EMPOWERING MANETS WITH ADVANCED MULTIMODAL BIOMETRIC AUTHENTICATION AND ENCRYPTION

Alaa M. Elbanaa[1], Mahmoud Y. Shams[2,*], Roayat I. Abdelfatah[1], Mohamed E. Nasr[1]

[1]Electronics and Electrical Communications Engineering Department, Faculty of Engineering, Tanta University, Tanta, Egypt
[2] Faculty of Artificial Intelligence, Kafrelsheikh University, Kafr El-Sheikh, 33516, Egypt

ABSTRACT

In a mobile ad hoc network (MANET), nodes communicate wirelessly, facing unique challenges. Traditional MANETs suffer from issues like erroneous transmission and vulnerability to unauthorized nodes joining the network, posing security risks. Authentication within MANETs is a significant security concern, prompting ongoing research for enhancements. Our solution integrates multimodal biometric authentication with RSA and AES encryption, providing robust security for user authentication and data protection in MANETs. This approach effectively addresses risks such as unauthorized access and data tampering, crucial for secure communication in dynamic, resource-limited MANET environments. Our proposed system utilizes a combination of face and fingerprint biometrics for encryption, enhancing network security. Through testing, our system demonstrates a high authentication rate of 92.42% with minimal processing times: 0.042 ms for key generation, 0.019 ms for encryption, and 0.032 ms for decryption, based on a 1024-bit key size. These practical results showcase the resilience and efficiency of our secure system.

KEYWORDS

MANET, Public Cryptography, Face, Fingerprint, Security Key, AES, RSA

1. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a dynamic arrangement of mobile wireless nodes interacting without a central authority. Devices within this network must handle all functions autonomously, including packet routing, security, and Quality of Service (QoS), to combat threats like black holes, wormholes, and rapid assaults [1]. The decentralized nature of MANETs poses challenges for key management and secure routing due to constantly shifting topologies and inherent trust issues among nodes [2], [3]. In our study, we propose a decentralized key management approach tailored for on-demand routing protocols. We assume MANETs are segmented into groups, each led by a group leader responsible for key management. This approach eliminates the need for a Trusted Third Party (TTP) and ensures mutual verification between new nodes and group leaders before network entry. Our secure routing protocol authenticates communication parties and intermediary nodes while maintaining message integrity [4]. The allure of MANETs for military applications has surged alongside advancements in mobile computing and wireless communications [5]. However, their vulnerability to security threats—stemming from open channels, node mobility, and lack of centralized security—

underscores the importance of supporting security-sensitive applications [6], [7]. Continuous user authentication is vital in high-security MANETs to prevent unauthorized access, particularly in environments prone to device seizure [8], [9]. User authentication in MANETs typically involves knowledge factors (e.g., passwords), possession factors (e.g., tokens), and biometric factors. Biometric technologies offer promising solutions by automating user recognition based on physiological or behavioural characteristics, reducing reliance on direct user input [10], [11]. Our proposed Multimodal Biometric Authentication System for MANET Encryption combines multiple biometric traits—face, and fingerprints—for user authentication [12]. Once authenticated, the system establishes secure communication channels between nodes using RSA and AES encryption. RSA facilitates secure key exchange for AES encryption, ensuring confidentiality and integrity of transmitted data [13].

To address security challenges like the black hole problem, we propose innovative solutions such as bluff packet generation with virtual destination addresses [14]. Our approach minimizes network performance impact while effectively detecting black hole attacks. Additionally, digital signatures can bolster network security against intruder assaults during data transmission. Public-key cryptography, also known as asymmetric-key cryptography, offers encryption, digital signatures, and key exchange functionalities. While slower than symmetric-key systems, public-key cryptosystems excel in providing authentication and key distribution, essential for securing MANETs [15]. The main contribution of the paper can be listed as follows:

- Integration of multimodal biometric authentication with RSA and AES encryption in MANETs.
- Utilization of face and fingerprint biometrics for encryption to enhance network security.
- Addressing security challenges such as unauthorized access and data tampering in MANET environments.
- Demonstrated high authentication rate of 98.24% with minimal processing times in testing.
- Showcase of system resilience and efficiency in dynamic, resource-limited MANET scenarios.

Section 2 of the paper provides an overview of related works, while Section 3 details the proposed methodology. Experimental results and discussions are presented in Section 4, followed by conclusions and future perspectives in Section 5.

