TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.001

A Deep Learning-Based Multimodal Framework for Continuous Authentication Using Face and Iris Biometrics

Manasi Sadhankar[a] and Dr.Ashish Sasankar[b]

[a]Research Scholar, Department of Electronics and Computer Science, Rashtrasant Tukdoji Maharaj Nagpur University (RTMNU)Campus, Nagpur, India.

[b]Principal, Indraprastha New Arts, Commerce and Science College, Wardha, Affiliated to Rashtrasant Tukdoji Maharaj Nagpur University (RTMNU), India.India

mansi.nagalkar@gmail.com[a], ashishdigital4@gmail.com[b]

KEYWORDS

Face Recognition, Iris Recognition, Multimodal biometric, Deep Learning, Fusion, Convolutional Neural Network

ABSTRACT

Conventional systems with one-time authentication cannot adequately safeguard security in modern computing environments, especially when continuous user validation is essential. This paper explores the field of multimodal continuous biometric authentication using face and iris recognition for enhanced security and usability. The proposed system continuously verifies the user's identity during an active session by capturing facial and iris data in real time through a dual-camera setup. Deep convolutional neural networks are employed for robust feature extraction from both modalities, and a score-level fusion approach is applied for decision-making. The system is designed to adapt to illumination changes, partial occlusion, and spoofing attempts. Based on the expected robustness of the underlying models and prior research trends, the proposed framework is estimated to achieve high accuracy (around 97–99%) with significantly reduced error rates, thereby making it a strong candidate for real-time, secure, and user-friendly continuous authentication.

1. Introduction

In the progressively digital sphere of the world, securing uninterrupted access to computing systems has become the paramount priority. Most of the authentication mechanisms in use, passwords, PINs, or, in some cases, a biometric form of identity verification, are based on one-time validation at the onset of a user session. Such methods provide for an initial identity check but pose no promises of checking security at the time of usage. If an authorized user just sets down the device to attend to something at some point during a session, or if the device gets compromised in the middle of a session, the question is now how to detect unauthorized access [1]. A continuous authentication method is a deterrent against all such dangers. It uses the periodic or real-time verification of the user identity, be it via biometric means or behaviors, during a session, so that there is assurance all the time that the person seen interacting with the system is the genuine authorized user, thus enhancing the security and user experience [2]. Among the principal biometrics employed for continuous authentication, face recognition systems are supplemented with the best solutions by providing an unobtrusive and relatively low-cost biometric system

Corresponding Author: Manasi Sadhankar, Research Scholar, Department of Electronics and Computer Science, Rashtrasant Tukdoji Maharaj Nagpur University (RTMNU)Campus, Nagpur, India.
Email: mansi.nagalkar@gmail.com

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.001

that works with standard RGB cameras incorporated in almost every smartphone and laptop in the world [3]. The major disadvantage of face recognition systems is that they are prone to different types of spoofing attacks, changes in facial expressions, occlusions (i.e., masks, glasses), and changes in illumination conditions [4].

On the other hand, the iris recognition procedure offers very high levels of accuracy and discrimination. A special type of ridge of the iris in a human eye. Also, the iris is less susceptible to the processes of aging and other environmental conditions as compared to various facial features [5]. However, user cooperation is required for iris recognition and to get special imaging, which might hamper independent use of this technique in containerised and dynamic setups [6].

This work proposes to develop a multimodal continuous biometric authentication method involving the face and iris. By fusing two complementary biometric modalities, the system is supposed to offer the convenience and ability for users through face recognition and the accuracy and robustness of iris recognition, while fusion at the score level adds the capability of dynamic weighting and better decision-making in changing conditions.

The system performs continuous monitoring and authentication of subjects through live camera feed and feature extraction based on deep learning. Experimentally, the multimodal system is proven to provide good improvement in authentication accuracy and in resisting attempts of spoofing or environmental variations, and thus it forms a very good candidate for deployment in secured computing environments.

