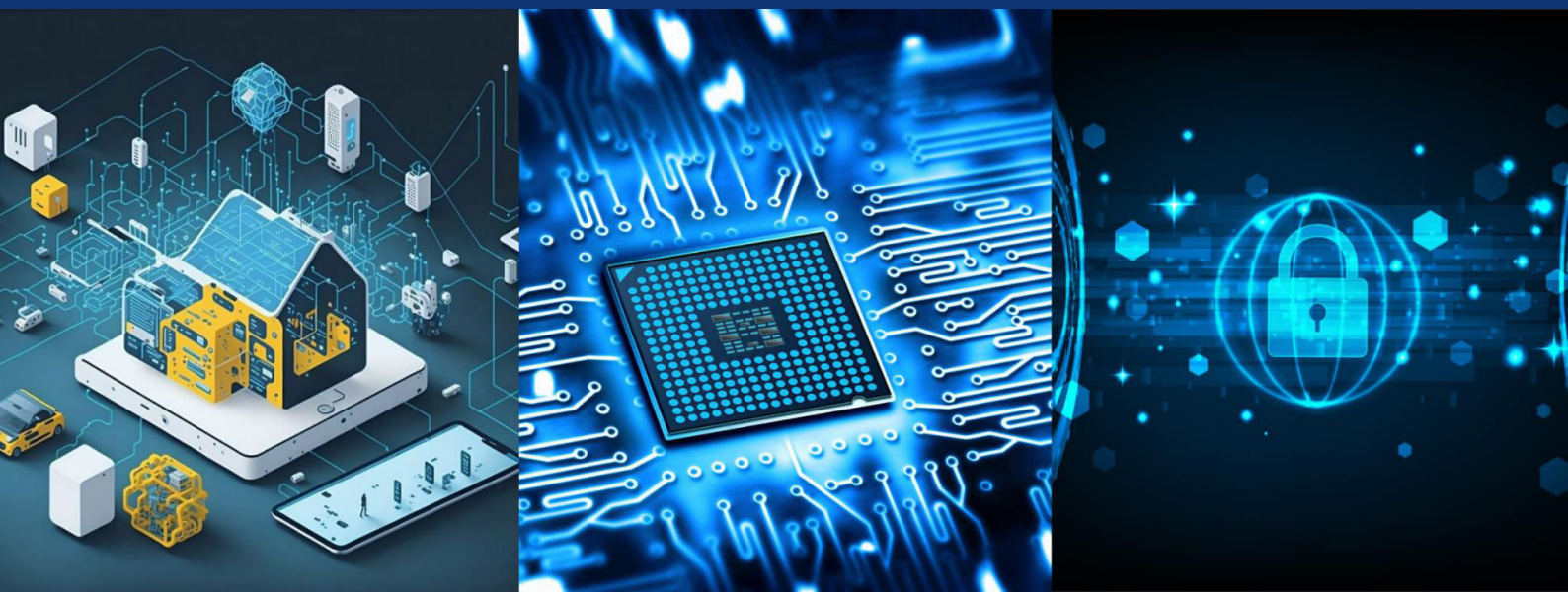
IJIRCCE

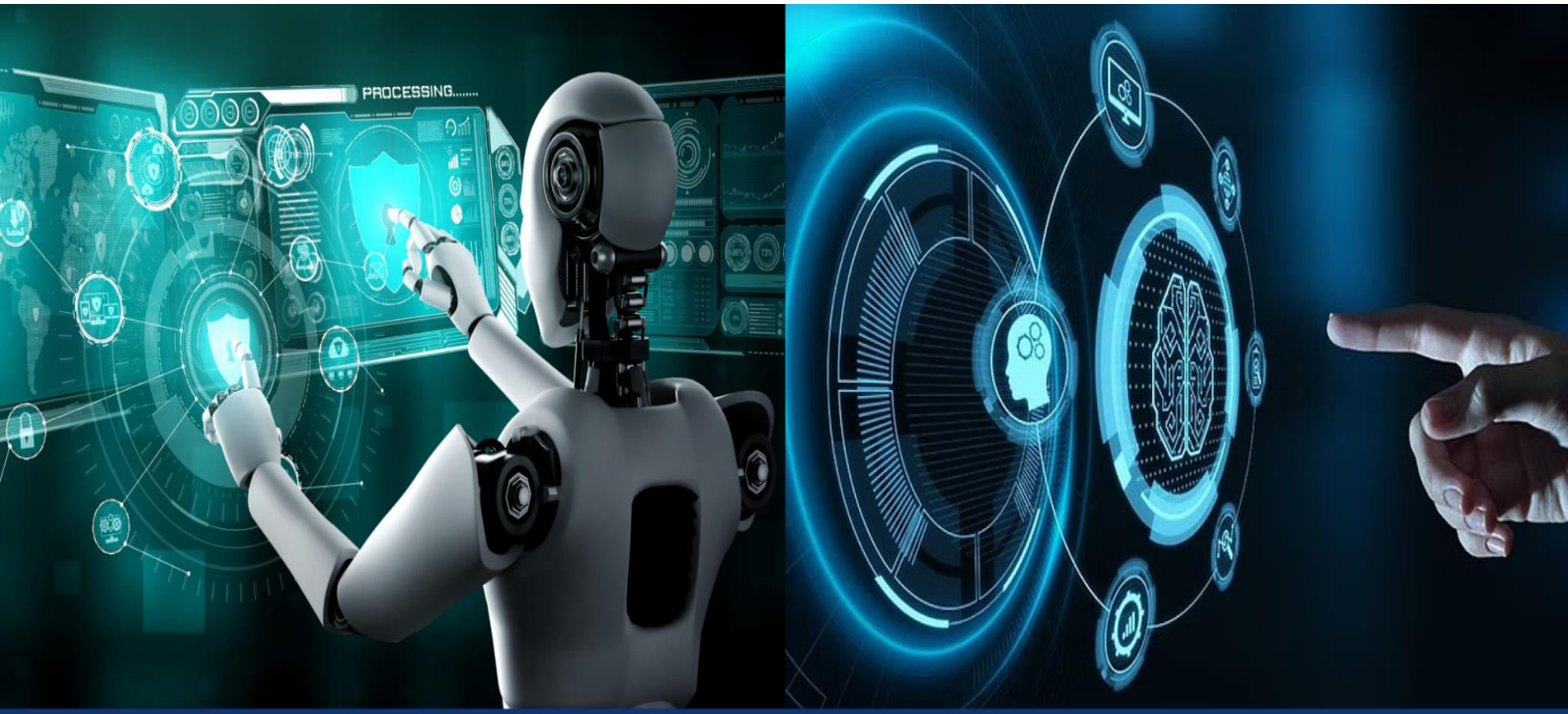
ISSN(O): 2320-9801

ISSN(P): 2320-9798



# International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)




**Impact Factor: 8.625**

**Volume 13, Issue 1, January 2025**

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301027

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

# Encryption of Biometric Traits for Privacy Attacks using AES Encryption

**Karen Rena C[1], Samprity Singha[2], Pavaman S Suraj[3], Himansu Sekhar Rout[4]**

UG Student, Department of Computer Science and Engineering, Presidency University, Bengaluru, Karnataka, India

UG Student, Department of Computer Science and Engineering, Presidency University, Bengaluru, Karnataka, India

UG Student, Department of Computer Science and Engineering, Presidency University, Bengaluru, Karnataka, India

Assistant Professor, Department of Information Science, Presidency University, Bengaluru, Karnataka, India

**ABSTRACT:** Biometric systems are pivotal for secure authentication due to their reliance on unique physical traits. However, their increased adoption raises concerns about data privacy and security. This study introduces a novel framework combining multimodal biometrics, machine learning, and Advanced Encryption Standard (AES) encryption to mitigate these concerns. Iris and facial biometrics are processed to generate cryptographic keys, leveraging pre-trained Convolutional Neural Networks (CNN) and Principal Component Analysis (PCA) for robust feature extraction. A 256-bit AES key is derived from fused biometric data and employed in Galois/Counter Mode (GCM) for encryption, ensuring data confidentiality and integrity. This research demonstrates a scalable, secure, and privacy-preserving system suitable for real-world applications.

**KEYWORDS**: Biometric encryption; multimodal biometrics; AES encryption; machine learning; privacy protection

## I. INTRODUCTION

This research, titled "Encryption of Biometric Traits to Avoid Privacy Attacks," proposes an advanced framework to address these challenges. By integrating multimodal biometrics (iris and facial features) with cryptographic techniques, the framework enhances the security of biometric systems. Machine learning is employed to extract features dynamically and accurately, while the Advanced Encryption Standard (AES) ensures robust data encryption. The proposed bio-cryptosystem combines authentication and data confidentiality, creating a scalable and secure solution suitable for real-world applications.

