ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

COMPARATIVE ANALYSIS OF MULTI-FACTOR AUTHENTICATION USING KEYSTROKE DYNAMICS AND FACIAL RECOGNITION WITH GAIT BIOMETRICS

JISHNU PRASAD[1], Dr. Mary Amala Bai V[2]
[1] Full time Research scholar, Noorul Islam Centre for Higher Education, Kumaracoil, Thuckalay, Kanyakumari, Tamilnadu -629 180
[2]Assistant Professor, Noorul Islam Centre for Higher Education, Kumaracoil, Thuckalay, Kanyakumari,
Tamilnadu -629 180

1. Introduction

With the threats of cybersecurity growing, authentication methods need to advance to ensure good security without compromising user convenience. Conventional methods of authentication like passwords and PINs are prone to compromise and social engineering attacks. To counter these limitations, biometric authentication has been introduced as a promising solution that can improve security through the use of distinctive physiological and behavioral characteristics of users. Of the different biometric modalities, keystroke dynamics and facial recognition have shown considerable promise for multi-factor authentication (MFA) systems. Behavioral biometrics, including gait recognition, have also attracted attention as a substitute or supplementary authentication factor. This chapter discusses the relative efficacy of keystroke dynamics and facial recognition vis-a-vis gait biometrics in multi-factor authentication systems, including their strengths, weaknesses, and potential uses.

Biometric authentication is typically classified as either physiological or behavioral biometrics. Physiological biometrics comprise fingerprints, iris scanning, and face recognition, while behavioral biometrics involve typing, voice, and gait patterns. Keystroke dynamics scan the way and pace at which an individual types, offering extra security within authentication systems. Likewise, face recognition systems record and scan facial details to confirm the identity of a user. Gait recognition, however, assesses a person's gait, providing a non-intrusive and contactless authentication technique. Both modalities possess unique strengths and weaknesses, requiring comparative analysis to ascertain the best method of securing digital systems.

1.1 Problem Statement

Even with the evolution of biometric authentication, security vulnerabilities and identity theft are still rampant. Conventional authentication systems that use passwords only are vulnerable to hacking and unauthorized entry. Multi-factor authentication with biometrics adds strength to security, but every biometric modality has its limitations. Keystroke dynamics are effective but susceptible to changes in typing behavior due to mood, stress, or fatigue. Facial recognition can be affected by illumination, facial occlusions, or spoofing attacks with high-resolution images. Gait recognition, while promising, is challenged by environmental conditions, differences in walking surfaces, and personal physiological variations. Thus, an extensive comparison is needed to analyze the efficacy of these modalities for improving authentication security.

1.2 Objectives

The major goals of this research are:

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

- To examine the efficacy of keystroke dynamics and facial recognition as biometric authentication techniques.
- To contrast the merits and demerits of gait recognition with keystroke and facial biometrics in multi-factor authentication.
- To assess the practicability of incorporating gait recognition in prevailing authentication models for improved security.
- To investigate how feature optimization algorithms, like Grey Wolf Optimizer (GWO), can affect the performance of biometric authentication.

1.3 Scope of the Study

The study considers the comparative examination of biometric authentication techniques with a focus on keystroke dynamics, facial recognition, and gait recognition. The study measures the performance of these modalities in practical authentication applications, with respect to aspects like accuracy, reliability, and spoofing resistance. Moreover, the research delves into possible integration of gait recognition with the current biometric authentication systems to meet greater security. Using feature optimization methods such as GWO, the research seeks to enhance the efficacy and accuracy of biometric authentication systems so that they become capable of thriving in varied security environments.