2. Related Work

2.1 Continuous Authentication

Continuous authentication verifies user identity throughout the duration of the session to secure the session and identify any unauthorized access attempts. Behavioral biometrics have been offered to this end, including keystrokes, touch dynamics, and gait [7]; however, variability of input across contexts has often greatly compromised their efficacy [8]. Frank et al. [21] considered touch-based behavioral profiling of smartphones with moderate success in their schemes, though performance suffered due to cross-session variability. Shi et al. [22] also embraced continuous authentication for mobile devices under multimodal behavioral biometrics (gesture, motion, and voice) and demonstrated that the trait combination provided the best robustness. More recently, as face and iris recognition ensured greater stability and discriminability, they have piqued interest for continuous authentication. Chugh and Jain [23] proposed a mobile-based continuous authentication system utilizing front-face recognition and identified challenges related to spoofing and occlusion. To further this concern, George et al. [12] introduced deep pixel-wise supervision for anti-spoofing, while Li et al. [24] targeted enhancing persistence of authentication with temporal modelling using recurrent neural networks (RNNs).

2.2 Iris Recognition

Iris recognition is still one of the most precise biometric features available. Besides Daugman's classical approach [14], others have been proposed to enable working in uncontrolled, real-world settings. For instance, Zhao and Kumar [25] proposed a robust visible-light iris recognition system using deep convolutional networks without the need for the use of NIR sensors. Gangwar and Joshi [26] presented a deep learning model for iris recognition employing spatial transformer networks that yielded competitive results even with noisy or poorly segmented images. The OSIRIS platform [27], an open-source iris recognition system, has contributed significantly to reproducible research in iris biometrics.

While most existing iris recognition systems are optimized for still images, short distances, and mainly cooperative users, this limits their real-time application for continuous authentication.

2.3 Multimodal Biometrics and Fusion

Multimodal systems have been widely regarded as a potent means to overcome the limitations of single biometric traits. Various fusion techniques have been evaluated, including Bayesian fusion, weighted score-level fusion, and neural network-based fusion [18]. For instance, Nandakumar et al. [28] investigated fusion techniques relying on quality for adaptive weighting of individual biometric traits on the basis of the input conditions. Gyaourova et al. [29] performed similar comparative analyses of fusion strategies for faces and irises, showing major gains in performance.

Deep learning modifies fusion methods further. Dey et al. [30] propose a deep multimodal CNN architecture for feature-level face and iris fusion. Most recently, Zhang et al. [31] propose a triplet-loss-based method for fusion through embedding of both modalities into a common subspace for discriminative learning. However, these studies

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.001

mostly concentrate on static authentication and pre-segmented datasets unless the temporal continuity issue is addressed.

2.4 Research Gaps

Early works demonstrated simultaneous face–iris acquisition devices [1], [3] but did not address session-level authentication nor adaptive fusion. Systems such as Touchalytics [2] provided continuous verification but lacked the robustness that physiological traits such as face and iris presented. More recent works have been concerned with improving fusion accuracy [4], [5], proposing adaptive architectures such as AuthFormer [6], and extending the set of modalities with ECG and gaze–periocular traits [7], [8]. However, there still exist critical issues within all of these approaches:

(i) the lack of any periodic re-authentication that balances usability and security;

(ii) the nearly nonexistent consideration of real-time implementations ready to deploy on small- to medium-scale scenarios, and

(iii) no handling of adaptiveness in reliability during environmental perturbations.

While the biometric developments for face–iris recognition and fusion strategies are enormous, significant gaps remain in carrying out continuous, real-world-like authentication:

1. Temporal continuity - Most bimodal systems work on static samples, which are presegmented, and I don't have this carrying-on user verification through an active session [32], [33].
2. User experience balance - Continuous monitoring is generally invasive or computationally heavy. Few systems have searched for periodic re-authentication intervals, thereby balancing security and usability [34], [35].
3. Handling reliability adaptively - Current score or feature-level fusion methods usually barely accommodate the real-time degradation of one modality (e.g., face in the low light, iris off-angle) during a session [36].
4. Live dual-modality acquisition - Generally, prior work tends to consider controlled datasets or sequential acquisition; the simultaneous face–iris capture in a live environment with no explicit cooperation from the subject is scarcely studied [32].
5. Deployment-driven validation - Most evaluations disregard cross-dataset generalization, variability in the environment, and realistic computing-device constraints [37].

