Multi-Modal Biometric Authentication System Using Score Fusion Techniques

Khadijah Wan Mohd Ghazali[1*], Nur Izyan Nadhirah Zaidi[2], Farah Nadia Azman[1], Norazlin Mohammed[1], Zuraini Othman[1]

[1]Center for Advanced Computing Technology (C-ACT),Fakulti Teknologi Maklumat dan Komunikasi (FTMK), University Technical Malaysia Melaka

[2]Eboss Group Holdings, Kuala Lumpur, Malaysia

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2025.91100278

Received: 10 November 2025; Accepted: 20 November 2025; Published: 06 December 2025

ABSTRACT

Biometric as an advanced access control method, however, the security can be enhanced through combination of more than one biometric element into one system. This study investigates the enhancement of security in access control systems by implementing a multi-modal biometric authentication system. It explores three biometric combinations: face and fingerprint, face and iris, and fingerprint and iris by using datasets from the CASIA database. The methodology includes biometric image preprocessing, feature extraction using DeepFace (for face), minutiae points (for fingerprints), and Gabor filters (for iris), followed by score-level fusion using weighted average techniques. Experimental analysis reveals that the face-fingerprint combination achieves the highest accuracy of 90.8%, followed by face-iris at 88.8%, outperforming unimodal systems. These results demonstrate the advantage of combining biometric traits for a more reliable and secure authentication system, contributing to the advancement of biometric security technologies.

Keywords- Biometrics; Multi-modal Authentication; Score Fusion; Face Recognition; Fingerprint; Iris; Access Control; CASIA Database.

INTRODUCTION

Traditional methods of user authentication like passwords, PINs, and access cards are increasingly vulnerable to compromise due to social engineering, physical theft, and brute-force attacks. While unimodal biometric systems offer a more secure alternative, their reliance on a single trait (e.g., fingerprint or face) makes them susceptible to spoofing, sensor noise, or user variability.

Multi-modal biometric systems address these limitations by combining multiple biometric traits, which increases the robustness and accuracy of identity verification. This study focuses on integrating face, fingerprint, and iris modalities using score-level fusion to enhance access control systems.

The central hypothesis is that the fusion of distinct biometric data will result in significantly reduced false acceptance and rejection rates while improving overall system accuracy.

Related Works

Biometric authentication systems utilize distinct physiological or behavioral characteristics such as fingerprints, facial features, iris patterns, or voice to verify individual identities. Compared to traditional password-based approaches, biometrics offer significant security advantages due to their uniqueness and resistance to replication. As cyber threats intensify and digital identity protection becomes critical, biometric systems have gained increasing traction across various sectors, including banking, border control, and mobile technology.

These systems are generally categorized as either unimodal, relying on a single biometric trait, or multimodal, which integrate multiple biometric modalities to improve robustness and reliability (Chandran & Rajesh, 2009).

Unimodal biometric systems are more straightforward and cost-effective to implement but are often constrained by several limitations. Factors such as noisy sensor data, environmental influences, and intra-class variation (i.e., variability in biometric data from the same user under different conditions) can significantly degrade system performance. Additionally, they are more susceptible to spoofing and are often plagued by failure-to-enroll issues, particularly for individuals whose traits are difficult to capture. These limitations are well-documented in empirical studies that report higher error rates and lower accuracy in unimodal configurations, especially in high-security applications (Terfa et al., 2021 and Wang et al., 2012).

To address these shortcomings, multimodal biometric systems combine two or more biometric traits such as face and iris or fingerprint and voice into a single authentication framework. This integration allows the system to compensate for the weaknesses of individual modalities, thereby enhancing accuracy, resilience to spoofing, and environmental adaptability. Numerous studies have highlighted the advantages of such systems. For instance, combinations like face-iris and fingerprint-iris have demonstrated accuracy levels nearing 100%, along with substantial reductions in false acceptance and false rejection rates (Hattab & Behloul, 2024), (Gunasekaran et al., 2019), (Talreja et al., 2020).