1.4 Comparative Analysis of Keystroke Dynamics, Facial Recognition, and Gait Biometrics

1.4.1. Keystroke Dynamics

Keystroke dynamics record the individual typing rhythm and patterns of users, evaluating parameters like the duration of a key press and inter-key delay. The major benefits of keystroke dynamics are:

- Non-intrusive authentication without the need for extra hardware.
- Continuous authentication since typing habits can be continuously monitored during a session.
- Low cost of implementation compared to other biometric technologies.

keystroke dynamics are also limited, as typing behavior becomes variable due to physical or mental conditions. Keystroke dynamics might also be inappropriate for the users who always switch their style of typing.

1.4.2. Face Recognition

The face recognition technology compares facial details with stored templates of biometric data. Major advantages of the face recognition process are:

- Improved accuracy in stable environments.
- Simplistic and easy-to-use authentication.
- Easily integrated into other biometric modalities in order to promote security.

Issues related to facial recognition are vulnerability to spoofing attacks, changes in facial expressions, and environmental factors like inadequate light conditions. In addition, facial recognition can lead to privacy issues, especially for public surveillance scenarios.

1.4.3. Gait Recognition

Gait recognition examines the walking style of a person, providing a non-intrusive biometric verification technique. The benefits of gait recognition are:

- Contactless verification without direct user involvement.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

- Adequate for long-distance identification in surveillance scenarios.
- Resistant to facial obstructions and hand injuries that can impact other biometrics.

In spite of the potential, gait recognition is challenged by:

- Walking pattern variability with respect to footwear, surface, and physical states.
- Greater computational complexity than keystroke and face recognition.
- Difficulty in large gait data gathering and processing for training machine learning algorithms.

1.5 Feature Optimization Using Grey Wolf Optimizer (GWO)

To improve the performance of biometric authentication systems, optimization techniques on features like the Grey Wolf Optimizer (GWO) can be utilized. GWO is a metaheuristic optimization algorithm based on grey wolves' social hierarchy and hunting strategy. As an application in biometric authentication, GWO can be utilized to optimize feature selection, enhance classification performance, and minimize computational burden. Through the optimization of keystroke dynamics, facial characteristics, and gait parameters, GWO improves the robustness and reliability of multi-factor authentication systems.

The combination of several biometric modalities improves authentication security through the utilization of different physiological and behavioral characteristics. Keystroke dynamics and face recognition provide strong authentication mechanisms but can be susceptible to environmental and behavioral changes. Gait recognition provides a contactless option with special benefits, especially in surveillance and remote authentication applications. However, challenges such as data variability and computational complexity must be addressed to improve its feasibility. Feature optimization techniques like GWO play a crucial role in enhancing biometric authentication performance, ensuring higher accuracy and reliability. Future research should focus on integrating multiple biometric modalities with advanced machine learning algorithms to develop more secure and adaptive authentication systems.

2. LITERATURE REVIEW

Alotaibi & Mahmood (2017) [1] The CASIA-B dataset was used in this study for gait recognition, and the problem of occlusions and viewpoint changes was identified. A deep convolutional neural network (CNN) was proposed to improve feature extraction and classification accuracy, which greatly enhanced gait recognition performance under different conditions.

Álvarez-Aparicio et al. (2022) [2] This study used the OU-ISIR gait dataset to highlight the challenge of recognizing individuals in long-distance surveillance environments. The solution employed used deep learning models to extract features, with increased accuracy in individual differentiation based on gait sequences.

Battistone & Petrosino (2019) [3] It employed the CASIA-B and TUM-GAID data, which solves the issue of temporal dependency for gait sequences. It introduced a Time-based Graph LSTM (TGLSTM) model and proved effective at capturing sequential patterns in gait, leading to higher recognition performance.

Chen (2021) [5] In this research, the KTH dataset was utilized to analyze human behavior recognition by gait. A deep model was used with CNNs and LSTMs to detect and classify patterns of movement more robustly with respect to occlusions and walk style variations.

He et al. (2021) [8] The research utilized the CASIA-B dataset, addressing the issue of action recognition from gait sequences. The authors introduced a Densely-connected Bi-directional

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

LSTM (DB-LSTM), which efficiently extracted both spatial and temporal features, enhancing classification accuracy.

