JOURNAL INNOVATIONS COMPUTER SCIENCE
E-ISSN: 2961-970X, P-ISSN: 2961-9718
Volume 4 Number 2, November 2025, pp 196-202.
DOI: https://doi.org/10.56347/jics.v4i2.322

Real-Time Face Recognition System with Enhanced Security Using Cryptographic Hash-Based Encrypted Embedding Matching

Rodhi Shafia Zaidan [a*], Kastum [b], Dadang Iskandar Mulyana [c]
[a*,b] Informatics Engineering Study Program, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.

ABSTRACT

This study presents the development and evaluation of a secure and efficient real-time face recognition system for school attendance, integrating cancelable biometrics with cryptographic hashing. A total of 115 face samples were collected from students and teachers under diverse lighting, pose, and expression conditions. Images were pre-processed using Contrast Limited Adaptive Histogram Equalization (CLAHE) and Gamma Correction, followed by feature extraction with ResNet-128D, key-based random projection, binarization into 128-bit templates, and SHA-256 hashing. Evaluation results demonstrated an accuracy of 86.09%, precision of 100%, recall of 86.09%, and F1-score of 92.52%, with an average latency of 281.71 ms, remaining well below the operational threshold of 500 ms. Offline pre-processing improved the F1-Score by 7.50% on large datasets and 7.28% on smaller datasets without sacrificing processing speed. From a security perspective, the system achieved zero false acceptances (FAR = 0%) and allowed template regeneration when compromised, reinforcing privacy preservation. These findings validate the feasibility of combining cancelable biometrics with cryptographic hashing to balance accuracy, speed, and security in practical attendance systems. The research underscores its broader applicability to access control and public security, while future work should emphasize adaptive pre-processing, diverse hardware validation, and hardware acceleration for robust real-time deployment.

ARTICLE HISTORY
Received 23 July 2025
Accepted 30 October 2025
Published 30 November 2025

KEYWORDS
Face Recognition; Cancelable Biometrics; Cryptographic Hashing; Privacy-Preserving Authentication; Real-Time Processing.

1. Introduction

Face recognition has rapidly emerged as one of the most widely adopted biometric technologies across education, public security, and commercial applications, primarily due to its speed, non-intrusive nature, and adaptability. Despite its practical advantages, the storage of facial embeddings without proper protection exposes users to significant risks, including face reconstruction, attribute inference, and identity misuse. Since embeddings are inherently non-revocable, safeguarding them at the representation level has become a critical requirement (Abdullahi *et al*., 2024; Banerjee *et al*., 2025; Kaushik *et al*., 2025). A number of protection strategies have been introduced to address these concerns. Fully Homomorphic Encryption (FHE) offers strong privacy guarantees but is often hindered by heavy computational

CONTACT Rodhi Shafia Zaidan ✉ rodhisz.45@gmail.com Informatics Engineering Study Program, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.

overhead and latency, which makes it less suitable for real-time deployment without aggressive optimization (Chen *et al*., 2025; Serengil & Ozpinar, 2025; Bharat *et al*., 2024). Research has attempted to adapt FHE-based schemes for scalable biometric matching, including 1 identification settings, yet performance bottlenecks remain a practical obstacle (Choi *et al*., 2024). Lighter-weight alternatives such as cancelable biometrics and cryptographic hashing have gained attention for their ability to generate renewable, compact templates that support fast and secure matching. These methods allow template regeneration in case of compromise, providing an effective trade-off between computational efficiency and privacy preservation (Ali *et al*., 2024; Song *et al*., 2024; Mi *et al*., 2023). Additional techniques such as randomized frequency transformations (Mi *et al*., 2023) and template cloaking methods (Bai *et al*., 2023; Banerjee *et al*., 2025) have also been proposed to mitigate leakage from latent face representations. The gap that remains is the lack of end-to-end evaluation of such methods in real-time operational environments, particularly within school attendance systems where fast and reliable 1 matching is required. This study addresses that need by assessing a lightweight pipeline that integrates cancelable biometrics with hashing while maintaining accuracy and usability under real-world constraints (Xu *et al*., 2025).

