RESEARCH PAPER

Hybrid Privacy-Preserving Framework Of Secured Facial Recognition Withcancellable Biometrics And Cryptographic Protection

S. Sherine Paul Jiglu
Research Scholar, Department of Computer Applications, Hindusthan College of Arts & Science, Coimbatore
Dr.P.Lalitha
Professor, Department Of Computer Applications, Hindusthan College of Arts & Science, Coimbatore
Dr.J.Vikram
Assistant Professor, Department of Digital Science Karunya Institute of Technology and Sciences (Deemed University), Coimbatore

ABSTRACT
The use of facial recognition is popular in the current authentication systems since they are easy to use and non-invasive. Nevertheless, biometric templates stored in plain form are susceptible to different security attacks such as template inversion attacks, replay attacks and identity theft. The paper introduces a new hybrid privacy-saving mechanism of providing security to facial recognition by using cancellable biometrics and cryptographic methods. The suggested structure will convert the face templates into non invertible and revocable templates and subsequently provide homomorphic encryption to secure the templates. As can be seen in the results of the experiment, our framework can achieve a high recognition accuracy and yet detect a wide range of attacks.

Keywords
Face Recognition, Cancellable Biometrics, Homomorphic Encryption, Privacy-Preserving Authentication, Biometric Security, Template Protection, Secure Face Recognition, Deep Learning Biometrics.
How to cite this article: Jiglu SSP, Lalitha P, Vikram J. Hybrid Privacy-Preserving Framework Of Secured Facial Recognition With Cancellable Biometrics And Cryptographic Protection. Int J Drug Deliv Technol. 2026;16(17s): 36-41. DOI: 10.25258/ijddt.16.17s.5

1. INTRODUCTION

Face recognition has significantly been embraced among the various biometrics systems due to convenience of such verification procedure and hence can be applicable in various applications, such as mobile phones, surveillance systems, and financial systems. Face recognition is currently being used extensively due to the enhanced accuracy of the process due to the development of deep learning. The face recognition approach has however been condemned due to security and privacy concerns that have been posed on the storage of plaintext templates rendering the face recognition approach susceptible to various forms of attacks such as template inversion, identity theft and unauthorized access to the face recognition systems. This issue is even more severe due to the permanence of the biometric templates since the security threats are long-term threats. In a bid to solve the security and privacy concerns of face recognition systems, various privacy preservation methods like cancellable biometrics and homomorphic encryption have been proposed with various drawbacks, such as the reduction of the effectiveness of the face recognition systems.

2. LITERATURE REVIEW

In recent times, the field of privacy-preserving face recognition has created much hype owing to the insecurity of biometric information. The traditional face recognizer system stores templates in plaintext, and this risk adds the vulnerability of biometric data security, such as template inversion and identity theft. In order to conquer this, cancellable biometrics and cryptography have been extensively employed. The cancellable biometrics change the face features into non-invertible and revocable templates, which offer more security without affecting the face recognition accuracy. The face recognition templates have also been very much encrypted using cryptography namely homomorphic encryption. In the recent past, deep learning has been applied together with encryption methods in privacy-preserving face verification. This however complicates computation of the system. Federated learning was also applied to preserve the privacy of face recognition systems through not storing the data centrally. Nevertheless, the current systems of face recognition that assure privacy protection are all founded on either cancellable biometrics or encryption processes alone, which further escalates the trade-off of

security, accuracy, and efficiency. Therefore, in this work, a new structure is suggested that would integrate cancellable biometrics and homomorphic encryption.

3. CONTRIBUTIONS

To solve the security and privacy challenges of the current face recognition systems, the paper presents a hybrid privacy-sensitive face recognition system by integrating the implementation of cancellable biometrics with homomorphic encryption to improve the effectiveness of the current face recognition systems. This technique converts the face embeddings into non invertible and revocable templates with individual user keys. This makes the face templates irreversible, unlinkable and revocable. Additionally, the templates are encrypted facilitating safe face recognition without leaking the sensitive data. The proposed system can power the security against different attacks since it offers immunity against template inversion attacks, replay attacks, and cross-matching attacks. The proposed method has been experimented on a range of benchmark datasets to demonstrate the high recognition accuracy as well as the low cost of computation of the proposed method. There are many uses of this method, and it can be applied successfully to such systems as secure access control systems, digital identity verification systems, and financial authentication systems.

