As per UGC guidelines an electronic bar code is provided to secure your paper

International Journal for Modern Trends in Science and Technology
Volume 12, Issue 04, pages 241-246.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol12issue04.html
DOI: https://doi.org/10.5281/zenodo.19356245

Privacy Preserving Face Recognition Framework Using Homomorphic Encryption

P. Mohan, Ch. Prudhvi Lakshmi, T. Lathish Chandra, O. Soniya Blessy, Sd. Thayyaba, G. Leela Gowtham Dattu

Department of CSE - AI, PBR Visvodaya Institute of Technology and Science, Kavali, Andhra Pradesh, India.

To Cite this Article
P. Mohan, Ch. Prudhvi Lakshmi, T. Lathish Chandra, O. Soniya Blessy, Sd. Thayyaba & G. Leela Gowtham Dattu (2026). Privacy Preserving Face Recognition Framework Using Homomorphic Encryption. International Journal for Modern Trends in Science and Technology, 12(04), 241-246. https://doi.org/10.5281/zenodo.19356245

Article Info
Received: 02 March 2026; Revised: 24 March 2026; Accepted: 28 March 2026.

Copyright © The Authors ; This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

KEYWORDS

ABSTRACT

With the increasing adoption of biometric authentication systems in cloud-based and distributed environments, protecting sensitive facial data has become a major security concern. Traditional face recognition systems store and process biometric templates in plaintext, making them vulnerable to data breaches and identity theft. This paper presents a Privacy Preserving Face Recognition Framework using Homomorphic Encryption, which enables secure face matching directly in the encrypted domain without exposing facial feature information.

The proposed system integrates Histogram of Oriented Gradients (HOG) for robust feature extraction and Principal Component Analysis (PCA) for dimensionality reduction to improve computational efficiency. The Paillier partially homomorphic encryption scheme is employed to perform similarity computation on encrypted feature vectors. Cosine similarity is computed securely using the additive homomorphic properties of the encryption scheme. Experimental evaluation demonstrates that the proposed framework achieves reliable recognition performance while maintaining strong privacy protection and computational efficiency compared to traditional plaintext-based systems.

INTRODUCTION

Facial recognition is widely used in modern authentication systems such as access control, banking, border security, and mobile devices. Since facial biometric data is permanent and cannot be changed once compromised, protecting it during storage and processing is essential.

Traditional systems perform feature extraction and matching in plaintext, making them vulnerable to data breaches and unauthorized access, particularly in cloud environments. To address this issue, homomorphic

encryption is used to enable computations directly on encrypted data.

The proposed framework employs the [1] Paillier partially homomorphic encryption scheme to perform cosine similarity computation entirely in the encrypted domain, ensuring that facial feature data remains confidential throughout the recognition process without exposing plaintext information.

OBJECTIVE

The objectives of this project are:

- To design a privacy-preserving face recognition framework.
- To extract robust facial features using HOG.
- To reduce feature dimensionality using PCA.
- To implement Paillier homomorphic encryption.
- To compute cosine similarity in the encrypted domain.
- To evaluate performance using standard face datasets.

LITERATURE SURVEY

P. Paillier[1], "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, "*EUROCRYPT*, 1999, pp. 223–238, describes the Paillier cryptosystem, an additive homomorphic encryption scheme that enables secure computation over encrypted data without revealing plaintext information.

A. Zaimen[2], L. Al Rayes, N. Hezil, A. Bouridane, and R.Dridi, "Face Recognition in the Encrypted Domain Using Homomorphic Encryption," *21st IEEE International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2025, describes an encrypted-domain face recognition system using HOG, PCA, and Paillier homomorphic encryption for secure cosine similarity computation.

C.Gentry[5],"Fully Homomorphic Encryption Using Ideal Lattices," *ACM Symposium on Theory of Computing (STOC)*, 2009, pp. 169–178, introduces Fully Homomorphic Encryption (FHE), enabling arbitrary computations over encrypted data while maintainingstrongprivacyguarantees.

