Indian Journal of Computer Science and Technology
https://www.doi.org/10.59256/indjcst.20260503110
Volume 5, Issue3 (September-December 2026), PP: 932-936.
www.indjcst.com
ISSN No: 2583-5300

Secure Face Recognition Using Local Binary Patterns and AES–GCM Authenticated Encryption

S. Sherine Paul Jiglu[1], Dr. P. Lalitha[2], Dr. J. Vikram[3]
[1]*Researcher Scholar, Department of Computer Applications, Hindusthan College of Arts & Science, Coimbatore, Tamilnadu, India.*
[2]*Professor, Department of Computer Applications, Hindusthan College of Arts & Science, Coimbatore, Tamilnadu, India.*
[3]*Assistant Professor, Department of Digital Science, Karunya Institute of Technology and Sciences (Deemed University), Coimbatore, Tamilnadu, India.*

To Cite this Article: *S. Sherine Paul Jiglu[1], Dr. P. Lalitha[2], Dr. J. Vikram[3], "Secure Face Recognition Using Local Binary Patterns and AES–GCM Authenticated Encryption", Indian Journal of Computer Science and Technology, Volume 05, Issue 03 (September-December 2026), PP: 932-936.*

Copyright: ©2026 This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution License; Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract: *For the applications of face recognition, not only the accurate identity verification but also the protection of the sensitive facial data are required in this paper, a hybrid model of local binary pattern feature extraction and Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) mode is proposed for the authenticated image encryption. Images of the face are pre-processed and represented in terms of texture histograms which are compared with enrolled images. The image protection section is used to encrypt the facial image data, and generates an image protection authentication tag for verification of the integrity of the image data during decryption. A prototype application accesses, recognizes, encrypts and recovers images in a single application. The screenshots shown here are intended to illustrate these operations, but are not intended to provide accuracy of recognition or processing speed or tamper resistance. The method provides a guideline for implementation of the fusion of texture-based recognition and real protection of image storage and transmission. During the recognition phase, plaintext representations of faces are used; during the matching phase, the records of facial images are encrypted. For measuring recognition performance, encryption/decryption overhead, and correct rejection of modified records are required to have quantitative testing.*

Key Word: *Face recognition, local binary patterns, AES-GCM, authenticated encryption, biometric security.*

I. INTRODUCTION

Contactless identity verification is possible with face recognition, however, storing and sharing facial data poses privacy and security concerns. Recent research has focused on the protection of various phases of a recognition system such as image processing, inference and template storage [1] and [2]. The study investigates the combination of the Local Binary Pattern (LBP) feature extraction with Advanced Encryption Standard in Galois/Counter Mode (AES–GCM) to establish the dependability of a biometric application. link.springer.com LBP histograms are used to compare facial features with enrolled samples, and AES–GCM is used to protect facial image records via authenticated encryption. Each component performs a different function: Facial Matching works on plaintext representation and Encryption ensures the protection of the image information during storage or transmission. Some recent methods such as CryptoFace [3] and IDFace [4] enable the processing or matching of encrypted facial data by using homomorphic encryption. The scope of the present work is, however, less broad, it is about the integration of the traditional facial recognition with the authenticated protection of images, not encrypted domain recognition. It investigates the integration of these components in a single application, as well as the evaluation that should be performed to obtain effectiveness. openaccess.thecvf.com To prevent the successful image encryption as proof of recognition accuracy or complete biometric security, recognition performance, cryptographic processing time and modified record rejection are considered separately.