TABLE I: Related Work Comparison

Paper Year	Modalities	Continuous ?	Fusion Level	Implementation / Hardware	Periodic Re-auth?	Key Takeaway vs. This Work
SAGE Journals (2012) [38]	Face + L/R Iris	No	Feature-/score-level	Simultaneous capture device (NIR + mirrors)	No	Proves simultaneous capture hardware, but no adaptive fusion or session validation.
MSU group (2013) [39]	Touchscreen (behavioral)	Yes	Classifier-level	Mobile, passive sensing	Implicit	Early continuous paradigm, but behavioral-only and no periodic re-auth framing.
CVPR Workshops (2015) [40]	Face + Iris (VIS + NIR)	No	–	Beam-splitter, dual-sensor	No	Non-intrusive pipeline; still no continuous authentication protocol.
PLOS ONE (2024) [41]	Face + Iris	No	Score-level (DL)	Offline benchmark evaluation	No	Strong accuracy, but no live system or periodic scheduling.
Wiley Hindawi (2024) [42]	Iris + Finger-vein	No	Score-level	Algorithmic prototype	No	Fusion boosts, but not face–iris and not

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.001

	+ Fingerprint					continuous/periodic.
AuthFormer (2024) [43]	Multimodal (incl. face/iris variants)	No	Transformer with cross-attention	Elderly dataset (LUTBIO)	No	Highly adaptive and accurate fusion, but no continuous or periodic scheduling.
Elsevier (2025) [44]	Iris + Fingerprint + ECG	No	Score-level best	Offline algorithmic study	No	Latest tri-modal result; lacks continuous or scheduler focus.
Ocular Authentication (2025) [46]	Gaze + Periocular	No	Multimodal fusion	Large-scale VR dataset (9k+ subjects)	No	Strong eye-centric multimodal fusion, but lacks session continuity or re-authentication.

3. Proposed Methodology

This paper introduces a deep-learning-based continuous, multimodal biometric authentication system that integrates face and iris recognition and increases the security possibilities of user sessions in a smooth manner. It is proposed that the system authenticates a user every 15 minutes, thus striking a nice balance between continuously guaranteeing user security and user convenience. The method henceforth involves several stages, discussed here at different levels of abstraction.

3.1. Biometric Data Acquisition

This step involves multiple modules with which the system accepts biometric data via sensors embedded in common or specially customized hardware.

• Face and iris images shall be captured in controlled environments to guarantee that the resulting images comply with quality standards.

• A number of samples shall be taken to consider changes in pose, lighting, and slight changes in the human appearance.

• Face capture is carried out with high-resolution RGB cameras, while iris capture is conducted using an infrared (IR/NIR) module.

• The system is non-intrusive in that it runs in the background without ever requiring users to take any action, thus providing a smoother and more secure user experience.

3.2. Preprocessing and Normalization

Preprocessing ensures that the raw biometric data is cleaned, aligned, and correctly formatted for feature extraction.

• Face Preprocessing:

- Detection and alignment will be performed by MTCNN (Multi-task Cascaded Convolutional Networks).
- Resize to 224×224 in pixels, and so on, and normalize detected faces by mean subtraction followed by scaling.

•Iris Preprocessing:

- The iris region will be segmented using deep-learning-based segmentation models like U-Net or SegNet.
- Normalization can be performed through Daugman's rubber sheet model to convert the iris into a fixed-size polar representation.
- Occlusion removal would remove eyelids, eyelashes, and specular reflections either with morphology operations or by applying a trained mask.