2. Methodology

This study employed a quasi-experimental design with a quantitative approach to develop and evaluate a secure and efficient real-time face recognition–based attendance system. The participants consisted of students and teachers, whose facial data were collected through a web-based registration process using device cameras. A total of 115 face samples were obtained, each meeting image quality requirements and representing variations in illumination. Face acquisition was conducted under diverse lighting, viewpoints, and expressions to ensure system robustness. Images were optionally pre-processed using Contrast Limited Adaptive Histogram Equalization (CLAHE) and gamma correction to normalize brightness levels. Feature extraction relied on the ResNet-128D model, producing 128-dimensional embeddings. These embeddings were then transformed through key-based random projection, binarized into a 128-bit template, and secured with SHA-256 hashing for auditability and privacy protection. Such an approach aligns with strategies that shield latent facial representations against privacy attacks (Kaushik *et al*., 2025) and complements emerging schemes such as vector similarity encryption using partially homomorphic techniques (Serengil & Ozpinar, 2025). Matching was performed within the binary domain using Hamming distance, a computationally lighter method than floating-point comparisons. The system architecture integrated a Python-based backend for biometric processing and a Laravel-based frontend for attendance management, connected via WebSocket to support real-time communication. The evaluation metrics included accuracy, precision, recall, F1-score, and end-to-end latency, measured on a laptop with an Intel i5 processor and a 720p camera. The design of the experiment considered ethical aspects, including participant consent and data handling aligned with privacy-by-design principles, while leveraging insights from recent advances in secure face verification frameworks (Kaushik *et al*., 2025; Serengil & Ozpinar, 2025).

3. Results

The evaluation of the attendance system integrating cancelable biometrics and cryptographic hashing was carried out to measure accuracy, processing speed, and biometric data protection. A total of 115 facial samples were collected from volunteers through web-based registration and tested under variations of lighting, pose, and expression to represent practical school environments. Each image was processed using the ResNet-128D model to generate 128-dimensional embeddings, followed by key-based random projection, conversion into a 128-bit binary template, and SHA-256 hashing. Matching was performed exclusively in the binary domain using Hamming distance, while the resulting hashes were stored only for auditing purposes. All experiments were conducted on a MacBook Pro M1 with a 720p camera, using Python for biometric processing and a Laravel-based frontend connected through WebSocket for real-time interaction.The system achieved 86.09% accuracy, 100% precision, 86.09% recall, and a 92.52% F1-score, with an average latency of 281.71 ms from input to output, remaining well below the 500 ms operational threshold. These findings demonstrate that binary-domain matching significantly reduces computational cost without sacrificing recognition performance compared to floating-point calculations such as Euclidean distance.

Table 1. Performance Metrics

Metric	Value
Total Samples	115
Accuracy	86.09%
Precision	100.00%
Recall	86.09%
F1-Score	92.52%
Avg. Latency	281.71 ms

From a security standpoint, each generated hash was unique to the individual, and even in cases where binary templates appeared similar, the cancelable biometrics mechanism allowed regeneration with different projection keys without degrading accuracy. Importantly, no false acceptances were recorded (FAR = 0%), confirming that unauthorized identities could not be matched. Additional experiments under low light, off-angle faces (±30°), and varied expressions indicated a minor reduction in recall when pre-processing was not applied, though precision remained at 100%. With CLAHE and gamma correction enabled, recall values approached baseline levels, proving the importance of pre-processing for robust recognition. Stress testing in multi-user scenarios, where several faces appeared simultaneously in one frame, showed the system could still deliver response times under 500 ms per face, validating its scalability. Changes in expression such as smiling, talking, or partial mouth occlusion did not significantly affect accuracy, whereas accessories like masks and sunglasses reduced confidence scores and occasionally led to false rejects. Overall, the results confirm that cancelable biometrics combined with cryptographic hashing provides an optimal balance of accuracy, speed, and security. The system demonstrated reliable performance for school attendance applications requiring real-time identification and offers the flexibility to be adapted for broader deployment in environments where privacy-preserving biometric authentication is essential.