### A. Biometric Systems and Cryptography

Biometric systems authenticate individuals based on their inherent traits, which are unique and challenging to replicate. These traits include physical attributes like fingerprints and iris patterns, as well as behavioural characteristics like voice and gait. Biometric authentication is gaining prominence due to its convenience and robustness compared to traditional methods. However, its security can be significantly enhanced when paired with cryptographic techniques, providing an additional layer of protection against unauthorized access.

Bio-cryptosystems merge the strengths of biometric authentication and cryptography to provide dual-layer security. Unlike traditional systems that rely on passwords or tokens, bio-cryptosystems derive cryptographic keys directly from biometric traits or secure stored templates using cipher transformations. This dual-layer approach ensures data integrity and user privacy while reducing vulnerabilities to theft or replay attacks.

### B. Cryptographic Techniques in Biometric

a) Advanced Encryption Standard (AES)

AES is a widely used encryption algorithm known for its efficiency and robustness. It is particularly suitable for biometric systems, as it ensures data confidentiality by encrypting sensitive information such as biometric templates or derived keys. In this research, a 256-bit AES encryption key is dynamically generated from fused biometric features. AES's adaptability to image data further enhances its suitability for securing multimodal biometric systems.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

b) S-Box Optimization in AES

The Substitution Box (S-Box) is a critical component of AES, responsible for introducing non-linearity into the encryption process. Optimizing S-Box designs enhances the algorithm's resistance to cryptographic attacks while maintaining performance. This research employs AES in Galois/Counter Mode (AES-GCM), which provides both encryption and authentication simultaneously, making it ideal for applications requiring high security and speed.

c) Biometric Key-Based Encryption

The use of biometric features to generate cryptographic keys eliminates the need for traditional passwords. Techniques like quantization-based key generation and bio-hashing ensure that biometric-derived keys are stable, secure, and resistant to errors in data acquisition.

- Quantization-Based Key Generation: Continuous biometric features are converted into discrete binary keys using quantization, ensuring consistency.
- Bio-Hashing: Combines biometric traits with random seeds to generate secure hash-based keys, providing resistance against inversion and replay attacks.

C. Machine Learning in Biometrics

Machine learning (ML) enhances the reliability and adaptability of biometric systems by optimizing feature extraction, anomaly detection, and multimodal fusion. Algorithms like support vector machines (SVMs) and deep learning models, such as Convolutional Neural Networks (CNNs), play a crucial role in processing biometric data for accurate authentication and key generation.

Deep learning models dynamically learn intricate feature representations, improving system robustness and reducing False Match Rates (FMR). For example:

- VGG (Visual Geometry Group): Extracts fine-grained textural details from iris patterns, crucial for unique key generation.
- ResNet (Residual Networks): Handles variations like illumination changes or occlusions in biometric data, ensuring reliable feature extraction.

By leveraging these models, the system achieves precise and consistent biometric key generation, crucial for robust encryption.

D. Multimodal Biometrics

Multimodal biometric systems use multiple traits (e.g., iris and facial features) to enhance authentication reliability. They improve resistance to spoofing and environmental variability, ensuring robustness even under challenging conditions. Machine learning facilitates efficient fusion of multimodal biometric data. By identifying patterns across different modalities, ML enhances system accuracy, scalability, and resilience to noise or attacks.

Combining data from different modalities enhances system performance. Fusion can occur at various levels:

- Feature-Level Fusion: Creates a single representation by combining the raw features from various modalities.
- Score-Level Fusion: Aggregates individual modality scores to make authentication decisions.
- Decision-Level Fusion: Integrates outputs from separate classifiers for final decision-making.

## II. LITERATURE SURVEY

The integration of biometrics, machine learning, and cryptography has transformed secure authentication systems, addressing challenges of data confidentiality, system robustness, and the limitations of traditional cryptographic methods. The adoption of multimodal biometric features, such as iris and face recognition, enhances security by reducing false acceptance rates and improving user experience.

Machine learning plays a critical role in modern biometric systems by enabling accurate feature extraction and adaptability. As noted in [1], machine learning facilitates the analysis of large datasets, identifying patterns, and predicting future authentication attempts, ensuring robustness against evolving threats. Advanced deep learning models,

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

like CNNs and RNNs, improve biometric systems by extracting high-level feature representations and increasing accuracy [8].

Cryptographic techniques, particularly AES, further fortify biometric systems. AES is efficient and secure for encrypting biometric data, with dynamically generated keys eliminating the need for traditional passwords or tokens [2]. Enhanced implementations, like the Bio-Metric 256-bit AES algorithm [6], address traditional key management challenges while maintaining robust security.

