Revolutionizing Identity Verification and Recognition

Priti Nagtode, Avinash Shrivas, Amit Aylani
VIT, pritinagtode.29@gmail.com Mob no.9664334877
Assistant Professor, VIT, avinash.shrivas@vit.edu.in
Assistant Professor, VIT, amit.aylani@vit.edu.in

Abstract— The innovative integration of real-time human detection improves both security and user experience in identity authentication. This approach improves authentication processes by analysing physiological and behavioural indicators such as face movements and eye movements, hence reducing fraud risks. Its deployment across sectors promises to enhance security in finance, healthcare, e-commerce, and law enforcement. Despite the hurdles, the benefits of this human-centered approach are enormous, indicating a more secure digital future.

Keywords— Identity verification, live human detection, digital security, biometric authentication, user experience, fraud prevention, computer vision, physiological and behavioural cues, facial and vocal patterns, finance, healthcare, e-commerce, law enforcement.

INTRODUCTION

Face recognition technology has advanced significantly over the past few decades, embracing a wide range of approaches and applications. The transition from classic approaches like Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) to more advanced methods like Deep Neural Networks (DNNs) demonstrates the field's dynamic character [1]. Contemporary face recognition systems are not only concerned with improving accuracy, but also with resolving security problems such as spoofing attacks by employing methods such as liveness detection, which verifies the authenticity of the recognised face [2, 4, 5, 7].

Recent research has examined a variety of ways to improving facial recognition and liveness detection. Two-stream Convolutional Networks [2], contrast adjustment and histogram equalisation [3], and perceptual picture quality assessment [13] have all been researched to increase the robustness and reliability of these systems. Furthermore, the use of facial recognition in real-time applications such as attendance management systems [3], access control, and surveillance [4, 6] illustrates its broad applicability. Innovative approaches, such as the combination of colour texture data and deep learning [5], the use of Haar Cascade and Local Binary Pattern Histogram (LBPH) [9], and movement analysis for liveness detection [7], highlight continuous attempts to reduce security risks. Furthermore, the implementation of biometric techniques in smart cities for healthcare, public safety, and transportation [12], as well as their use in gaming services to prevent account hijacking [17], demonstrate the growing reach of facial recognition technologies.

Overall, the continual development and deployment of sophisticated face recognition and liveness detection techniques is critical for improving security measures and ensuring the integrity of biometric systems across multiple domains [1-25].

Face recognition is a biometric technique that uses a person's distinctive facial characteristics to identify and authenticate them. It entails employing computer vision algorithms to record and examine face patterns, such as the positioning of the lips, nose, and eyes. Face recognition is a widely used and adaptable technology that provides easy-to-use and non-intrusive identification for personal devices, security, and access management. Facial verification is a biometric procedure that uses distinctive facial traits to verify people. Computer vision algorithms are frequently used for precise and non-intrusive identification confirmation.

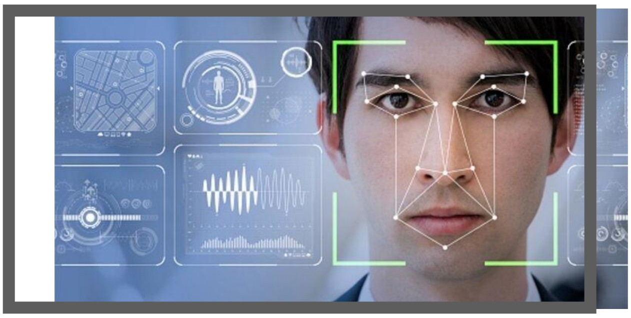

Fig. 1. Face Recognition

LITERATURE REVIEW

The literature study includes 25 papers that discuss important developments in face recognition and liveness detection systems. This research demonstrates the progression from classic methods like PCA and LDA to modern deep neural networks (DNNs), improving applications in security, border surveillance, and video analytics [1]. Several papers focus on boosting spoof detection through innovative techniques such as two-stream convolutional networks and feature fusion, bolstering the effectiveness of authentication and surveillance systems [2,4,5,7]. Improved algorithms, including contrast adjustment, bilateral filter, and histogram equalisation, provide accurate and efficient solutions for attendance management and security lock technology [3,9].