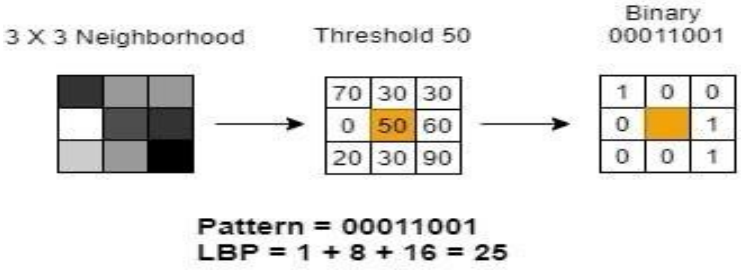


Fig 1 Local Binary Pattern Binary Conversion

II. RELATED WORK

There have been recent works on facial privacy by transforming images, protecting image templates, and computing with encrypted images. Sun and Liu [1] discuss protection at the data generation, inference, and storage stages, and Laishram et al. [2] discuss information leakage and protection. These works highlight the need to consider security in conjunction with the recognition performance, and CryptoFace [3] protects feature extraction, storage and matching through fully homomorphic encryption. IDFace [4] is interested in the efficient identification using homomorphically encrypted facial template. Huang et al. [5] have proposed a prototype that encrypts the facial image records in addition to plaintext representations while preserving the ability to recognize images by learning local features, but at the same time reducing the visual disclosure given by these representations. Kim et al. [6] discusses deep face template protection in the absence of constraints. Other authors like Otheri Shahreza et al. [7] evaluate cancelable biometric schemes in terms of the three recognition performance, unlinkability and irreversibility. Their results confirm the importance of assessing privacy aspects separately from the matching rate. Other attack research involves complementary work that uses 3D reconstruction for facial template inversion by Otroshi Shahreza and Marcel [8]. Bassit et al. [9] examine how to recover a template from an encrypted unprotected decision recognition system, and show that there are not only multiple leakage channels, but some can be overcome by successful encryption of selected parts. Springer Nature Link

A more recent survey of biometric template attacks and protection mechanisms [10] also points out weaknesses in biometric authentication systems. This background motivates the present study which considers a more restricted implementation goal: the integration of LBP based recognition and AES–GCM image protection. It is essential to test its effectiveness by the recognition measurements, processing-time analysis, and authentication failure tests; it is not a new method of cryptography or template protection.

III. PROPOSED METHODOLOGY

The proposed system use a combination of LBP face recognition and AES–GCM protection of face images. It is based on the following workflow: preprocessing, feature extraction, matching, encryption and authenticated decryption. Preprocessing and feature extraction in

A. Preprocessing and Feature Extraction.

All the facial images are converted to grayscale and are resized to the same resolution. LBP is a local texture method which compares the intensity of the central pixel with that of its neighboring pixels: The codes that are obtained are stored in a normalized histogram to represent the facial image.

B. Facial Matching

The histogram of the query is compared to the enrolled histograms by calculating a distance. The recognised object is the one with the minimum distance. Both enrollment and recognition should employ the same preprocessing, same LBP parameters, and the same histogram construction. If the rejection of the unknown persons is used, the threshold will be set through validation samples.

C. Image Encryption and Recovery

The key is stored and transmitted separately from the Ciphertext, Nonce and Tag. In the case of authenticated decryption, the tag is checked prior to releasing the recovered image for use. In case of failure in authentication, record will be rejected. If it is successfully verified, the image can be reconstructed.

D. Implementation Scope

The prototype combines the load, recognize, encrypt and recover images. No encrypted domain computation as studied in [3],[4] will be considered in matching since it is not done on plain text facial descriptors. Template unlinkability/inversibility is not also established by image encryption, and needs to be evaluated separately [7].

IV. EXPERIMENTAL SETUP AND EVALUATION

A. Image Input and Application Setup

An image input is used to get an image by an application. An application takes an image from an image input. The actual face image was used as the input to the recognition, encryption and decryption process in the prototype. In the application, there are four display panels: The input image panel, The recognized reference image panel, The encrypted image visualization panel and the recovered image panel. Special controls allow each operation to be done in turn.

B. Evaluation Procedure

The image of the face was loaded into the application and sent for recognition to the reference images enrolled. Returned identity label and reference picture were examined. Then the input image was encrypted, and then decrypted to obtain the face image. Evaluation was based on the recognition output that was observed, visual concealment of facial content and visual consistency of recovered image. The experiment presented here is a functional demonstration with one of the subjects. The provided results did not set the size of the dataset, independent enrollment, or repeated-trial measurements.

