Anusandhanvallari
Vol 2025, No.1
January 2025
ISSN 2229-3388

A Data Mining–Based Multimodal Biometric Authentication System for Secure Access Control

[1]Dr. Shweta Shirpurkar, [2]Dr. Diwakar Ramanuj Tripathi

[1]HOD & Assistant Professor Department of Computer Science, Mohota Science College, Nagpur

shwetashirpurkar20@gmail.com

[2]HOD & Assistant Professor Department of Computer Science, S.S. Maniar College of computer & Management, Nagpur

drtcomptech@live.com

Abstract: The rising need to have safe and trustworthy access control systems has increased the rate at which biometric authentication systems are being adopted. Unimodal biometric systems are however usually plagued with limitations like noise, intra-class variations and spoofing attacks. In order to overcome these obstacles, this paper presents the suggested multimodal biometric authentication system based on data mining; the system combines fingerprint, face, and iris modalities through feature-level and score-level fusion. The evaluation of the system performance based on the conventional measures of biometrics was an experiment based on the following measures: accuracy of authentication, False Acceptance Rate (FAR), False Rejection Rate (FRR), system reliability, and acceptance of the system by its users. Results of the experiment indicate that the suggested multimodal system has a great accuracy of authentication of 98.2% with much lower FAR (0.9) and FRR (1.3) than unimodal systems. Moreover, the system is highly reliable (96.9%) and is well accepted by the users (95.4%), which proves its strength and practicability. The results indicate that the pattern of using a combination of several biometric characteristics plus data mining methods are effective in increasing the security, accuracy, and general system efficiency, which implies the framework of correlation to the actual secure access control systems.

Keywords: *Multimodal Biometric Authentication, Data Mining, Secure Access Control, Feature-Level Fusion, Score-Level Fusion, FAR, FRR.*

1. INTRODUCTION

In recent years, the accelerated development of digital systems and delicate exchange of information has augmented the need to have robust and dependable access control systems. The conventional authentication systems like passwords, personal identification numbers, and access cards are limited with failure to forget, theft, and susceptibility to unauthorized access. One of the promising alternatives has been biometric authentication which uses some unique physiological features of individuals. Nevertheless, unimodal biometric systems that rely on one trait usually have problems with data acquisition noise, intra-class variability, and vulnerability to spoofing, so tend to undermine the security and accuracy of the system.

To address these drawbacks, multimodal biometric authentication systems incorporate more than one biometric characteristic (fingerprint, face and iris) to increase the reliability and security of recognition. Multimodal systems used together with data mining methods can effectively process large biometric data and optimize features selection and enhance classification accuracy using smart pattern recognition and decision making algorithms.

In this paper, a multimodal biometric authentication system is suggested as a data mining-based system to ensure secure access control, with the emphasis placed on the combination of biometric traits via feature-level

and score-level fusion approaches. The approach proposed will strive to attain greater accuracy in authentication, reduced false acceptance and rejection as well as increased reliability of the system. The system is also highly applicable in the real-world by providing greater protection and ease of use, which makes the system applicationable in the high security context of banking systems, healthcare facilities, and critical infrastructure protection.

2. LITERATURE REVIEW

Coelho et al. (2023) presented a multimodal biometric authentication approach using federated learning to improve security without infringing on the privacy of data. In their work, they concentrated on the joint training of several biometrics indicators in a decentralized learning model, enabling the models to be trained without involving raw biometric information. The findings showed that the authentication accuracy and strength were better than in the traditional centralized methods, especially in the applications that involved privacy.

Fathima and Saravanan (2024) investigated cloud user access control basing on behavioral biometric-based authentication and continuous monitoring measures. Their work pointed out the significance of the dynamic authentication mechanism in the cloud environment through user behavior analysis aimed at enhancing security. According to the study, the detention of illicit access attempts and system adaptability were better.

Kolluri et al. (2024) performed a thorough review of multimodal biometric authentication systems based on artificial intelligence and machine learning methods. Their study compared different neural network designs to enhance feature extraction, fusion and classification in mutilimodal settings. The results showed that AI-based models were able to boost the accuracy in authentication and minimized the number of errors than traditional approaches.

3. RESEARCH METHODOLOGY

This study paper uses an experimental design to test a multimodal biometric authentication system that is based on data mining and combines fingerprint, face and iris data by feature level and score level fusion. Quantitative performance measures, including accuracy of authentication, FAR, FRR, reliability of the system, and system acceptance between unimodal and multimodal methods are compared.