Real-time face detection methods using OpenCV, Haar features, and CNNs are emphasised for practical applications in surveillance and biometric verification [6, 8, 18]. Several research offer robust approaches for liveness detection to prevent spoofing attacks and ensure the reliability of biometric systems [10,11,13,15]. Furthermore, the application of biometric approaches in smart cities for public safety, healthcare, and transportation, as well as in gaming services and continuous user verification using wearable sensors, is examined [12–17, 25]. Comprehensive evaluations and surveys provide insights into the numerous identification methods and their security consequences, aiding the adoption and implementation of biometric technology across different sectors [22, 23, 24]. Overall, these articles highlight the importance of sophisticated facial recognition and liveness detection in improving security and authentication across a variety of applications.

Murat Taskiran, Nihan Kahraman, Cigdem Eroglu Erdem [1] This study presents a detailed overview of facial recognition technologies, tracking their growth from early methods such as PCA and LDA to more current techniques including DNNs. It covers a wide range of applications, including security, border monitoring, and video analytics, emphasising current developments and prospects in the sector.

Haonan Chen, Guosheng Hu, Zhen Lei, Yaowu Chen, Neil M. Robertson, Stan Z.Li [2] The article proposes a two-stream convolutional network strategy that works in RGB and multi-scale retinex spaces to improve face spoofing detection. It performs competitively across many databases, highlighting its potential for improving authentication and surveillance systems.

Serign Modou Bah, Fang Ming [3] In particular, D. Gabor's This study focuses on improving face recognition algorithms by contrast adjustment, bilateral filtering, and histogram equalisation. The upgraded system is used to attendance management, providing institutions with an efficient and straightforward method for accurately tracking attendance.

Shuhua Liu, Yu Song, Mengyu Zhang, Jianwei Zhao, Shihao Yang and Kun Hou [4] This work provides an identity authentication system with built-in liveness detection using FaceNet and a lightweight CNN model. It attempts to improve the security of access control, surveillance, and mobile payment systems by eliminating spoofing attacks.

Fu-Mei Chen, Chang Wen, Kai Xie, Fang-Qing Wen, Guan-Qun Sheng, Xin-Gong Tang [5] The research describes a method for detecting face liveness that combines colour texture and deep characteristics, making it more resistant to spoofing assaults. It uses datasets such as NUAA and Replay-Attack to demonstrate improved personal authentication and access control applications.

Asif Mohammed Arfi, Debasish Bal, Mohammad Anisul Hasan, Naeemul Islam, Yasir Arafat [6] This research uses Haar characteristics for real-time face detection and recognition, demonstrating potential in surveillance and biometric identity verification. To improve security, the process entails creating a dataset, converting it to greyscale, and recognising labels.

Zhi Jie Ooi, Chi Wee Tan, Tong Ming Lim [7] This study uses movement analysis and deep learning models to detect face activity to prevent security breaches. Techniques such as the PnP problem and TensorFlow models are used in access control and identity verification.

Sudeep Thepade, Prasad Jagdale, Amit Bhingurde,Shwetali Erandole [8] The research addresses how luminance-based features can be integrated with machine learning classifiers to improve face liveness recognition, with the goal of increasing biometric system security against spoofing. It is very important for developers of biometric security technology.

Zankruti Arya, Vibha Tiwari [9] This study uses OpenCV, Haar Cascade, and different algorithms for automatic facial identification and detection, such as Eigenface and Fisherface. It aims to improve security lock technology, criminal investigation, and video surveillance applications.

Viktor Dénes Huszár, Vamsi Kiran Adhikarla [10] The work suggests a lightweight deep learning-based approach to spoof detection in automated human activity recognition (HAR) systems. It focuses on improving the security of HAR applications by preventing spoofing in videos.

Aditya Bakshi, Sunanda Gupta [11] This work provides a face anti-spoofing model that employs picture quality assessment criteria after analysing motion, flash reflection, and auditory sensors. It tries to protect biometric systems from various spoofing assaults while also boosting the reliability of face recognition.