V. RESULTS AND DISCUSSION

A. Recognition and Image Protection Results

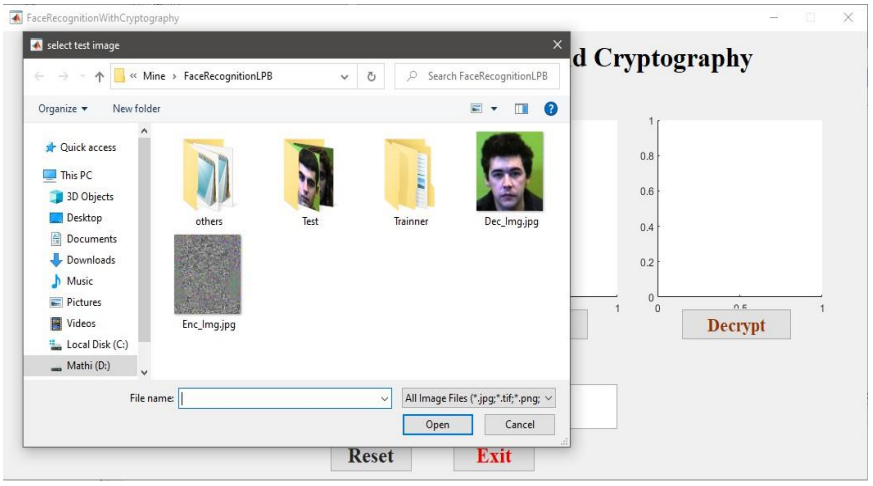
The results of this recognition and image protection were presented.This recognition and image protection results were presented. The application showed the face image and output the identity label “SHERINE” and the reference image. After being encrypted, a noise-like representation emerged in the encrypted output panel. The text was decrypted to yield a recognizable facial image that was visually consistent with the input. A summary of these observations is given in Table I.

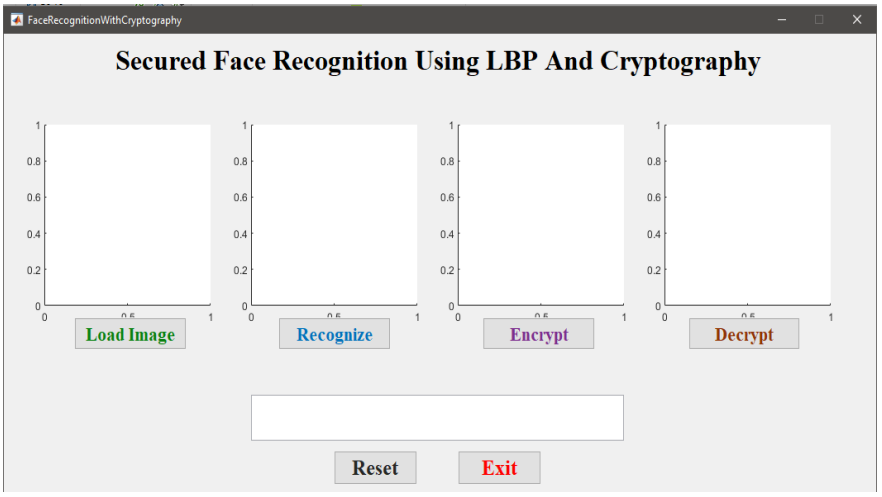
Operation	Observed result
Face image loaded	The face image was displayed in the input panel.
Face recognition:	The reference image and the identity label “SHERINE” were shown.
Encryption	A noise-like visualization appeared with the message “Image Encrypted.”
Decryption	The recovered face image was displayed with the message, “Image Decrypted.”

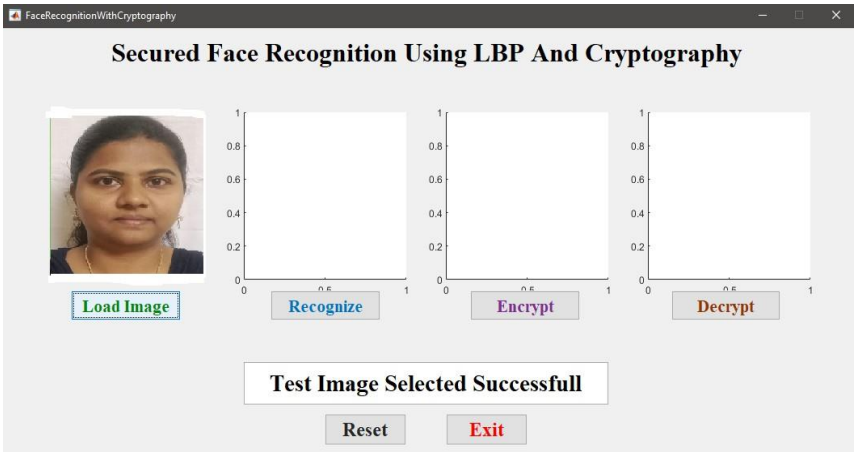
Observed Results of the Prototype Demonstration