3.1 Research Design

This study adheres to the experimental research design in order to test a multimodal biometric authentication system based on data mining to ensure secure access control. Quantitative measures are used to determine the performance of the system in terms of accuracy in authentication, False Acceptance Rate (FAR), False Rejection Rate (FRR) and the reliability of the system.

3.2 Dataset and Biometric Modalities

The testing of the proposed system involved a benchmark biometric dataset of fingerprint, face and iris modalities. These biometric characteristics were chosen because of their reliability and complementation nature. Several samples were taken on each person to compensate the differences in the condition of biometric acquisition.

3.3 Feature Extraction and Multimodal Fusion

Preprocessing measures were used to improve the quality of biometric data and afterwards feature extraction. The extractive process was carried out on discriminative features by each modality individually and optimized by means of data mining. The system uses feature level fusion to integrate biometric features and score level fusion to integrate matching scores, which enhance system recognition accuracy and robustness.

3.4 Classification and Authentication Process

The fused biometric features were subjected to data mining-based classifiers to undertake authentication. The eventual conclusion was based on the comparison of the matching score that had been combined against a predetermined threshold. This method is the best way to achieve a compromise between the security and usability since the false acceptance and false rejection errors are minimized.

3.5 Performance Evaluation Metrics

The system performance was assessed in terms of a standard biometric measure, such as accuracy of authentication, FAR, FRR, reliability of the system, and acceptance rate by the user. A comparative study was made between the unimodal and multimodal systems and results were illustrated using tables and graphs.

4. RESULT AND DISCUSSION

The effectiveness of the suggested data mining based multimodal biometric authentication system was assessed by several biometric characteristics combined at features and score-level fusion. The system was validated using a benchmark dataset that contained fingerprint, face and iris modalities data. Common performance measures like accuracy of authentication, False Acceptance Rate (FAR), False Rejection rate (FRR) and overall system reliability were evaluated to determine the success of the proposed model.

4.1 Authentication Accuracy Across Biometric Modalities

Table 1 shows the accuracy of authentication using each of the biometric modalities, which are fingerprint, face, and iris, and compares them to the suggested multimodal biometric authentication system.

Table 1: Authentication Accuracy of Biometric Modalities

Biometric Modality	Accuracy (%)
Fingerprint	92.4
Face	89.1
Iris	94.6
Proposed Multimodal System	**98.2**

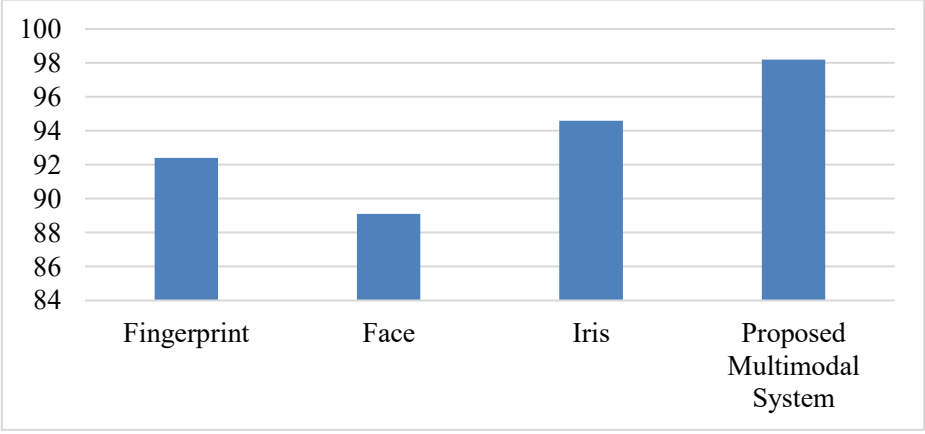

Figure 1: Graphical Representation of Authentication Accuracy of Biometric Modalities

The results show that every one of the unimodal biometric systems offers relatively high accuracy, but the accuracy of the proposed multimodal system is the highest (98.2%). This enhancement shows that the use of multi-modal biometric traits with data mining methods is effective in improving recognition accuracy by counterbalancing the weaknesses of a single modality, and increasing the overall accuracy in the decision.

4.2 Security Performance: FAR and FRR Analysis

Table 2 presents a summary of the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) of unimodal biometric and the proposed multimodal authentication system.