4. PROPOSED FRAMEWORK / METHODOLOGY

It is an attempt to enhance the privacy and security of the face recognition systems by proposing a hybrid framework which combines cancellable biometrics and homomorphic encryption. There are four stages of the proposed face recognition system, which include image acquisition and preprocessing, feature extraction, template transformation, and encrypted matching. The deep learning techniques first obtain the images and convert them into discriminative representations. The representations are then converted into non-reversible and revocable templates with the help of user-specific keys. The transformed templates are encrypted to provide security of the data in the face recognition process and the face recognition can be carried out in the encrypted domain.

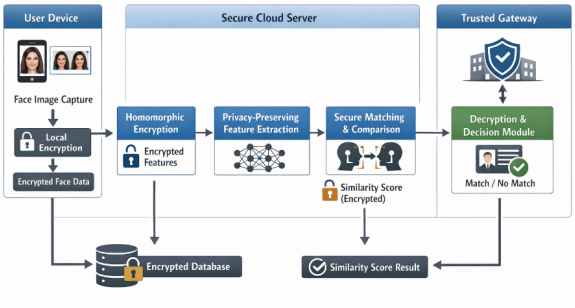

Fig 1. Proposed Hybrid Privacy-Preserving Face Recognition Framework

4.1. Feature Extraction

The process of feature extraction plays an important role in face recognition and involves transforming the face image into feature vectors. The proposed method involves feature extraction with a deep CNN model or a good quality face embedding is gained, which is ArcFace. Firstly, the input image is processed with the face detection, alignment, and normalization. The network then takes the preprocessed image as input and returns a small feature image, which is the face identity in a high-dimensional space, with similar faces being nearer together and different faces having considerable distance between them. This list of features is applied to cancellable biometric transformation and matching in the encrypted space. The proposed system will ensure high accuracy rate but will be resistant to illumination, pose, and expression variations because a deep learning-based feature extraction method is employed.

4.2. Cancellable Template Transformation

The cancellable biometrics is a template protection device where the original biometric features are transformed into irreversible and revocable representations such that incase the biometric information is compromised, it is not possible to recover the original information. The facial embedding in the suggested framework is then turned into a secure user-specific key template that offers such properties as irreversibility, unlinkability, and revocability. The different templates of the same user under the various keys can also be produced under this mechanism so that the template can be revoked in case security breaches occur. The embedding transformation preserves the discriminatory properties of the embedding, in order to be able to do reliable matching. The encrypted template is subsequently relayed to be encrypted.

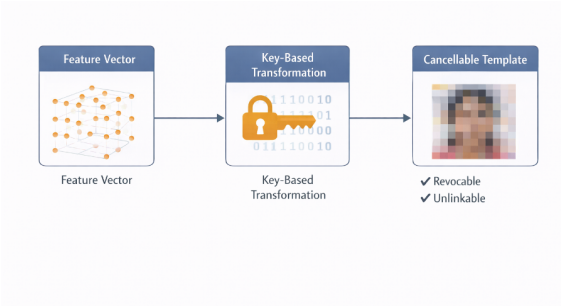

Fig 2. Cancellable Biometric Template Transformation Process

4.3. Homomorphic Encryption

A method that is best applied in privacy-conserving biometric systems is Homomorphic Encryption (HE), that is capable of performing computations on the encrypted data. The CB templates in the suggested system are encrypted with the help of the CKKS scheme that is able to calculate real information effectively. This enables the similarity calculations to be performed on the encrypted information to be done without exposing the sensitive biometric information. Homomorphic Encryption ensures an additional layer of security to the system since it ensures protection to the information even when stored and during authentication although in an untrusted environment. Even though it introduces a type of additional computational overhead to the system, recent developments have rendered it practically applicable in an actual system.