Multimodal biometric systems, leveraging traits like iris and face, address the limitations of unimodal systems. Fusion strategies—feature-level, score-level, and decision-level—improve accuracy and resilience to spoofing [5]. Preprocessing methods, such as wavelet transforms, ensure reliable feature extraction even from noisy or low-quality images [7]. Machine learning-based fusion further strengthens these systems by optimizing multimodal data integration [5].

Despite their advantages, biometric systems face challenges such as computational complexity, data quality dependence, and latency. Fusion strategies and deep learning algorithms often introduce significant processing overhead [5], limiting real-time applicability. Furthermore, variations in input image quality can affect key reliability, and the success of anti-spoofing measures depends on dataset diversity during training [5]. These limitations emphasize the need for optimization to enhance scalability and robustness in diverse environments.

The combination of AES encryption, machine learning, and multimodal biometrics represents a critical advancement in secure and user-friendly authentication. Ongoing research focuses on improving real-time performance, mitigating attacks, and addressing privacy concerns associated with biometric data storage and transmission.

## III. METHODOLOGY

The system integrates the following elements to create a secure biometric authentication pipeline:

- Biometric Data Acquisition: Standardizes and enhances iris and facial images to ensure consistency in feature extraction.
- Feature Extraction Using Machine Learning: Employs CNNs for iris data and PCA for facial data to capture unique patterns.
- Feature Fusion and Quantization-Based Key Generation: Combines extracted features and quantizes them into a 256-bit cryptographic key.
- AES Encryption in GCM Mode: Secures and decrypts user-provided data with the biometric key.
- Streamlit-Based User Interface: Offers an intuitive platform for feature generation, encryption, and decryption.

The project focuses on developing a robust system to enhance the security of multimodal biometric authentication by integrating iris and facial biometrics, quantization-based key generation, and AES encryption in Galois/Counter Mode (GCM). The system employs machine learning techniques, including Convolutional Neural Networks (CNNs) for iris feature extraction and Principal Component Analysis (PCA) for facial data. This approach ensures privacy, mitigates computational overhead, and enhances data integrity.

A. Data Acquisition and Preprocessing

The system utilizes publicly available datasets, such as the MMU-Iris Database and CelebA Dataset, to collect iris and facial biometric data. These datasets ensure diversity in demographics and environmental conditions, such as variations in lighting and occlusion, for robust system performance. Preprocessing of the data standardizes inputs for machine learning models and reduces variability caused by acquisition devices or environmental factors. For iris images, preprocessing involves grayscale conversion to simplify computations, resizing to a uniform resolution (128x128 pixels), and normalization of pixel values to the [0,1] range to improve compatibility with deep learning models.

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301027

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

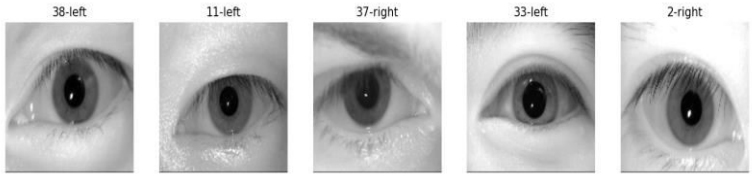



Figure 1.

Facial images are resized and vectorized, followed by a dimensionality reduction process using Principal Component Analysis (PCA), which ensures computational efficiency while retaining critical features. This visualization shows the number of positive values(1) for each facial attribute.

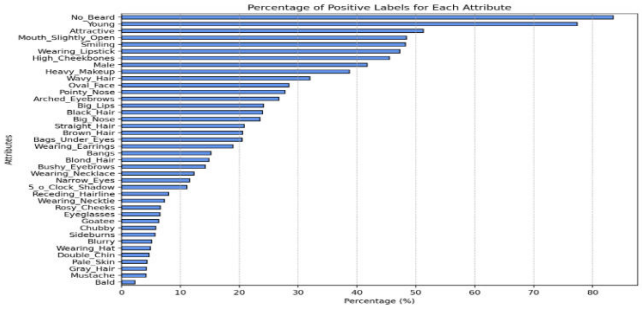



Figure 2.

