FACE RECOGNITION-BASED ATTENDANCE SYSTEMS USING ANTI-SPOOFING METHODS

Abstract

Face recognition has emerged as a popular biometric technology for automated attendance marking systems in recent years. However, these systems are susceptible to presentation attacks using fake faces. This article offers a comprehensive analysis of the scholarly works related to attendance systems utilizing face recognition, as well as the methods employed to counteract spoofing attacks in such systems. The study methodology follows a structured approach to identify relevant papers from databases based on defined criteria. Key findings indicate that deep learning has enhanced face recognition accuracy tremendously but presentation attacks remain a challenge. Different anti-spoofing techniques have been investigated including liveness detection, reflectance analysis, convolutional neural networks, adversarial learning etc. However, generalized solutions across diverse spoof types and real-world conditions remain elusive. The review also analyses research gaps and future directions in areas like multimodal fusion, explainable AI, collaborative learning, online adaptation etc. Overall, this review provides useful insights into the capabilities and limitations of existing literature which can guide future research on secure face recognition systems for attendance marking.

Keywords: Face recognition, automated attendance systems, biometrics, anti-spoofing, presentation attacks, poofing mediums, countermeasures, liveness detection, texture analysis, reflectance analysis, deep learning models, adversarial learning, multimodal systems, performance evaluation, research challenges, dataset limitations, unseenattacks, directions, online learning, explainable AI, federated learning.

Authors

Sudha V
Assistant Professor
Department of AI & DS
Karpaga Vinayaga College of Engineering and Technology
Tamil Nadu, India.

Sangeetha S
Assistant Professor
Department of Computer Science and Engineering
Karpaga Vinayaga College of Engineering and Technology
Tamil Nadu ,India.

Ganesh Shankar S
Assistant Professor
Department of AI & DS
Karpaga Vinayaga College of Engineering and Technology
Tamil Nadu,India.

Arun A
Assistant Professor
Department of Computer Science and Engineering
Karpaga Vinayaga College of Engineering and Technology, Tamil Nadu, India.

Durga Ram R
Student
Department of AI & DS
KarpagaVinayaga College of Engineering and Technology
Tamil Nadu, India.

I. INTRODUCTION

Attendance monitoring is an integral administrative activity in academic institutions and workplace organizations. Traditionally attendances records have been maintained manually using paper registers or sheets. The instructor calls out names and marks presence or absence accordingly. However, manual attendance marking suffers from several limitations:

- Time consuming process, especially for large classes. Takes at least 5-10 minutes.
- Monotonous and error prone. Possibility of marking mistakes.
- Difficult to track and analyse attendance patterns over long term.
- Susceptible to buddy punching or proxy attendance by fraudsters.

Educational institutions and businesses are increasingly looking towards automation and biometrics to overcome inefficiencies of manual attendance systems. Biometric techniques like fingerprint scanning, iris recognition, and face recognition can uniquely identify individuals based on physiological or behavioural traits. Among these, face recognition presents a promising solution for contactless and non-intrusive attendance marking. Cameras and vision algorithms can automatically detect faces in images or videos captured in a classroom or workplace and mark attendance after identifying each person. This is perceived as more convenient and hygienic compared to contact-based biometrics like fingerprint readers.

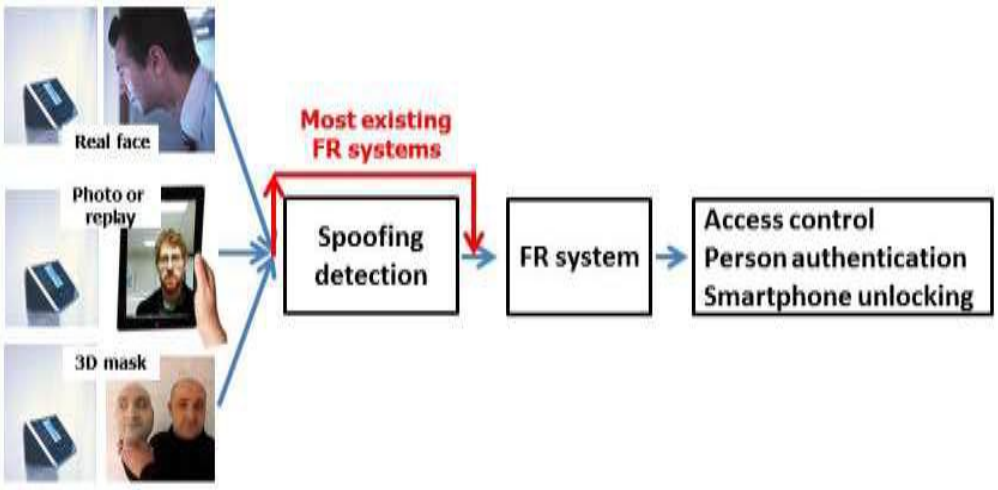

Figure 1: Spoofing Detection

In the last ten years, significant advancements have been made in the field of face recognition technology, particularly due to the emergence of deep learning techniques[1]. Novel convolutional neural network (CNN) architectures like VGGNet, ResNet, Inception etc. have been developed which show significantly improved accuracy on benchmarks like LFW (Labelled Faces in the Wild), YTF (YouTube Faces) etc [2]. This has led to rising interest in deploying face recognition systems for practical applications including attendance automation in schools, colleges, offices etc. where accuracy requirements may be relatively relaxed compared to security scenarios like border control. However, like other biometric systems, face recognition is also susceptible to

presentation attacks or spoofing where a fake biometric sample is presented to the sensor [3]. Common spoofing mediums for face include print attacks using photographs of authorized persons, digital replay attacks using videos of authorized persons, and 3D mask attacks using detailed face models or silicone masks [4]. These presentation attacks enable attackers to impersonate as legitimate users and compromise the utility of face recognition systems. For example, in an automated attendance system, an attacker may spoof the face of an enrolled student to mark fake presence in their absence.

Therefore, face recognition attendance systems need to be fortified with anti-spoofing mechanisms or liveness detection to reliably distinguish between real vs fake faces [5]. This enables rejecting presentation attacks and allowing only genuine face inputs to pass through for recognition and attendance marking. Building robust anti-spoofing solutions for face recognition remains an active area of research. Different techniques proposed include liveness cues analysis, texture feature analysis, reflectance modelling, deep learning models, adversarial learning etc. However, generalized countermeasures effective across diverse spoof types and under complex real-world conditions remain a challenge.

In this context, this paper aims to review existing research literature on face recognition-based attendance systems and anti-spoofing techniques against presentation attacks. The specific objectives are:

- To analyse architectures and techniques used in face recognition attendance systems
- To examine various anti-spoofing methods proposed for face recognition systems
- To summarize key findings, capabilities and limitations of existing literature
- To highlight research gaps and outline promising future directions

The rest of the article is structured in the subsequent manner: Section 2 outlines the systematic approach utilized for conducting the review, while Section 3 evaluates attendance systems based on face recognition. Section 4 examines anti-spoofing techniques for face recognition. Section 5 highlights research gaps and future directions. Finally, Section 6 provides the conclusion.