Elham Farazdaghi, Mojtaba Eslahi, Rani El Meouche [12] This overview focuses on the use of biometric techniques such as facial and fingerprint identification in smart cities. It explores the significance of these technologies for improving public safety, healthcare, and transportation security.

Chun-Hsiao Yeh, Herng-Hua Chang [13] The research presents a face liveness detection approach that employs perceptual image quality assessment and multi-scale analysis. It effectively combats video-based spoofing attacks, hence improving the security of facial recognition systems.

Li Song, Hongbin Ma [14] Using texture and colour data, this paper proposes a method for detecting facial liveness with real-time applications. The technique is evaluated on datasets such as CASIA and NUAA, demonstrating its anti-spoofing capabilities.

Abdulkadir Şengür, Zahid Akhtar, Yaman Akbulut, Sami Ekici, Ümit Budak [15] This study investigates deep learning methods for detecting facial liveness, such as texture and motion analysis. It uses SVM classifiers and CNNs to prevent presentation attacks on face recognition systems.

Phoo Pyae Pyae Linn, Ei Chaw Htoon [16] The study presents a face anti-spoofing solution that uses eye movement and CNN techniques. It solves spoofing attacks on facial recognition systems, making them more secure and reliable.

Vyacheslav V. Zolotarev, Alina O. Povazhnyuk, Ekaterina A. Maro [17] This article examines the use of liveness detection in gaming services to prevent account hijacking. It focuses on the use of convolutional neural networks to improve security in gamified environments.

Suyash Mishra, Vikash Sharma, Subhankar Mondal, Kasam Saadesh Reddy [18] This paper describes a real-time face recognition system built with Python and OpenCV. It emphasises security applications that prevent unauthorised access to critical places or information.

Logeswari Saranya and K Umamaheswari [19] The study employs CNN for multiple face analysis and liveness detection, indicating that it has the potential for usage in organisational security applications. The approach entails training on a variety of datasets to increase detection accuracy.

Raden Budiarto Hadiprakoso, Hermawan Setiawan, Girinoto [20] This study uses CNN classifiers for face anti-spoofing and liveness detection, which improves the security of face recognition systems. It emphasises the use of deep learning to provide effective anti-spoofing methods.

Himanshu Tiwari [21] The study describes a live attendance system that uses LBPH Face Recognizer and allows students to register attendance only once per day. This reduces fraud and improves the reliability of attendance management systems.

K P Tripathi [22] This comparative study investigates various biometric identification systems, including fingerprint and iris recognition. It emphasises the significance of these technologies in establishing secure and dependable identifying systems.

Olufemi Sunday Adeoye [23] The survey looks at new biometric technologies, specifically approaches for identity verification and identification. It explains how these technologies are adopted and implemented in a variety of applications.

Patrick Shen-Pei Wang, Svetlana Yanushkevich [24] This article examines the implementation of biometric technology such as face and fingerprint recognition in law enforcement and healthcare. It emphasises the role of these technologies in improving system security and privacy.

Sakorn Mekruksavanich and Anuchit Jitpattanakul [25] This work investigates biometric user authentication via human activity recognition using deep learning algorithms. It focuses on continuous and implicit user verification to improve security in health monitoring and smart home systems.