Table 2: FAR and FRR Comparison

System Type	FAR (%)	FRR (%)
Fingerprint-based	3.8	4.2
Face-based	5.1	5.8
Iris-based	2.9	3.4
Proposed Multimodal System	**0.9**	**1.3**

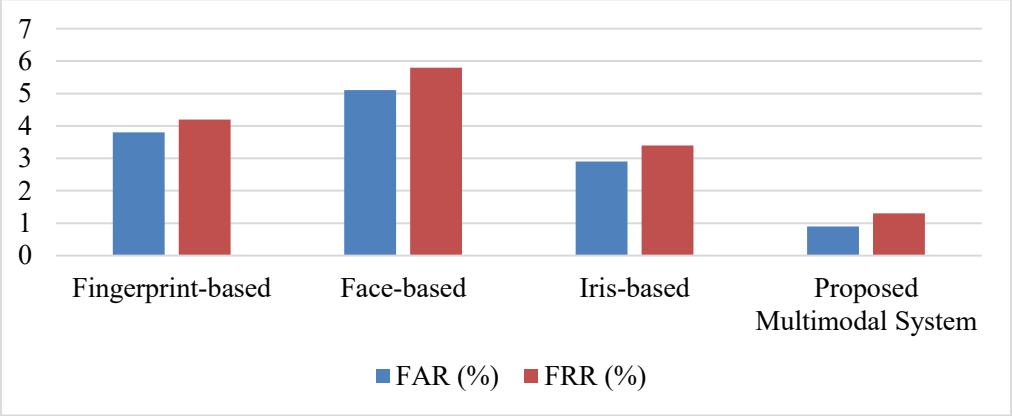

Figure 2: Graphical Representation of FAR and FRR Comparison

The suggested multimodal system has the smallest FAR (0.9%) and FRR (1.3%), which means increased security and usability. The decrease in both of the error rates proves that multimodal fusion facilitated by the data mining-based classification is effective in minimizing the unauthorized access and minimizes the actual user rejection.

4.3 Overall System Reliability and User Acceptance

Table 3 shows the key performance indicators in terms of reliability of the system, successful authentication and acceptance of the system in the real-life operating conditions.

Table 3: System Reliability and User Acceptance

Performance Metric	Percentage (%)
Successful Authentication Rate	97.8
System Reliability	96.9
User Acceptance Rate	95.4

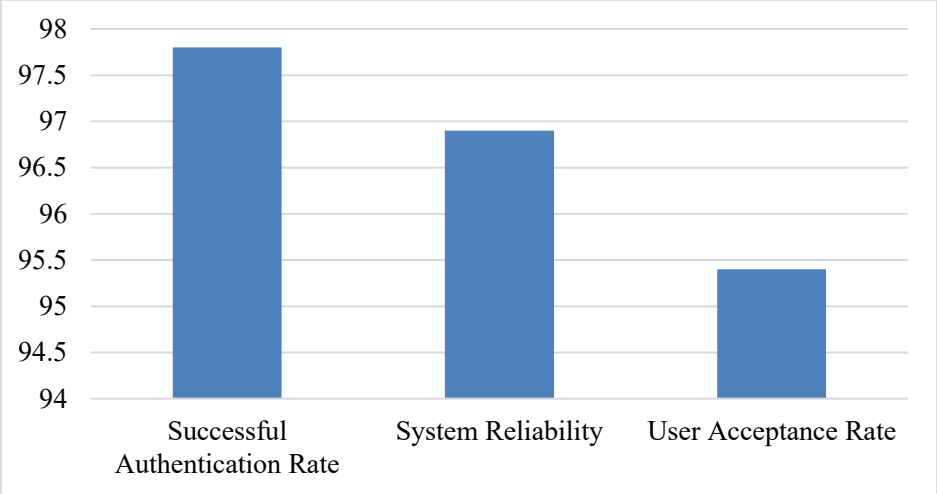

Figure 3: Graphical Representation of System Reliability and User Acceptance

The great values of successful authentication rate (97.8%), system reliability (96.9%), user acceptance (95.4%) indicate that the proposed system is very reliable in all the environments and users are pleased with it. These findings underscore the functionality and strength of the system in secure access controls applications.

4.4 Discussion

The results demonstrate that the suggested multimodal biometric authentication system, which involves data mining, is much more effective than the unimodal biometric systems. Multimodal method has the greatest authentication accuracy (98.2%) and at the same time, lower error rate reflected by the lowest FAR (0.9%) and FRR (1.3). This enhancement affirms that the use of biometric traits in conjunction with each other improves recognition and the security of the system.

