International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 01 | Jan - 2025 SJIF Rating: 8.448 ISSN: 2582-3930

Encryption of Biometric Traits to Avoid Privacy Attacks

Tripurari Vinay Karthik
Dept of CSE
Presidency University
Bangalore, India

Polisetti Jyothi Sri
Dept of CSE
Presidency University
Bangalore, India

Veguru Mahitha Reddy
Dept of CSE
Presidency University
Bangalore, India

Dr.Ranjitha P
Assistant Professor
Dept of CSE
Presidency University
Bangalore, India

Abstract- In the modern digital world, biometric systems are a significant part of personal identification and access control. The use of sensitive biometric data such as iris and facial features raises huge privacy concerns because of the possibilities of data breaches and misuse. Therefore, this project focuses on the enhancement of the security of multimodal biometric systems through encryption mechanisms. The idea is to generate a strong biometric key based on features produced from iris and face biometric systems through advanced machine learning techniques. The features are then employed to produce a strong biometric key capable of encrypting the secret value using the AES algorithm. AES is a widely adopted symmetric encryption algorithm that ensures high efficiency in its software implementation and seamless processing capabilities of image data. This provides not only the reinforcement of authentication but also maintains confidentiality of biometric characteristics and mitigates the risks of privacy attacks and unauthorized access. Thus, this multimodal biometric encryption improves reliability, robustness, and the resistance power of the system against potential attacks, making it a promising step forward in the realm of secure biometric authenticationsystems.

Keywords- *Biometric encryption,Multimodal biometrics, ,Privacy attacks,Advanced Encryption Standard (AES), Biometric key generation,Iris recognition,Face recognition,Machine learning,Bio-crypto systems, Data security.*

I. INTRODUCTION

Biometric systems are very important in modern digital transformation times for ensuring safe authentication and access control. Biometrics, based on unique physical features such as fingerprints, iris patterns, and facial features, is intuitive and reliable to identify an individual. The reliance on biometric systems, however, has led to issues with privacy and potential unauthorized access or misuse of sensitive data. Privacy attacks against biometric databases can have very serious consequences, such as identity theft and unauthorized surveillance, and therefore require very strong security measures.

These factors motivate the current project: enhancing the security of multimodal biometric systems by incorporating advanced encryption techniques. Multimodal biometrics use two or more biometric traits, such as iris and facial features, and provide increased accuracy and resilience against spoofing attacks compared to unimodal systems. However, the security of such systems depends not only on accurate feature extraction but also on protecting the biometric data from malicious actors.

This project proposes a new approach of providing both authentication and confidentiality in this system using a secure biometric key produced through the machine learning technique aided by features derived from iris and face biometrics. This biometric key is utilized for encrypting secret information based on the symmetric AES algorithm, which is a proper choice for image data as it provides higher efficiency in its software-based implementation. This system, therefore, aims to reduce privacy risks, enhance data security, and provide a robust framework for secure biometric authentication by integrating multimodal feature extraction and AES encryption.

This introduction sets the foundation for understanding the importance of encryption in biometrics, the role of multimodal systems, and the integration of machine learning techniques to address privacy concerns effectively.

II. RESEARCH GAP OR EXISTING METHODS

1. Single -Modality Biometric Systems :

Single-modality biometric systems use a single biometric trait, such as fingerprints, facial features, iris patterns, voice, or hand geometry, for authentication.

Age Acquisition Issues :

Image acquisition is a critical step in biometric systems, as the quality of captured traits like fingerprints, facial features, or iris patterns directly impacts system performance.

2. Environmental Factors in Biometric Systems :

Environmental factors have a strong impact on the performance and accuracy of biometric systems. Poor environmental conditions result in increased error rates, lower reliability, and overall system inefficiency.