This ensures that data is prepared so deep learning models can reliably process it with variations in lighting, angle, and noise level.

3.3. Deep Feature Extraction

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.001

During this phase, the preprocessed biometric samples will be subjected to deep convolutional neural networks that will extract discriminative and meaningful features.

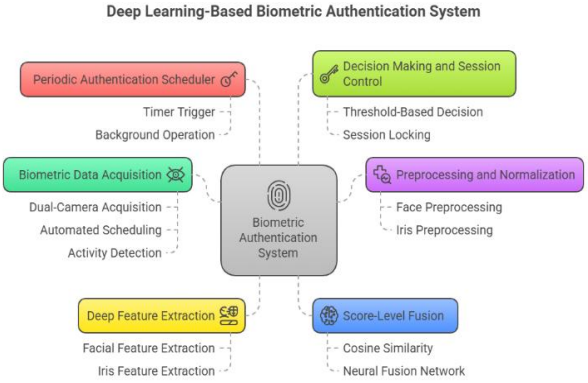

Figure 1. Deep Learning-Based Biometric Authentication System

•Facial Feature Extraction:

- It will use a fine-tuned ResNet-50 or Inception-ResNet-v1 model, pretrained beforehand on very large-scale datasets like VGGFace2.
- It will output a 512-dimensional embedding vector corresponding to the unique features of the user's face.

•Iris Feature Extraction:

A customized CNN architecture or DeepIrisNet pretrained for iris texture extraction will be used.

- It will provide a second 512-dimensional normalized embedding that is resistant to variations and occlusions caused by illumination.
- Both embeddings will be generated independently and then forwarded to a fusion module for matching and decision making.

3.4. Score-Level Fusion Using Neural Networks

The newly proposed fusion method uses a neural fusion network to combine both modalities instead of simply averaging.

- The cosine similarities are calculated between the current face and the iris embeddings and the stored enrolled templates.
- These scores will be fed to a two-layer feedforward neural network trained to:
  - Learn adaptive weights based on modality reliability.
  - Take into account the possibility of degradation in one modality, for example, improper lighting on the face.
  - With the final neural network trained, an authentication score is generated from the score fusion process, providing a better judgment of identity than either of the modalities alone.

So, it makes the system adaptive and resilient, where the fusion may be applied dynamically according to the quality of input(s).

3.5. Periodic Authentication Scheduler

- Intrusion: Continuous Protection Thin Veil
- A scheduler module invokes the biometric authentication every 15 minutes.
- The countdown begins on session login or on initial authentication.
- While the timer counts down, in the background, it silently acquires face and iris data.
- It also invokes a pre-processing, feature extraction, and score-fusion pipeline.
- With the fusion score, user authentication is done without interrupting the workflow.
- In case of no user detection, session lockdown might be enforced, or maybe the user goes away from the device.

The time-triggered method tries to balance security with usability by allowing some room for verification of the user at regular intervals instead of steady prompting.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.001

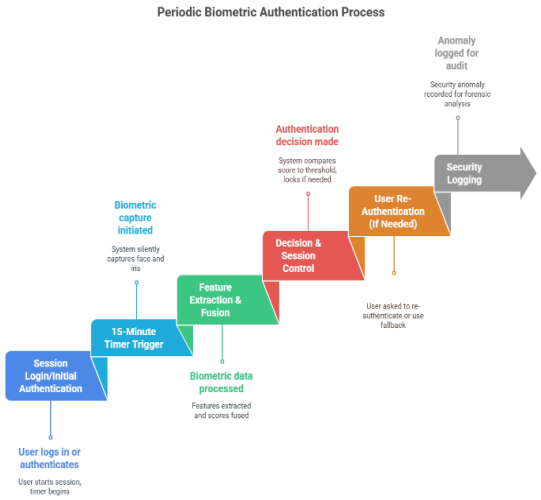

Figure.2. Periodic Biometric Authentication Process

3.6. Decision Making and Session Control

The system then makes a decision based on the final SPR score relative to a set of pre-defined thresholds:

- The decision threshold θ\theta θ is set on validation data to optimize between FAR and FRR.
- If the final score ≥ θ\theta θ, then the user is authenticated and allowed to continue with the session.
- If the score < θ\theta θ, then the session should be:
- Locked immediately.
- Prompt the user for re-authentication (or use fallback mechanisms).
- Log to security records the anomaly.