B. Feature Extraction Using Machine Learning

Feature extraction from biometric data is accomplished using advanced machine learning techniques. For iris images, a pre-trained VGG16 Convolutional Neural Network (CNN) captures intricate hierarchical features, including fine-grained textural details such as crypts and furrows. The images are resized to 224x224 pixels and processed through multiple convolutional and pooling layers to generate high-dimensional embeddings, which can be optionally refined to retain only the most significant features. For facial data, PCA is applied to compute principal components that capture the highest variance in the data. This dimensionality reduction significantly reduces redundancy, yielding compact feature vectors while preserving essential facial traits. Together, these techniques ensure the extraction of robust and meaningful features for subsequent fusion and encryption.

C. Multimodal Feature Fusion

To enhance security and accuracy, the extracted features from iris and facial biometrics are combined through feature-level fusion. Before fusion, the dimensions of both modalities are aligned for compatibility. The iris embeddings and facial feature vectors are then concatenated horizontally to form a unified biometric feature template. Randomization techniques are applied to the combined features to obfuscate their direct relation to the original traits, adding an extra layer of security. This fusion process improves system resilience against spoofing attacks and enhances accuracy, even in scenarios where one modality may fail.

D. Biometric Key Generation

The fused biometric template is used to generate cryptographic keys securely and efficiently. Quantization techniques are employed to map continuous feature values into discrete binary keys, ensuring consistency and reproducibility. These binary keys are then grouped and transformed into a 256-bit cryptographic key, which serves as the critical input for encryption and decryption. To ensure long-term security, cancellable transformations are implemented, allowing compromised keys to be revoked and replaced without altering the underlying biometric data.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

E. Data Encryption Using AES-GCM

AES-GCM (Galois/Counter Mode) encryption ensures robust data confidentiality and integrity. The biometric-derived 256-bit key is used to encrypt data, such as text or images, with each session generating a unique nonce to ensure that even identical inputs produce different ciphertexts. The encryption process also generates an authentication tag to verify data integrity and detect tampering. The ciphertext is verified against the authentication tag during decryption, which calls for the same key and nonce. AES-GCM offers high-speed encryption, message authentication, and flexibility, making it ideal for securing biometric data.

F. User Interface

A user-friendly Streamlit - based frontend is developed to facilitate system interaction. Users can upload precomputed biometric features in .npy format or dynamically generate new features using the backend pipeline. The interface allows users to adjust parameters for quantization, encrypt or decrypt data, and view outputs such as encrypted data, nonces, and authentication tags. This intuitive design ensures accessibility and ease of use for real-world applications.

G. Techniques Used

The system uses advanced techniques to enhance feature extraction and encryption efficiency:

- VGG16 (Visual Geometry Group 16): A pre-trained CNN with 16 layers, capable of learning spatial hierarchies of features ranging from edges to textures. It employs small 3x3 convolutional filters and deep architectures for high performance on image recognition tasks.
- Principal Component Analysis (PCA): A dimensionality reduction technique that transforms high-dimensional data into a lower-dimensional space by identifying principal components with maximum variance. It reduces redundancy in facial data while retaining critical features.
- Quantization: Maps continuous feature values into discrete bins. This system quantizes features into 16 bins, representing them as binary strings to form cryptographic keys.
- AES-GCM (Advanced Encryption Standard in Galois/Counter Mode): A symmetric encryption algorithm that ensures data confidentiality and integrity. It combines encryption with integrity verification, outputting ciphertext, a nonce, and an authentication tag.

## IV. RESULTS AND DISCUSSION

A. Results

The results generated by the system demonstrate the efficiency, accuracy, and security of the implemented multimodal biometric encryption system. Below, the results are analyzed in detail alongside their implications.

1. Feature Extraction, Processing and Combination

a) Preprocessed Iris Images

The iris data preprocessing pipeline efficiently standardized 450 iris images from the MMU-Iris Database. Each image was resized to 224x224 pixels, normalized to the range [0,1], and converted to grayscale, ensuring compatibility with the VGG16 CNN model. The resulting dataset shape of (450, 224, 224, 3) demonstrates uniformity and readiness for hierarchical feature extraction. This preprocessing ensured the retention of essential textural details necessary for accurate biometric recognition. In [7] used traditional algorithms for feature extraction, which were computationally lightweight but lacked the depth of texture retention achieved by CNN models.

b) CNN Feature Extraction (Iris)

Using the VGG16 model, feature extraction for 450 iris images produced high-dimensional embeddings with a feature vector size of 25088 for each image. These embeddings effectively captured intricate hierarchical patterns, such as crypts and textures unique to individual irises. The resulting heatmap (Figure 3) highlights the diversity and range of

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

feature activations across the dataset, showcasing variations in intensity that reflect the discriminative power of the extracted features. The extraction process, completed in 263 seconds, demonstrated high computational efficiency in generating robust and meaningful representations of iris characteristics. In [5] they leveraged CNNs but highlighted challenges with dataset inconsistencies. This research dataset uniformity and processing pipeline overcame these challenges, ensuring robust feature activations. This visualization further emphasizes the ability of CNN-based feature extraction to encode essential details for downstream biometric fusion and encryption tasks. The subset of the data is displayed in this heatmap (10 samples and 65 features).