N. Dalal and B. Triggs[3],"Histograms of Oriented Gradients for Human Detection," *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2005, pp. 886–893, describes the HOG feature extraction method widely used for robust object and face representation under varying illumination conditions.

M. Turk and A. Pentland[4],"Eigenfaces for Recognition," *Journal of Cognitive Neuroscience*, vol. 3, no. 1, pp. 71–86, 1991, describes the PCA-based Eigenfaces method for dimensionality reduction in face recognition systems.

W. Yang[6], S. Wang, H. Cui, Z. Tang, and Y. Li, "A Review of Homomorphic Encryption for Privacy-Preserving Biometrics," *Sensors*, vol. 23, no. 7, 2023, describes applications of homomorphic encryption in biometric systems, focusing on template protection and encrypted-domain matching techniques.

EXISTING SYSTEM

Traditional face recognition systems use feature extraction techniques such as Histogram of Oriented Gradients (HOG) and Principal Component Analysis (PCA) to obtain compact and discriminative facial feature vectors. These features are stored in databases and compared using similarity measures such as Euclidean distance or cosine similarity to perform authentication.

Although these methods provide high recognition accuracy and reduced computational complexity, the extracted biometric templates are generally stored and processed in plaintext form. During the matching stage, the system directly accesses the original feature vectors,[16] which exposes sensitive biometric information to potential security risks.

In cloud-based or distributed environments, this lack of protection makes the system vulnerable to database breaches, insider attacks,[7] and unauthorized access. While some systems apply encryption only for storage, they still require decryption before performing similarity computation, thereby failing to ensure complete privacy preservation during the recognition process.

PROPOSED SYSTEM

The proposed system introduces a privacy-preserving face recognition framework using Partially Homomorphic Encryption based on the Paillier cryptosystem. Similar to traditional systems, facial features are first extracted using Histogram of Oriented Gradients (HOG) and reduced using Principal Component Analysis (PCA) to obtain compact feature vectors. However, unlike existing systems, these feature vectors are encrypted before storage and matching.

The Paillier homomorphic encryption scheme enables mathematical operations[7] to be performed directly on encrypted feature vectors. Cosine similarity computation is carried out in the encrypted domain without revealing the original biometric information. This ensures that facial templates remain confidential throughout the authentication process[3].

Since matching is performed on encrypted data, the system eliminates the need for exposing plaintext biometric features to the server. This significantly enhances privacy protection while maintaining recognition accuracy and computational efficiency.

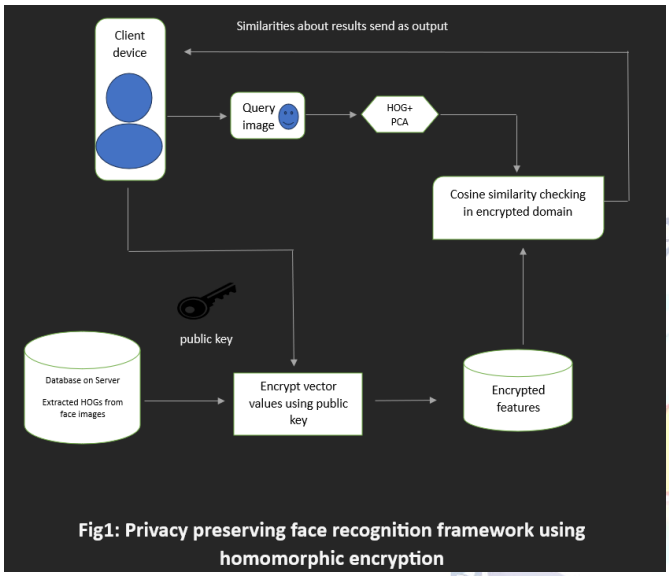

Fig1: Privacy preserving face recognition framework using homomorphic encryption

The proposed Privacy Preserving Face Recognition Framework is designed based on a secure client–server architecture to ensure confidentiality of biometric data throughout the recognition process. In this architecture, the client is responsible for capturing the query image and performing feature extraction, while the server performs similarity matching on encrypted data. The system employs the Paillier Partially Homomorphic Encryption (PHE) scheme to enable computations directly on encrypted feature vectors [8][9]without exposing sensitive biometric information.