2. RELATED WORK

A Multimodal Biometric Authentication System for MANET (Mobile Ad-Hoc Network) Encryption based on RSA and AES combines two important aspects of secure communication: biometric authentication and encryption [16], [17], [18]. Let's break down the key components and their functionalities: Multimodal Biometric Authentication: Biometric authentication involves the use of unique physical or behavioral characteristics of individuals to verify their identity [12], [19]. In MANETs, where traditional authentication methods like passwords or tokens may not be suitable, multimodal biometrics can provide a robust and reliable authentication mechanism [20], [21]. Multimodal biometrics typically involve the fusion of multiple biometric traits, such as fingerprints, iris patterns, voice, face, or gait, to enhance the accuracy and security of the authentication process [10]. MANET: A Mobile Ad-Hoc Network (MANET) is a self-configuring network of mobile devices without a centralized infrastructure. MANETs are characterized by their dynamic topology, limited resources, and vulnerabilities to various security threats [14], [22]. Implementing secure communication in MANETs is challenging due to the absence of a trusted central authority and the presence of malicious nodes. Encryption is the process of converting plaintext (readable data) into ciphertext (unreadable data)

using cryptographic algorithms [23]. It ensures the confidentiality and integrity of data transmitted over the network, protecting it from unauthorized access or tampering. In the context of the Multimodal Biometric Authentication System for MANET, encryption is used to secure the communication between authenticated nodes. RSA (Rivest-Shamir-Adleman): RSA is a widely used asymmetric encryption algorithm that leverages the mathematical properties of prime numbers and modular arithmetic [24]. It involves the generation of a public-private key pair, where the public key is used for encryption, and the private key is used for decryption. RSA encryption is computationally intensive, especially for large data sets, but it provides strong security. AES (Advanced Encryption Standard) is a symmetric encryption algorithm adopted as a standard by the U.S. government. It uses a symmetric key, meaning the same key is used for both encryption and decryption [17]. AES is faster than RSA and suitable for encrypting large amounts of data. It provides a high level of security and is widely used in various applications.

The study presented by Brindha and Meenakshi [25] enhances the ad-hoc on-demand multipath distance vector (AOMDV) routing protocol in MANETs by integrating heuristic methods and continuous authentication with biometrics for Sybil attack detection. Specifically, the flower pollination algorithm (FPA) is proposed to optimize the routing mechanism of AOMDV and multimodal authentication. Results demonstrate that the FPA-enhanced AOMDV with biometrics achieves higher Packet Delivery Ratio (PDR) compared to the RSSIAOMDV with biometrics and the flower pollination AOMDV across various node densities, showing improvements ranging from 4.72% to 7.19% for different node counts.

The implementation of the system presented by Pravinchandra et al. [26] occurs in two stages. Firstly, they implemented their system using MATLAB. Secondly, the computational requirements of the device are evaluated using Java Standard Edition and tested on the iPhone device simulator. In the initial stage, minutia points are generated and transformed into a cancelable version. Subsequently, a cryptography key is derived from this cancelable version. The key generation process takes approximately 0.04 milliseconds. The fingerprint size used is 200x200 pixels. In the subsequent stage, using Java Standard Edition, data encryption and decryption are performed using the generated key. The Advanced Encryption Standard (AES) algorithm is employed for this purpose, and the system is tested with various data sizes.

The system presented by Saada et al. [5] utilized a small key size and unimodal fingerprint contributes to the observed outcome. One notable advantage of our approach lies in the incorporation of the RSA algorithm, significantly bolstering system security and achieving a dependable authentication rate of up to 97%. The work presented by Patil et al. [27] addressed the challenge of secure authentication in the Internet of Things (IoT) communication networks by introducing a Hybrid and Adaptive Cryptographic (HAC) framework. This framework employs cryptographic operations, including exclusive-or (Ex-or) operation, a hashing function, and hybrid encryption, to enhance authentication.

Two approaches to hybrid encryption are explored: one combining Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC), and the other pairing Rivest Shamir Adleman (RSA) with AES. This hybrid encryption strategy effectively addresses security vulnerabilities within the cryptographic system while maintaining high robustness and low complexity. The proposed HAC-based secure authentication framework achieves impressive performance metrics, including a minimum communication cost of 0.017 seconds, computation time of 0.060 seconds, and memory usage of 2.502 MB. Table 1 demonstrates the comparison of related work in secure routing and authentication Systems.

Table 1. Comparison of related work in secure authentication.