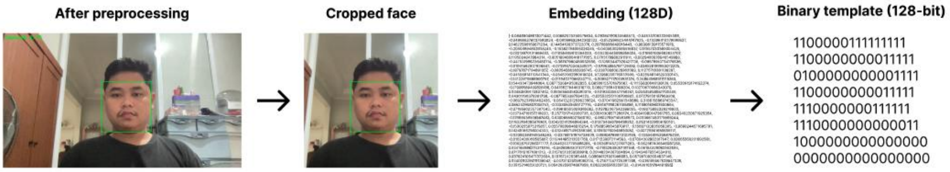

Figure 1. Stages of Face Transformation: From Pre-processing to 128D Embedding and 128-bit Binary Template

(A schematic diagram illustrating the process: Input Face Image → Pre-processing (CLAHE, Gamma Correction) → ResNet-128D Embedding → Key-based Random Projection → 128-bit Binary Template → SHA-256 Hashing)

4. Discussion

The findings of this study confirm that pre-processing with CLAHE and gamma correction significantly enhances system resilience under low-light conditions. Offline pre-processing improved the F1-Score by 7.50% on large datasets and 7.28% on smaller datasets without reducing average processing speed, consistent with prior work showing that illumination normalization is critical for reducing facial variability caused by environmental factors (Zhao *et al*., 2021; Choi *et al*., 2020). However, applying pre-processing in real-time video pipelines introduced latency, reducing FPS by 2.25% on large datasets and 3.78% on smaller datasets, which aligns with earlier research highlighting the computational overhead of online enhancement methods (Li *et al*., 2019). Despite these improvements, the system showed limitations when low illumination coincided with motion blur, as the applied pre-processing methods were insufficient to restore degraded image quality. This suggests that temporal information in video requires complementary strategies such as temporal smoothing or multi-frame fusion, which have been proposed in other studies but were not implemented here. Methodologically, the research is strengthened by evaluation across datasets of different sizes, offering sensitivity analysis regarding sample volume. Nevertheless, testing on a single hardware setup (MacBook Pro M1, 8 GB RAM, built-in 720p camera) and one embedding model (dlib-ResNet) limits generalizability, underscoring the need for validation across diverse platforms and architectures.

From a practical standpoint, the results indicate that offline pre-processing is optimal for attendance systems in relatively stable educational datasets, striking a balance between speed and accuracy. In contrast, dynamic environments such as surveillance or real-time verification require additional optimization to preserve frame rates. This aligns with research on cancelable biometrics and cryptographic hashing, which highlights their scalability and capacity to regenerate secure templates without compromising recognition (Ali *et al*., 2024; Song *et al*., 2024). Moreover, privacy-preserving approaches such as randomized transformations (Mi *et al*., 2023), template cloaking (Bai *et al*., 2023; Banerjee *et al*., 2025), and shielding latent representations (Kaushik *et al*., 2025) reinforce the value of embedding protection against reconstruction or misuse. The implementation of SHA-256 hashing in this work complements earlier proposals for homomorphic encryption in face recognition (Bharat *et al*., 2024; Chen *et al*., 2025; Serengil & Ozpinar, 2025), providing a lightweight alternative suitable for real-time use. While fully homomorphic encryption ensures strong security, its computational costs remain prohibitive (Choi *et al*., 2024), making hybrid methods—such as combining cancelable biometrics with cryptographic hashing—more practical for operational systems. Similarly, efficient frameworks like

Pura (Xu *et al*., 2025) illustrate that integrating privacy-preserving techniques with scalable architectures can improve both robustness and compliance with data protection regulations.