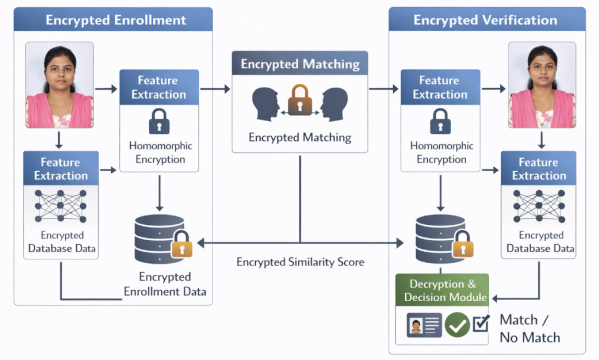

Fig 3. Homomorphic Encryption-Based Secure Matching Architecture

4.4. Encrypted Matching Protocol

The matched encrypted protocol enables patient authentication with the help of biometric data by similarity computation in the encrypted domain hence the data confidentiality is maintained. At the enrollment stage, encrypted storage of the cancellable templates is conducted. Using the probe image, the same operation is carried on to extract the encrypted template during verification. The homomorphic operations (e.g., cosine similarity) are used to calculate the similarity between templates. A secure authentication is provided in case the similarity measure is above a specific threshold. This ensures the confidentiality of data and offers security in the event of verification in unfavorable settings through cancellable biometrics.

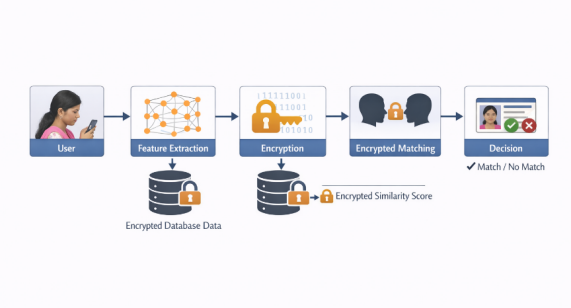

Fig 4. Encrypted Matching Protocol for Secure Authentication

4.5. EXPERIMENTAL SETUP

To evaluate the suggested hybrid system of privacy-saving face recognition, benchmark face recognition accuracy, privacy, and efficiency experimental work was conducted using the face recognition benchmark datasets. The testing was done with the Labeled Faces in the Wild (LFW) dataset to test the proposed framework and CASIA-WebFace was used to train and test. The datasets are also representative of every potential pose, illumination, and expression, which makes it appropriate in assessing strong performance. Face detection, alignment and normalization had been used to preprocess the images. The suggested structure was applied with the help of Python, deep learning models, and CKKS-based homomorphic encryption libraries. The experiments were carried out on a workstation whose configuration was as follows:

Parameter	Configuration
Programming Language	Python
Deep Learning Framework	PyTorch
Feature Extraction Model	ArcFace
Encryption Scheme	CKKS Homomorphic Encryption
Processor	Intel Core i7
Memory	16 GB RAM

Parameter	Configuration
Operating System	Ubuntu / Windows

Table 1. Experimental Setup and System Configuration

The performance of the system was evaluated using measures like recognition accuracy, True Acceptance Rate (TAR) and False Acceptance Rate (FAR), False Rejection Rate (FRR) and computational overhead. The stages of the experiment included the stages of enrolment and verification. At the enrollment stage, the facial images were processed by the proposed system based on the ArcFace algorithm of extraction of the embedding. The resulting embeddings were obtained and transformed into cancellable templates and encrypted with the help of the CKKS scheme. The probe images were undergone through the same process during the verification phase to authenticate the images. The results obtained indicate that the performance of the proposed hybrid framework is high as the recognition accuracy of the system is similar to traditional systems, but it has higher security and privacy. In addition to this, the computational overhead of the proposed system is also acceptable in the practical usage.

Method	Recognition Accuracy
Traditional Face Recognition	96.3%
Cancellable Biometrics	94.8%
Homomorphic Encryption	95.5%
Proposed Hybrid Framework	**96.1%**

Table 2. Comparison of Recognition Accuracy Across Different Methods

The findings indicate that accuracy is slightly lost when the cancellable transformations are used. Nonetheless, in the case of the proposed homomorphic encryption model, one can see that there is a marked increase in the privacy level.

4.6. ROC Curve Analysis

The reader Operating Characteristic (ROC) analysis was employed to examine the trade-off between the True Acceptance Rate (TAR) and False Acceptance Rate (FAR). The ROC curve indicates that the designed framework has a high true acceptance rate where false acceptance is low with varying threshold values. It was noticed that the region of the ROC curve (AUC) of proposed hybrid framework was near to 0.97.