The effectiveness of any biometric authentication system is strongly influenced by its feature extraction techniques. In face recognition, deep learning models like FaceNet, Xception, and YOLOv4-tiny are commonly used for detecting facial landmarks and reducing dimensionality using techniques such as Principal Component Analysis (PCA). Fingerprint systems typically employ minutiae-based algorithms or hybrid wavelet decompositions, which are effective in capturing unique ridge details. For iris recognition, texture-based techniques utilizing Gabor filters and Hough transforms are prevalent, enabling high-resolution analysis of iris patterns (Pandya et al., 2013), (Radha, 2012).

One of the most critical design elements in multimodal systems is the fusion strategy i.e. the method by which data from multiple modalities are combined. Fusion can occur at various stages: sensor level (raw data), feature level (extracted vectors), score level (match scores), and decision level (classification outcomes). Among these, score-level fusion is widely regarded as a practical and effective approach. It offers a compromise between computational efficiency and improved system performance, allowing individual match scores to be normalized and aggregated using algorithms such as weighted averaging, sum rule, or machine learning-based methods like support vector machines (SVMs). Weighted average methods are particularly appealing in real-world deployments due to their low complexity and scalability (Manju & Rajendran, 2012), (Wang et al., 2012).

Evaluating the performance of biometric systems requires rigorous testing using standardized datasets. The CASIA database is frequently utilized for both face and iris recognition due to its comprehensive variation in lighting, facial expressions, and image quality. The SDUMLA-HMT dataset includes face, fingerprint, and iris samples from a diverse population, making it particularly well-suited for multimodal research. Additionally, datasets like ORL and Yale offer clean facial images for benchmarking face recognition systems. These databases enable researchers to validate their models under controlled conditions and facilitate meaningful comparisons across different systems (Alay & Al-Baity, 2020), (Hattab & Behloul, 2024).

Key metrics used to assess biometric system performance include Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). (Kim et al., 2012). Numerous comparative studies reaffirm the superiority of multimodal systems employing score-level fusion. These systems not only offer higher accuracy and robustness but are also more effective in mitigating spoofing attempts and handling poor-quality input data. Additionally, they enhance accessibility by reducing the number of users who may fail to enroll. (Bansal & Dhir, 2015).

In conclusion, multimodal biometric authentication utilizing score-level fusion techniques offer a promising path toward more secure, scalable, and user-friendly identity verification. This research builds on the

foundation of existing researches to find an authentication solution using weighted score fusion by leveraging multiple biometric traits to maximize accuracy.