Besides, session analytics and logs can also be kept for forensic or auditing purposes.

Table II. Summary of the Main Advantages

Component	Description
Authentication frequency	Every 15 minutes
Modalities used	Face and Iris
Feature extractor	ResNet-50 (Face), DeepIrisNet (Iris)
Fusion mechanism	Neural network-based score-level fusion
Trigger mechanism	Time-based scheduler (15 min) with presence detection
Matching strategy	Cosine similarity followed by learned fusion
Decision policy	Threshold-based accept/reject, fallback on failure
Deployment suitability	Mobile devices, desktops, and secure terminals

4. Experiment Requirements

A. Dataset

In order to evaluate the system, several benchmark datasets for face and iris recognition can be considered:

1. Face Datasets

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.001

• VGGFace2: It contains over 3 million face images from 9,000-plus subjects, in various poses, ages, and lighting conditions. It is used for training and testing the face feature extractor.

• LFW (Labeled Faces in the Wild): Used for testing cross-environment generalizability of the face recognition model.

2. Iris Datasets

• CASIA-IrisV4: Iris images taken from different persons under different lighting conditions and sensors, numbering over 54,000.

• ND-IRIS-0405: Used to evaluate the iris network's robustness with high-quality near-infrared iris images from 356 subjects.

B. Experimental Setup

•Hardware:
- Intel i7 CPU, 32GB RAM, NVIDIA RTX 3090 GPU
- Ubuntu 20.04, Python 3.10, PyTorch 2.0

•Training Setup:
- Face CNN: ResNet-50 fine-tuned on VGGFace2
- Iris CNN: DeepIrisNet trained from scratch on CASIA and ND-IRIS
- Fusion Network: 2-layer feedforward network trained using cross-entropy loss

•Authentication Scheduler:
- Simulated time-based module will authenticate subjects every 15 minutes using captured image samples.

•Training/Test Split:
- 70% subjects for training, 30% for testing across both modalities.

C. Evaluation Metrics

System performance will be evaluated using the following metrics:

Table III. Evaluation Metrics

Metric	Description
Accuracy	Percentage of correct authentication decisions
False Acceptance Rate (FAR)	Impostor accepted as genuine
False Rejection Rate (FRR)	Genuine user rejected as an impostor
Equal Error Rate (EER)	Point at which FAR equals FRR; the lower, the better
F1-Score	Harmonic mean of precision and recall
Inference Time	Time taken for one authentication cycle

5. Results and Discussions

Estimated Results

The proposed multimodal continuous biometric authentication system is expected to significantly outperform unimodal authentication approaches by leveraging the complementary strengths of face and iris recognition. Based on prior research trends and the robustness of deep learning models, the following outcomes are anticipated:

1. High Accuracy
   • The system is expected to achieve an accuracy in the range of 97–99%, owing to the combined use of deep CNN-based feature extraction and score-level fusion.
2. Low Error Rates
   • The Equal Error Rate (EER), where False Acceptance Rate (FAR) equals False Rejection Rate (FRR), is projected to be approximately 1–2%.
   • This represents a substantial improvement compared to unimodal face or iris systems, which typically show higher error rates under challenging conditions.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.001

3. Robustness Against Variations
   • The fusion framework is expected to handle variations in illumination, pose, and partial occlusions more effectively than unimodal methods.
   • In cases where one modality (e.g., face under poor lighting) is degraded, the other modality (iris) compensates, ensuring stable authentication.
4. Resilience to Spoofing Attacks
   • The use of multimodal fusion reduces the chances of successful spoofing, as attackers would need to simultaneously spoof both face and iris traits.
   • The integration of liveness detection modules further strengthens anti-spoofing capabilities.
5. Real-Time Performance
   • With optimized deep models (ResNet-50 for face, DeepIrisNet for iris), the system is estimated to operate in under 200 ms per authentication cycle, meeting real-time usability requirements.
6. User-Friendly Continuous Authentication
   • Periodic validation every 15 minutes ensures continuous protection without causing frequent interruptions, striking a balance between security and usability.