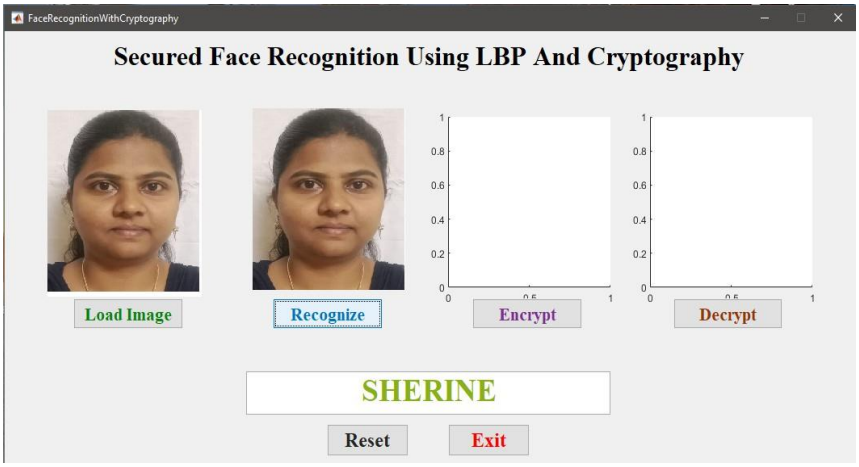
B. Discussion and Limitations:

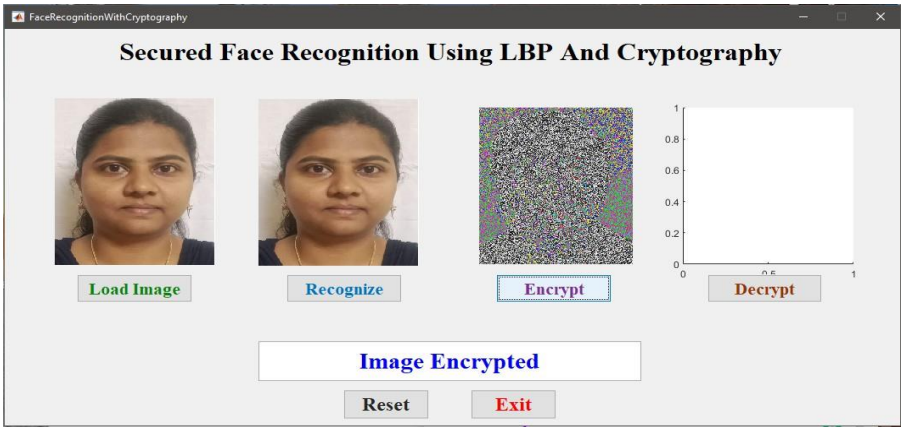
The results demonstrate the implementation of the recognition of images as well as their encryption and recovery in one application. The recognition example shows the output of the desired face identities, and the encrypted visualization obscures the face material that could be used to recognize the faces. The recovered image is a visual proof of the decryption process illustrated. These observations can be used as a working prototype! The level of recognition accuracy achieved with a single example is not necessarily the level of accuracy achieved with the other subjects and lighting, pose and expression. Similarly, visual concealment does not mean cryptographic security, and visual recovery does not mean a "byte-for-byte recovery", or that an authentication-tag has been recovered. Other tests are rejection of modified encrypted records, exact recovery tests, processing-time measurements, multiple subjects and independent face images. The four prototype demonstrations shown with an actual face image: (a) loading image, (b) recognition output, (c) visualization of encrypted image and (d) recovery of decrypted image.

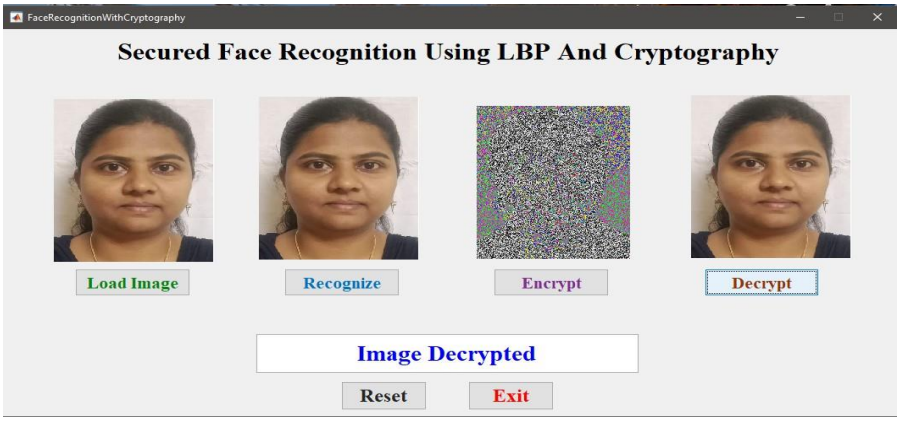





FaceRecognitionWithCryptography
Secured Face Recognition Using LBP And Cryptography
Load Image
Recognize
Encrypt
Decrypt
Test Image Selected Successfull
Reset
Exit