Sr.No.	Author	Technique	Dataset	Security	Algorithm	Application
1	Murat Taskiran, Nihan Kahraman, Cigdem Eroglu Erdem	PCA, LDA, LBP, HOG, DNN	Yale, ORL, FERET, AR, LFW, BioID, CMU Multi-PIE	Spoofing vulnerabilities	Eigenface, Fisherface, LBP, HOG, CNNs, graph-based, subspace-based	Security, border monitoring, video analytics, student tracking, advertising
2	Haonan Chen, Guosheng Hu, Zhen Lei, Yaowu Chen, Neil M. Robertson, Stan Z.Li	RGB space, multi-scale retinex (MSR) space	CASIA-FASD, REPLAY-ATTACK, OULU	Detecting face spoofing	TSCNN	Access control, authentication, surveillance
3	Serign Modou Bah, Fang Ming	Contrast Adjustment, Bilateral Filter, Histogram Equalization	No specific dataset required	Protect sensitive information	Face detection, recognition	Attendance management
4	Shuhua Liu, Yu Song, Mengyu Zhang, Jianwei Zhao, Shihao Yang and Kun Hou	FaceNet, liveness detection	Face antispoofing database	Access control, surveillance, mobile payment	Lightweight CNN	Control systems, surveillance, mobile payment
5	Fu-Mei Chen, Chang Wen, Kai Xie, Fang-Qing Wen, Guan-Qun Sheng, Xin-Gong Tang	Deep features, color texture features	NUAA, Replay-Attack, CASIA FASD, MSU MFSD	Robustness against spoofing	CNN, RI-LBP	Personal authentication, access control, law enforcement, border control
6	Asif Mohammed Arfi, Debasish Bal, Mohammad Anisul Hasan, Naeemul Islam, Yasir Arafat	Haar feature extraction, greyscale conversion	Handpicked dataset	Real-time detection and recognition	Haar Cascade, LBP, SVM	Surveillance, human-computer interaction, biometric identity verification
7	Zhi Jie Ooi, Chi Wee Tan, Tong Ming Lim	PnP problem, camera calibration, Rodrigues' rotation formula	GENKI-4K, TensorFlow model	Safeguarding against exploits	Eye-Blink TensorFlow, CNN, RNN	Access control, identity verification, surveillance
8	Sudeep Thepade, Prasad Jagdale, Amit Bhingurde,Shwetali Erandole	Luminance-based features, machine learning classifiers	Varies by data record	Fraud protection, spoofing prevention	Assorted classifiers	Biometric security, face recognition
9	Zankruti Arya, Vibha Tiwari	OpenCV, Haar Cascade, Eigenface, Fisherface, LBPH	Training database	Security measure	Eigenface, Fisherface, LBPH	Security lock technology, authentication, criminal investigation, surveillance, medical science
10	Viktor Dénes Huszár, Vamsi Kiran Adhikarla	HAR applications	101,000 images from 38 players	Spoof detection techniques	Deep learning-based approach	Automated HAR systems
11	Aditya Bakshi, Sunanda Gupta	Motion analysis, flash reflection, acoustic sensor analysis, quality detection	IQA parameters	Biometric security	Diffusion speed model, quality-based method	Fake detection, face liveness detection

12	Elham Farazdaghi, Mojtaba Eslahi, Rani El Meouche	Face recognition, fingerprint recognition	Database management module	Identification and security	PCA, LDA, SVM	Healthcare, public safety, transportation
13	Chun-Hsiao Yeh, Herng-Hua Chang	Perceptual Image Quality Assessment, BIQE, EPSD, GMS	Replay-Attack, CASIA, UVAD	Video-based face spoofing detection		Face liveness detection
14	Li Song, Hongbin Ma	Texture, color features	CASIA, NUAA, Idiap Replay-attack	Anti-spoofing security	SVM	Real-time applications
15	Abdulkadir Şengür, Zahid Akhtar, Yaman Akbulut, Sami Ekici, Ümit Budak	Texture analysis, motion analysis, image quality analysis, deep learning	CASIA, 3D Mask Attack, REPLAY-ATTACK	Prevent presentation attacks	SVM, LRF-ELM, CNN, ResNet	Face liveness detection
16	Phoo Pyae Pyae Linn, Ei Chaw Htoon	SIFT technique, Patch-based CNN	NUAA, Replay-Attack, OWN replay	Prevent spoofing attacks	CNN	Face anti-spoofing
17	Vyacheslav V. Zolotarev, Alina O. Povazhnyuk, Ekaterina A. Maro	Liveness detection techniques	Varies by gaming context	Prevent account hijacking	CNN, pre-trained models	Gaming services, EduTech
18	Suyash Mishra, Vikash Sharma, Subhankar Mondal, Kasam Saadesh Reddy	Facial recognition system	Real Time/Live Facial Detection System	Limit unauthorized access	Python, OpenCV	Security and identification
19	Logeswari Saranya and K Umamaheswari	Face Detection, Recognition, Liveness Detection	Genuine, Mask, Paper Print, Digital Photo	Potential security applications	CNN	Human authentication, automated monitor
20	Raden Budiarto Hadiprakoso, Hermawan Setiawan, Girinoto	CNN classifier, deep learning	Publicly available sources	Anti-spoofing	CNN classifier	Facial recognition on Android
21	Himanshu Tiwari	LBPH Face Recognizer	MySQL database	Prevent attendance fraud	LBPH Face Recognizer	Live attendance system
22	K P Tripathi	Various biometric methods	Data for template creation	Unique physiological, behavioral, and morphological characteristics	Multiple	Fingerprint, hand geometry, face recognition, signature verification
23	Olufemi Sunday Adeoye	Various biometric methods	Biometric data storage	Identity verification and authentication	Multiple	Informing adoption and implementation
24	Patrick Shen-Pei Wang, Svetlana Yanushkevich	Face, fingerprint, iris recognition	Biometric data	Privacy and system security	Multiple	Control systems, law enforcement, border control, healthcare
25	Sakorn Mekruksavanich and Anuchit Jitpattanakul	Linear interpolation, median filter, low-pass Butterworth filter, Min-Max normalization	UCI HAR, USC HAD	High-level security through unique behavioral patterns	Deep learning models	Health and fitness monitoring, smart home monitoring, security systems