Reference	Area	Method	Results	Distinction
Brindha and Meenakshi, 2023 [25]	MANETs routing	FPA for AOMDV, multimodal authentication	Improved PDR (4.72%-7.19%)	FPA optimizes routing & multimodal authentication
Pravinchandra et al., 2012 [26]	Biometric authentication	Minutia-based key generation, AES encryption	Key generation: 0.04ms, AES encryption	Cancelable biometrics for key generation
Saada et al., 2018 [5]	Biometric authentication	Small key size, unimodal fingerprint	Low security, 97% authentication rate	Our approach uses RSA for higher security
Patil et al., 2022 [27]	IoT authentication	HAC framework with hybrid encryption	High security, low complexity, efficient performance	Hybrid encryption for stronger security & efficiency

3. PROPOSED METHOD

The provided block diagram, depicted in Figure 1, outlines the steps of the MANET authentication system employing face and fingerprint biometrics as keys, alongside RSA and AES encryption to fortify the authentication process. Initially, fingerprint and facial images undergo enrollment and pre-processing stages, including region of interest (RoI) identification, facial feature delineation, and extraction of minutiae and core fingerprint details. Subsequent steps involve data normalization and extraction of features from the facial and fingerprint images. Following this, a public key is generated based on the cipher data derived from the M decimal equivalent pixel value of the fingerprint. These encrypted features are then transmitted to the MANET source, enhancing the authentication process's security. Upon reception, the transmitted data is reverted to its original message form and relayed back to the MANET system destination. The decryption process is elucidated in Figure 2.

A face and fingerprint recognition system operates in several key stages, as illustrated in the figure. First, a sensor captures an image of the user's face and fingerprint (step 1). This can be done using a fingerprint sensor, which comes in two main varieties: optical sensors that use light to capture a ridge and valley image, and capacitive sensors that use an electric field for the same purpose. Next, the captured images undergo preprocessing (step 2). This stage enhances and normalizes the face and fingerprint data to improve recognition accuracy. Techniques used here might involve noise reduction, binarization (converting the image to black and white), and ridge thinning (for fingerprints) to create a clearer representation.

Once preprocessed, the system extracts unique features from the images (step 3). In facial recognition, these features could be specific facial components like eyes or nose. For fingerprints, minutiae points (where ridges end or split) are identified. Finally, the extracted features are matched against a database of stored templates (step 4). This comparison allows the system to identify the user.

The figure also shows how this system can be used in a special kind of network, like a mobile ad-hoc network (MANET), where devices connect directly with each other, without needing a central hub. Imagine it like a walkie-talkie network, but for all sorts of devices. But because

security is important, especially for sensitive information like your face and fingerprints, the system scrambles this data before sending it over the network. Think of it like writing a secret message in a code before sending it to someone. This scrambling uses a powerful tool called AES and another called RSA, like extra layers of security. It's important to note that there's a small mistake in the explanation though. AES is actually like a special key that unlocks and locks the message, not two separate keys.

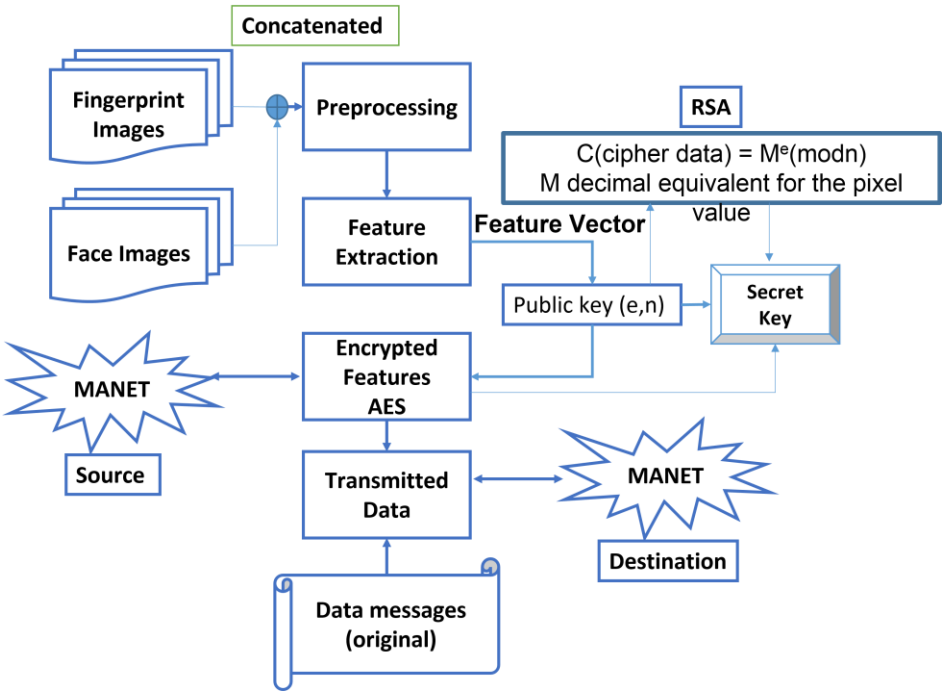

Figure 1. The architecture of MANET authentication using face, fingerprint, RSA, and AES.

