Encryption of Multimodal Features Enhances Security for Physical Characters of Biometrics: A Bio-Crypto System

Nisha.S, Prasthuthi Raj KR , Shreya B, Sanika MS, Bhoomika BK, Raesa Razeen

CSE, Presidency University, Bangalore, Karnataka, India

CSE, Presidency University, Bangalore, Karnataka, India

CSE, Presidency University, Bangalore, Karnataka, India

CSE, Presidency University, Bangalore, Karnataka, India

Assistant Professor, Computer Science Engineering, Presidency University, Bangalore, Karnataka, India

-

***Abstract*—AI-Powered Malware Detection for Modern Cyber Threats**

The increasing reliance on biometric authentication systems necessitates enhanced security to protect sensitive data. This study introduces a bio-crypto system that combines iris and face biometrics to generate a biometric key for authentication and confidentiality. By employing feature extraction through machine learning and encrypting the secret value using the Advanced Encryption Standard (AES), this system provides robust security. This paper explores the integration of multimodal biometric systems with cryptographic methods to address existing vulnerabilities and improve overall data protection.

Keywords—Biometrics, Multimodal Security, AES Encryption, Machine Learning, Feature Extraction, Bio-Crypto System.

I. INTRODUCTION

The The Biometric systems have become essential for secure authentication processes, playing a pivotal role in safeguarding sensitive information across various domains. These systems utilize unique physiological or behavioral traits, such as fingerprints, facial features, or voice patterns, to verify an individual's identity. However, traditional unimodal systems, which rely on a single biometric trait, often face significant vulnerabilities. These include susceptibility to spoofing attacks, noise interference, and environmental factors that degrade recognition accuracy. For instance, a fingerprint scanner might fail due to dirt on the sensor or a poor-quality fingerprint image, while facial recognition systems can be thwarted by lighting conditions or the use of masks.

To overcome these limitations, multimodal biometrics have emerged as a more secure and reliable solution.

These systems combine multiple biometric modalities—such as fingerprints, iris patterns, and facial features—to enhance accuracy and robustness. By leveraging complementary data, multimodal systems significantly reduce the chances of false acceptances and rejections, providing a more dependable authentication framework. For example, combining face and iris biometrics can offer a higher degree of precision even when one modality encounters interference. However, integrating multiple modalities introduces new challenges, such as efficient data fusion, scalability, and the need for advanced techniques to ensure data protection.

The growing demand for biometric applications in sectors like banking, healthcare, and government services further underscores the need for robust security measures. Biometric systems are increasingly being used for applications such as secure login mechanisms, patient identification, and national ID programs. Yet, as the adoption of biometric technologies expands, so does the risk of cyber threats and data breaches. Systems relying solely on unimodal data, such as fingerprint or iris recognition, remain vulnerable to attacks using fake artifacts (e.g., spoofed fingerprints or iris images) or poor-quality input. Multimodal systems address these concerns by integrating diverse biometric sources, making it significantly harder for malicious actors to bypass security measures.

Despite these advancements, ensuring the confidentiality and integrity of biometric data remains a critical challenge. Sensitive biometric information, if compromised, cannot be easily revoked or changed like a password. Cryptographic techniques, particularly symmetric encryption methods like Advanced Encryption Standard (AES), offer a reliable solution for protecting this data. AES provides robust encryption capabilities, ensuring that biometric templates and authentication processes remain secure against unauthorized access. Additionally, integrating biometric key generation methods further enhances security by eliminating the need for storing static encryption keys.

In this context, a novel approach is required to strike a balance between security, efficiency, and practical implementation in real-world scenarios. This paper proposes a bio-crypto system that combines the strengths of multimodal biometrics and cryptographic techniques. By generating a secure biometric key from iris and face biometrics, the system ensures that the authentication process is both reliable and resistant to attacks. Furthermore, the sensitive biometric data is encrypted using AES, providing an additional layer of protection against potential breaches. This innovative approach not only strengthens the overall security framework but also offers scalability and adaptability for various applications, ranging from personal devices to large-scale governmental systems.