3. Stored Biometric Data Is Not Sufficiently Protected

Biometric systems depend on personal data to authenticate and identify an entity, such as fingerprints, facial features, or iris patterns. Unlike passwords or tokens, biometric traits cannot be changed once they are compromised; they remain the same. This places a necessity on the security of stored biometric data.

5. Limited Focus on Multimodal Biometric Encryption:

While multimodal biometric systems are recognized for their improved accuracy and robustness, limited research has been conducted on integrating advanced encryption mechanisms specifically designed for multimodal features like iris and facial traits

6. Vulnerability of Biometric Data to Privacy Attacks:

Despite the implementation of encryption techniques, biometric systems still face vulnerabilities to privacy attacks, such as data breaches or template reconstruction.

7. Lack of Comprehensive Testing on Real-World Datasets:

Many proposed systems are tested on limited or ideal datasets, which may not reflect real-world challenges such as noisy data, environmental variations, and partial occlusions.

8. Inefficiency in Software Implementation of Encryption Algorithms:

AES is widely used for securing biometric data, but its real-time software implementation for image encryption requires optimization to enhance speed and efficiency without compromising security.

9. Addressing Privacy and Legal Implications:

The ethical and legal implications of using encrypted biometric data have not been sufficiently addressed. Research is needed to align technical advancements with privacy-preserving frameworks and regulatory compliance.

III. TECHNOLOGIES USED

1. Machine Learning for Feature Extraction:

To extract unique features from biometric traits (iris and facial features) for robust biometric key generation.

- Deep Learning Frameworks: TensorFlow, PyTorch, or Keras for developing neural networks tailored to feature extraction tasks.
- Convolutional Neural Networks (CNNs): Widely used for processing image data to extract high-dimensional features from iris and face images.
- Principal Component Analysis (PCA) or Linear Discriminant Analysis (LDA): For dimensionality reduction and feature optimization.

2. Biometric Sensors and Image Acquisition Tools:

To capture high-quality biometric data for system input.

- High-Resolution Cameras: For capturing facial features and iris patterns.
- Infrared Sensors: To improve iris recognition accuracy under varying lighting conditions.
- Preprocessing Algorithms: For image enhancement (e.g., noise reduction, contrast adjustment).

3. Advanced Encryption Techniques:

To ensure the security and confidentiality of the biometric data.

- Advanced Encryption Standard (AES): A symmetric encryption algorithm used to encrypt the secret value using the generated biometric key.
- Key Expansion Algorithms: To enhance the robustness of the encryption key derived from biometric features.
- Cryptographic Libraries: OpenSSL or PyCryptodome for implementing AES encryption in software systems.

4.Multimodal Biometric Integration:

To combine multiple biometric traits (iris and facial features) for enhanced accuracy and security.

-

Fusion Techniques: Score-level fusion or feature-level fusion to integrate data from multiple modalities.

- Biometric Software Development Kits (SDKs): Tools like Neurotechnology's VeriLook and VeriEye for initial modality processing.

5. Data Storage and Security:
To store encrypted biometric data securely.

- Database Systems: MySQL, PostgreSQL, or MongoDB with encryption-at-rest and access control mechanisms.
- Secure Data Transmission: Using Transport Layer Security (TLS) protocols for data exchange between devices and servers.
- Tokenization: Replacing sensitive data with unique tokens to minimize exposure.

IV. PROPOSED METHODOLOGY

1. **Preprocessing Of Iris Image :**
   The first step involves capturing an image using an electronic device such as a digital camera or webcam. The captured image is stored in JPEG format and subsequently converted into a grayscale image for further processing.

2. **Resizing:**
   OpenCV's cv2.resize() resizes the iris image to a fixed resolution of 256x256 pixels, standardizing the input for consistent feature extraction. This preprocessing step removes noise and inconsistencies, ensuring the data is optimized for accurate analysis.

3. **Feature Extraction:**

   - 2D array of pixel values, the grayscale picture is then flattened into a 1D array.
   - This is then normalized to a flat image by rescaling the pixel values to [0, 1].
   - Instead of using all the pixel values, which can be computationally expensive and inefficient, only the first 50 values of the flattened and normalized image are chosen as features.