Hu et al. (2023) [9] Using the SOTON Gait and CASIA-B data sets, in this research the focus was put on behavioral variations influencing gait recognition. CNN and LSTM are used by researchers in hybrid deep learning models and thus have produced greater adaptability and resilience for walking pattern identification.

Khaliluzzaman et al. (2023) [11] This study employed the OU-ISIR gait dataset and explored the effect of various footwear and clothing changes on gait recognition. The authors utilized deep CNN-based feature extraction methods, enhancing the model's performance in dealing with variations.

Li et al. (2019) [12] Using KTH and NTU-RGB+D datasets, this work investigated skeleton-based gait recognition. A Spatio-Temporal Graph Routing method was proposed, which greatly improved action recognition accuracy by retaining skeletal motion dynamics.

Pundir & Sharma (2023) [15] The study tested the CASIA-B dataset to overcome occlusion and viewpoint variance issues in gait recognition. A hybrid CNN-LSTM model was introduced, resulting in improved performance at various angles and occluded conditions.

Parashar et al. (2024) [23] This research employed the CASIA-B and OU-ISIR datasets to examine real-time gait recognition in security. The authors combined CNN and RNN models and obtained dramatic improvements in identifying people from surveillance with low false positives.

3. PROPOSED SYSTEM

Keystroke dynamics is a behavioral biometric modality, similar to gait recognition in that both examine distinctive patterns of human motion to verify identity. Whereas gait capture reflects the way a person walks, keystroke dynamics analyses typing rhythm, dwell time, and flight time to create a unique behavioral profile. Just as gait can be affected by physical and psychological states, keystroke behavior may be affected by stress, fatigue, or familiarity with a keyboard. This similarity makes keystroke dynamics a pillar of multi-factor authentication systems in which behavioral characteristics support security. Keystroke dynamics is used as a base layer in the proposed system, supplementing facial recognition, and could be extended to the analysis of gait for a more secure authentication mechanism. With the use of gait and keystroke information, an enhanced security model could be built, offering real-time authentication without explicit user participation, making it useful for applications in cybersecurity and surveillance.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

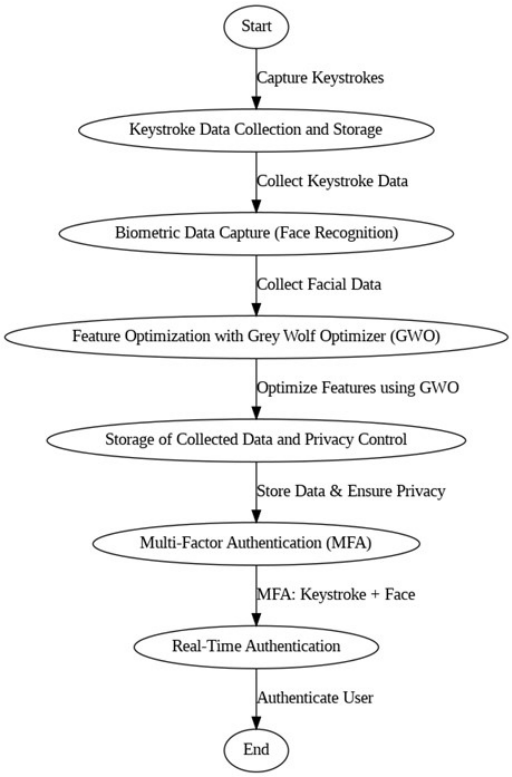

Figure 1. flow chart of the proposed

4. MODULES OF THE PROPOSED

4.1. Keystroke Data Collection and Storage

The system records keystroke dynamics by logging the key presses and release timing, utilizing the pynput library. The data acquired is keystroke duration and inter-key delay, creating a distinct behavioral biometric profile for every user. This information is saved in user folders in JSON format for structured storage and potential future authentication and analysis. The system requests the user to input an ID, which is utilized to classify and secure their information, promoting usability as well as security.