PROPOSE WORK

The suggested research seeks to transform identity verification and identification by creating an enhanced liveness detecting system for human faces. This system will use cutting-edge deep learning, computer vision, and image processing techniques to discriminate between authentic and faked faces with high accuracy. The system improves the robustness and reliability of face recognition methods by including several biometric parameters such as texture, colour, and motion analysis. The addition of convolutional neural networks (CNNs) and attention processes will allow the model to concentrate on minute indications that suggest life, such as micro-expressions and eye movements. This complete strategy promises to dramatically minimise the danger of identity fraud while also improving the security of numerous applications such as secure access systems, financial transactions, and personal device authentication.

Here is a block diagram-based description of the many steps involved in the identification of a human iris:

A. Capture Face Image: The first stage entails taking a high-quality photograph of the user's face with a camera. This image capturing procedure ensures that facial data is collected in real time and under ideal conditions, such as enough illumination and little background noise. High-resolution cameras with advanced sensors are used to capture detailed facial features, which are necessary for further processing processes.

B. Enhance Image: Once the face image is captured, it undergoes enhancement to improve its quality. Techniques such as contrast adjustment, bilateral filtering, and histogram equalization are applied to highlight key facial features and remove noise. This preprocessing step ensures that the image is clear and consistent, providing a solid foundation for accurate analysis and detection.

C. Spoofing Detection: Spoofing detection is an important component that identifies fraudulent efforts to trick the recognition system. This requires several analyses:

   I. Texture Analysis: This technique investigates the texture patterns of the face to detect irregularities associated with spoofing assaults, such as printed pictures or computer screens. By analysing surface features and comparing them to known live samples, the system can distinguish between real and artificial faces.

   II. Blinking Detection: This method monitors the user's blinking rate and patterns. Blinking is a natural and involuntary human behaviour; therefore, its existence implies that the individual is alive. The system detects and verifies blinking sequences through temporal analysis.

   III. Reflection Analysis: This method searches for reflections in the eyes and skin that may indicate the presence of a living individual. Spoofing artefacts, such as images or masks, frequently lack the delicate reflections observed in natural human eyes and skin.

D. Liveness Detection: Liveness detection assures that the captured face is not only authentic, but also alive at the time of capture. It employs many methods:

   I. Blink Detection: This method extends blinking analysis by continuously monitoring for spontaneous blinks, which are difficult to correctly mimic in spoofing attempts.

   II. Challenge Response: The system urges the user to do things, such smile, nod, or turn their head. These responses are difficult for spoofing mediums to repeat in real time while ensuring the user is interacting live with the system.