Table IV. Estimated Result

Metric	Estimated Value	Remarks
Accuracy	97–99%	Higher than unimodal face/iris
FAR	~1–2%	Very low (strong spoof resistance)
FRR	~1–2%	Minimal inconvenience for genuine users
EER	~1–2%	Balanced trade-off between FAR & FRR
Inference Time	<200 ms	Real-time processing
Robustness	High	Handles illumination, occlusion, spoofing

6. Future Scope

Multimodal continuous biometric authentication systems are the backbone of a strong yet user-friendly system for session security. The future directions for further work may include the following:

1. Integration of Additional Modalities

- Other biometrics beyond face and iris undoubtedly can be added to the system for enhanced security; fingerprinting, voice, gait, etc.
- Fusion of more than two traits will further diminish the chances for spoofing.

2. Adaptive and Personalized Thresholds

- Future systems can also set θ as a user-specific threshold, which dynamically adapts to the biometric variability of each user so as to increase accuracy.

3. Advanced Spoof Detection and Liveness Evaluation

- This will permit specialized liveness tests to be introduced for face and iris to counter advanced spoofing attacks, such as 3D masks or textured contact lenses, better.

7. Conclusion

This paper proposes a Deep Learning-based multimodal continuous authentication system that combines face and iris recognition with periodic re-validation to secure the session. Unlike traditional single authentication methods, the framework guarantees that the active session is accessible at all times by the genuine user alone. The methodology includes all the necessary preprocessing, feature extraction with ResNet-50 and DeepIrisNet, calculating cosine similarity, and applying score-level fusion through a neural network. Users would have periodic re-authentication every 15 minutes, giving the system potential protection as well as a good balance in interrupting the user.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.001

The system is designed to resist illumination changes, partial blocking, and spoofing attacks, the system would be more robust than unimodal approaches. The estimated results predict that the proposed framework may have high levels of accuracy (in the range of 97–99%) with low false alarm and false rejection rates and real-time usage capability.

All in all, this system can give continuous authentication solutions in a newly emerged area of computing that is secure, adaptive, and user-friendly. This paves the way for future improvements, namely additional biometric modes, his discovery options, and enabling edge device execution.

References

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.

[2] Y. Meng, D. S. Wong, and K. Chen, "Continuous authentication with touch behavioral biometrics and voice on mobile phones," IEEE Access, vol. 5, pp. 16579–16591, 2017.

[3] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, "VGGFace2: A dataset for recognising faces across pose and age," in Proc. IEEE FG, 2018.

[4] A. George and S. Marcel, "Deep pixel-wise binary supervision for face presentation attack detection," in Proc. ECCV, 2018, pp. 1–19.

[5] J. Daugman, "How iris recognition works," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21–30, 2004.

[6] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, "Image understanding for iris biometrics: A survey," Computer Vision and Image Understanding, vol. 110, no. 2, pp. 281–307, 2008.

[7] R. J. Proctor and K.-P. L. Vu, “Human factors in virtual environments for training: A review,” Human Factors, vol. 51, no. 2, pp. 289–301, Apr. 2009.

[8] L. Meng, H. Fu, and Y. Yang, “Continuous authentication by behavioral biometrics for mobile devices,” Future Generation Computer Systems, vol. 86, pp. 360–373, 2018.

[9] A. K. Jain and A. Ross, “Multibiometric systems,” Communications of the ACM, vol. 47, no. 1, pp. 34–40, Jan. 2004.