Additionally, the data on high system reliability (96.9%) and user acceptance rate (95.4%) shows that the proposed system is strong and practically feasible in the applications of secure access control in the real world. On the whole, these results confirm the usefulness of multimodal fusion and data mining algorithms in the creation of a secure and reliable system of authentication.

5. CONCLUSION

The study has effectively proved the relevance of a data mining based multimodal biometric authentication system in enforcing secure access control through the combination of fingerprint, face as well as iris modalities. The findings of the experiment demonstrate that the system being proposed shows much better results than the biometric schemes based on unimodal, as it can achieve better accuracy in authentication and significantly reduces the error rates. The low FAR and FRR, high system reliability, and usability of the proposed approach indicates the strength, safety, and usability of the approach. In general, the results confirm that multimodal fusion and data mining methods present a consistent and effective way to improve the authentication process and is therefore highly applicable in high security-sensitive system, i.e., banking, healthcare and critical infrastructure systems.

REFERENCES

1. Coelho, K. K., Tristão, E. T., Nogueira, M., Vieira, A. B., & Nacif, J. A. (2023). Multimodal biometric authentication method by federated learning. Biomedical Signal Processing and Control, 85, 105022.

2. Fathima, A. R., & Saravanan, A. (2024). An approach to cloud user access control using behavioral biometric-based authentication and continuous monitoring. International Journal of Advanced Technology and Engineering Exploration, 11(119), 1469.
3. Kolluri, V., Jain, S., Malaga, M., & Das, J. (2024). Advancing biometric security through AI and ML: a comprehensive analysis of neural network architectures for multimodal authentication systems. International Journal of Communication Networks and Information Security, 16(5), 487-505.
4. Krishna Khanth, N., Jain, S., & Madan, S. (2022, December). Sentinel: an enhanced multimodal biometric access control system. In International Conference on Big Data Analytics (pp. 95-109). Cham: Springer Nature Switzerland.
5. Kumar, S., Chaube, M. K., Nenavath, S. N., Gupta, S. K., & Tetarave, S. K. (2022). Privacy preservation and security challenges: a new frontier multimodal machine learning research. International Journal of Sensor Networks, 39(4), 227-245.
6. Mohammed, A., Salama, A., Shebka, N., & Ismail, A. (2025). Enhancing network access control using multi-modal biometric authentication framework. Engineering, Technology & Applied Science Research, 15(1), 20144-20150.
7. Pahuja, S., & Goel, N. (2024). Multimodal biometric authentication: A review. AI Communications, 37(4), 525-547.
8. Rajasekar, V., Saracevic, M., Hassaballah, M., Karabasevic, D., Stanujkic, D., Zajmovic, M., ... & Jayapaul, P. (2023). Efficient multimodal biometric recognition for secure authentication based on deep learning approach. International Journal on Artificial Intelligence Tools, 32(03), 2340017.
9. Ryu, R., Yeom, S., Kim, S. H., & Herbert, D. (2021). Continuous multimodal biometric authentication schemes: a systematic review. IEEe Access, 9, 34541-34557.
10. Savitha, M., & Senthilkumar, M. (2023). A unique secure multimodal biometrics-based user anonymous authenticated key management protocol (SMUAAKAP) based on block chain mechanism for generic HIoTNs. Theoretical Computer Science, 941, 77-90.
11. Sumalatha, U., Prakasha, K. K., Prabhu, S., & Nayak, V. C. (2024). A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection. IEEE Access, 12, 64300-64334.
12. Tarannum, A., Rahman, Z. U., Rao, L. K., Srinivasulu, T., & Lay-Ekuakille, A. (2020). An efficient multi-modal biometric sensing and authentication framework for distributed applications. IEEE Sensors Journal, 20(24), 15014-15025.
13. Tarek, M., Hamouda, E., Alsirhani, A., Alomari, A., & Mostafa, A. M. (2025). A keyless multimodal-based user authentication scheme using generative adversarial networks. PeerJ Computer Science, 11, e3360.
14. Umer, S., Sardar, A., Rout, R. K., Tanveer, M., & Razzak, I. (2023). IoT-enabled multimodal biometric recognition system in secure environment. IEEE Internet of Things Journal, 10(24), 21457-21466.
15. Xia, F., Wei, X., Zhao, Q., Jin, B., Yu, Z., Zha, Z., ... & Hu, J. (2024, April). Exploration on the Application of Multimodal Biometric Feature Recognition in System Access Control. In 2024 IEEE 13th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 1-6). IEEE.