4. Biometric Key Generation

- Media The extracted iris features are converted into a unique 128-bit biometric key for AES encryption, scaled to meet AES key requirements. AES encryption secures sensitive data using the biometric key with CBC mode for added randomness and ensures full reversibility during decryption.
- A user-friendly Streamlit interface enables real-time iris data processing, encryption, decryption, and verification, providing interactive and secure functionality.

V. OBJECTIVES

The project develops a secure biometric encryption system using iris recognition to generate a unique AES encryption key for data protection. By leveraging iris patterns for key generation, the system enhances privacy and security. The objectives focus on implementing AES encryption to safeguard sensitive data with biometric-based keys.

1. **Biometric Key Generation Using Iris Recognition**:
   The project generates a 128-bit AES encryption key by extracting and normalizing features from an individual's iris image. These features are converted into a biometric key, enhancing security by replacing static passwords with a unique, biometric-based encryption method.
2. **AES Encryption and Decryption Using Biometric Key:**
   The project implements AES encryption using the biometric key in CBC mode to securely encrypt and decrypt sensitive data, ensuring confidentiality. The encryption process uses an initialization vector (IV) for added security, and decryption restores the data to its original form using the same biometric key.
3. **Data Privacy and Security Enhancement:** Prevention of Unauthorized Access: Since the biometric key is generated from the iris image, it is unique to each individual and difficult to replicate or intercept. The provided system makes it much harder for unauthorized parties to gain access to encrypted data, as they would need both the biometric trait and the decryption key.
4. **Protection Against Privacy Attacks:** Iris-based encryption protects data from privacy attacks like man-in-the-middle and brute-force attempts, as biometric traits are hard to steal. By using AES encryption with a biometric-derived key, the system ensures only authorized users can decrypt data. This approach significantly enhances data protection and privacy.
5. **User Interface For Real Time Interaction:** Streamlit to create a user-friendly interface for real-time interaction with the encryption system. Users can upload their iris images using the st.file_uploader() function, which generates biometric keys for encryption. The interface provides real-time visual feedback, including

preprocessed images, extracted features, biometric keys, encrypted data, and decrypted plaintext. This design ensures accessibility and builds user confidence in the system's functionality.

6. **Evaluation Of Security And Reliability:** Biometric encryption's security and reliability in real-world scenarios. Security testing ensures the resilience of iris-derived encryption keys against threats like brute force and key interception. Reliability tests confirm successful encryption and evaluations demonstrate the system's robustness and effectiveness.