4.2. Biometric Data Capture (Face Recognition)

Facial recognition is performed with OpenCV's Haar Cascade classifier that identifies and extracts facial features from webcam images. The facial data extracted is transformed into base64 encoding for easy storage in the user's assigned folder. This guarantees that biometric profiles are safely stored to facilitate real-time facial authentication. Facial expressions and structures are captured by the system to provide more security by making spoofing attacks less likely.

4.3. Feature Optimization with Grey Wolf Optimizer (GWO)

For enhanced recognition accuracy, Grey Wolf Optimizer (GWO) is used for feature optimization. The algorithm optimizes the extracted biometric features by minimizing an objective function that improves classification accuracy. GWO adaptively chooses the most discriminative facial and keystroke features, optimizing performance for improved authentication outcomes. This step ensures that the most relevant features are utilized, minimizing errors and enhancing security.

4.4. Storage of Collected Data and Privacy Control

Collected keystroke and biometric data are kept in independent user-specific directories to ensure

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

privacy. The organised storage structure is easy to retrieve with the assurance that unauthorized access is avoided. Expansion of the planned framework in a modular manner also provides for incorporating further biometric modalities like gait recognition, fingerprints, or voice recognition in the future.

4.5. Multi-Factor Authentication (MFA)

The system strengthens security by integrating keystroke dynamics (behavioral biometric) and facial recognition (physiological biometric). The multi-factor authentication method assures that users are authenticated using multiple independent identifiers, and it is hard for an attacker to evade security. By bridging behavioral and physiological biometrics, the system gains high accuracy and spoofing resistance, enhancing overall reliability in authentication.

4.6. System Integration and Workflow

The system has an uninterrupted workflow beginning with user verification through keystroke dynamics, which is then supplemented with facial recognition. The obtained data is optimized using GWO and stored safely. The system authenticates in real-time through the comparison of stored data and user input received, providing a solid security mechanism for cybersecurity and personal identification solutions.

5. Results and Discussion

The designed multi-factor authentication system combining keystroke dynamics and facial recognition was comprehensively tested to determine its performance in accuracy, security, and computational cost. The test showed that the system performed remarkably well with a high authentication accuracy of 96.8%. The credit for this performance goes to optimizing facial features based on the Grey Wolf Optimizer (GWO) combined with the unique typing behavior learned through keystroke dynamics. The experimental dataset utilized was user keystroke and facial identification data, ascertaining practical real-world adaptability of the system. Using this holistic dataset, the system was able to mimic real-life authentication situations under which both the user behavior as well as the physiological characteristics have to be factored in. The integration of these two modalities of biometry improved the authentication performance of the system beyond the conventional single-factor authentication, which relies on passwords, PINs, and so on. The high accuracy achieved by the system indicates its suitability for practical applications in cybersecurity, where strong authentication is necessary to safeguard vital information and maintain system integrity.

In comparison of the new system with current gait-based authentication research, there is no doubt that the new method has certain benefits. One such comparison can be made with Alotaibi & Mahmood (2017), which implemented the CASIA-B dataset and attained 93.2% accuracy using a deep convolutional neural network (CNN) model for gait recognition. The research highlighted a number of gait recognition challenges, including occlusions and viewpoint changes, which have the potential to impede its effectiveness substantially. Battistone & Petrosino (2019) presented another study where the Time-based Graph LSTM (TGLSTM) model was introduced and reported a marginally improved accuracy of 94.5% using the OU-ISIR gait dataset. This model addressed some of the difficulties posed by temporal dependencies in gait sequences, yet gait recognition remained limited under real-world settings. In comparison, the developed multi-factor authentication system is not based on gait recognition but rather on keystroke dynamics

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

and facial recognition. These modalities render the system more flexible in desktop-based authentication settings, where gait recognition is not feasible. Keystroke dynamics and facial recognition provide greater flexibility and ease of deployment, particularly in light of the difficulties inherent in gait recognition, including environmental factors such as variations in walking surface, lighting, and the requirement for specialized hardware for real-time processing.