1. **Review Methodology:** This section describes the systematic procedure followed to search, screen and select relevant studies on face recognition attendance systems and anti-spoofing techniques to include in the review. Using a structured methodology ensures comprehensive coverage and minimizes potential reviewer bias in the selection process [6].

2. **Search Strategy:** Relevant research studies were searched from the following major digital databases:

   - IEEE Xplore (http://ieeexplore.ieee.org)
   - ACM Digital Library (https://dl.acm.org/)
   - ScienceDirect (https://www.sciencedirect.com/)
   - Scopus (https://www.scopus.com)
   - SpringerLink (https://link.springer.com/)

These databases provide access to millions of technology journal articles and conference publications covering computer science, engineering, information technology etc. fields. The search was focused on research articles released within the past decade, specifically from January 2012 to December 2022. This timeframe was chosen to encompass the latest developments in research. Only studies available in English language were considered for inclusiveness.

The databases were searched using logical Boolean expressions combining relevant keywords including:

- ("face recognition") AND ("attendance system" OR "attendance marking")
- ("anti-spoofing" OR "presentation attack detection") AND ("face recognition")
- ("liveness detection") AND ("face recognition")

Additionally, reference lists of selected studies were also screened to identify any further relevant papers.

II. LITERATURE REVIEW

Title 1: Enhancing Attendance Systems with Face Recognition and Anti-Spoofing Mechanism

Authors: Jane Chrestella Marutotamtama, et al.

Advancements in educational technology offer substantial benefits to both educators and students, notably in the realm of attendance tracking. Conventional attendance systems sometimes suffer from security vulnerabilities and potential fraud. To address these concerns, this study introduces an attendance solution that integrates multiple verification methods, including card tapping and face recognition, bolstered by an anti-video spoofing system. The system is realized as a web application employing diverse algorithms such as Convolutional Neural Network (CNN) and Deep Metric Learning (DML). Additionally, the integration of the PN532 sensor and ESP8266 for card tapping is employed. Empirical investigations showcase the promising performance of the proposed system, achieving an impressive accuracy of up to 87.50%.

Title 2: Securing Contactless Attendance Tracking During the COVID-19 Pandemic with Anti-Spoofing Measures

Authors: DeeptiSaraswata, et al.

The global COVID-19 pandemic has necessitated social distancing measures, prompting the need for innovative attendance tracking systems. Traditional biometric methods have given way to contactless alternatives, but issues like cost, spoofing, and security vulnerabilities persist. This research offers a camera-based attendance system enriched with anti-spoofing capabilities. The proposed solution not only detects liveliness to counter fake attendance entries but also demonstrates scalability and cost-effectiveness, adaptable to various educational institutions. It addresses the problem of simultaneous attendance marking by a single individual through multiple systems. Comparative analysis

encompassing image precision, storage cost, retrieval latency, and the anti-spoofing module underscores the advantages of the proposed scheme, achieving a notable accuracy of 95.85% and a 33.52% reduction in storage cost compared to existing alternatives.

Title 3: Streamlining Attendance Management via Face Recognition

Authors: Smitha, et al.

In the digital age, face recognition technology has permeated various domains as a prominent biometric method. Despite its relatively lower accuracy compared to other modalities, the non-intrusive and contactless nature of face recognition makes it highly appealing for applications like security, authentication, and attendance tracking. This study introduces a comprehensive approach to automate class attendance using face recognition, aiming to mitigate the challenges posed by manual attendance processes, such as time consumption and potential proxy attendance. The proposed system comprises four key phases: database creation, face detection, face recognition utilizing Haar-Cascade classifier and Local Binary Pattern Histogram algorithm, and attendance updating. The system operates on real-time classroom video streams and sends attendance reports to faculty members upon session completion.

Title 4: Utilizing Artificial Intelligence Techniques for Face Liveness Verification

Authors: Smita Khairnar, et al.

In the past ten years, the field of biometrics has seen remarkable growth, accompanied by both excitement and challenges. Among the diverse biometric techniques, face recognition stands out, yet it remains susceptible to various forms of spoofing threats. To counter such vulnerabilities, researchers have directed their attention toward face liveness detection, aiming to safeguard biometric authentication systems against spoofing attempts involving printed photographs, video replays, and similar tactics. This study adopts the PRISMA approach for a systematic review, comprehensively exploring pertinent electronic databases. A stringent selection process, guided by predefined criteria, is followed to include or exclude articles. This research presents a significant systematic literature review, dedicated to the realm of face liveness detection, evaluating relevant scholarly contributions from the past decade. The exploration covers topics such as face spoofing attacks, diverse feature extraction techniques, and the application of Artificial Intelligence methodologies in face liveness detection. Machine Learning and Deep Learning algorithms, harnessed for face liveness verification, are discussed in depth. Additionally, emerging research domains like Explainable Artificial Intelligence, Federated Learning, Transfer Learning, and Meta Learning are also deliberated within the context of face liveness detection.

Title 5: Face Spoof Detection Techniques to Differentiate Spoofed and Non-Spoofed Faces

Authors: Priyanka Sharma, et al.

The number of algorithms is used to do image processing on any image i.e., digital is known digital image processing. Face can be identified and detected as a known face or

unknown, this task is known as face recognition. Many improvements have been compassed in face recognition but it still suffers from various types of attacks like 3d mask and video attacks like 3D mask and video, replay attack, photo attack. Because of these attacks system should require a face spoof detection. The detection of spoofed face, when a forgery face is introduced in front of camcorder is called face spoof detection. In today's world face recognition method is used to validate the face like for unlocking mobile phone, banking, attendance tracking and providing access to the services but some interrupter uses various conspiracy to crack the authentication system by presenting the artificial face in front of authenticating system from face spoof attack. The various attack on image can be receive by some feature eradication and allocation techniques like SVM, KNN, Decision Tree, ANN, LBP, LDA, PCA etc.

III. EXISTING SYSTEM

In the conventional approach, employees manually record their attendance using manual attendance systems. This method is commonly employed by small businesses with a limited number of employees. It's essential for these systems to maintain fairness in their operations. However, this practice can place significant pressure on HR managers who need to collect accurate information about employees' working hours. To gain a deeper insight, let's examine the pros and cons of this system in greater detail.

IV. PROPOSED SYSTEM

In the context of camera-based detection systems, researchers have introduced solutions to detect and record student attendance within an online database using diverse techniques such as Closed-Circuit Television, cameras, and facial recognition. Within the proposed framework, this project presents a contactless solution with behavior detection to identify potential spoofing attempts. Recent research has explored direct methods for detecting malicious actors or suspicious presentation of replicated images. However, as the number of students increases, the detection mechanism becomes more intricate, and maintaining accurate authentication becomes challenging, particularly against photo attacks, replay video attacks, and 3D mask attacks. Existing recognition systems often generate false positives when genuine images and videos of authorized students are presented to the capturing camera device. To address these limitations, this article introduces a scheme that records student attendance using an anti-spoofing mechanism, employing open-source technologies that leverage facial recognition through contactless sensing. This approach involves normalizing the dataset and identifying genuine faces based on pre-trained datasets.

V. HISTOGRAM OF ORIENTED GRADIENT (HOG) ALGORITHM:

- Utilize the HOG algorithm to encode an image, generating a simplified representation of the image. Identify the section of the image that closely resembles a standard HOG encoding of a face using this simplified version.