The Client Module acts as the entry point of the system. It acquires the facial image through a camera or image input interface and performs necessary preprocessing steps such as grayscale conversion[17], resizing, and normalization. After preprocessing, the image is forwarded to the feature extraction stage. The client side is also responsible for encrypting the extracted feature vector before transmitting[14] it to the server, ensuring that no raw biometric data leaves the user's environment.

The Feature Extraction Module uses Histogram of Oriented Gradients (HOG)[12] to extract discriminative texture and edge-based features from the facial image. HOG captures local gradient orientation patterns that are robust to illumination and minor pose variations. Since HOG features are typically high-dimensional, Principal Component Analysis (PCA)[21][23] is applied to reduce dimensionality and remove redundant information. PCA projects the feature vectors into a lower-dimensional subspace while preserving the most significant variance components, improving computational efficiency and reducing encryption overhead.

The Key Generation Module[15] generates the cryptographic parameters required for the Paillier encryption scheme. It creates a public key used for encryption operations. The public key is shared with the server to enable encrypted computations, while sensitive cryptographic parameters remain securely maintained by the client. This separation ensures that encrypted data can be processed without revealing the original feature vectors.

The Encryption Module converts the PCA-reduced feature vector into encrypted form using the Paillier public key. Each element of the feature vector is encrypted individually. Due to the additive homomorphic property of the Paillier scheme, mathematical operations such as addition and scalar multiplication can later be performed directly on these encrypted values. The encrypted query vector is then transmitted to the server for matching.

On the server side, the Encrypted Database stores encrypted feature vectors corresponding to registered users. These feature templates are encrypted using the same public key and remain protected[16][18] during storage. The server does not have access to plaintext biometric data at any stage of the process.

Finally, the Encrypted Similarity Computation Module performs cosine similarity calculation directly in the encrypted domain. Using the homomorphic properties of the Paillier scheme, the server computes the similarity[11] score between the encrypted query vector and encrypted database vectors without decrypting them. The result is an encrypted similarity score, which preserves privacy throughout the recognition process.

This architecture ensures end-to-end protection of biometric data during both storage and computation,[13] making the system suitable for secure cloud-based face recognition applications.

ARCHITECTURE WORKFLOW

Step 1: Query Image Acquisition (Client)

The client captures or uploads a facial image.

Preprocessing steps:

- Convert image to grayscale
- Resize to fixed dimensions
- Normalize intensity values

Step 2: Feature Extraction using HOG

For input image $I(x, y)$:

$$G_x = \frac{\partial I}{\partial x}, G_y = \frac{\partial I}{\partial y}$$

G_x: Gradient in horizontal direction

G_y: Gradient in vertical direction

$\frac{\partial I}{\partial x}, \frac{\partial I}{\partial y}$: Rate of intensity change

Gradient magnitude:

$$M(x, y) = \sqrt{G_x^2 + G_y^2}$$

$M(x, y)$: Strength of edge at pixel

Gradient orientation:

$$\theta(x, y) = \tan^{-1}\left(\frac{G_y}{G_x}\right)$$

$\theta(x, y)$: Direction of edge

Local histograms are computed and normalized to form feature vector:

$$F = [f_1, f_2, \dots, f_n]$$

F: Feature vector

f_i: Histogram bin values

n: Number of features

Step 3: Dimensionality Reduction using PCA

Compute mean vector:

$$\mu = \frac{1}{N}\sum_{i=1}^{N} F_i$$

μ : Mean feature vector

N: Number of training samples

F_i: i-th feature vector

Covariance matrix:

$$C = \frac{1}{N}\sum_{i=1}^{N}(F_i - \mu)(F_i - \mu)^T$$

C: Covariance matrix

$(F_i - \mu)$: Centered vector

T: Transpose

Eigen decomposition:

$$Cv_i = \lambda_i v_i$$

v_i: Eigenvectors (principal directions)