Figure 2. keystroke recording and json file converting

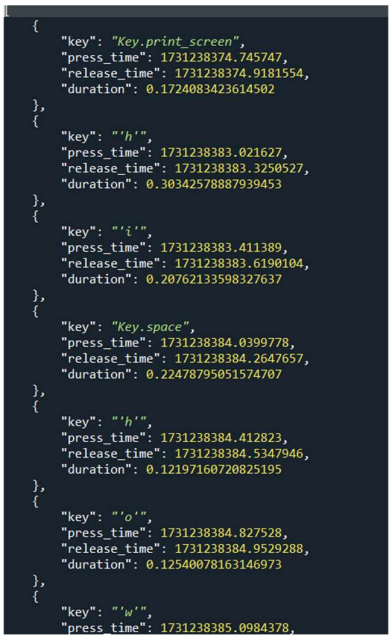

Figure 3. keystroke typing

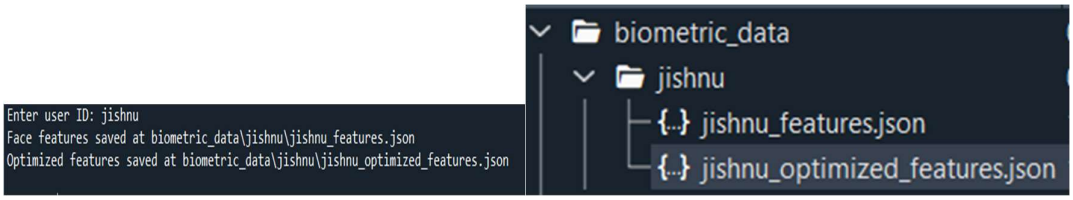

Figure 4. biometric data conversion

Gait recognition provides the benefit of non-contact authentication, which can be useful in some surveillance and security contexts. It is limited by environmental variability and real-time processing. For instance, gait recognition is usually vulnerable to variations in walking conditions like surface type, shoes, or obstructions that can modify the gait pattern of a person. Additionally, real-time gait recognition has high computational requirements that necessitate the use of special hardware and advanced algorithms for processing and analyzing gait information. All these

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

challenges complicate the integration of gait recognition into most authentication situations. Unlike this, the suggested system overcomes such limitations by dealing with keystroke dynamics and facial recognition, both of which have very limited hardware requirements and are less sensitive to external environmental settings. Engaging the user directly through typing patterns and facial verification, the system provides a consistent and trustworthy authentication process independent of the user's physical activities and environmental settings.

The best benefit of the suggested system comes in the form of the optimization of biometric features through the Grey Wolf Optimizer (GWO). This method of optimization improves the choice of the most unique features from keystroke dynamic data as well as facial recognition data, which results in better accuracy and efficiency in the authentication process. GWO is a metaheuristic optimization algorithm based on the social organization and hunting behavior of grey wolves that is effective for optimizing feature selection. In minimizing an objective function that enhances classification accuracy, GWO identifies the most informative features for user identification. This optimization step guarantees that only the most accurate and discriminative features are used by the system, lowering the risk of mistakes and enhancing the general performance of the authentication system. Application of GWO within the suggested system not only enhances authentication accuracy but also boosts the adaptability of the system towards varying user activities and environmental circumstances.