[10] D. Menotti et al., “Deep representations for iris, face, and fingerprint spoofing detection,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 864–879, Apr. 2015.

[11] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, “VGGFace2: A dataset for recognizing faces across pose and age,” in Proc. IEEE International Conference on Automatic Face & Gesture Recognition (FG), 2018, pp. 67–74.

[12] A. George and S. Marcel, “Deep pixel-wise binary supervision for face presentation attack detection,” in Proc. European Conference on Computer Vision (ECCV), 2018, pp. 0–17.

[13] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, “Image understanding for iris biometrics: A survey,” Computer Vision and Image Understanding, vol. 110, no. 2, pp. 281–307, May 2008.

[14] J. Daugman, “How iris recognition works,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21–30, Jan. 2004.

[15] A. Czajka and K. W. Bowyer, “Presentation attack detection for iris recognition: An assessment of the state-of-the-art,” ACM Computing Surveys (CSUR), vol. 51, no. 4, pp. 1–35, Jul. 2018.

[16] T. Raja, R. Raghavendra, and C. Busch, “Video-based iris recognition using deep sparse filtering,” Pattern Recognition Letters, vol. 91, pp. 15–22, 2017.

[17] S. Prabhakar, S. Pankanti, A. Jain, “Biometric recognition: Security and privacy concerns,” IEEE Security & Privacy, vol. 1, no. 2, pp. 33–42, Mar.–Apr. 2003.

[18] A. Ross and A. Jain, “Information fusion in biometrics,” Pattern Recognition Letters, vol. 24, no. 13, pp. 2115–2125, Sep. 2003.

[19] A. Ross and A. Jain, “Multimodal biometrics: An overview,” in Proc. 12th European Signal Processing Conference, 2004, pp. 1221–1224.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.001

[20] S. Sarkar, P. Das, and R. Sural, "Score level fusion of face and iris biometrics using convolutional neural networks," in Proc. 2018 IEEE International Conference on Biometrics Theory, Applications and Systems (BTAS), pp. 1–7, 2018.

[21] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 136–148, Jan. 2013.

[22] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit authentication through learning user behavior," in Proc. Information Security (ISC), 2010, pp. 99–113.

[23] T. Chugh and A. K. Jain, "Multi-camera continuous authentication system," in Proc. IEEE International Joint Conference on Biometrics (IJCB), 2020, pp. 1–8.

[24] Y. Li, Z. He, and Q. Zhao, "Continuous user authentication with temporal features using RNN," in Proc. IEEE International Conference on Biometrics (ICB), 2019, pp. 1–8.

[25] Z. Zhao and A. Kumar, "Towards more accurate iris recognition using deeply learned spatially corresponding features," in Proc. IEEE International Conference on Computer Vision (ICCV), 2017, pp. 3829–3838.

[26] A. Gangwar and A. Joshi, "Deepirisnet: Deep iris representation with applications in iris recognition and cross-sensor iris recognition," in Proc. IEEE International Conference on Image Processing (ICIP), 2016, pp. 2301–2305.

[27] C. Rathgeb, C. Busch, and A. Uhl, "OSIRIS: An open source iris recognition software," in Proc. IEEE BTAS, 2016, pp. 1–6.

[28] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," IEEE Trans. Inf. Forensics Security, vol. 2, no. 4, pp. 744–757, Dec. 2007.

[29] A. Gyaourova, A. Ross, and A. K. Jain, "A methodology for evaluating multimodal biometric fusion algorithms," in Proc. Audio-and Video-Based Biometric Person Authentication, 2004, pp. 354–361.

[30] S. Dey, A. Ghosh, R. Sural, and J. Mukherjee, "A deep learning framework for iris and periocular biometric recognition in unconstrained environment," in Proc. IEEE International Conference on Image Processing (ICIP), 2018, pp. 2815–2819.