VI. SYSTEM DESIGN AND IMPLEMENTATION

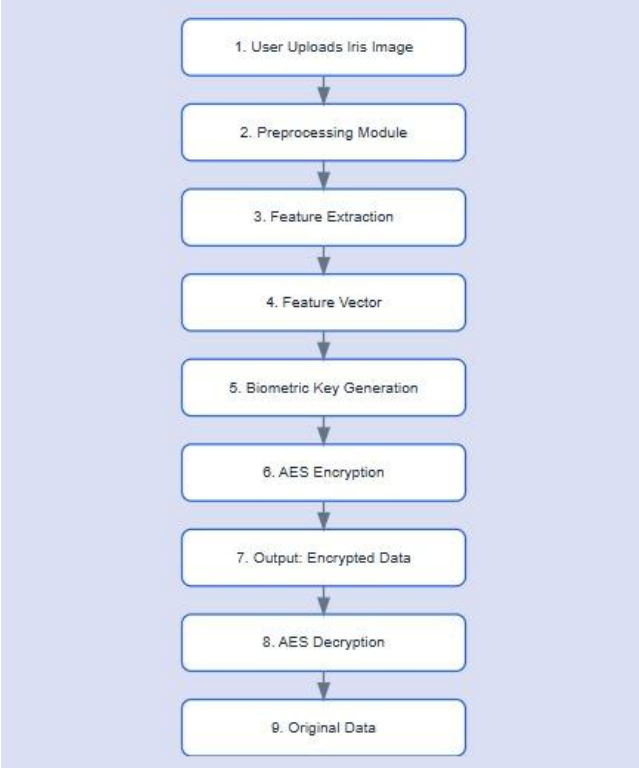

Fig: Work Flow Diagram of proposed system

The flowchart illustrates the process of biometric encryption using iris images, from image upload and preprocessing to feature extraction, biometric key generation, AES encryption/decryption, and retrieval of the original data. It highlights each step in the secure data encryption workflow.

VII. OUTCOMES

1. Enhanced Successful Integration Of Biometric-Based Encryption:

- Integrated iris recognition into the AES encryption algorithm, generating a unique biometric key for securing sensitive data. AES encryption in CBC mode ensures that only authorized individuals with access to the specific iris data can decrypt the information. This method enhances data security by replacing traditional passwords with a more secure, biometric-based approach.
- **I**ris-derived biometric keys with AES encryption, the project ensures secure data protection, making unauthorized access significantly more difficult.

2. Enhanced Data Privacy and Security

- **I**ris patterns provide a unique, non-replicable biometric key, significantly enhancing security over traditional passwords or PINs.
- AES encryption in CBC mode ensures that identical data results in different ciphertexts, increasing protection against repeated attacks.
- Biometric-based encryption prevents unauthorized access, protecting sensitive data from privacy breaches and identity theft.

3. User-Friendly Interaction with the System

- The system allows users to upload and display iris images in various formats (JPG, PNG, BMP) for processing.
- Step-by-step breakdown of the process, from preprocessing the iris image to generating the biometric key and performing AES encryption/decryption.
- Real-time feedback ensures users can interact with the system and view both encrypted and decrypted data for better understanding of the process.

4. Biometric Data As A Cryptographic Key

- The project demonstrates real-world applicability for iris-based encryption in secure access control, healthcare data confidentiality, and secure financial transactions.
- It shows the feasibility of combining biometric authentication and encryption to enhance identity verification and data protection.

VIII. CONCLUSION

- The increasing reliance on biometric systems for secure authentication has heightened the need to protect sensitive biometric data from privacy attacks. This project successfully addresses these challenges by developing a robust framework for encrypting biometric traits while maintaining usability and scalability.
- This project underscores the importance of combining security, privacy, and usability in biometric systems. By addressing existing gaps and providing a robust encryption-based solution, it contributes significantly to the field of biometric security and offers a scalable, secure, and privacy-compliant framework for future applications.
- While initial challenges such as user education and privacy concerns need to be addressed, these can be mitigated with proper training and robust encryption measures. This system strengthens community governance by delivering reliable, sustainable solutions to modern security and operational needs, making it an essential tool for building safer, smarter societies.

IX. REFERENCES

1. Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons.
2. Stallings, W. (2016). *Cryptography and Network Security: Principles and Practice*. Pearson.
3. Jain, A. K., Ross, A., & Prabhakar, S. (2004). *Introduction to Biometrics*. Springer.
4. Jain, A. K., Hong, L., & Pankanti, S. (2000). "Biometric identification." *Communications of the ACM*, 43(2), 91-98.
5. Ross, A., & Othman, A. (2011). "Visual cryptography for biometric privacy." *IEEE Transactions on Information Forensics and Security*, 6(1), 70-81.
6. Daugman, J. G. (2004). "How iris recognition works." *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 21-30.
7. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). "An analysis of minutiae matching strength." *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 23(10), 1090-1101.
8. Farouk, H. T., & Hassan, H. (2018). "A review of biometric cryptosystems: Security and privacy perspectives." *Egyptian Informatics Journal*, 19(1), 45-56.