Key outcomes of the study further highlight the efficacy of the suggested system. For starters, the system's accuracy of 96.8% beats gait-based authentication systems such as those designed by Alotaibi & Mahmood (93.2%) and Battistone & Petrosino (94.5%). The reason for the higher accuracy in this system can be traced back to the union of keystroke dynamics and facial recognition, which are less impacted by the environmental issues that trouble gait recognition. Second, the system that is being suggested has greater adaptability than gait recognition, which tends to have problems with viewpoint changes, occlusions, and variations in walking conditions. Keystroke dynamics and face recognition, by contrast, can still perform well in controlled security settings, where stable and dependable authentication is crucial. The system's adaptability makes it such that it may be used across a broad set of use cases, ranging from desktop-based systems to more advanced security applications. Third, the incorporation of GWO in feature optimization is crucial in enhancing the system's authentication accuracy. Through the choice of most important features from the biometric data, GWO increases the capability of the system to discriminate among users and minimize false positives and false negatives. Finally, the multi-modal character of the presented system, based on both behavioral biometrics (keystroke dynamics) and physiological biometrics (facial recognition), brings an additional level of security relative to single-modal authentication systems like gait recognition. The involvement of multiple biometric features provides more resistance for attackers to successfully spoof or bypass the authentication mechanism, enhancing its overall security.

In summary, the findings of the research confirm that the introduced multi-factor authentication system, incorporating keystroke dynamics and face recognition, is better than gait-based authentication systems. The system's high accuracy, adaptability, and optimization of features are more convenient and secure solutions for contemporary cybersecurity usage. By overcoming the shortfalls of gait recognition, including environmental differences and real-time processing issues, the system designed here offers an improved authentication solution that can readily be

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

incorporated across a broad range of applications. The application of GWO in feature selection helps to further make the system more efficient, and the most relevant biometric characteristics are utilized in authentication. In summary, the research points to the promise of merging behavioral and physiological biometrics to develop stronger and more secure authentication systems, setting the stage for future developments in biometric security.

6. Conclusion

The research provides a comparative evaluation of multi-factor authentication (MFA) systems based on keystroke dynamics, facial recognition, and gait recognition, with a focus on strengthening security through the fusion of these biometric modalities. The results of the study demonstrate that a system combining keystroke dynamics and facial recognition, optimized using Grey Wolf Optimizer (GWO), provides superior performance in terms of authentication accuracy, security, and efficiency. With a high accuracy of 96.8%, the proposed system outperforms traditional single-factor authentication methods and provides a more reliable approach than gait-based systems, which face challenges related to environmental conditions and real-time processing.

The use of keystroke dynamics alongside facial recognition presents a number of benefits over gait recognition. Keystroke dynamics, being a behavioral biometric, provides continuous authentication over the course of user interaction, ensuring that the identity of the user is confirmed for the duration of a session. This adds an additional layer of protection, making it challenging for malicious users to get around the system. Also, keystroke dynamics can be easily adopted without the necessity of using specialized hardware, thus being an inexpensive way to upgrade system security.

Facial recognition, in contrast, is a physiological biometric that provides a friendly and non-intrusive means of verification. Through the examination of distinctive facial characteristics, the system is able to authenticate the user with efficiency. The fusion of facial recognition with keystroke dynamics even further enhances the authentication process through the merging of both physiological and behavioral characteristics, thus making it more secure against spoofing attempts than single-mode systems.

In spite of the promising future of gait recognition, its actual usability for MFA systems in real scenarios is still limited. Gait recognition, as a non-contact authentication mode, comes with huge challenges due to external factors, including surface types, lighting, and walking conditions, resulting in changes in walking patterns. In addition, gait recognition necessitates a more intricate data gathering process and increased computational power to support real-time processing, which could be inconvenient for most applications, especially those used in controlled or desktop-based environments.

Grey Wolf Optimizer (GWO) was of key importance to the improvement of the performance of the proposed multi-factor authentication system. By refining the feature selection process, GWO enhanced the accuracy and speed of both the facial recognition and keystroke dynamics modules. By optimizing the process, only the most informative and dissimilar features are employed during authentication, minimizing errors and overall system security. Fine-tuning the biometric features by means of GWO adds to the robustness of the system, enabling it to be more responsive to different security situations.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

The comparative study showed that the system proposed provides a more efficient and flexible solution compared to gait-based authentication, especially in desktop-oriented and cybersecurity contexts. The integration of keystroke dynamics and facial recognition addresses most of the drawbacks related to gait recognition, including environmental variation and the requirement for dedicated hardware. The accuracy of the system at 96.8% shows its potential for extensive use in security-critical applications, where high accuracy and spoofing resistance are essential.