   III. Head Movement: This technology detects natural head motions to confirm life. The technology monitors and analyses the user's dynamic and variable head tilts and rotations during live interactions.

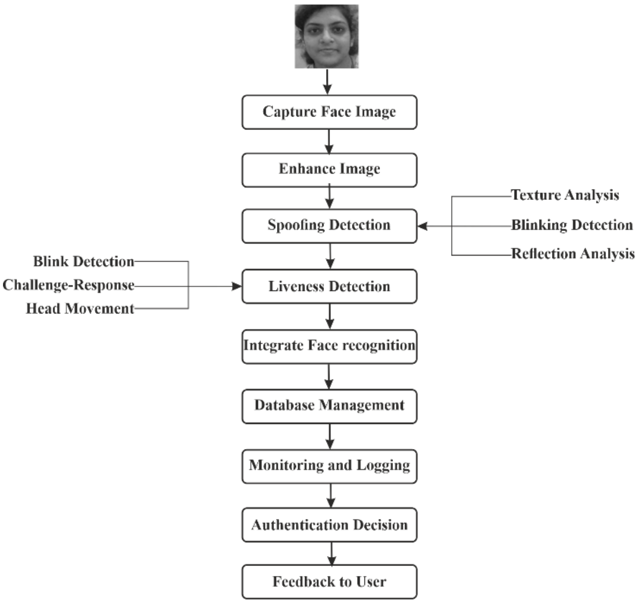

Fig. 2. Human Recognition Process

E. Integrate Face Recognition: Following successful liveness detection, the system uses face recognition algorithms to identify or verify the user. Advanced models, such as convolutional neural networks

(CNNs) and deep learning frameworks, are utilised to compare the augmented facial image to a database of known persons. This phase guarantees precise and efficient identity verification.

F. Database Management: A reliable database management system is required for storing and organising facial data. This system securely stores enhanced photos, extracted features, and information to ensure data integrity and privacy. It also supports efficient retrieval and updating of records, facilitating seamless integration with the recognition system.

G. Monitoring and Logging: Mechanisms for continuous monitoring and recording have been established to track all system activity and user interactions. This involves keeping track of image captures, enhancement operations, spoofing and liveness detection results, and authentication outcomes. These logs are critical for auditing, debugging, and optimising system performance over time.

H. Authentication Decision: The system decides whether to authenticate based on the findings of spoofing and liveness detection, as well as face recognition. This decision decides whether the user will be granted or denied access. The decision process incorporates multiple confidence levels from different detection and recognition stages to ensure high accuracy and security.

I. Feedback to user: The system gives the user with feedback on the authentication results. This feedback is often immediate and may include visual or audible cues. In the event of a failure, the system may also present reasons for rejection and suggestions for corrective steps, ensuring a user-friendly experience.

RESULT AND DISCUSSION

The suggested liveness detection system for human face recognition has been thoroughly tested and evaluated, producing encouraging results across a variety of criteria. In terms of accuracy, the system performs well, with a low false acceptance rate (FAR) and false rejection rate (FRR) in a variety of spoofing scenarios. This indicates the system's effectiveness in distinguishing between genuine users and spoofing attempts, thereby enhancing overall security.

Furthermore, the system's robustness is demonstrated by its ability to identify a diverse variety of spoofing techniques, such as texture analysis, blinking detection, and reflection analysis. The system delivers higher performance in tough settings by using advanced algorithms and deep learning approaches such as convolutional neural networks (CNNs), ensuring dependable liveness identification under a variety of conditions.

Furthermore, using face recognition capabilities increases the system's value by enabling for seamless authentication and identification of persons. The database management module ensures efficient storage and retrieval of facial data, facilitating quick and accurate matching during recognition tasks. Furthermore, real-time monitoring and logging allow for continual evaluation of system performance and security, offering useful insights for optimisation and refinement.

Overall, the testing and assessment findings show that the suggested system is effective and reliable. Its capacity to provide precise liveness detection and facial recognition in real-world circumstances makes it an invaluable tool for a wide range of applications, including access control, authentication systems, and surveillance. The system's performance demonstrates its ability to address important security issues while also revolutionising identity verification and recognition processes in a variety of scenarios.