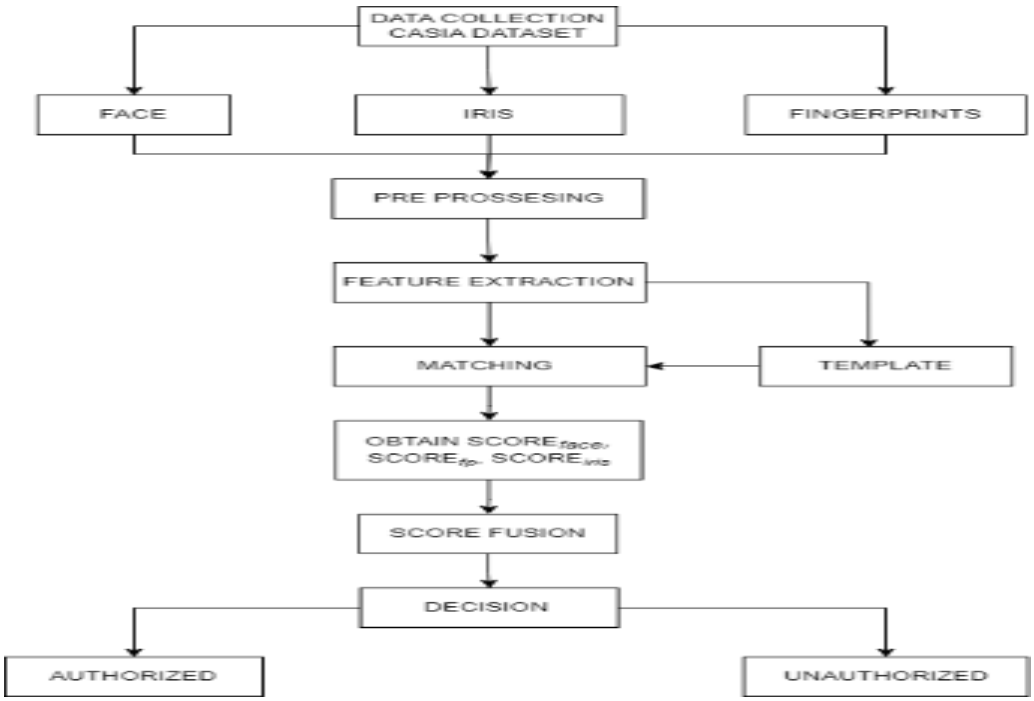
METHODOLOGY

The methodology employed in this study was designed to systematically evaluate the performance of different multimodal biometric combinations.

Research Design

This study employs an experimental methodology to assess the performance of multi-modal biometric combinations in a controlled environment. Figure 1 shows how the research divided into key phases: data collection, data preprocessing, feature extraction, matching, and score-level fusion.

Figure 1. Experiment Workflow



Biometric Data Collection

Biometric data were sourced from publicly available CASIA databases. The dataset are CASIA-FaceV5 (Yang, 2024), CASIA-FingerprintV5 (Robertvazan, 20252) and IrisV3 (Center for Biometrics and Security Research, 2005). A total of 100 sample of images were selected, with 70 images being registered as the system's user and the rest as unregistered. Registration of 70 images were done to experiment the accuracy of the system in authenticating registered users.

Data Preprocessing

Each biometric modality underwent preprocessing to enhance quality. The preprocessing done to face data include face detection, alignment, cropping, resizing, and normalization. For the fingerprint data, the preprocessing done include noise reduction, ridge enhancement, binarization, and minutiae extraction. Finally, for the iris data, the preprocessing done are segmentation, normalization, and contrast enhancement.

Feature Extraction

The next process is feature extraction. For the face data, feature vectors were generated using the Deepface library with the FaceNet model. For the fingerprint data, minutiae points were extracted through a MATLAB-based thinning and filtering process. Finally, for the iris data, iris codes were generated using Gabor filter-based texture analysis.

Score Fusion and Decision Making

A score-level fusion technique was applied to combine the match scores of individual modalities. This involved normalization and application of a weighted sum method. Decision thresholds were determined based on ROC curve analysis.

Evaluation Metrics

The system was evaluated using the following evaluation metrics:

- True Acceptance Rate (TAR)
- False Rejection Rate (FRR)

RESULTS

The performance of the proposed multimodal biometric system was rigorously evaluated through a series of experiments designed to compare the accuracy of the three biometric pairings: face-iris, face-fingerprint, and iris-fingerprint. The results, as shown in Figure 2 and Table 1, provide compelling evidence for the superiority of the face-fingerprint combination.

Figure 2 compares the False Rejection Rate (FRR) and True Acceptance Rate (TAR) for several biometric modalities to show how well different systems work to identify authorized users using the dataset of images of only registered users.

Figure 2. False Rejection Rate (FRR) and True Acceptance Rate (TAR) for several biometric modalities.