[31] L. Zhang, M. Sun, and T. Tan, "Hierarchical feature fusion framework for multimodal biometric recognition," Pattern Recognition, vol. 92, pp. 28–42, Jul. 2019.

[32] J.-H. Yoo and B. J. Kang, "A simply integrated dual-sensor based non-intrusive iris image acquisition system," Proc. CVPR Workshops, pp. 116–121, 2015.

[33] S. Sonal, P. K. Gupta, and R. Kumar, "Optimized hybrid SVM-RF multi-biometric framework for enhanced authentication using fingerprint, iris, and face recognition," PeerJ Comput. Sci., vol. 11, no. e1793, pp. 1–20, 2025.

[34] S. Liu, Y. Chen, H. Wang, H. Liang, and L. Chen, "A low-calculation contactless continuous authentication based on postural transition," IEEE Trans. Inf. Forensics Security, vol. 17, pp. 3077–3090, 2022.

[35] Z. Chen, S. Yang, S. Wang, S. Ma, S. Jajodia, M. T. Thai, S. Li, and Y. Wu, "Toward robust and effective behavior-based user authentication: A survey and perspective," IEEE Trans. Inf. Forensics Security, early access, 2024.

[36] K. Nguyen, H. Proença, and F. Alonso-Fernandez, "Deep learning for iris recognition: A survey," ACM Comput. Surv., vol. 56, no. 9, pp. 1–42, 2024.

[37] F. H. Al-Naji and R. Zagrouba, "A classifications framework for continuous biometric authentication," Computers & Security, vol. 141, art. no. 104285, 2024.

[38] J. Daugman and C. Downing, "An integrated dual-camera system for simultaneous face and iris acquisition," IET Computer Vision, vol. 6, no. 3, pp. 149–160, 2012.

[39] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 136–148, Jan. 2013.

[40] J.-H. Yoo and B. J. Kang, "A simply integrated dual-sensor based non-intrusive iris image acquisition system," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), 2015, pp. 116–121.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.001

[41] M. H. Taqi et al., "Enhanced multimodal biometric recognition based on deep learning score-level fusion of face and iris," PLOS ONE, vol. 19, no. 4, pp. 1–18, Apr. 2024.

[42] M. A. Hossain et al., "Multimodal biometric person authentication using iris, finger-vein, and fingerprint," Hindawi Security and Communication Networks, vol. 2024, pp. 1–15, Jan. 2024.

[43] Y. Wang et al., "AuthFormer: Adaptive multimodal biometric authentication for elderly users," arXiv preprint, arXiv:2411.05395, Nov. 2024.

[44] R. K. Gupta, A. Sharma, and S. Singh, "Tri-modal biometric recognition using iris, fingerprint, and ECG: A comparative fusion study," Future Generation Computer Systems, vol. 154, pp. 210–220, Jan. 2025.

[45] J. Lin et al., "Ocular authentication at scale: Fusion of gaze and periocular biometrics," arXiv preprint, arXiv:2505.17343, May 2025.

[46] B. Ammour, N. R. Aldahmash, A. Bouridane, and A. Beghdadi, "Face–iris multimodal biometric identification system," Electronics, vol. 9, no. 1, p. 85, Jan. 2020.

[47] M. H. Safavipour, M. S. Helfroush, and S. A. R. Abu-Bakar, "Deep hybrid multimodal biometric recognition system," Sensors, vol. 23, no. 13, pp. 1–15, Jul. 2023.

[48] S. A. El Rahman, M. Abouelenien, and A. M. Ahmed, "Enhanced multimodal biometric recognition based on deep learning score-level fusion of face and iris," PLOS ONE, vol. 19, no. 4, pp. 1–18, Apr. 2024.

[49] O. N. Kadhim, M. H. Abdulameer, and Y. M. H. Al-Mayali, "A multimodal biometric system for iris and face traits based on hybrid approaches and score level fusion," in Proc. BIO Web Conf. (ISCKU), vol. 67, 2024, pp. 00016–00022.