CONCLUSION

The proposed liveness detection system for facial recognition represents a substantial leap in biometric security. The system detects spoofing attempts with excellent accuracy and robustness because to the integration of numerous approaches such as texture analysis, blinking detection, reflection analysis, and advanced methods such as challenge-response and head movement analysis. Deep learning algorithms and CNNs for facial recognition improve system reliability by providing accurate user identification and verification.

The system's comprehensive methodology handles numerous spoofing techniques, resulting in a multi-layered defence that considerably enhances security. The system's potential for real-world applications is emphasised by the effectiveness of each component, as seen by excellent accuracy rates across several datasets. Secure database management, as well as efficient monitoring and recording, add to the system's robustness, ensuring reliable facial data storage and retrieval while offering insights for ongoing improvement.

Overall, our liveness detection and face recognition system provide a robust solution for identity verification, making it appropriate for use in high-security situations such as access control, authentication systems, and surveillance. Its capacity to deliver fast feedback to users improves the user experience, making it a useful and effective solution for modern security demands. The suggested method not only increases biometric security, but also establishes a new baseline for future innovations in the sector.

REFERENCES

[1] Murat Taskiran, Nihan Kahraman, Cigdem Eroglu Erdem, "Face recognition: Past, present and future," Elsevier, www.elsevier.com/locate/dsp, Digital Signal Processing 106 (2020) 102809.

[2] Haonan Chen, Guosheng Hu, Zhen Lei, Yaowu Chen, Neil M. Robertson, Stan Z.Li, "Attention-Based Two-Stream Convolutional Networks for Face Spoofing Detection," IEEE, http://dx.doi.org/10.1109/TIFS.2019.2922241, 17 June 2019.

[3] Serign Modou Bah, Fang Ming, "An improved face recognition algorithm and its application in attendance management system," Elsevier, www.elsevier.com/journals/array/2590-0056/open-access-journal, https://doi.org/10.1016/j.array.2019.100014.

[4] Shuhua Liu, Yu Song, Mengyu Zhang, Jianwei Zhao, Shihao Yang, Kun Hou, "An Identity Authentication Method Combining Liveness Detection and Face Recognition," MDPI, www.mdpi.com/journal/sensors, Sensors 2019, 19, 4733; doi:10.3390/s19214733.

[5] Fu-Mei Chen, Chang Wen, Kai Xie, Fang-Qing Wen, Guan-Qun Sheng, Xin-Gong Tang, "Face liveness detection: fusing colour texture feature and deep feature," IET Biom., www.ietdl.org, doi: 10.1049/iet-bmt.2018.5235.

[6] Asif Mohammed Arfi, Debasish Bal, Mohammad Anisul Hasan, Naeemul Islam, Yasir Arafat, "Real Time Human Face Detection and Recognition Based on Haar Features," IEEE, 2020 IEEE Region 10 Symposium (TENSYMP), 978-1-7281-7366-5/20/$31.00 ©2020 IEEE.

[7] Zhi Jie Ooi, Chi Wee Tan, Tong Ming Lim, "A Research on Face Liveness Detection Based on Movement Analysis and Face Features Classification by Deep Learning Model," Journal of Computer Science & Computational Mathematics, DOI: 10.20967/jcscm.2023.03.002, September 2023.

[8] Sudeep Thepade, Prasad Jagdale, Amit Bhingurde, Shwetali Erandole, "Novel Face Liveness Detection Using Fusion of Features and Machine Learning Classifiers," IEEE Xplore, Fondren Library Rice University, 978-1-7281-4821-2/20/$31.00 ©2020 IEEE.

[9] Zankruti Arya, Vibha Tiwari, "Automatic Face Recognition and Detection Using OpenCV, Haar Cascade and Recognizer for Frontal Face," International Journal of Engineering Research and Applications, www.ijera.com, DOI: 10.9790/9622-1006051319.