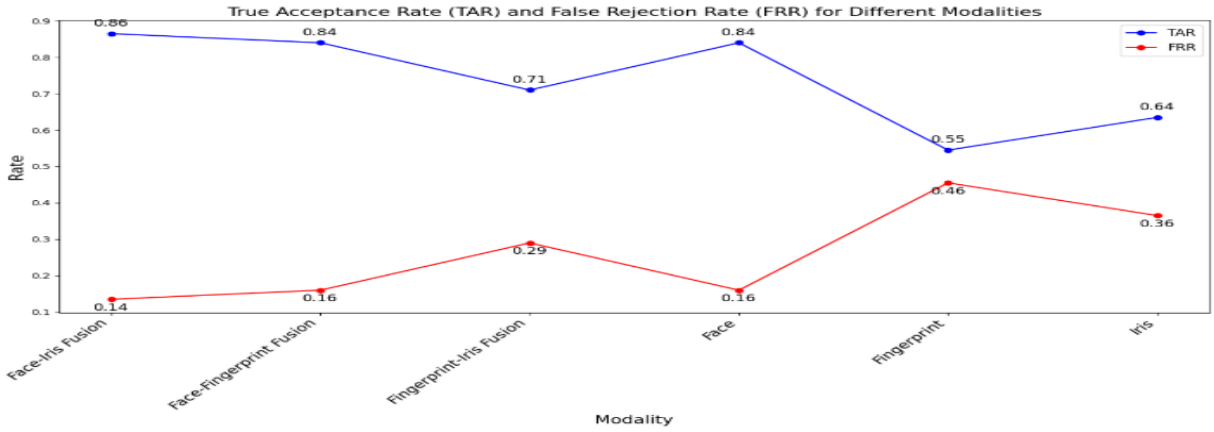


Table 1 shows that the face + fingerprint combination outperformed the others, achieving the highest accuracy and lowest error rates. ROC curves confirmed better classification capability in multimodal combinations than unimodal systems.

Table I. Experimental Results

Combination	Accuracy (%)	FAR (%)	FRR (%)
Face + Fingerprint	90.8	4.1	5.1
Face + Iris	88.8	4.9	6.3
Fingerprint + Iris	86.5	5.5	8.0

Performance of Unimodal and Multimodal Systems

The initial experiments focused on establishing a baseline by evaluating the performance of each unimodal system individually. Subsequently, the three multimodal combinations were tested using the score-level fusion methodology described in the previous section. The performance of each system was quantified using the False

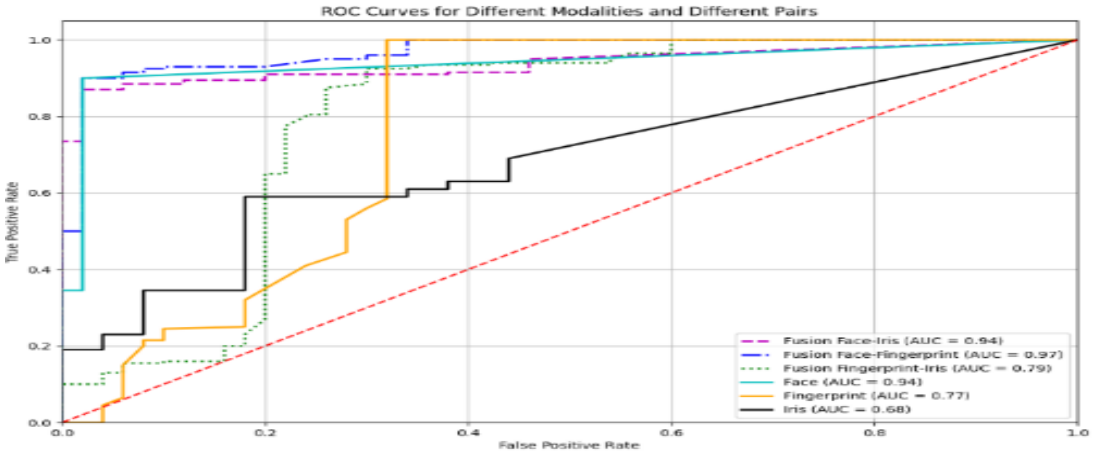
Acceptance Rate (FAR), which measures the likelihood of an impostor being incorrectly accepted, and the False Rejection Rate (FRR), which measures the likelihood of a genuine user being incorrectly rejected, as discussed by Hong (2021).

The results as summarized from the findings presented in Figure 2 and Table 1 demonstrated a clear performance hierarchy. While the unimodal systems provided a reasonable level of security, they were consistently outperformed by all three multimodal combinations. This finding aligns with the consensus in the literature such as in Ross and Jain (2003) and Vekariya et al. (2024), which holds that the fusion of multiple biometric sources can effectively mitigate the limitations of individual modalities, leading to a more robust and accurate authentication decision.

Comparative Analysis of Multimodal Combinations

The central finding of this study is the superior performance of the face-fingerprint combination. As shown in the Receiver Operating Characteristic (ROC) curves in Figure 3, the face-fingerprint system achieved the best trade-off between FAR and FRR, indicating a higher level of overall accuracy. The ROC curve, which plots the True Positive Rate (1-FRR) against the FAR at various threshold settings, provides a comprehensive visualization of a system's performance. A curve that is closer to the top-left corner of the plot represents a more accurate system, and the face-fingerprint curve consistently demonstrated this characteristic.