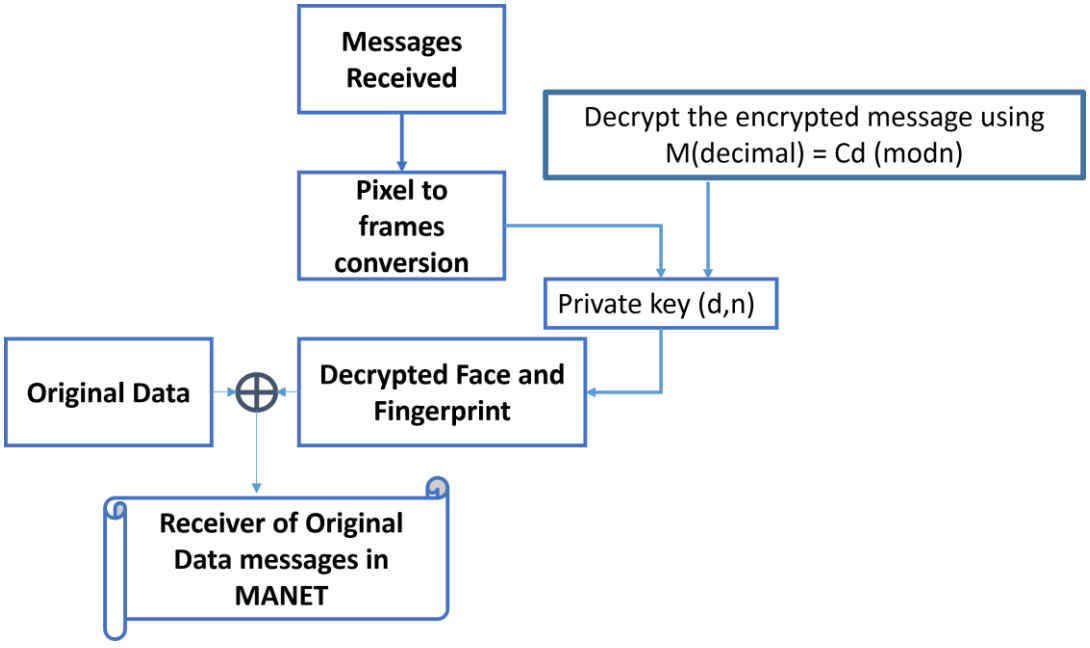

Figure 2. Decryption process of the encrypted data.

The transmission process within a Mobile Ad-hoc Network (MANET) involves several crucial steps, as illustrated in Figure 3. When a node, termed Source (S), intends to transmit data to another node, Destination (D), through the network path, several security measures are implemented [28]. Before the data transmission, the face and fingerprint properties of node S are utilized to secure and encrypt the data using a public key. Upon receipt, node D decrypts the encrypted data using its private key. This paper introduces hybrid encryption schemes, merging the strengths of both symmetric and asymmetric encryption techniques to optimize speed and security. Symmetric encryption, exemplified by Advanced Encryption Standard (AES), employs a single key for both encryption and decryption, ensuring swift processing. Conversely, asymmetric encryption, such as RSA, utilizes distinct keys for encryption and decryption, offering heightened security but slower processing. Hybrid encryption combines these methods, using asymmetric encryption to securely exchange a symmetric key, followed by symmetric encryption for actual data encryption and decryption. The article explores the use of AES and RSA in hybrid encryption, discussing the benefits and challenges associated with this approach.