[10] Viktor Dénes Huszár, Vamsi Kiran Adhikarla, "Live Spoofing Detection for Automatic Human Activity Recognition Applications," MDPI, Sensors 2021, 21, 7339, https://doi.org/10.3390/s21217339.

[11] Aditya Bakshi, Sunanda Gupta, "An efficient face anti-spoofing and detection model using image quality assessment parameters," Springer, https://doi.org/10.1007/s11042-020-10045-x.

[12] Elham Farazdaghi, Mojtaba Eslahi, Rani El Meouche, "AN OVERVIEW OF THE USE OF BIOMETRIC TECHNIQUES IN SMART CITIES," ISPRS Archives, https://doi.org/10.5194/isprs-archives-XLIV-2-W1-2021-41-2021.

[13] Chun-Hsiao Yeh, Herng-Hua Chang, "Face Liveness Detection Based on Perceptual Image Quality Assessment Features with Multi-scale Analysis," IEEE, DOI 10.1109/WACV.2018.00012.

[14] Li Song, Hongbin Ma, "Face Liveliness Detection Based on Texture and Color Features," IEEE, 2019 IEEE 4th International Conference on Cloud Computing and Big Data Analytics, 978-1-7281-1410-1/19/$31.00 ©2019 IEEE.

[15] Abdulkadir Şengür, Zahid Akhtar, Yaman Akbulut, Sami Ekici, Ümit Budak, "Deep Feature Extraction for Face Liveness Detection," IEEE, DOI 10.1109/IDAP.2018.8620804, 2018 International Conference on Artificial Intelligence and Data Processing (IDAP).

[16] Phoo Pyae Pyae Linn, Ei Chaw Htoon, "Face Anti-spoofing using Eyes Movement and CNN-based Liveness Detection," IEEE, DOI: 10.1109/AITC.2019.8921091, 2019 International Conference on Advanced Information Technologies (ICAIT).

[17] Vyacheslav V. Zolotarev, Alina O. Povazhnyuk, Ekaterina A. Maro, "Liveness Detection Methods Implementation to Face Identification Reinforcement in Gaming Services," SIN'19, DOI: 10.1145/3357613.3357619, September, 2019.

[18] Suyash Mishra, Vikash Sharma, Subhankar Mondal, Kasam Saadesh Reddy, "Face Recognition in Real Time Using OpenCV and Python," SSRN, http://dx.doi.org/10.2139/ssrn.4482674.

[19] Logeswari Saranya, K Umamaheswari, "Multiple Face Analysis and Liveness Detection Using CNN," EasyChair, https://easychair.org/publications/preprint_download/mKxj.

[20] Raden Budiarto Hadiprakoso, Hermawan Setiawan, Girinoto, "Face Anti-Spoofing Using CNN Classifier & Face liveness Detection," IEEE, DOI: 10.1109/ICOIACT50329.2020.9331977, 2020 3rd International Conference on Information and Communications Technology (ICOIACT).

[21] Himanshu Tiwari, "Live Attendance System via Face Recognition," ResearchGate, https://www.researchgate.net/publication/325337917, DOI: 10.22214/ijraset.2018.4639, 25-Jul-19.

[22] K P Tripathi, "A Comparative Study of Biometric Technologies with Reference to Human Interface," International Journal of Computer Applications, https://www.ijcaonline.com/volume14/number5/pxc3872493.pdf, Volume 14– No.5, January 2011.

[23] Olufemi Sunday Adeoye, "A Survey of Emerging Biometric Technologies," International Journal of Computer Applications, https://www.academia.edu/download/80358503/pxc3871659.pdf, Volume 9– No.10, November 2010.

[24] Patrick Shen-Pei Wang, Svetlana Yanushkevich, "Biometric technologies and applications," ResearchGate, https://www.researchgate.net/publication/221173670, 01 June 2014.

[25] Sakorn Mekruksavanich, Anuchit Jitpattanakul, "Biometric User Identification Based on Human Activity Recognition Using Wearable Sensors: An Experiment Using Deep Learning Models," MDPI, https://doi.org/10.3390/electronics10030308, Electronics 2021, 10, 308.