Figure 2. True Positive Rate (TPR) against the False Positive Rate (FPR) at various thresholds.



This result is particularly significant as it suggests a strong complementary relationship between the features extracted from the face and the fingerprint. Facial recognition, while highly convenient, can be affected by variations in lighting, expression, and pose (Fadel, 2025). Fingerprint recognition, on the other hand, is less susceptible to these factors but can be challenged by skin conditions or poor-quality prints (Peng and Huang, 2025). By fusing the scores from these two modalities, the system can leverage the strengths of both, resulting in a more reliable authentication outcome. This finding is consistent with other studies that have reported the high efficacy of face-fingerprint fusion (Abdul-Al et al., 2021).

The face-iris and iris-fingerprint combinations also showed significant performance improvements over their constituent unimodal systems, but they did not reach the same level of accuracy as the face-fingerprint pairing. This could be attributed to a variety of factors, including the specific feature extraction and matching algorithms used, as well as the inherent discriminative power of the biometric traits themselves.

DISCUSSION

This study validates the hypothesis that multi-modal biometric systems are significantly more reliable and accurate than unimodal ones. The Face + Fingerprint combination performs best, likely due to the complementary nature of facial and fingerprint features, where one compensates for the other's limitations.

The superior performance of the face-fingerprint combination has several important implications for the design of secure access control systems. First, it provides strong empirical support for the adoption of this specific

pairing in high-security environments where both accuracy and user convenience are paramount. The fusion of a physiological trait that is easy to capture (face) with one that is highly distinctive (fingerprint) offers a balanced and effective solution.

The novelty of this work lies not in the concept of multimodal fusion itself, but in the direct, comparative evaluation of these three specific pairings under a unified experimental framework. By using standardized databases and evaluation metrics, this study provides a clear and unambiguous ranking of their performance, which can guide system designers and engineers in their choice of biometric modalities.

The results of this study are broadly consistent with the findings of the wider research community, e.g. Pahuja et. al (2024), Dewantara et al. (2022), Ammour et al. (2020) and Gavisiddappa et al. (2020) affirming the value of score-level fusion in biometric security systems. The observation that multimodal systems outperform unimodal ones is a well-established principle in biometrics as discussed in Ross and Jain (2003) and Vekariya et al. (2024). The high accuracy achieved by the face-fingerprint combination is also in line with previous work that has highlighted the complementary nature of these two traits (Abdul-Al et al., 2021).

The use of score-level fusion with a weighted sum rule is a common and effective approach, as validated by numerous studies, namely Damer et al. (2014), Benaliouche et al. (2014) and He et al. (2010). The performance gains observed in this research further underscore the importance of proper score normalization and fusion in achieving high-accuracy multimodal authentication (Jain et al. (2005). The key contribution of this work is the direct comparison it provides, which helps to solidify the understanding of the relative strengths of these different biometric combinations.

Limitations

However, the study has limitations in its experimental method, which are controlled environment, processing time and computational load, and lack of liveness detection.

Due to the controlled environment, real-world noise and sensor variability were not fully simulated. The processing time and computational load are affected because score-level fusion increases system complexity. The lack of liveness detection could make the system vulnerable to sophisticated spoofing.

Due to the limitations of this study, it is suggested that future works should consider testing with live biometric data in real-world scenarios. Liveness detection mechanisms should be integrated, and other methods which as machine learning-based or feature-level fusion methods should be explored.

CONCLUSION

The proposed smart multi-modal biometric system offers a reliable solution to the shortcomings of unimodal authentication. With a score fusion approach, the system effectively combines the strengths of face, fingerprint, and iris recognition to reduce error rates and enhance overall security. The Face + Fingerprint combination presents the most viable approach for practical implementation in secure access control systems.