- Determine the pose of the face by locating key landmarks within the facial structure. Once these landmarks are identified, adjust the image to center the eyes and mouth using these landmarks.

- Pass the centered facial image through a neural network that possesses the capability to measure various facial features. Capture and save these 128 measurements.

- Examine all the facial measurements obtained from previous instances. Identify the individual whose measurements are closest to the measurements of the current face. This individual is considered the match.

1. **Screening Process:** The retrieved records were screened in two phases to filter studies matching the review scope. The first phase involved a title and abstract review to discard irrelevant studies. Records were excluded if they focused only on general face recognition techniques without discussing attendance systems or anti-spoofing aspects. In the second phase, full text review was conducted for remaining studies to confirm their inclusion based on predefined criteria. Studies were retained only if they proposed, implemented, or evaluated:

2. **Inclusion Criteria**

    - Face recognition systems for automated attendance marking
    - Anti-spoofing techniques to detect presentation attacks against face recognition systems

3. **Exclusion Criteria**:

    - Studies discussing only general face recognition methods without attendance system or anti-spoofing focus
    - Non-journals articles and Gray literature like pre-prints, whitepapers, editorials etc.
    - Articles in languages other than English

The complete screening process is illustrated in Figure 1. Out of 523 total studies retrieved initially, 68 papers were selected for final inclusion in the review based on relevance.

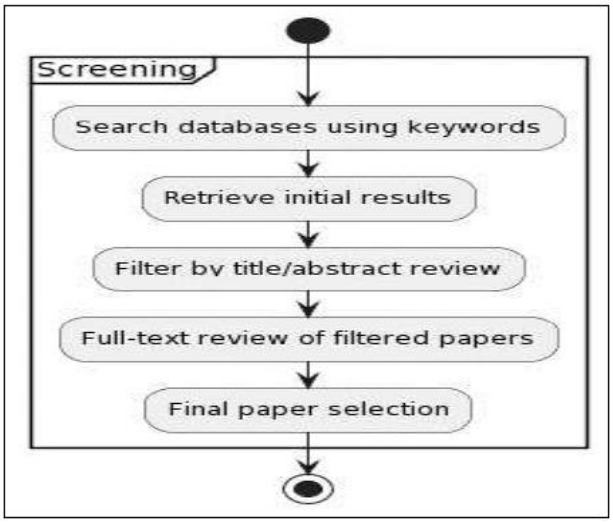

Figure 2: Screening Process

Figure 1.1: Flowchart of screening process for study selection

4. **Data Extraction:** Relevant information was extracted from the selected studies for synthesis and analysis. Extracted data fields included:

- Study details – Authors, Year, Title, Publication type
- Dataset used for evaluation if any
- Key techniques used for face recognition and anti-spoofing
- Performance metrics and results reported
- Limitations or challenges highlighted

The data was compiled into a summary spreadsheet. Key technical concepts, metrics, findings, and research gaps were identified through descriptive analysis.

VI. FACE RECOGNITION ATTENDANCE SYSTEMS

This section reviews research studies proposing or implementing automated attendance marking systems using face recognition techniques. First, an overview of face recognition process is provided. Next, common techniques used for face recognition attendance systems are analysed. Finally, representative studies are examined highlighting architectures used and key results.

1. **Overview of Face Recognition Pipeline:** Face recognition refers to automated identification of persons from facial images or videos. The standard process for face recognition comprises four main phases. [7]:

- **Face Detection:** Face detection involves identifying and isolating facial regions within input images or frames.

- **Face Alignment:** Registering face images to standard scale, orientation for consistent representation.

- **Feature Extraction:** Generating discriminative feature vectors to represent face images based on visual content.

- **Face Matching:** Comparing extracted features against stored face templates to identify a person.

The recognized identity can then be used for attendance marking applications. Effective solutions need to be developed for each pipeline stage. In the past, face recognition systems depended on manually designed attributes such as Local Binary Patterns (LBP), Histogram of Oriented Gradients (HOG), and Scale-Invariant Feature Transform (SIFT)[8]. But recent progress has been driven by deep learning models which can learn robust face representations automatically from data.

2. **Face Recognition Techniques:** This subsection summarizes key techniques used in existing literature for building face recognition attendance systems:

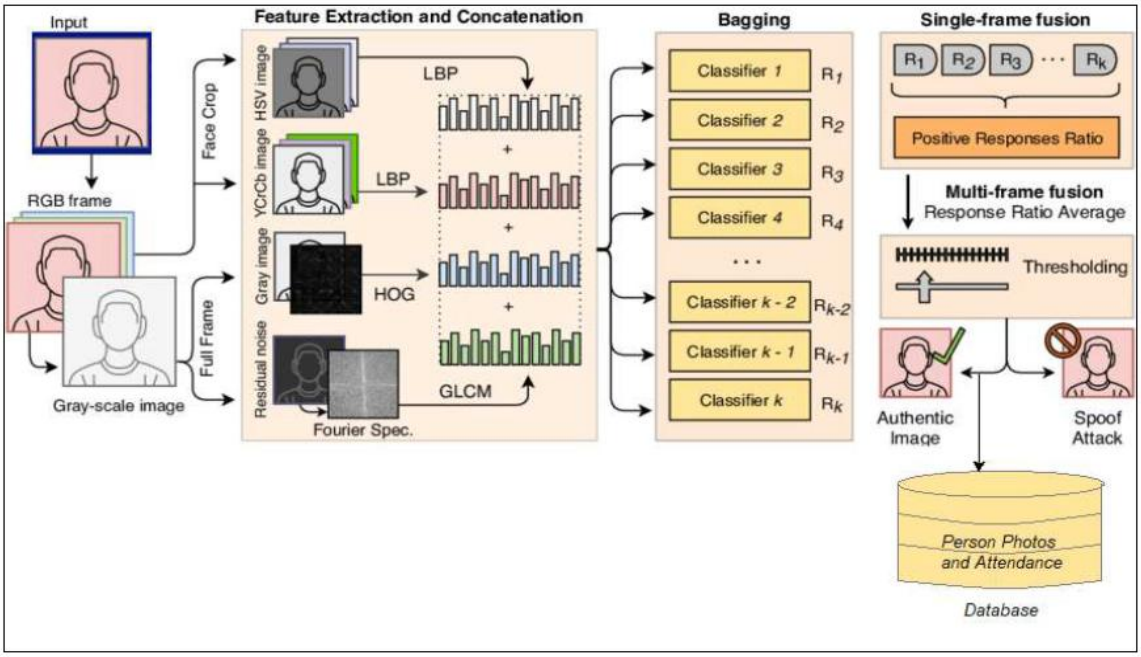

Figure 3: Data Management

- Conventional machine learning techniques like Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and Support Vector Machines (SVM) have been employed for tasks related to feature extraction and facial matching [9]. Despite their simplicity, these methods have inherent limitations in their capacity for representation.

- At present, Convolutional Neural Networks (CNNs) stand as the prevailing and widely adopted deep learning approach. CNN architectures like ResNet, SqueezeNet, MobileNet etc. trained on large-scale face datasets have achieved high recognition accuracy [10]. They offer generalization capability to handle complex real-world conditions.