FaceRecognitionWithCryptography
Secured Face Recognition Using LBP And Cryptography
Load Image
Recognize
Encrypt
Decrypt
SHERINE
Reset
Exit


FaceRecognitionWithCryptography
Secured Face Recognition Using LBP And Cryptography
Load Image
Recognize
Encrypt
Decrypt
Image Encrypted
Reset
Exit


FaceRecognitionWithCryptography
Secured Face Recognition Using LBP And Cryptography
Load Image
Recognize
Encrypt
Decrypt
Image Decrypted
Reset
Exit

VI. CONCLUSION AND FUTURE WORK

In the present paper, the proposed system was introduced that integrated the face recognition technology based on LBP and protect the image using AES–GCM. Using a real-time face image as the demonstration, it showed the results of the recognition of the image, encrypted image visualization, and the recovery of the image. The following is a list of some of the observations for the recognition and image protection that are observed in one interface. The accuracy of the recognition, processing speed or tamper resistance is not demonstrated through this demonstration. Future tests will include various subjects, independent enrolment and test images, recognition performance, cryptographic overhead, and true image recovery and rejection of altered encrypted images. The approach will be further assessed under varying light conditions, poses and expressions to determine the applicability of the approach.

REFERENCES

1. Z. Sun and Z. Liu, "Ensuring privacy in face recognition: A survey on data generation, inference and storage," *Discover Applied Sciences*, vol. 7, Art. no. 441, 2025, doi: 10.1007/s42452-025-06987-2.
2. L. Laishram, M. Shaheryar, J. T. Lee, and S. K. Jung, "Toward a privacy-preserving face recognition system: A survey of leakages and solutions," *ACM Computing Surveys*, vol. 57, no. 6, Art. no. 147, 2025, doi: 10.1145/3673224.
3. W. Ao and V. N. Boddeti, "CryptoFace: End-to-end encrypted face recognition," in *Proc. IEEE/CVF Conf. Computer Vision and Pattern Recognition (CVPR)*, 2025, pp. 19197–19206.
4. S. Kim, S. Paik, C. Hwang, D. Kim, J. Shin, and J. H. Seo, "IDFace: Face template protection for efficient and secure identification," in *Proc. IEEE/CVF Int. Conf. Computer Vision (ICCV)*, 2025, pp. 13995–14005.
5. Y. Huang, Z. Wu, J. Chen, and H. Xiang, "Privacy-preserving face recognition method based on randomization and local feature learning," *Journal of Imaging*, vol. 10, no. 3, Art. no. 59, 2024, doi: 10.3390/jimaging10030059.
6. S. Kim, H. Shin, and J. H. Seo, "Deep face template protection in the wild," *Pattern Recognition*, vol. 162, Art. no. 111336, 2025, doi: 10.1016/j.patcog.2024.111336.
7. H. Otroshi Shahreza *et al.*, "Benchmarking of cancelable biometrics for deep templates," *Journal on Image and Video Processing*, vol. 2026, Art. no. 4, 2026, doi: 10.1186/s13640-025-00679-y.
8. H. Otroshi Shahreza and S. Marcel, "Template inversion attack against face recognition systems using 3D face reconstruction," in *Proc. IEEE/CVF Int. Conf. Computer Vision (ICCV)*, 2023, pp. 19662–19672.
9. A. Bassit, F. Hahn, Z. Rezgui, H. O. Shahreza, R. Veldhuis, and A. Peter, "Template recovery attack on encrypted face recognition systems with unprotected decision using synthetic faces," *Frontiers in Imaging*, vol. 4, Art. no. 1476377, 2025, doi: 10.3389/fimag.2025.1476377.
10. S. M. Abdullahi, S. Sun, B. Wang, N. Wei, and H. Wang, "Biometric template attacks and recent protection mechanisms: A survey," *Information Fusion*, vol. 103, Art. no. 102144, 2024, doi: 10.1016/j.inffus.2023.102144. 9–423, Jul. 194