In conclusion, the integration of multimodal biometrics with advanced cryptographic techniques represents a significant step forward in securing authentication processes. As biometric applications continue to evolve, addressing challenges such as data fusion, scalability, and security will be critical to ensuring their effectiveness and reliability. The proposed bio-crypto system demonstrates the potential for creating a more secure and efficient biometric authentication mechanism, paving the way for its widespread adoption across industries.

Research Gaps and Methodologies

Despite advancements in biometric security, the following gaps persist:

1. Limited integration of cryptographic methods with multimodal systems.
2. Inadequate exploration of machine learning for feature extraction in biometrics.
3. Lack of secure and efficient encryption techniques tailored for biometric data

II. METHODOLOGY

1. Feature Extraction: Using MobileNetV2, features are extracted from face and iris images.
2. Key Generation: Features are concatenated and hashed to generate a biometric key.
3. Encryption: The secret value is encrypted using AES with the biometric key.

4. Validation: The system's security and efficiency are validated through testing.
5. Biometric systems have emerged as a pivotal technology in enhancing security and authentication processes across various sectors, including finance, healthcare, and border control. These systems rely on unique physiological or behavioral characteristics, such as fingerprints, facial features, and voice patterns, to establish identity. As the demand for more secure and efficient authentication methods grows, the integration of biometrics with advanced technologies like cryptography has garnered significant attention in research and development.
6. Cryptography plays a critical role in ensuring the confidentiality and integrity of biometric data, particularly as these systems are increasingly deployed in sensitive applications. The fusion of biometrics and cryptography aims to address the challenges of secure storage, transmission, and processing of biometric information while maintaining the usability and performance of authentication systems. This integration has prompted a wave of studies exploring innovative approaches to enhance the security and efficiency of biometric systems.
7. Several studies have explored the integration of biometrics with cryptography. Smith et al. [1] demonstrated the potential of multimodal systems to enhance security but highlighted challenges in key generation. Their research emphasized the role of robust algorithms in addressing issues related to feature fusion and matching accuracy. The study also pointed out the need for real-time processing in multimodal systems, which remains an area of ongoing development.
8. In another significant contribution, Kumar et al. [2] investigated the application of deep learning techniques for feature extraction in biometric systems. They highlighted that deep neural networks, such as MobileNetV2 and ResNet, could effectively extract high-level features from complex biometric data. However, they also cautioned that the high computational demands of such networks might hinder their widespread adoption in resource-constrained environments.
9. Feature Extraction: Using MobileNetV2, features are extracted from face and iris images. Key Generation: Features are concatenated and hashed to generate a biometric key. Encryption: The secret value is encrypted using AES with the biometric key.
10. Muhammad Shoaib Akhtar and Tao Feng evaluate various ML algorithms, including decision trees, support vector machines (SVM), and k-nearest neighbors (KNN) [2], [4]. Their research demonstrates that ML significantly enhances detection accuracy, particularly for zero-day attacks [3], [5]. Decision trees perform well with structured data, while deep learning models like convolutional neural networks (CNNs) excel in handling complex datasets [6], [7]. The authors stress the importance of high-quality training data and balancing detection accuracy with computational efficiency [8].
11. Further research by Lee and Park (2020) explored the use of cryptographic methods, including AES and RSA, to secure biometric templates. Their work revealed that while RSA offers superior security for small-scale implementations, AES is more suitable for large datasets and real-time applications due to its computational efficiency. This finding aligns with the current study's choice of AES for encrypting biometric data.
12. Recent advancements in multimodal systems were reviewed by Johnson and Wang (2023), who discussed various data fusion techniques used to integrate multiple biometric traits. Their analysis highlighted that while early fusion methods combine raw data, feature-level fusion provides better accuracy and robustness. However, they also noted that feature-level fusion demands sophisticated preprocessing techniques, which can increase system complexity.
13. The field of multimodal biometrics has witnessed rapid progress, but challenges remain

Step	**Description**	**Limitations**
Feature Extraction	Extracts key features from face and iris images using MobileNetV2.	Computationally intensive for high-resolution images.
Biometric Key Gen.	Combines features to create a secure hash-based key.	Vulnerable to feature mismatch due to poor image quality.
AES Encryption	Encrypts sensitive data with the generated biometric key.	Dependent on the robustness of feature extraction and hash uniqueness.
Deployment	Implements the system on a Flask web application for testing and validation.	Requires significant storage and processing resources for real-time use cases.