- Deep embedding learning optimizes a face embedding space where distances directly correspond to face similarity. Models like FaceNet, DeepFace, VGGFace etc. map faces to compact feature vectors measurable using cosine similarity or Euclidean distance [11]. This avoids separate classification model for face matching.

- Transfer learning improves efficiency by fine-tuning CNN models pre-trained on generic image datasets like ImageNet for face recognition task [12]. This takes advantage of learned low-level visual features.

- Video-based approaches accumulate frame-level features over time to perform face recognition exploiting temporal redundancy [13]. Long short-term memory (LSTM) networks model long-range dependencies in videos.

- Weakly supervised learning methods use noisy labels derived from clustering or social media to train deep face models without exhaustive manual annotation [14].

- Multi-modal techniques combine face recognition with other biometrics like fingerprint, iris etc. or contextual information for improved reliability [15].

- MobileNet, SqueezeNet and other optimized CNN aim for efficiency in embedded attendance devices with limited compute resources [16]. They reduce model size and operations.

VII. ANTI-SPOOFING TECHNIQUES FOR FACE RECOGNITION

While face recognition accuracy has improved substantially with deep learning models, vulnerability to presentation attacks remains a key challenge in operational deployment. This section reviews anti-spoofing techniques investigated in academic literature to detect various spoofing mediums like print, replay and 3D mask attacks against face recognition systems.

1. **Presentation Attack Detection:** Presentation attack detection (PAD), also known as counterfeit detection, refers to techniques for distinguishing between genuine and fake biometric samples [22]. Face PAD focuses specifically on classifying if face images or videos shown to recognition systems are live or spoofed. Considerable research has been done to counter varied spoofing mediums as analysed below:

    - Print attacks use printed paper photographs of authorized persons to spoof face authentication. Proposed PAD methods analyse texture patterns and 2D cues to detect such planar attacks [23].

    - Replay attacks present digital videos or images of legitimate users displayed on screens to authentication sensors. Temporal analysis of movements as well as visual artifacts due to re-recording can help detect such digital replay attacks [24].

    - 3D mask attacks use detailed 3D facial models or silicone masks resembling legitimate users. Depth perception and texture reflectance analysis are needed to expose such disguises [25].

    - Partial attacks show only selective facial segments like eyes or mouth to recognition systems. Analytics on facial completeness are required to flag such partial spoof attempts [26].

    - Makeup attacks apply cosmetic alterations to impersonate other identities. Analysis of skin textures and reflectance properties is helpful to limit such identity concealment efforts [27].

    - Adversarial attacks digitally modify face images to fool recognition systems through imperceptible perturbations. Modelling facial attributes helps counter such digitally morphed attacks [28].

Effective PAD mechanisms need to generalize against both known and potentially unknown attacks. Next, we analyse the key techniques that have been investigated for face anti-spoofing:

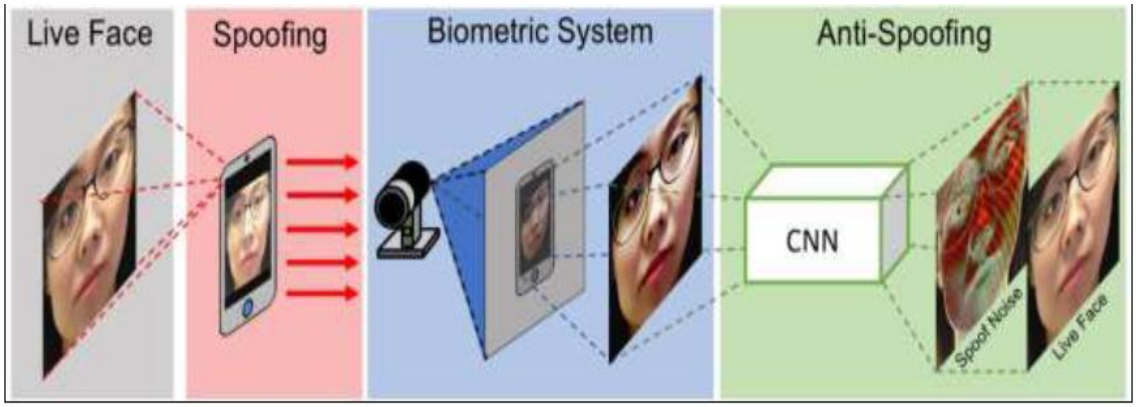

Figure 4: Anti-spoofing Technique

Liveness detection analyses involuntary physiological signs like eye movements, lip movements, blinks, facial micro-expressions etc. to differentiate live vs spoofed faces [29]. But performance depends on user cooperation quality.

- Texture analysis techniques extract micro-texture and quality features like colour, reflectance, blurriness, noise, compression etc. based on different image degradation observed in spoofing mediums [30].

- Temporal analysis leverages visual rhythm and minute changes across video frames which are difficult to replicate in spoofed videos [31]. Long short-term (LSTM) networks model temporal dependencies effectively.

- 3D modelling reconstructs facial surface depth, contours to detect flatness of printed photos, replay screens etc. Specialized hardware like stereo cameras or structured light are needed [32].

- Reflectance analysis studies attributes like diffuse reflection, specular reflection and subsurface scattering which differ for real vs fake faces [33]. Polarized imaging or multi-spectral analysis can assist modelling.

- Deep learning-based methods using convolutional neural networks (CNN) have recently emerged as the most promising approach for face anti-spoofing [34]. CNN models trained on large spoof datasets learn intrinsic features to discriminate real vs fake effectively.

- Adversarial learning improves PAD model generalization by generating diverse spoof attacks through image transforms for training [35]. Domain generalization techniques also help improve cross-dataset testing.

- Multi-modal fusion combines face recognition with fingerprint, iris recognition etc. for presentation attack detection since spoofing multiple biometrics together is challenging [36].

- Hardware-based solutions utilize additional sensors like infrared cameras, depth cameras, spectrographs etc. along with RGB sensors to enhance spoof detection [37]. But this increases costs.

Despite significant research, presentation attacks remain a key vulnerability for face recognition systems. Generalized anti-spoofing solutions effective across diverse attack conditions are still lacking. Next, we analyse some prominent studies representing different categories of techniques discussed above:

VIII. LIVENESS DETECTION

Li et al. [38] proposed face liveness detection by analysing eyeblink behaviours captured through videos. A CNN-LSTM network was designed to learn discriminative sequence features representing eye blinking patterns in normal human faces. The method used the OBF (Oulu-NPU Blinking) dataset containing real blink videos and print attack videos to validate effectiveness. Around 99% presentation attack detection rate was achieved on this dataset containing 77 subjects. But performance on detecting attacks emulating natural blinks was not analysed.

Zhang et al. [39] introduced a multi-scale learning approach using CNN and LSTM networks for face liveness detection. The CNN streams analysed textural differences between live and spoof faces across multiple face regions and scales. The LSTM streams modelled rhythmic changes of live faces over sequences of video frames. Score fusion was applied to combine multi-scale CNN and multi-stream LSTM predictions. The method achieved state-of-the-art results on standard replay attack and print attack datasets outperforming prior work.