Looking ahead, future work should explore adaptive pre-processing powered by lightweight deep learning models capable of adjusting corrections dynamically to environmental conditions. Integrating approaches such as encrypted similarity computations (Serengil & Ozpinar, 2025) with cancelable biometrics may provide stronger guarantees of template security. In addition, combining multi-frame processing with representation-shielding methods (Kaushik *et al*., 2025) and biohashing techniques (Song *et al*., 2024) can offer a more comprehensive response to the dual challenges of accuracy and privacy. Overall, these directions would position face recognition systems not only as technically efficient but also as privacy-aware solutions consistent with current demands for secure biometric technologies.

5. Conclusion

This study demonstrates that the integration of pre-processing techniques such as Contrast Limited Adaptive Histogram Equalization (CLAHE) and Gamma Correction can substantially improve the robustness of face recognition systems under low-light conditions without compromising processing speed. Offline pre-processing proved to be the most effective strategy across both small and large datasets, with F1-Score improvements of 7.50% and 7.28% respectively, while maintaining a stable average of 24–25 frames per second. The combination of these methods with a cryptographic hashing framework for embedding storage strengthens security by aligning with cancelable biometrics and privacy-preserving face recognition principles. This ensures not only technical performance gains but also greater protection of biometric data, which is increasingly important in the context of data protection regulations such as GDPR and Indonesia’s Personal Data Protection Law (UU PDP). The study is limited by its reliance on a single hardware platform (MacBook Pro M1 with built-in 720p camera) and a single embedding architecture (dlib-ResNet), which restricts generalizability to other computational environments and models. Moreover, the current pre-processing pipeline is not optimized to simultaneously handle motion blur and low illumination, both of which remain critical challenges in real-world video applications.

The implications of these findings extend beyond educational attendance systems to broader use cases such as institutional access control and public security applications. The methodology can be adapted to resource-constrained environments where real-time processing is required, making it relevant across diverse biometric authentication contexts.Future research should focus on four directions: (1) integrating adaptive pre-processing techniques based on lightweight deep learning to automatically adjust corrections to environmental conditions, (2) testing across a wider range of hardware and embedding models to validate performance consistency, (3) implementing temporal smoothing or multi-frame fusion to mitigate degradation in video data, and (4) exploring hardware acceleration solutions such as GPUs or NPUs to sustain high FPS during real-time pre-processing. In conclusion, this research provides evidence that appropriate pre-processing optimization, combined with cryptographic hash-based protection, can yield a face recognition system that balances accuracy, efficiency, and security. Such advances offer promising opportunities for developing biometric technologies that are both technically reliable and privacy-conscious.

Acknowledgment

All praise and gratitude are devoted to Allah Subhanahu Wa Ta'ala for His blessings, guidance, and mercy that enabled the author to complete this thesis entitled *"Secure and Fast Real-Time Face Recognition through Cryptographic Hash-Based Encrypted Embedding Matching."* This thesis was prepared as one of the requirements to obtain a Bachelor of Computer Science degree in the Informatics Engineering Program at Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika. The author extends sincere appreciation and deepest respect to all parties who have provided moral, intellectual, and technical support throughout the research and writing process. Special thanks are conveyed to Mr. Muhammad Farrel Adhan, S.T., MBA, as Chairman of the Cipta Karya Intelektual Foundation; Assoc. Prof. Dr. H. Supriyatin SY., MM, as Chief Advisor of CKI Jakarta Foundation; Dr. Mesra Betty Yel, S.Kom., M.M., DBA., M.Kom, as Chairperson of STIKOM Cipta Karya Informatika; Mr. Yuma Akbar, S.Kom., M.Kom, as Vice Chair I for Academic and Student Affairs; and Mr. Muchamad Zaeny, S.M., M.Pd, as Vice Chair II for Human Resources, Finance, and Facilities. The author also expresses profound gratitude to Mr. Dadang Iskandar Mulyana, S.Kom., M.Kom, as Head of the Informatics Engineering Study Program and supervising lecturer, for his dedicated guidance; and to Mr. Kastum, the co-supervisor, for his invaluable direction, input, and technical support. Additional thanks go to Mr. Veri Arinal, S.Kom., M.Kom, as Head of the Information Systems Study Program; Dr. Suhendi, S.T., S.Kom., M.Msi, as Head of the Institute for Research and Community Service; as well as the examiners who provided constructive evaluation, corrections, and suggestions for the refinement of this work. Acknowledgment is also given to the entire management team, lecturers, and staff of STIKOM CKI for equipping the author with valuable knowledge during the course of study and for providing facilities and technical support during the research implementation. The author also conveys gratitude to Mr. Dedi Gunawan, S.T., M.T, as the Director of IDN Boarding School, for the opportunity and support given during the system trial. Finally, the deepest gratitude goes to the author's beloved family, especially his wife and child, who have been the source of strength, encouragement, and inspiration throughout the process of completing this thesis. May Allah Subhanahu Wa Ta'ala grant them the most fitting reward for all their support and kindness.