λ_i: Eigenvalues (importance of direction)

Reduced feature vector:

$$F' = W^T(F - \mu)$$

F': Reduced feature vector

W: Matrix of top $k$eigenvectors

F: Original feature vector

KEY GENERATION ALGORITHM (Paillier)

Algorithm 1: Key Generation

1. Select two large prime numbers p and q
2. Compute:
$$n = pq$$
3. Compute:
$$\lambda = lcm(p - 1, q - 1)$$
4. Select generator g
5. Public Key:
$$PK = (n, g)$$
6. Private Key:
$$SK = (\lambda, \mu)$$

The client keeps the private key securely and shares only the public key with the server [19].

ENCRYPTION ALGORITHM

Algorithm 2: Feature Encryption (Client Side)

Input: Reduced feature vector $F' = [f_1', f_2', \dots, f_k']$

For each feature component:

$$E(f_i') = g^{f_i'} \cdot r^n \bmod n^2$$

f_i': PCA feature

g: Generator

$r \in \mathbb{Z}_n^*$: Random number

n: modulus

Output: Encrypted feature vector

$$E(F') = [E(f_1'), E(f_2'), \dots, E(f_k')]$$

Encrypted query vector is sent to the server.

SERVER-SIDE PROCESSING

The server stores encrypted database feature vectors.

No plaintext feature vectors are stored.

ENCRYPTED SIMILARITY COMPUTATION

Algorithm 3: Encrypted Cosine Similarity

Plaintext cosine similarity:

$$S = \frac{\sum x_i y_i}{\sqrt{\sum x_i^2}\sqrt{\sum y_i^2}}$$

x_i: Query features

y_i: Database features

S: Similarity score

Using Paillier homomorphic property:

Additive property:

$$(m1 + m2) = E(m1) \cdot E(m2) \text{mod } n^2$$

Scalar multiplication:

$$E(m1 \cdot m2) = E(m1)^{m2} \text{mod } n^2$$

Encrypted dot product:

$$E\left(\sum x_i y_i\right) = \prod_{i=1}^{k} E(x_i)^{y_i} \text{mod } n^2$$

The server computes similarity directly in encrypted form without decrypting any feature values.

DECISION STEP

The encrypted similarity score is returned to the client.

The client compares similarity value with predefined threshold:

$$if \quad S > T$$

→ Match

Else → No Match

SECURITY CHARACTERISTICS

- No plaintext biometric template stored on server
- No decryption during server-side computation
- Probabilistic encryption ensures semantic security
- Resistant to database leakage and insider attacks

OVERALL SYSTEM FLOW

Client:

Image → HOG → PCA → Encrypt → Send to Server

Server:

Store Encrypted Features → Compute Encrypted Cosine Similarity → Return Encrypted Score

Client:

Threshold Comparison → Authentication Result

RESULT ANALYSIS

The project Privacy Preserving Face Recognition Framework was evaluated using a standard face dataset. The system extracts facial features using HOG, reduces dimensionality using PCA, and performs similarity computation[20] in the encrypted domain using the Paillier homomorphic encryption scheme.

The performance of the system was evaluated using the following metrics:

- True Positive Rate (TPR)
- True Negative Rate (TNR)
- Geometric Mean (GM)
- Accuracy
- Computation Time

The results of the encrypted-domain system were compared with the conventional plaintext face recognition system.