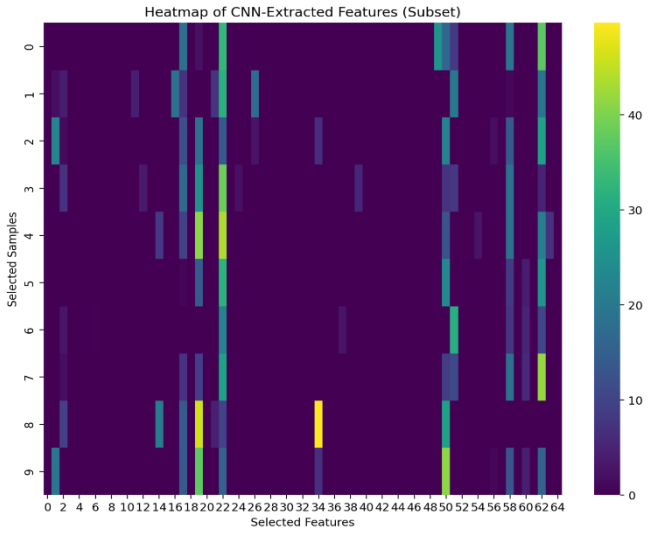



Figure 3.

c) PCA Face Attribute Analysis

Principal Component Analysis (PCA) was applied to the facial attribute data from the CelebA dataset to reduce the dimensionality of the feature space while preserving the most significant features. The explained variance ratio plot (Figure 4) highlights that the first few principal components account for the majority of the variance, with a steep decline in variance contribution as additional components are included. The cumulative explained variance plot (Figure 5) shows that approximately 34 principal components are required to retain 95.43% of the total variance, indicating the importance of considering more components for preserving critical facial features. Compared to [9], which used binary feature quantization for dimensionality reduction, the PCA approach in this research offers a broader and computationally efficient solution to retain critical variance while discarding redundant features.

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301027

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

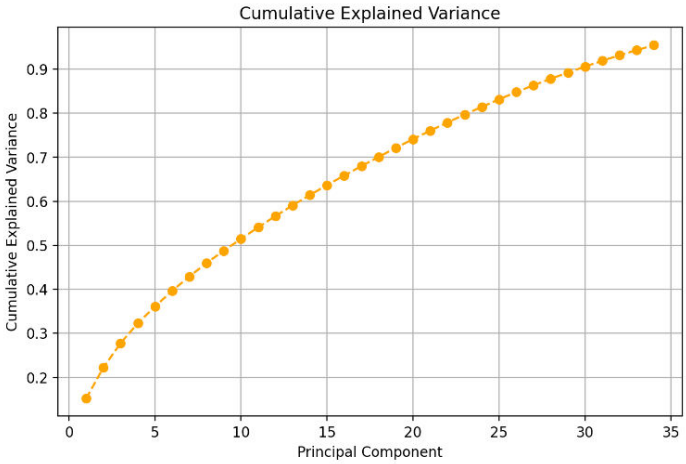



Figure 4.

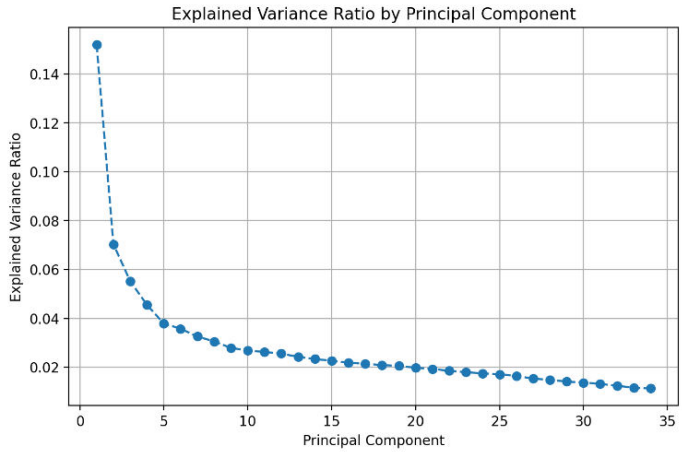



Figure 5.