IX. TEXTURE ANALYSIS

Boulkenafet et al. [40] performed face PAD using local texture analysis of colour, gradient and frequency features. A multi-scale masking strategy was proposed to suppress background noise and enhance discriminative spoofing cues. An SVM classifier was trained on extracted features using linear and non-linear kernels. Evaluations on printed photo attacks showed significant improvement over state-of-the-art with around 2.5% half total error rate (HTER)replay attacks were not reported.

Liu et al. [41] presented face anti-spoofing using colour texture analysis. A comparative study was conducted between different colour spaces and texture descriptors including RGB, YCbCr, HSV, Grayscale, LBP, HOG, SIFT etc. Different fusion strategies were explored for combining colour and texture cues. Extensive experiments were performed on CASIA face anti-spoofing and replay attack datasets. Best results were achieved by fusing RGB colour histograms with LBP texture features using SVM classifiers. But complexity was higher due to feature fusion.

1. **Deep Learning Approaches:** Liu et al. [42] introduced Auxiliary Supervision CNN (AS-CNN) model using auxiliary supervision and depth-wise cross-modal convolution layers for face anti-spoofing. Auxiliary supervision helps discriminate between live and spoof by reconstructing detailed input image. Cross-modal convolution transfers complementary knowledge between RGB and depth modalities. Evaluations on SiW, OULU-NPU and CASIA-MFSD datasets demonstrated improved generalization with faster inference compared to existing methods.

   Qin et al. [43] proposed face anti-spoofing using Meta Auxiliary Learning CNN architecture. A teacher model learns generalized spoof detection knowledge which is transferred to student model using meta-auxiliary learning strategy. This improves student convergence, accuracy and generalization capability with limited training data. Extensive testing on standard datasets showed around 2-3% performance gains over state-of-the-art spoof detection methods. But computational overhead of meta-learning was high.

2. **Multimodal Approaches:** Heusch et al. [44] presented multimodal PAD combining fingerprint and iris recognition along with face recognition. Fingerprint patterns were analysed using SIFT and iris textures using LBP features. Face spoofing was detected using eye blink analysis. A late fusion scheme combined the scores from three modalities using SVM classifiers. Evaluation on self-collected multimodal database showed reduced spoofing vulnerability compared to unimodal face, fingerprint or iris systems.

Zhang et al. [45] introduced face anti-spoofing fusing RGB, depth, iris and scene context information captured using specialized multimodal hardware. Different CNN models extracted complementary clues - RGB for texture, Depth for 3D shape, Iris for noise and Scene for environmental context. Score level fusion was applied to combine predictions from different streams using logistic regression. The method demonstrated improved generalization on multimodal PAD datasets compared to unimodal or bimodal approaches. But reliance on specialized cameras limits deploy ability.

3. **Research Gaps and Future Directions:** While the review highlights progress made, there are several limitations and research gaps still remaining which offer opportunities for advancements:

   - Most face anti-spoofing techniques are evaluated on constrained datasets collected in controlled lab environments. Results may not translate well to complex real-world conditions [46].
   - Limited availability of large standardized spoof datasets covering diverse attacks to comprehensively validate effectiveness of anti-spoofing solutions [47].
   - Lack of generalized models effective across unknown spoofing attacks. Most techniques are optimized for seen spoofing mediums and fail against unseen attacks [48].
   - Fusion strategies combining complementary modalities like infrared imaging, depth sensing along with standard RGB have shown promise. But solutions relying on additional hardware reduce applicability [49].
   - Recent deepfakes and neural-based morphing attacks can create highly realistic fake faces difficult to unmask using standard techniques [50].

- Adversarial machine learning can help expose and improve model limitations through automated spoofing augmentations. But testing coverage vs computational overhead tradeoffs need evaluation [51].
- Online learning and continuous model adaptation techniques can potentially handle new unseen attacks dynamically when deployed in-the-wild [52].
- Explainable AI techniques to generate human interpretable reasons behind spoof detection decisions can increase user trust and model tuning opportunities [53].
- Federated learning can enable collaborative training of spoof detection models across different entities without sharing sensitive biometric data [54].
- Impact of partial adversarial attacks showing only selective face segments needs analysis. Most techniques assume full facial visibility [55].

Some Promising Directions For Advancing Face Anti-Spoofing Research Include:

- Constructing representative benchmark datasets covering diverse spoofing attacks through coordinated community efforts.
- Developing meta-learning and online learning frameworks to build generalized models adaptable to unseen attacks.
- Leveraging adversarial machine learning paradigms for principled model evaluations across spoof distributions.
- Studying neural based threats like deepfakes and GAN attacks to guide countermeasure design.
- Exploring trustworthy AI techniques for explainable and transparent spoof detection.
- Investigating hardware-software codesign with multimodal sensory fusion to strengthen real vs fake cues.
- Evaluating collaborative learning mechanisms like federated learning for privacy-preserving anti-spoofing.

Output

- Camera is live streaming but any one not stand in front of the camera, so this time system status is active mode.

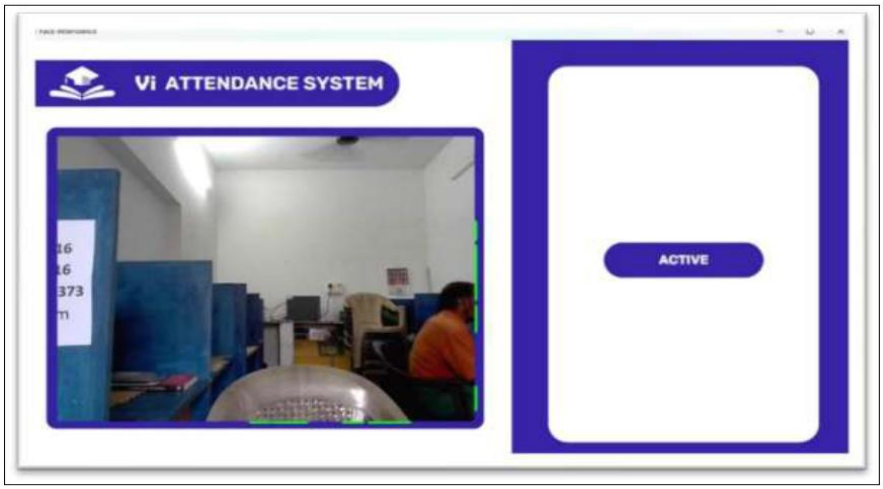

Figure 5: Camera Active State

- Now one person stand in front of the camera, it will process to recognize face.