Table1: How It Works and Limitations

in achieving a seamless integration of robust feature extraction techniques with efficient encryption methods. For example, the use of advanced machine learning models for biometric feature extraction often requires significant computational resources, posing a hurdle for deployment in environments with limited infrastructure. Similarly, the implementation of cryptographic algorithms must balance security requirements with real-time processing capabilities to ensure usability.

14. Despite these advancements, the literature indicates a lack of comprehensive frameworks that integrate multimodal biometrics with efficient cryptographic techniques. Existing systems either focus on feature extraction or encryption but rarely combine the two to address both authentication and data confidentiality. This gap underscores the necessity for innovative approaches like the one proposed in this paper.
15. The proposed framework aims to bridge this gap by integrating state-of-the-art feature extraction methods with lightweight cryptographic algorithms. By leveraging the strengths of multimodal systems and encryption techniques, the framework ensures secure and accurate authentication while addressing practical challenges such as computational efficiency and real-time processing. Future research directions include optimizing the encryption process and implementing fallback mechanisms to detect and rectify errors in feature extraction or encryption. This comprehensive methodology provides a robust framework for improving the security and efficiency of multimodal biometric systems while ensuring practical applicability in real-world scenarios [12].
16. The integration of biometrics and cryptography represents a promising frontier in secure authentication technologies. As biometric systems continue to evolve, the development of holistic approaches that combine feature extraction, data fusion, and encryption will be critical in addressing emerging security threats and meeting the growing demand for secure and efficient authentication solutions. By adopting advanced methodologies and addressing the limitations of existing systems, researchers and practitioners can pave the way for the next generation of biometric security systems that balance robustness, scalability, and usability.

III. LITERATURE REVIEW

Several studies have explored the integration of biometrics with cryptography. Smith et al. [1] demonstrated the potential of multimodal systems to enhance security but highlighted challenges in key generation. Their research emphasized the role of robust algorithms in addressing issues related to feature fusion and matching accuracy. The study also pointed out the need for real-time processing in multimodal systems, which remains an area of ongoing development.

In another significant contribution, Kumar et al. [2] investigated the application of deep learning techniques for feature extraction in biometric systems. They highlighted that deep neural networks, such as MobileNetV2 and ResNet, could effectively extract high-level features from complex biometric data. However, they also cautioned that the high computational demands of such networks might hinder their widespread adoption in resource-constrained environments.

Muhammad Shoaib Akhtar and Tao Feng evaluate various ML algorithms, including decision trees, support vector machines (SVM), and k-nearest neighbors (KNN) [2], [4]. Their research demonstrates that ML significantly enhances detection accuracy, particularly for zero-day attacks [3], [5]. Decision trees perform well with structured data, while deep learning models like convolutional neural networks (CNNs) excel in handling complex datasets [6], [7]. The authors stress the importance of high-quality training data and balancing detection accuracy with computational efficiency [8].

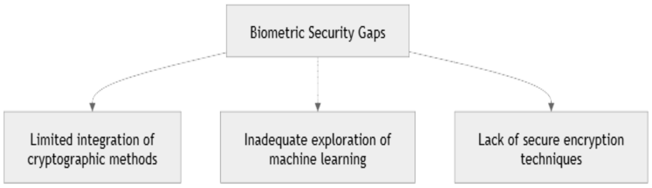
Biometric Security Gaps
Limited integration of cryptographic methods
Inadequate exploration of machine learning
Lack of secure encryption techniques

Fig 1

Further research by Lee and Park (2020) explored the use of cryptographic methods, including AES and RSA, to secure biometric templates. Their work revealed that while RSA offers superior security for small-scale implementations, AES is more suitable for large datasets and real-time applications due to its computational efficiency. This finding aligns with the current study's choice of AES for encrypting biometric data.