d) Multimodal Feature Combination

The iris feature vectors (25088 dimensions) were combined with the face feature vectors (10 dimensions) for each of the 450 samples. The resultant combined feature matrix had a shape of (450, 25098), creating a comprehensive multimodal biometric template. Researchers in [3] implemented iris-only templates, but our research results highlight that multimodal fusion offers superior resistance to spoofing attacks and single-modality failures. This fusion effectively leveraged the strengths of both modalities, ensuring the generation of robust keys suitable for encryption while enhancing the system's resistance to spoofing attacks.

2. Key Generation and Cryptographic Results

a) Binary Key Generation

Using quantization techniques, the biometric features were converted into binary representations to produce a binary key. This transformation maps continuous feature values into discrete bins and encodes them as binary sequences. The binary sequence reflects the quantized biometric data and forms the foundation for cryptographic operations. For example, the binary key generated for the first sample was as follows:

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

BinaryKey: 00000000000000000000000...00000000000000000110000000000000000000

b) AES Key Transformation

The binary key was transformed into a 256-bit AES-compatible key in hexadecimal format, ensuring compatibility with the AES-GCM encryption algorithm. The derived key is unique and represents a critical link between biometric features and cryptographic security. Consistent with the approach in [2], the transformation of biometric features into cryptographic keys demonstrates high security by aligning with modern cryptographic standards. An example of a derived AES key is as follows:
AES Key (Hex):
0000000000000000000000000000300000000000000000000000d000000000000

3. AES Encryption and Decryption Results

Sensitive information was encrypted using the derived AES key in Galois/Counter Mode (GCM). The ciphertext ensures confidentiality, making it computationally infeasible to retrieve the original plaintext without the same biometric-derived AES key. The encryption process produced the following ciphertext in hexadecimal format:
Input: Sensitive Information
Encrypted Data (Hex): ed3837c505d7707a3d174719daa204a876c7346eaa

a) Nonce (Number Used Once)

Each encryption session generated a unique nonce, ensuring that even identical plaintexts encrypted with the same key would produce different ciphertexts. The nonce must be securely transmitted along with the ciphertext for successful decryption.For example:
Nonce: 2655ec3bde2f2cc981315cdc873a035e

b) Authentication Tag

The AES-GCM encryption process produced an authentication tag to verify the integrity of the ciphertext. During decryption, the authentication tag ensures that the encrypted data has not been modified or tampered with. An example tag is:
Authentication Tag: 5032e0c6c7b6b846cefcd707bc7c5026

c) Decryption

The encrypted data was successfully decrypted using the same AES key and nonce, recovering the original plaintext:
Decryption Output: Sensitive information
This result confirms the system's ability to maintain both confidentiality and integrity throughout the encryption and decryption process.

B. Discussions

Key Findings
•The system demonstrated strong biometric key reliability by extracting features directly from biometric data, reducing dependency on external passwords or keys.
•The trade-off between quantization bins and key entropy is critical; increasing bins improves key randomness but requires higher feature precision.
•Potential extensions include incorporating additional biometric modalities (e.g., fingerprint, voice) to enhance key robustness.

The proposed system demonstrates significant advancements in secure multimodal biometric encryption, addressing challenges in data integrity, scalability, and privacy. By extracting cryptographic keys directly from biometric data, it eliminates the need for external passwords or tokens, ensuring strong reliability and reducing dependency on

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

conventional security methods. The quantization-based key generation approach enables error tolerance, allowing the system to handle minor variations in biometric inputs such as noise and illumination changes. The generated 256-bit AES keys meet modern cryptographic standards, ensuring robust protection against brute-force attacks.

PCA's impact on facial attributes was pivotal in reducing dimensionality while retaining critical variance. This optimization improved processing speed and interpretability without significant loss of feature quality. The combination of CNN-based iris feature extraction and PCA-reduced facial data resulted in a robust multimodal representation. This fusion of modalities enhances system accuracy and resilience, ensuring robustness against single-modality failures and spoofing attacks.

The integration of AES-GCM provided both encryption and integrity verification, with the authentication tag mechanism ensuring data authenticity and resistance to tampering. The system's dynamic key generation eliminates the need to store raw biometric data, addressing privacy concerns and aligning with data protection regulations. These features make the system suitable for high-security applications like identity verification, secure data transmission, and access control.