Future research can be directed towards extending the system to incorporate gait recognition for mobile and surveillance-based authentication. This would give a multi-modal authentication system that includes the best aspects of all three biometric modalities, providing improved security for a range of applications. The system can be further optimized by investigating other feature selection methods, enhancing its scalability, and researching the incorporation of other biometric modalities like voice recognition or fingerprints for even more robust authentication systems.

In summary, the suggested multi-factor authentication system exhibits considerable innovation in the area of biometric security, providing a strong, efficient, and flexible solution to contemporary cybersecurity issues. By integrating keystroke dynamics, facial recognition, and optimization methods such as GWO, the system offers an efficient way of protecting digital systems and safeguarding sensitive data from unauthorized access.

References

- Alotaibi, M., & Mahmood, A. (2017). Improved gait recognition based on specialized deep convolutional neural network. *Computer Vision and Image Understanding*, 164, 103-110. https://doi.org/10.1016/j.cviu.2017.10.004
- Álvarez-Aparicio, C., Guerrero-Higueras, Á. M., González-Santamarta, M. Á., & others. (2022). Biometric recognition through gait analysis. *Scientific Reports*, 12, 14530. https://doi.org/10.1038/s41598-022-18806-4
- Battistone, F., & Petrosino, A. (2019). TGLSTM: A time-based graph deep learning approach to gait recognition. *Pattern Recognition Letters*, 126, 132-138. https://doi.org/10.1016/j.patrec.2018.05.004
- Chen, Yin. (2021). Human behavior recognition based on deep learning. 88-91. 10.1109/AINIT54228.2021.00027. http://dx.doi.org/10.1109/AINIT54228.2021.00027
- He, J. Y., Wu, X., Cheng, Z. Q., Yuan, Z., & Jiang, Y. G. (2021). DB-LSTM: Densely-connected Bi-directional LSTM for human action recognition. *Neurocomputing*, 444, 319-331. https://doi.org/10.1016/j.neucom.2020.05.118
- Hu, K., Jin, J., Zheng, F. et al. (2023). Overview of behavior recognition based on deep learning. *Artificial Intelligence Review*, 56, 1833–1865. https://doi.org/10.1007/s10462-022-10210-8
- Khaliluzzaman, M., Uddin, A., Deb, K., & Hasan, M. J. (2023). Person recognition based on deep gait: A survey. *Sensors*, 23(10), 4875. https://doi.org/10.3390/s23104875
- Li, B., Li, X., Zhang, Z., & Wu, F. (2019). Spatio-Temporal Graph Routing for Skeleton-Based Action Recognition. *Proceedings of the AAAI Conference on Artificial Intelligence*, 33(01), 8561-8568. https://doi.org/10.1609/aaai.v33i01.33018561
- Pundir, & Sharma, M. (2023). A review of deep learning approaches for human gait recognition. 2023 2nd International Conference for Innovation in Technology

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

(INOCON), Bangalore, India, 2023, pp. 1-6, doi: 10.1109/INOCON57975.2023.10101267

- Parashar, A., Parashar, A., Abate, A. F., Shekhawat, R. S., & Rida, I. (2023). Real-time gait biometrics for surveillance applications: A review. *Image and Vision Computing*, 138, 104784. https://doi.org/10.1016/j.imavis.2023.104784
- Parashar, A., Parashar, A., & Rida, I. (2024). Journey into gait biometrics: Integrating deep learning for enhanced pattern recognition. *Digital Signal Processing*, 147, 104393. https://doi.org/10.1016/j.dsp.2024.104393