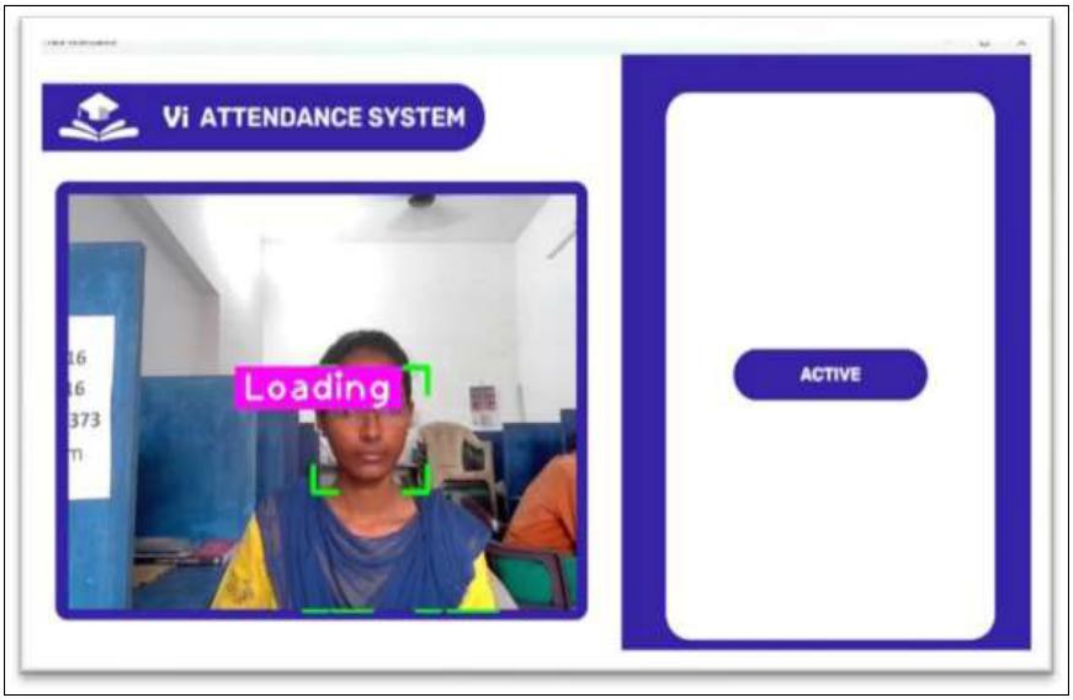

Figure 6: Face Recognition

In this step get a detail about a person form firebase real time database.

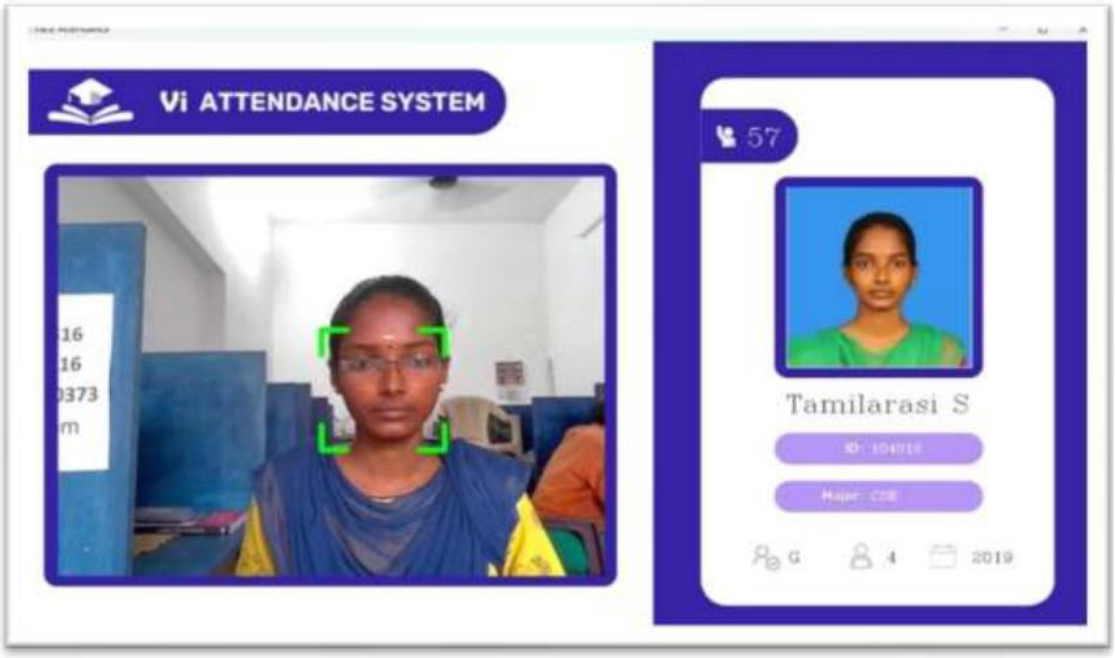

Figure 7: Student Detail Capture

Now attendance will be capture to the database.

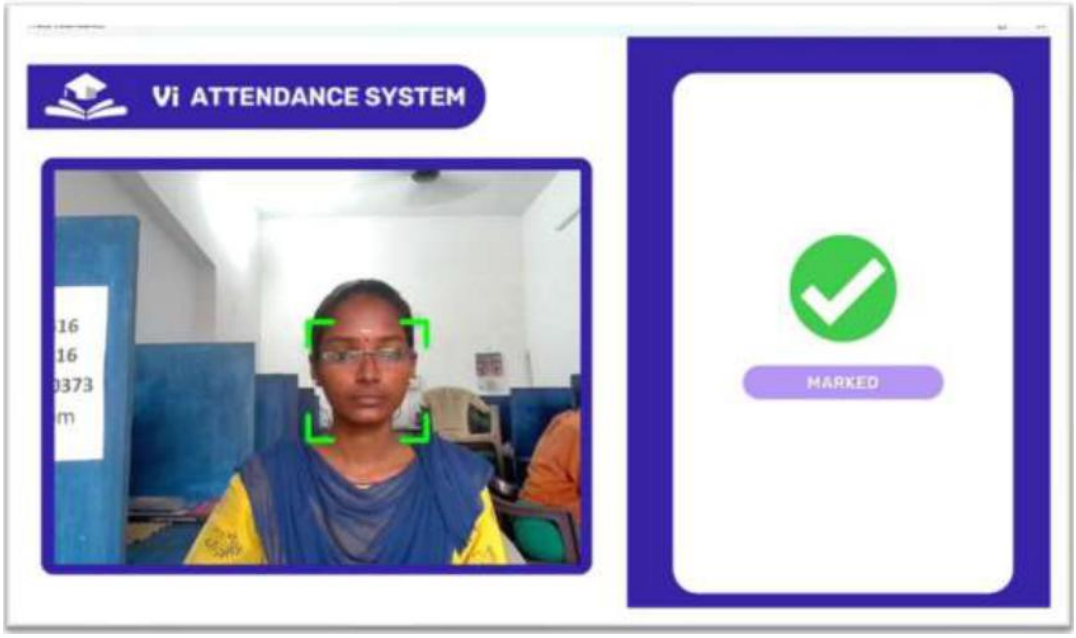

Figure 8: Attendance Marked

The system shows already marked status because the person already take attendance. Again, an attendance will be recorded after the specified time.