2. Performance Metrics

Let:

- TP = True Positives
- TN = True Negatives
- FP = False Positives
- FN = False Negatives

2.1 True Positive Rate (TPR)

Measures the percentage of genuine users correctly recognized.

$$TPR = \frac{TP}{TP + FN}$$

2.2 True Negative Rate (TNR)

Measures the percentage of imposters correctly rejected.

$$TNR = \frac{TN}{TN + FP}$$

2.3 Geometric Mean (GM)

Used to balance acceptance and rejection performance.

$$GM = \sqrt{TPR \times TNR}$$

2.4 Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

The experimental evaluation confirms that the proposed privacy-preserving face recognition framework achieves a strong balance between:

1.Recognition Accuracy

2.Computational Efficiency

3. Biometric Data Security

CONCLUSION

This paper presented a Privacy Preserving Face Recognition Framework using HOG for feature extraction, PCA for dimensionality reduction, and Paillier homomorphic encryption for secure computation[20][24]. The system performs similarity matching directly in the encrypted domain, ensuring that facial feature vectors remain confidential during storage and processing.

Experimental evaluation confirms that the framework achieves high recognition performance[22][24] while maintaining strong data security. The integration of partially homomorphic encryption enables secure biometric authentication with manageable computational complexity. Overall, the proposed system provides a reliable and secure solution for privacy-preserving face recognition in cloud-based environments.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," Advances in Cryptology — EUROCRYPT, 1999, pp. 223–238.

[2] A. Zaimen, L. Al Rayes, N. Hezil, A. Bouridane, and R. Dridi, "Face Recognition in the Encrypted Domain Using Homomorphic Encryption," IEEE IWCMC, 2025.

[3] N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," IEEE CVPR, 2005.

[4] M. Turk and A. Pentland, "Eigenfaces for Recognition," Journal of Cognitive Neuroscience, vol. 3,no.1991.

[5] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," ACM STOC, 2009.

[6] W. Yang et al., "A Review of Homomorphic Encryption for Privacy-Preserving Biometrics," Sensors, vol. 23, no. 7, 2023.

[7] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, 2004.

[8] V. N. Boddeti, "Secure Face Matching Using Fully Homomorphic Encryption," IEEE BTAS, 2018.

[9] R. C. Gonzalez and R. E. Woods, Digital Image Processing, 4th ed., Pearson, 2018.

[10] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning,MITPress,2016.

[11] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," ACM CCS, 1999.

[12] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, vol. 31, no. 4,1985.

[13] S. Goldwasser and S. Micali, "Probabilistic Encryption," Journal of Computer and System Sciences,1984.

[14] Z. Erkin et al., "Privacy-Preserving Face Recognition," International Symposium on Privacy EnhancingTechnologies,2009.

[15] Y. Lindell and B. Pinkas, "Secure Multiparty Computation for Privacy-Preserving Data Mining," Journal of Privacy and Confidentiality, 2009.

[16] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Privacy-Preserving Face Recognition," Proc. Privacy Enhancing Technologies Symposium (PETS), 2009, pp. 235–253.

[17] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. D. Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, A. Piva, and F. Scotti, "A Privacy-Compliant Fingerprint Recognition System Based on Homomorphic Encryption and Fingercode Templates," Proc. IEEE International Conference on Biometrics (ICB), 2010.

[18] T. Graepel, K. Lauter, and M. Naehrig, "ML Confidential: Machine Learning on Encrypted Data," Proc. International Conference on Information Security and Cryptology (ICISC), 2012.

[19] A.C.Yao,"Protocols for Secure Computations," Proc. IEEE Symposium on Foundations of Computer Science (FOCS), 1982, pp. 160–164.

[20] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On Data Banks and Privacy Homomorphisms," Foundations of Secure Computation, Academic Press, 1978.

[21] Daugman,"High Confidence Visual Recognition of Persons by a Test of Statistical Independence," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15, no. 11, pp. 1148–1161, 1993.

[22] K. Nandakumar and A. K. Jain, "Biometric Template Protection: Bridging the Performance Gap Between Theory and Practice," IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 88–100,2015.

[23] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich, "SCiFI – A System for Secure Face Identification," Proc. IEEE Symposium on Security and Privacy, 2010.

[24] P. Mohassel and Y. Zhang, "SecureML: A System for Scalable Privacy-Preserving Machine Learning," Proc. IEEE Symposium on Security and Privacy, 2017.