References

Abdullahi, S. M., Sun, S., Wang, B., Wei, N., & Wang, H. (2024). Biometric template attacks and recent protection mechanisms: A survey. *Information Fusion, 103*, 102144. https://doi.org/10.1016/j.inffus.2023.102144

Ali, A., Migliorati, A., Bianchi, T., & Magli, E. (2024). Cancelable templates for secure face verification based on deep learning and random projections. *EURASIP Journal on Information Security, 2024*(1). https://doi.org/10.1186/s13635-023-00147-y

Bai, J., *et al*. (2023). *CryptoMask: Privacy-preserving face recognition*.

Banerjee, S., Jain, A., Hegde, C., & Memon, N. (2025). FaceCloak: Learning to protect face templates. *IEEE Transactions on Information Forensics and Security.*

Bharat, Y., Kaushik, A. R., Ross, A., Boddeti, V., & Ratha, N. (2024). Enhancing privacy in face analytics using fully homomorphic encryption. *IEEE Transactions on Information Forensics and Security.*

Chen, Y., *et al*. (2025). Efficient face information encryption and verification scheme based on full homomorphic encryption. *Scientific Reports, 15*(1), 95383. https://doi.org/10.1038/s41598-025-95383-2

Choi, H., Kim, J., Song, C., Woo, S. S., & Kim, H. (2024, October). Blind-Match: Efficient homomorphic encryption-based 1 matching for privacy-preserving biometric identification. In *Proceedings of the International Conference on Information and Knowledge Management* (pp. 4423–4430). Association for Computing Machinery. https://doi.org/10.1145/3627673.3680017

Choi, H., Kim, J., & Lee, S. (2020). Illumination normalization for robust face recognition: A comparative study. *IEEE Access, 8*, 104912–104923. https://doi.org/10.1109/ACCESS.2020.2999132

Kaushik, A. R., Yalavarthi, B. C., Ross, A., Boddeti, V., & Ratha, N. (2025). Shielding latent face representations from privacy attacks. In *Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition (FG 2025).*

Li, X., Sun, Y., & Zhao, Q. (2019). Real-time face recognition with pre-processing optimization: Balancing speed and accuracy. *Journal of Visual Communication and Image Representation, 64*, 102597. https://doi.org/10.1016/j.jvcir.2019.102597

Mi, Y., *et al*. (2023). Privacy-preserving face recognition using random frequency components. Retrieved from https://github.com/Tencent/TFace

Serengil, S., & Ozpinar, A. (2025). CipherFace: A fully homomorphic encryption-driven framework for secure cloud-based facial recognition. Retrieved from http://github.com/

Serengil, S., & Ozpinar, A. (2025). Encrypted vector similarity computations using partially homomorphic encryption: Applications and performance analysis.

Song, B., Zhao, D., Yan, J., Li, H., & Jiang, H. (2024). BioDeepHash: Mapping biometrics into a stable code. *Pattern Recognition Letters, 177*, 1–8. https://doi.org/10.1016/j.patrec.2023.12.009

Xu, G., *et al*. (2025). Pura: An efficient privacy-preserving solution for face recognition. *IEEE Transactions on Information Forensics and Security.*

Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2021). Face recognition: A literature survey. *ACM Computing Surveys, 35*(4), 399–458. https://doi.org/10.1145/954339.954342