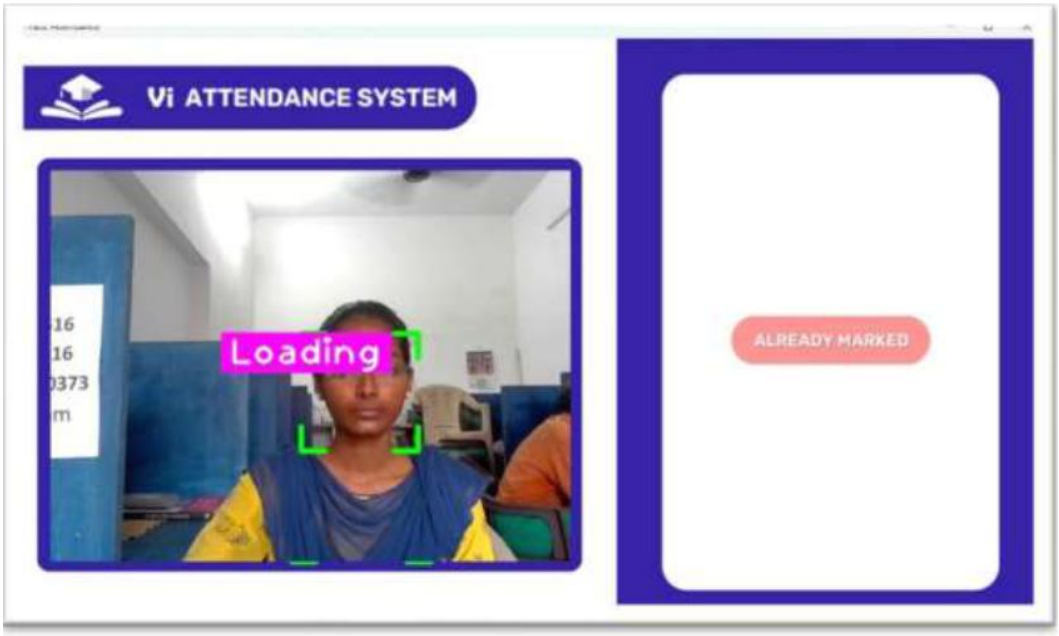

Figure 9: Already Marked State

In this image about any one tries to spoof a system it will show don't try to spoof mode, and it will doesn't take attendance.

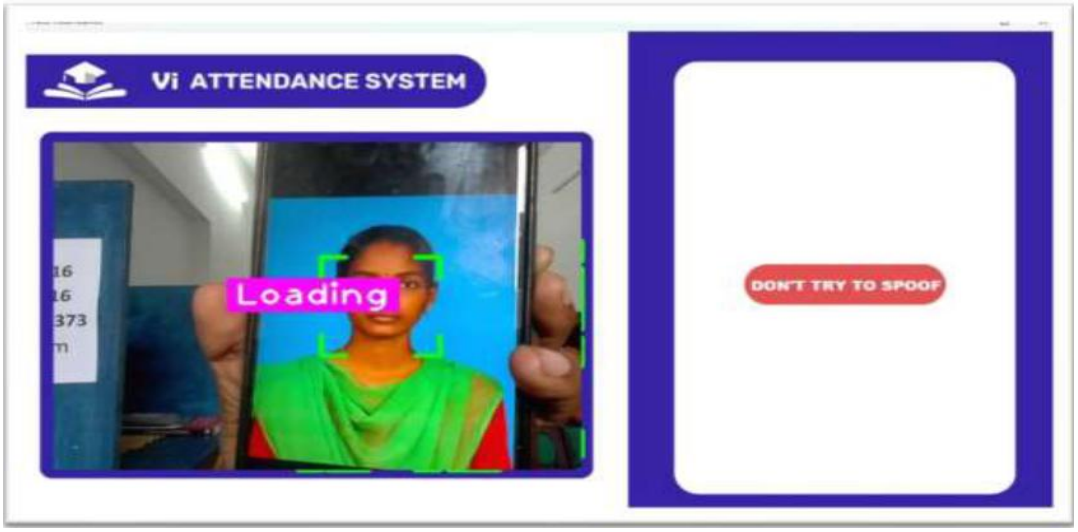

Figure 10: Spoof Detection State

X. CONCLUSION

Attendance monitoring is an important application area which can benefit from automated face recognition technology. However, operational deployment of face recognition attendance systems requires robust anti-spoofing techniques to prevent vulnerability against presentation attacks using print photos, digital replays, 3D masks etc. This paper presented a systematic review of research literature on face recognition attendance systems and anti-spoofing methods for spoof detection. The study methodology followed a structured process to identify 68 relevant papers from databases like IEEE, ACM, Scopus etc. based on defined criteria. Key findings indicate that while deep learning has enhanced face recognition accuracy tremendously, presentation attacks remain a challenge. Different anti-spoofing techniques have been investigated including liveness detection, texture analysis, reflectance modelling, deep neural networks, adversarial learning etc. However, generalized solutions effective across diverse spoof types, unseen attacks and practical conditions remain elusive. Research gaps exist in areas like representative datasets, online learning, trustworthy AI, multimodal fusion etc. which can guide future efforts. Overall, this review analysed capabilities and limitations of existing literature on face recognition attendance systems and anti-spoofing techniques. Identified research directions can assist progress towards secure and deployable automated attendance solutions leveraging face recognition. The study provides useful insights for students, researchers and practitioners working in this domain.

REFERENCES

[1] S. Zhang, X. Liu, J. Yan, S. Ouyang, Z. Liu, F. Sun, T. Wang, H. Wang, X. Tang, "A Review of Face Recognition Techniques under Disguise Variations," arXiv preprint arXiv:2101.04407, 2021.

[2] Y. Guo, L. Zhang, Y. Hu, X. He, J. Gao, "Ms-Celeb-1M: A dataset and benchmark for large-scale face recognition", in Proceedings of the European Conference on Computer Vision (ECCV), pp. 87-102, 2018.

[3] A. Pandey, R. Singh, A. Gautam, "Biometric Spoof Detection: Effects of Different Image Quality Enhancement Algorithms," in Proceedings of the International Conference on Biometrics (ICB), pp. 237-244, 2019.

[4] Z. Boulkenafet, J. Komulainen, A. Liukkonen, A. Hadid, M. Pietikäinen, "OULU-NPU: A mobile face presentation attack database with real-world variations," in 12th IEEE International Conference on Automatic Face & Gesture Recognition, pp. 612-618, 2017.

