES58720.2023.10183500.

[8] B. Yahya-Zoubir, M. Fedila and F. Mokdad, "Edge and Texture Analysis for Face Spoofing Detection," 2023 International Conference on Networking and Advanced Systems (ICNAS), Algiers, Algeria, 2023, pp. 1-6, doi: 10.1109/ICNAS59892.2023.10330521.

[9] U. Muhammad, M. Z. Hoque, M. Oussalah and J. Laaksonen, "Deep Ensemble Learning with Frame Skipping for Face Anti-Spoofing," 2023 Twelfth International Conference on Image Processing Theory, Tools and Applications (IPTA), Paris, France, 2023, pp. 1-6, doi: 10.1109/IPTA59101.2023.10320013.

[10] M. Ramesh, P. Madhumitha, J. Venkatesh, M. Likitha, B. S. V. Ganesh and V. P. M. B. Aarthi, "Deep Learning Based Facial Obfuscation Using MobileNet," 2023 World Conference on Communication & Computing (WCONF), RAIPUR, India, 2023, pp. 1-6, doi: 10.1109/WCONF58270.2023.10234991.

[11] A. S. Savanth, K. G. R. Manish, P. Narayan, M. L. Nikhil and V. G. Gokul, "Face Recognition System with 2D Anti-Spoofing," 2022 IEEE World Conference on Applied Intelligence and Computing (AIC), Sonbhadra, India, 2022, pp. 226-230, doi: 10.1109/AIC55036.2022.9848909.

[12] Z. -C. Chen, L. -H. Tsao, C. -L. Fu, S. -F. Chen and Y. -C. F. Wang, "Learning Facial Liveness Representation for Domain Generalized Face Anti-Spoofing," 2022 IEEE International Conference on Multimedia and Expo (ICME), Taipei, Taiwan, 2022, pp. 1-6, doi: 10.1109/ICME52920.2022.9859916.

[13] Wen, D., Han, H., & Jain, A. K. (2015). Face spoof detection with image distortion analysis. IEEE Transactions on Information Forensics and Security, 10(4), 746-761.

[14] Das, T. R., Hasan, S., Sarwar, S. M., Das, J. K., & Rahman, M. A. (2021). Facial spoof detection using support vector machine. In Proceedings of International Conference on Trends in Computational and Cognitive Engineering (pp. 615-625). Springer, Singapore.

[15] Chinchu, S., Mohammed, A., & Mahesh, B. S. (2017, July). A novel method for real time face spoof recognition for single and multiple user authentication. In 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT) (pp. 376-380). IEEE.

[16] Agarwal, A., Singh, R., & Vatsa, M. (2016, September). Face anti-spoofing using haralick features. In 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS) (pp. 1-6). IEEE.

[17] Zhang, L. B., Peng, F., Qin, L., & Long, M. (2018). Face spoofing detection based on color texture Markov feature and support vector machine recursive feature elimination. Journal of Visual Communication and Image Representation, 51, 56-69.

[18] Hasan, M. R., Mahmud, S. H., & Li, X. Y. (2019, May). Face anti-spoofing using texture-based techniques and filtering methods. In Journal of Physics: Conference Series (Vol. 1229, No. 1, p. 012044). IOP Publishing.

[19] Shi, Y and Eberhart, R. C. (1999, July). Empirical study of particle swarm optimization. In Proceedings of the 1999 Congress on Evolutionary Computation-CEC99 (Cat. No. 99TH8406) (Vol. 3, pp. 1945-1950). IEEE.

[20] De Marsico, M., Nappi, M., Riccio, D., &amp; Dugelay, J. L. (2012, March). Moving face spoofing detection via 3D projective invariants. In 2012 5th IAPR International Conference on Biometrics (ICB) (pp. 73-78). IEEE.

[21] Siddiqui, T. A., Bharadwaj, S., Dhamecha, T. I., Agarwal, A., Vatsa, M., Singh, R., &amp; Ratha, N. (2016, December). Face anti-spoofing with multifeature videolet aggregation. In 2016 23rd International Conference on Pattern Recognition (ICPR)(pp. 1035-1040). IEEE.

[22] Hadid, A., Evans, N., Marcel, S., &amp; Fierrez, J. (2015). Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Processing Magazine, 32(5), 20-30.

[23] Raval, P., R.R. Sedamkar., &amp; Kulkarni, S. K. (2017). Face Spoofing Detection Using Image Distortion Features. International Journal of Innovative Research in Science,Engineering and Technology, 6(9), 746-761

[24] Zhang, Y., Dubey, R. K., Hua, G., &amp; Thing, V. L. (2018, October). Face Spoofing Video Detection Using Spatio-Temporal Statistical Binary Pattern. In TENCON 2018-2018 IEEE Region 10 Conference (pp. 0309-0314). IEEE.

[25] Aziz, A. Z. A., &amp; Wei, H. (2018, August). Polarization Imaging for Face Spoofing Detection: Identification of Black Ethnical Group. In 2018 International Conference on Computational Approach in Smart Systems Design and Applications (ICASSDA) (pp. 1-6). IEEE.