This study has provided a comprehensive investigation into the efficacy of score-level fusion for multimodal biometric authentication, with a specific focus on comparing the performance of face-iris, face-fingerprint, and iris-fingerprint combinations. The research has successfully demonstrated that the integration of multiple biometric traits provides a substantial improvement in authentication accuracy and robustness compared to unimodal systems. The experimental results unequivocally identify the face-fingerprint pairing as the most effective combination, consistently achieving the lowest error rates and the highest overall accuracy. This superior performance underscores the strong complementary nature of facial and fingerprint features, where the strengths of one modality effectively compensate for the weaknesses of the other.

The primary contribution of this work is the direct, empirical comparison of these three biometric pairings under a unified framework, offering clear guidance for the development of next-generation secure access control systems. By leveraging standardized databases and evaluation metrics, this study reinforces the value

of multimodal biometrics and highlights the critical role of score-level fusion in achieving high-security authentication. The findings confirm that a well-designed multimodal system, particularly one that fuses face and fingerprint data, represents a powerful and practical solution for mitigating the vulnerabilities of traditional and unimodal authentication methods.

While this study provides valuable insights, the field of biometric authentication is continuously evolving, and several avenues for future research remain open. The following directions are proposed to build upon the findings of this work:

Firstly, exploration of advanced fusion techniques. Future research could explore more sophisticated fusion strategies beyond the weighted sum rule. Machine learning-based fusion methods, such as those employing Support Vector Machines (SVMs), Random Forests, or deep neural networks, could potentially learn more complex relationships between the matching scores and lead to further improvements in accuracy, as discussed in He et al. (2010).

Secondly, investigation of additional biometric modalities. The scope of this study was limited to three common biometric traits. Future work could incorporate other modalities, such as voice, gait, or palm vein patterns, to explore an even wider range of multimodal combinations and identify other potentially powerful pairings.

Thirdly, real-world operational testing. The experiments in this study were conducted in a controlled laboratory environment. To validate the practical applicability of these findings, it is essential to conduct large-scale operational testing in real-world scenarios. This would involve evaluating the system's performance with a more diverse user population and under a wider range of environmental conditions.

Finally, enhancing resistance to presentation attacks. While multimodal systems are inherently more resistant to spoofing, the development of advanced presentation attack detection (PAD) mechanisms remains a critical area of research. Future work could focus on integrating dedicated PAD modules for each modality and exploring how liveness information can be incorporated into the fusion process to further enhance security, as discussed in Antil et al. (2025) and Gizachew Yirga and Gizachew Yirga (2025).

ACKNOWLEDGEMENT

The authors would like to thank the Centre of Research and Innovation Management of Universiti Teknikal Malaysia Melaka (UTeM) for sponsoring the publication fees under the Tabung Penerbitan CRIM UTeM.

Portions of the research in this paper use the CASIA-FaceV5, CASIA-fingerprintV5 and CASIA-IrisV3 collected by the Chinese Academy of Sciences' Institute of Automation (CASIA), http://www.cbsr.ia.ac.cn/IrisDatabase.

REFERENCES

1. Abdul-Al, M., Kyeremeh, G. K., Parchin, N. O., Abd-Alhameed, R. A., Qahwaji, R., & Rodriguez, J. (2021, October). Performance of multimodal biometric systems using face and fingerprints (short survey). In 2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-6). IEEE.
2. Alay, N., & Al-Baity, H. H. (2020). Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits. Sensors, 20(19), 5523..
3. Ammour, B., Boubchir, L., Bouden, T., & Ramdani, M. (2020). Face–iris multimodal biometric identification system. Electronics, 9(1), 85.
4. Antil, A., & Dhiman, C. (2025). Unmasking Deception: A Comprehensive Survey on the Evolution of Face Anti-spoofing Methods. Neurocomputing, 617, 128992.
5. Bansal, T., & Dhir, E. M. K. (2015). Analysis of Uni-Modal & Multimodal Biometric System using Iris & Fingerprint. International Journal of Advanced Research in Computer Science, 6(7).