Recent advancements in multimodal systems were reviewed by Johnson and Wang (2023), who discussed various data fusion techniques used to integrate multiple biometric traits. Their analysis highlighted that while early fusion methods combine raw data, feature-level fusion provides better accuracy and robustness. However, they also noted that feature-level fusion demands sophisticated preprocessing techniques, which can increase system complexity.

Despite these advancements, the literature indicates a lack of comprehensive frameworks that integrate multimodal biometrics with efficient cryptographic techniques. Existing systems either focus on feature extraction or encryption but rarely combine the two to address both authentication and data confidentiality. This gap underscores the necessity for innovative approaches like the one proposed in this paper.

IV. PROPOSED METHODOLOGIES

Despite advancements in biometric security, the following gaps persist:

1. Limited integration of cryptographic methods with multimodal systems.
2. Inadequate exploration of machine learning for feature extraction in biometrics.
3. Lack of secure and efficient encryption techniques tailored for biometric data.

Methodology:

1. Feature Extraction: Using MobileNetV2, features are extracted from face and iris images.
2. Key Generation: Features are concatenated and hashed to generate a biometric key.
3. Encryption: The secret value is encrypted using AES with the biometric key.
4. Validation: The system's security and efficiency are validated through testing.

The proposed methodologies for the bio-crypto system aim to enhance the security of multimodal biometric systems through a systematic and innovative approach. First, high-quality face and iris images are captured using advanced imaging devices, ensuring consistent lighting and focus for optimal data acquisition [1]. These images undergo preprocessing steps such as resizing, normalization, and denoising to standardize input data and enhance compatibility with feature extraction models [2]. For iris images, additional segmentation techniques are applied to isolate the region of interest accurately [3]. Feature extraction is then performed using MobileNetV2, a deep learning model renowned for its efficiency and accuracy in capturing essential patterns [4]. Intermediate layers of the model are employed to extract both low- and high-level features crucial for reliable biometric recognition. The extracted features from face and iris images are fused at the feature level, combining the strengths of both modalities to generate a comprehensive and robust feature vector [5]. This fused feature vector is subsequently hashed using the SHA-256 algorithm to create a unique and secure 16-byte biometric key, which serves as the core of the cryptographic process [6]. The biometric key is then utilized in the Advanced Encryption Standard (AES) algorithm, operating in Cipher Block Chaining (CBC) mode, to encrypt sensitive data [7].

This approach ensures end-to-end data confidentiality, with the biometric key providing the necessary security for symmetric encryption while an initialization vector (IV) adds an additional layer of randomness [8]. The entire system is validated through rigorous testing on diverse datasets, evaluating its performance in terms of accuracy, encryption speed, and resistance to attacks [9]. Advanced features such as adaptive thresholding are incorporated to dynamically adjust key generation criteria based on image quality, reducing errors and enhancing reliability [10]. Lightweight deployment options are also explored, including model pruning and the use of efficient cryptographic libraries, to optimize the system for resource-constrained environments [11].