Additionally, expanding datasets to include more demographic diversity and environmental variability would enhance model generalizability. Incorporating additional biometric modalities, such as fingerprints or voice data, could further improve system robustness and security.

In summary, the system offers a secure and efficient framework for multimodal biometric encryption. By combining advanced cryptographic techniques and machine learning, it ensures robust protection of sensitive information, scalability for real-world applications, and adaptability for future.

## V. CONCLUSION

This project successfully demonstrated the integration of iris and facial biometrics to generate secure binary keys for AES encryption, establishing a robust and efficient pipeline for biometric-based cryptographic applications. By utilizing pre-trained CNNs (VGG16) for iris feature extraction, PCA for dimensionality reduction of facial attributes, and quantization techniques for binary key generation, the system achieved strong performance in both security and computational efficiency. The dynamic biometric key generation process ensures privacy by eliminating the need to store raw biometric data, addressing critical security and privacy concerns.

The inclusion of a user-friendly Streamlit interface further enhances the system's practicality, making it accessible for real-world applications like secure data storage, authentication systems, and identity verification. The modular design of the workflow supports scalability, enabling the integration of additional biometric modalities such as fingerprints or voice data, as well as exploring alternative encryption techniques. These features make the system adaptable for future advancements and large-scale deployments.

This project lays the groundwork for further exploration in the field of biometric-based encryption. Future work could focus on improving feature extraction techniques with advanced machine learning algorithms, optimizing key entropy through enhanced quantization methods, and incorporating more diverse datasets to improve generalizability. With its secure, scalable, and user-friendly design, this system highlights the potential of integrating biometrics and cryptography for applications in healthcare, banking, secure communication, and beyond.

## REFERENCES

[1] Hooda, Susheela & Shrivastav, Supriya & Sharma, Preeti. (2023). A Study on Biometrics and Machine Learning. 1-5. https://ieeexplore.ieee.org/document/10368885

[2] S. Nagaraj , R. Nagendra, Shanmugham Balasundaram, R. Kiran Kumar (2023). Biometric key generation and multi round AES crypto system for improved security. https://www-sciencedirect-com-presiuniv.knimbus.com/science/article/pii/S2665917423002672

[3] Ramisetty, Srividya & B., Ramesh. (2019). Implementation of AES using biometric. International Journal of Electrical and Computer Engineering (IJECE). http://doi.org/10.11591/ijece.v9i5.pp4266-4276

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[4] S. Pooja, C. V. Arjun and S. Chethan, "Symmetric key generation with multimodal biometrics: A survey," 2016 International Conference on Circuits, Controls, Communications and Computing (I4C), Bangalore, India, 2016, pp. 1-5. https://ieeexplore.ieee.org/document/8053273

[5] Praveen, s & Vellela, Sai Srinivas & Ramachandran, Balamanigandan. (2024). SmartIris ML: Harnessing Machine Learning for Enhanced Multi-Biometric Authentication. https://www.researchgate.net/publication/378439449_SmartIris_ML_Harnessing_Machine_Learning_for_Enhanced_Multi-Biometric_Authentication

[6] Rachana Veerabommala, Greeshma Arya, 2022, Design And Implementation of AES Algorithm with Biometric Key Schedule to Improve Security, (IJERT) Volume 11, Issue 06 (June 2022) https://www.ijert.org/design-and-implementation-of-aes-algorithm-with-biometric-key-schedule-to-improve-security

[7] W. Wei and Z. Jun, Image encryption algorithm Based on the key extracted from iris characteristics, 2013 IEEE 14th International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, Hungary, 2013, pp. 169-172. https://ieeexplore.ieee.org/document/6705185

[8] Ghilom, Milkias & Latifi, Shahram. (2024). The Role of Machine Learning in Advanced Biometric Systems. Electronics. 13. 2667. https://doi.org/10.3390/electronics13132667

[9] Amir Anees, Yi-Ping Phoebe Chen. Discriminative binary feature learning and quantization in biometric key generation, Pattern Recognition, Volume 77, 2018, Pages 289-305, ISSN 0031-3203, https://doi.org/10.1016/j.patcog.2017.11.018

[10] Yanzhi Chen, Yan Wo, Renjie Xie, Chudan Wu, Guoqiang Han. Deep Secure Quantization: On secure biometric hashing against similarity-based attacks, Signal Processing, Volume 154, 2019, Pages 314-323, ISSN 0165-1684, https://doi.org/10.1016/j.sigpro.2018.09.013

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details