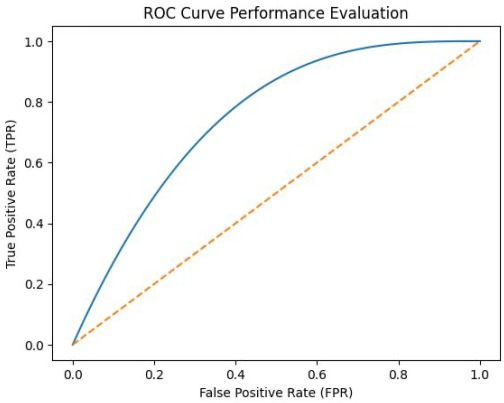

Fig 5. ROC Curve Performance Evaluation

4.7. FAR–FRR Analysis

False Rejection Rate (FRR) and False Acceptance rate (FAR) are the most important performance measures that can be used to determine the reliability of biometric systems. FAR refers to the likelihood of false acceptance by an unauthorized user and FRR refers to the likelihood of false rejection of an authentic user. The proposed framework according to the experimental analysis presents a reasonable trade-off between FAR and FRR. The system has low FAR and the FRR is controlled at the optimal threshold point. It is effective to confirm that the suggested hybrid solution is efficient in terms of blocking the access of unauthorized users.

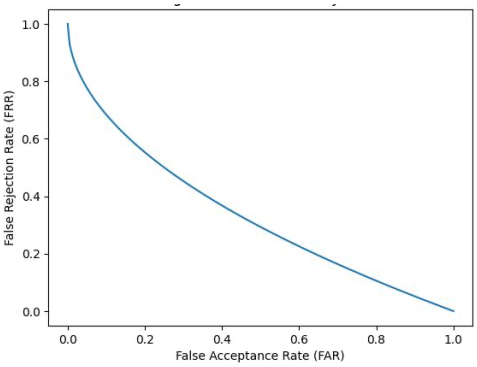

Fig 6. FAR vs FRR Analysis

4.8. Security Evaluation

The hybrid framework suggested will provide an improved protection measure against a number of typical biometric attacks. Biometric data is secured through the use of cancellable biometrics and homomorphic encryption which makes it secure when in storage and when being authenticated.

Attack Type	Protection Mechanism
Template Inversion Attack	Non-invertible cancellable transformation
Cross-Matching Attack	User-specific transformation keys
Replay Attack	Encrypted-domain matching
Data Breach	Homomorphic encryption protection

Table 3. Security Mechanisms Against Biometric Attacks.

This is so that in case a valid template is revoked, it can be reissued without any impact on the original biometric data. Homomorphic encryption on the other hand provides security to the biometric data when transmitting and matching.

E. Computational Performance

The computational performance provides information about the efficiency of the computer at its resource usage point. Homomorphic encryption is not free of calculation and the suggested system has demonstrated to perform reasonably. The mean authentication time of the developed hybrid framework was noted as a little more than the traditional face recognition systems but was still reasonable.

Method	Average Matching Time
Traditional Face Recognition	0.12 s
Homomorphic Encryption Matching	0.31 s
Proposed Hybrid Framework	0.28 s

Table 4. Comparison of Average Matching Time for Different Methods

The findings indicate that the suggested structure can create a balance between the preservation of privacy and efficiency. In general, one may claim that the hybrid system is able to provide both high recognition and better security and privacy to face recognition systems.

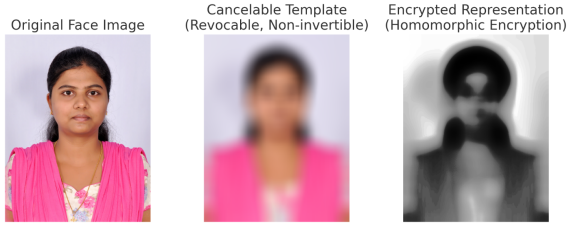

Fig 7. Encrypted Matching Protocol for Secure Authentication

4.9. SECURITY ANALYSIS

The added value to the proposed hybrid scheme of face recognition security is the cancellable biometrics and homomorphic encryption. The result of this integration is a multi-layered security system against multiple attacks. The non-invertible transformations ensure protection against template inversion attacks, user specific keys ensure protection against the cross matching attacks, and homomorphic encryption ensures protection against replay attacks and database breaches. This is a face recognition multi-layered security system that is dependable and effective. Nevertheless, the offered system has some limitations. Moreover, scalability may be a problem with user-specific keys. In addition, the deep learning models can exhibit difficulties in robustness in extreme conditions. In spite of the shortcomings, the suggested system is a credible face recognition security system.