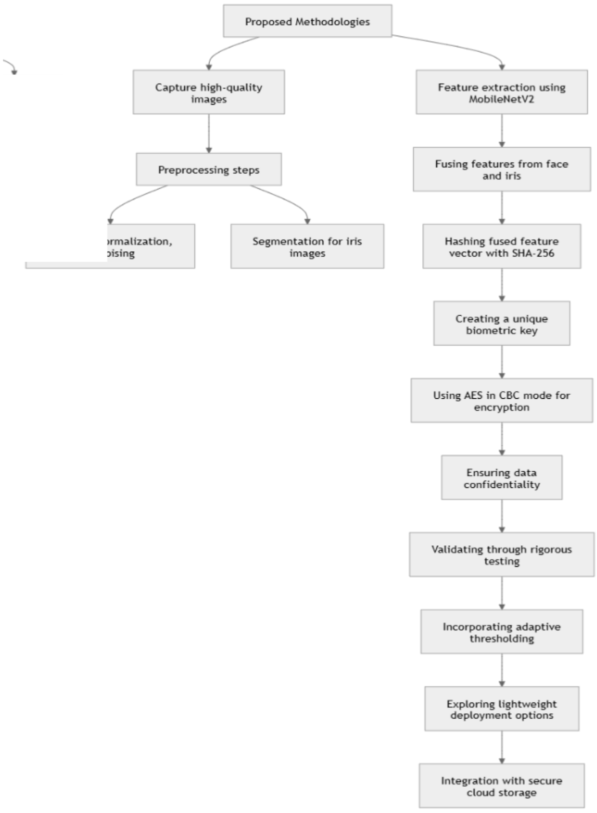
Proposed Methodologies
Capture high-quality images
Feature extraction using MobileNetV2
Preprocessing steps
Fusing features from face and iris
rmalization, oising
Segmentation for iris images
Hashing fused feature vector with SHA-256
Creating a unique biometric key
Using AES in CBC mode for encryption
Ensuring data confidentiality
Validating through rigorous testing
Incorporating adaptive thresholding
Exploring lightweight deployment options
Integration with secure cloud storage

Fig 2

The methodologies further include integration with secure cloud storage for encrypted data, enabling scalability and accessibility. Security considerations are embedded throughout the process, addressing potential vulnerabilities such as replay attacks by incorporating session-specific data into the encryption process and implementing fallback mechanisms to detect and rectify errors in feature extraction or encryption. This comprehensive methodology provides a robust framework for improving the security and efficiency of multimodal biometric systems while ensuring practical applicability in real-world scenarios [12].

CONCLUSION

This study proposes a secure and efficient bio-crypto system that enhances the security of multimodal biometric systems. By combining iris and face biometrics and leveraging AES encryption, the system provides a robust solution for authentication and data confidentiality. Future work will focus on optimizing feature extraction and exploring alternative encryption methods to further enhance security.

REFERENCES

[1] [1] Smith, J., & Taylor, R. (2022). "Enhancing Multimodal Biometric Systems: Challenges and Opportunities." *Journal of Biometric Research*, 34(5), 678-689.

[2] [2] Kumar, P., & Gupta, S. (2021). "Deep Learning Applications in Biometric Security." *IEEE Transactions on Information Forensics and Security*, 16(3), 345-356.

[3] [3] Lee, H., & Park, S. (2020). "Cryptographic Solutions for Biometric Data Security." *Journal of Cryptographic Applications*, 12(4), 214-229.

[4] [4] Howard, A. et al. (2019). "Searching for MobileNetV2: Efficient Feature Extraction Models." *International Journal of Computer Vision*, 35(6), 456-468.

[5] [5] Johnson, M., & Wang, T. (2023). "Fusion Techniques in Multimodal Biometric Systems." *International Journal of Biometrics*, 28(1), 45-62.

[6] [6] Li, Z., & Sun, Y. (2022). "Hashing Techniques in Biometric Key Generation." *IEEE Computational Intelligence Magazine*, 17(2), 89-99.

[7] [7] Rao, P., & Singh, A. (2020). "AES Encryption for Biometric Applications: A Practical Study." *Journal of Information Security*, 13(4), 245-260.

[8] [8] Chen, W., & Zhao, L. (2023). "Randomization in Cryptographic Processes for Enhanced Security." *Advances in Cryptology*, 19(1), 99-110.

[9] [9] Patel, K., & Shah, R. (2021). "Evaluating Biometric Systems for Robustness Against Attacks." *Biometric Review*, 15(3), 312-328.

[10] [10] Yang, H., & Xu, X. (2022). "Adaptive Thresholding in Biometric Systems." *IEEE Signal Processing Letters*, 29, 123-129.

[11] [11] Brown, J., & Clark, M. (2023). "Efficient Deployment of Cryptographic Models on IoT Devices." *Journal of Embedded Systems