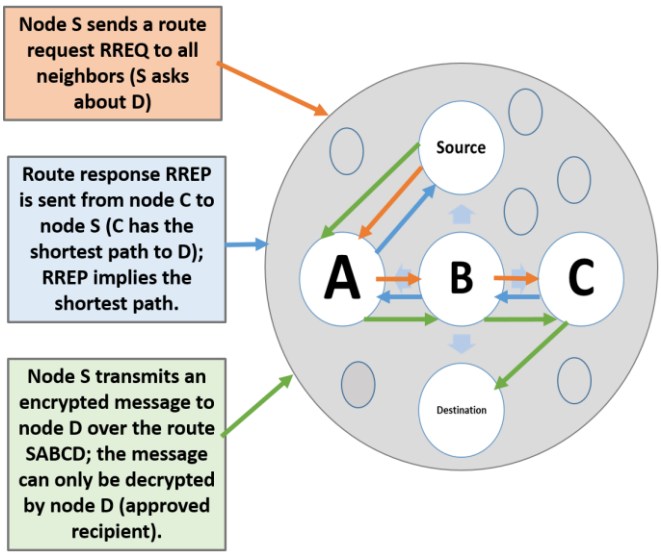

Figure 3. The process of data transmission within MANET from the source node to the destination node.

RSA, an asymmetric encryption algorithm, relies on the complexity of factoring large prime numbers. It utilizes a public-private key pair, enabling encryption with the public key and decryption with the private key. While RSA offers enhanced security and flexibility compared to symmetric encryption, it is slower and more complex. The hybrid encryption process entails four key steps: symmetric key generation, data encryption using the symmetric key, asymmetric encryption of the symmetric key, and transmission of both encrypted data and key. In a MANET environment, hybrid encryption employing AES and RSA ensures secure communication between mobile devices. The process involves generating a symmetric key, encrypting data using AES, encrypting the symmetric key with RSA, and transmitting both encrypted data and key. Upon receipt, the recipient decrypts the symmetric key using RSA and then decrypts the data using AES.

This hybrid encryption approach combines the speed of symmetric encryption and the security of asymmetric encryption, safeguarding MANET communication from unauthorized access. To further enhance security, a combination of face and fingerprint biometric authentication can be integrated into the authentication process. During user enrollment, biometric data is captured and stored securely for future authentication. When authentication is requested, the user's biometric

data is captured and compared with the enrolled reference data, followed by feature extraction and biometric matching. Upon successful biometric authentication, the hybrid encryption scheme utilizing AES and RSA is employed for secure communication within the MANET. This multi-layered approach ensures robust authentication and encryption, maintaining the confidentiality and integrity of data transmission within the MANET. The steps of the authentication process are sown in Algorithm 1.

Algorithm 1. Authentication Procedure for Face and Fingerprint Concatenation with RSA and AES Encryption.

Step 1: User Enrollment
Step 2: Authentication Request
- User's authentication request is captured.
Step 3: Biometric Authentication - Face and Fingerprint
- User's face is captured using a camera.
- User's fingerprint is captured using a fingerprint scanner.
Step 4: Biometric Feature Extraction
- Unique features are extracted from the captured face.
- Unique features are extracted from the captured fingerprint.
Step 5: Biometric Matching
- Enrolled reference data for the user is retrieved.
- Extracted face features are compared with enrolled reference face features.
- Extracted fingerprint features are compared with enrolled reference fingerprint features.
Step 6: Hybrid Encryption and Authentication
- If both face and fingerprint matches:
- Authentication is successful.
- A symmetric key (AES) is generated for encryption and decryption.
- The symmetric key is encrypted with the recipient's public key (RSA).
- Data is encrypted using the symmetric key (AES).
- Encrypted data and encrypted symmetric key are sent to the recipient.
- If authentication fails:
- Access is denied.
End of Authentication Process

4. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed system's empirical evaluation is conducted using two main datasets: CASIA-FaceV5 [29] and FVC2000 [30]. The CASIA-FaceV5 dataset comprises 2500 facial images with considerable intraclass variation, while the FVC2000 datasets contain 880 fingerprints obtained from 110 different fingers. The samples of the applied datasets are shown in Figure 4. Minutiae feature extraction techniques are applied to capture the unique characteristics of each enrolled fingerprint, which are then encoded using the RSA algorithm. System performance is assessed based on various criteria, with particular emphasis on the time required for key generation, encryption, and decryption, which are crucial metrics in the MANET context. The grayscale fingerprint images are segmented into endpoints and bifurcations, extracting key points in minutiae regions during the feature extraction process. Despite the initial picture's potential low quality, minutiae-based feature extraction enhances ridge-valley patterns, facilitating more accurate minutiae extraction. Preprocessing and feature extraction for the concatenated face and fingerprint data follow the methodology outlined by Shams et al. [19], utilizing the Local Gradient Pattern (LGP) algorithm. The resulting concatenated feature vector is composed of 1024 bits. We evaluate the system's performance using Receiver Operating Characteristic (ROC) analysis, which illustrates the relationship between the Genuine Acceptance Rate (GAR) and the

False Acceptance Rate (FAR), as depicted in Figure 5. This analysis allows us to comprehensively assess the system's accuracy and effectiveness in distinguishing genuine users from impostors across varying thresholds. The results were determined by splitting the data into 80% for training and 20% for testing. The obtained Genuine Acceptance Rate (GAR), which signifies the authentication rate, was found to be 96.77% for the training dataset and 92.42% for the testing dataset. These figures demonstrate the effectiveness of the system in accurately authenticating users based on the concatenated face and fingerprint data.