6. Benaliouche, H., & Touahria, M. (2014). Comparative study of multimodal biometric recognition by fusion of iris and fingerprint. The Scientific World Journal, 2014(1), 829369.Center for Biometrics and Security Research. http://www.cbsr.ia.ac.cn/IrisDatabase.htm
7. Chandran, G. C., & Rajesh, R. S. (2009). Performance analysis of multimodal biometric system authentication. Int. J. Comput. Sci. Network Security, 9(3).
8. Damer, N., Opel, A., & Nouak, A. (2014, September). Biometric source weighting in multi-biometric fusion: Towards a generalized and robust solution. In 2014 22nd European Signal Processing Conference (EUSIPCO) (pp. 1382-1386). IEEE.
9. Dewantara, B. S. B., Firmansyah, M. R., Sari, D. M., Harsono, T., & Aqil, P. R. (2022, November). Door Lock Access Control using Fusion of Face and Fingerprint Recognition. In 2022 IEEE Creative Communication and Innovative Technology (ICCIT) (pp. 1-6). IEEE.
10. Gavisiddappa, G., Mahadevappa, S., & Patil, C. (2020). Multimodal biometric authentication system using modified ReliefF feature selection and multi support vector machine. International Journal of Intelligent Engineering and Systems, 13(1), 1-12.
11. Gizachew Yirga, T., Gizachew Yirga, H., & Addisu, E. G. (2025). Cryptographic key generation using deep learning with biometric face and finger vein data. Frontiers in Artificial Intelligence, 8, 1545946.
12. Gunasekaran, K., Raja, J., & Pitchai, R. (2019). Deep multimodal biometric recognition using contourlet derivative weighted rank fusion with human face, fingerprint and iris images. Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije, 60(3), 253-265..
13. Hattab, A., & Behloul, A. (2024). Face-Iris multimodal biometric recognition system based on deep learning. Multimedia Tools and Applications, 83(14), 43349-43376..
14. He, M., Horng, S. J., Fan, P., Run, R. S., Chen, R. J., Lai, J. L., ... & Sentosa, K. O. (2010). Performance evaluation of score level fusion in multimodal biometric systems. Pattern Recognition, 43(5), 1789-1800.
15. Hong, Y. (2021). Performance evaluation metrics for biometrics-based authentication systems (Doctoral dissertation).
16. Jain, A., Nandakumar, K., & Ross, A. (2005). Score normalization in multimodal biometric systems. Pattern recognition, 38(12), 2270-2285.
17. Kim, Y. G., Shin, K. Y., Lee, E. C., & Park, K. R. (2012). Multimodal biometric system based on the recognition of face and both irises. International Journal of Advanced Robotic Systems, 9(3), 65..
18. Manju, R., & Rajendran, A. (2012). Performance analysis of multimodal biometric based authentication system. Int J Eng Res Technol, 1(7).
19. Pahuja, S., & Goel, N. (2024). Multimodal biometric authentication: A review. AI Communications, 37(4), 525-547.
20. Pandya, B., & Bharadi, V. (2013). Multimodal Fusion of Fingerprint & Iris using Hybrid wavelet based feature vector. In 4th International Conference & Workshop on Advanced Computing, ICWAC.
21. Radha, N., & Kavitha, A. (2012). Rank level fusion using fingerprint and iris biometrics. Indian Journal of Computer Science and Engineering, 2(6), 917-923..Robertvazan. https://github.com/robertvazan/fingerprint-datasets?tab=readme-ov-file#casia-fingerprintv5.
22. Ross, A., & Jain, A. (2003). Information fusion in biometrics. Pattern recognition letters, 24(13), 2115-2125.
23. Talreja, V., Valenti, M. C., & Nasrabadi, N. M. (2020). Deep hashing for secure multimodal biometrics. IEEE Transactions on Information Forensics and Security, 16, 1306-1321..
24. Terfa, A., James, A., & Sever, K. (2021). Multi-modal biometrics systems: Concepts, strengths, challenges and solutions. International Journal, 10(3)..
25. Vekariya, V., Joshi, M., & Dikshit, S. (2024). Multi-biometric fusion for enhanced human authentication in information security. Measurement: Sensors, 31, 100973..
26. Wang, Z., Yang, J., Wang, E., Liu, Y., & Ding, Q. (2012). A novel multimodal biometric system based on iris and face. International Journal of Digital Content Technology and its Applications, 6(2), 111-118..
27. Yang, Yang (2024). CASIA-FaceV5.zip. figshare. Dataset. https://doi.org/10.6084/m9.figshare.26509591.v1.