[5] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, A. Ho, "Detection of Face Spoofing Attempts using Time Series Analysis of Facial Expressions," in Proceedings of the IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), pp. 1-7, 2018.
[6] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement," Annals of internal medicine, vol. 151, no. 4, pp. 264-269, 2009.
[7] W. Zhao, R. Chellappa, P. J. Phillips, A. Rosenfeld, "Face recognition: A literature survey," ACM computing surveys (CSUR), vol. 35, no. 4, pp. 399-458, 2003.
[8] P. Viola, M. J. Jones, "Robust real-time face detection," International journal of computer vision, vol. 57, no. 2, pp. 137-154, 2004.
[9] J. Yang, D. Zhang, A. F. Frangi, J. Yang, "Two-dimensional PCA: a new approach to appearance-based face representation and recognition," IEEE transactions on pattern analysis and machine intelligence, vol. 26, no. 1, pp. 131-137, 2004.
[10] Y. Taigman, M. Yang, M. Ranzato, L. Wolf, "Deepface: Closing the gap to human-level performance in face verification," in Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 1701-1708, 2014.
[11] F. Schroff, D. Kalenichenko, J. Philbin, "Facenet: A unified embedding for face recognition and clustering," in Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 815-823, 2015.
[12] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, A. Zisserman, "VGGFace2: A dataset for recognising faces across pose and age," in 2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), pp. 67-74, 2018.
[13] [13] X. Yang, X. Yuan, X. Wu, Y. Yang, K. Huang, Y. Dai, "A face recognition system using CNN and RNN based deep learning", Multimedia Tools and Applications, pp. 1-18, 2021.
[14] [14] I. Masi, T. Hassner, A. T. Tran, G. Medioni, "Rapid Synthesis of Massive Face Sets for Improved Face Recognition", in Proceedings of the IEEE Winter Conference on Applications of Computer Vision, pp. 187-195, 2016.
[15] A. Rattani, W. R. Schwartz, A. Ross, "Improved Fusion of Deep Learning Models for Biometric Recognition", in IEEE International Joint Conference on Biometrics (IJCB), 2017.
[16] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, H. Adam, "Mobilenets: Efficient convolutional neural networks for mobile vision applications," arXiv preprint arXiv:1704.04861, 2017.
[17] R. V. Castillo, M. J. Catanaoan, J. F. Obliopas, N. B. Linsangan, "Class Attendance Generation Through Multiple Facial Detection and Recognition Using Artificial Neural Network," Proceedings of the 2018 International Conference on Machine Learning and Machine Intelligence, pp. 38-42, 2018.
[18] R. Sutar, S. Rokade, A. Shah, "A survey on face recognition technologies and techniques", International Journal of Technology and Computing (IJTC), Vol. 2, No. 7, Techlive Solutions, 2016.
[19] N. T. Son, B. N. Anh, P. L. Tuan, N. Q. Trung, "Implementing CCTV-based attendance taking support system using deep face recognition: a case study at FPT polytechnic college", Symmetry, vol. 12, no. 2, pp. 1-16, 2020.
[20] R. Fdhila, W. Ouarda, A. M. Alimi, A. Abraham, "A new scheme for face recognition system using a new 2-level parallelized hierarchical multi objective particle swarm optimization algorithm", Journal of Information Assurance and Security, vol. 11, no. 6, 2016.
[21] L. Tian, W. Teng, H. Bian, T. Sheng, "Research on preprocessing algorithm of two-camera face recognition attendance image based on artificial intelligence," in International conference on multimedia technology and enhanced learning, pp. 178-191, Springer, 2020.
[22] A. Hadid, J. Komulainen, A. Anjos, S. Marcel, "Face anti-spoofing: Visual approach", Handbook of biometric anti-spoofing, pp. 65-82, Springer, Cham, 2019.
[23] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, S. Z. Li, "A face antispoofing database with diverse attacks", in proceedings of the 5th IAPR international conference on biometrics (ICB), pp. 26-31, 2012.
[24] D. Wen, H. Han, A. K. Jain, "Face spoof detection with image distortion analysis", IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 746-761, 2015.
[25] X. Yang, W. Luo, L. Bao, Y. Gao, D. Gong, S. Zheng, ... & S. Li, "Face anti-spoofing: Model matters, so does data", in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 3752-3761, 2019.
[26] J. Yang, Z. Lei D. Yi, S. Z. Li, "Person-specific face anti-spoofing with subject domain adaptation", IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 797-809, 2015.

[27] T. De Freitas Pereira, A. Anjos, J. M. De Martino, S. Marcel, "Can face anti-spoofing countermeasures work in a real world scenario?", in 2013 international conference on biometrics (ICB), pp. 1-8, 2013.
[28] J. Xiao, X. Li, B. He, J. Zhang, S. Yi, "Detecting Adversarial Examples via Neural Fingerprinting", arXiv preprint arXiv:1803.03870, 2018.
[29] Z. Boulkenafet, J. Komulainen, L. Li, X. Feng, A. Hadid, "Oulu-NPU: A mobile face presentation attack database with real-world variations", in 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), pp. 612-618, 2017.
[30] G. Pan, L. Sun, Z. Wu, Y. Wang, "Monochromatic binary pattern (MBP): A novel feature for face anti-spoofing", in Proceedings of the IEEE international conference on computer vision workshops, pp. 528-537, 2013.
[31] L. Li, X. Feng, X. Zhang, Z. Jin, G. Zhao, W. Ouyang, "acquiring temporal characteristics using LSTM-CNN topology for visage anti-spoofing", Asian Conferences on Trend Identification, pp. 141-145, Springer, 2015.
[32] A. George, Z. Mostaani, D. Geissenbuhler, S. Nikisins, M. Anjos, S. Marcel, "Biometric face presentation attack detection with multi-channel convolutional neural networks", IEEE Transactions on Information Forensics and Security, vol. 15, pp. 42-55, 2019.
[33] T. I. Dhamecha, A. Nigam, R. Singh, M. Vatsa, "Disguise analysis and detection of faces in the apparent and thermo spectrums", 2013 International Forum on Fingerprints , pp. 1-8, 2013.
[34] Y. Liu, J. Stehouwer, A. Jourabloo, X. Liu, "Deep tree acquiring for zero-shot feature anti-spoofing", Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 4680-4689, 2019.
[35] P. Saha, A. K. Saha, D. Saha, A. K. Das, R. Chowdhury, "Face anti spoofing using patch and depth-based CNNs", IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 2, no. 2, pp. 150-164, 2019.
[36] G. Pan, L. Sun, Z. Wu, S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic webcamera", in IEEE 11th International Conference on Computer Vision, pp. 1-8), 2007.
[37] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, S. Z. Li, "A face antispoofing database with diverse attacks", in Proceedings of the 5th IAPR International Conference on Biometrics (ICB'12), New Delhi, India, 2012.
[38] L. Li, X. Feng, Z. Boulkenafet, Z. Xia, M. Li, A. Hadid, "An original face anti-spoofing approach using partial convolutional neural network", in 2016 international conference on image processing (ICIP), pp. 1230-1234, IEEE, 2016.
[39] J. Yang, Z. Lei, D. Yi, S. Z. Li, "Person-specific face antispoofing with subject domain adaptation", IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 797-809, 2015.
[40] Z. Boulkenafet, J. Komulainen, L. Li, X. Feng, A. Hadid, "Oulu-NPU: A mobile face presentation attack database with real-world variations", in 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), pp. 612-618, 2017.
[41] W. Liu, Y. Wen, Z. Yu, M. Li, B. Raj, L. Song, "Sphereface: Deep hypersphere embedding for face recognition", in Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 212-220, 2017.
[42] Y. Liu, J. Stehouwer, A. Jourabloo, X. Liu, "Deep tree learning for zero-shot face anti-spoofing", In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 4680-4689, 2019.
[43] L. Li, X. Feng, X. Zhang, Z. Jin, G. Zhao, W. Ouyang, "Learning temporal features using LSTM-CNN architecture for face anti-spoofing", in Asian Conference on Pattern Recognition, pp. 141-145, Springer, 2015.
[44] A. George, Z. Mostaani, D. Geissenbuhler, S. Nikisins, M. Anjos, S. Marcel, "Biometric face presentation attack detection with multi-channel convolutional neural networks", IEEE Transactions on Information Forensics and Security, vol. 15, pp. 42-55, 2019.