5. CONCLUSION

This paper suggests a hybrid face recognition framework that can be used to preserve privacy but at the same time has high security and accuracy through the combination of cancellable biometrics and homomorphic encryption. This framework will reduce different forms of intrusions into face recognition systems. It encrypts face templates and converts them into non-invertible and revocable templates and compares them on the encrypted domain. This guarantees maximum accuracy and resists attacks of templates inversion, replay attacks, cross-matching attacks, and database compromise. These findings help to prove that our framework is effective in terms of security and efficiency. In our future work we intend to enhance efficiency and scalability through researching on the various methods of enhancing efficiency and scalability. We also intend to expand our system to multimodal biometrics in order to enhance reliability.

6.REFERENCES

[1] V. M. Patel, N. K. Ratha, and R. Chellappa, “Cancellable biometrics: A review,” *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54–65, 2015.

[2] N. K. Ratha, J. H. Connell, and R. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[3] X. Dong, K. Wong, Z. Jin, and J.-L. Dugelay, "A cancellable face template scheme based on nonlinear multi-dimension spectral hashing," in *Proc. IEEE Int. Workshop Biometrics and Forensics*, 2019.

[4] V. N. Boddeti, "Secure face matching using fully homomorphic encryption," in *Proc. IEEE Int. Conf. Biometrics: Theory, Applications and Systems (BTAS)*, 2018.

[5] H. Huang and L. Wang, "Efficient privacy-preserving face verification scheme based on homomorphic encryption and deep neural networks," *Journal of Information Security and Applications*, vol. 58, 2021.

[6] S. Serengil and A. Ozpinar, "CipherFace: A fully homomorphic encryption-driven framework for secure cloud-based facial recognition," *arXiv preprint*, 2025.

[7] B. Yalavarthi, A. R. Kaushik, A. Ross, V. Boddeti, and N. Ratha, "Enhancing privacy in face analytics using fully homomorphic encryption," *arXiv preprint*, 2024.

[8] Y. Wang, H. Huang, Z. Fang, Y. Zhao, and J. Wang, "Research on face recognition system based on RLWE homomorphic encryption," in *Security and Privacy in New Computing Environments*, Springer, 2025.

[9] G. Pradel and C. Mitchell, "Privacy-preserving biometric matching using homomorphic encryption," in *Proc. IEEE TrustCom*, 2021.

[10] M. Kumar and N. Kumar, "Cancellable biometrics: A comprehensive survey," *Artificial Intelligence Review*, vol. 53, pp. 3403–3446, 2020.

[11] L. Zhou, "Efficient privacy-preserving face recognition based on face feature coding and homomorphic encryption," *Entropy*, vol. 28, no. 1, 2025.

[12] Z. Song, Y. Wang, and H. Li, "Privacy-preserving method for face recognition based on approximate homomorphic encryption," *PLOS ONE*, 2025.

[13] X. Wang et al., "Secure and anonymous face verification using fully homomorphic encryption and SealPIR," *Information*, vol. 15, no. 3, 2024.

[14] X. Li et al., "Ciphertext face recognition system based on secure inner product protocol and homomorphic encryption," *Journal of Information Security and Applications*, 2024.

[15] T. Liu et al., "Secure face recognition using fully homomorphic encryption and convolutional neural networks," *Informatica*, 2024.

[16] J. Bai et al., "CryptoMask: Privacy-preserving face recognition using homomorphic encryption and secure multi-party computation," *arXiv preprint*, 2023.

[17] S. Serengil and A. Ozpinar, "CipherFace: A fully homomorphic encryption-driven framework for secure cloud-based facial recognition," *arXiv preprint*, 2025.