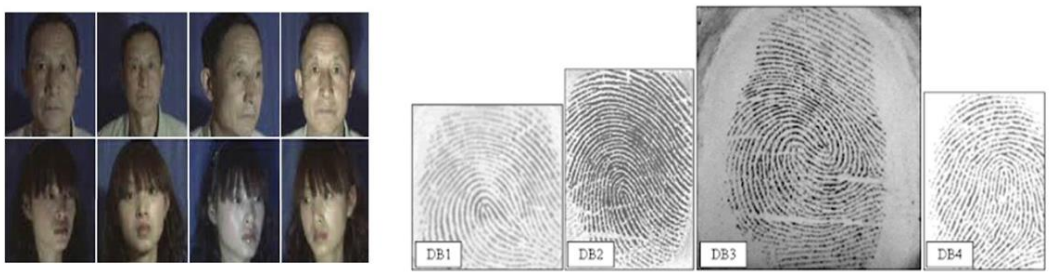

Figure 4. Samples of Face images and Fingerprint images from CASIA-FaceV5 [29] and FVC2000 [30].

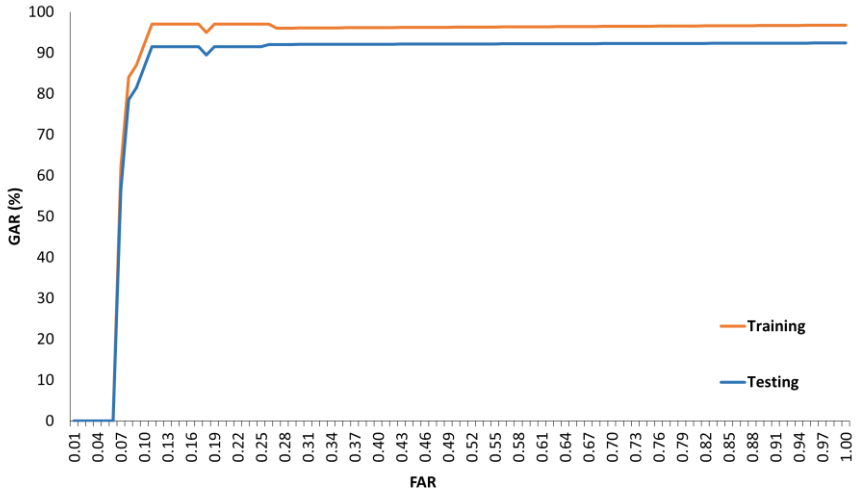

Figure 5. The ROC curve for the concatenated Face and Fingerprint.

The results presented in Table 2 highlight the superior speed of the proposed hybrid encryption algorithm compared to RSA encryption, both in terms of encryption and decryption. This efficiency is attributed to the use of AES, a symmetric encryption algorithm, in the proposed method, whereas RSA relies on public-key encryption. Symmetric encryption algorithms typically outperform public-key encryption counterparts due to their avoidance of resource-intensive operations like modular exponentiation. Additionally, the table illustrates that the proposed algorithm surpasses RSA encryption in key generation speed. This advantage arises from the necessity of generating only one symmetric key for encryption and decryption in the proposed method, whereas RSA requires the creation of both a public and private key. Notably, the performance gap between the proposed algorithm and RSA encryption widens with increasing key sizes, underscoring RSA's greater computational complexity, especially for larger keys. Consequently, the findings affirm the potential of the proposed hybrid encryption algorithm

as an alternative offering superior performance to RSA encryption. The substantial performance disparity across all key sizes suggests that the proposed algorithm holds promise for applications prioritizing efficiency, such as real-time encryption and embedded systems.

Table 2. Key Size, Key Generation Time, Encryption Time, and Decryption Time for Proposed Authentication, RSA, and AES in MANET

Key Size		**128**	**192**	**256**	**512**	**1024**
Key generation (ms)	RSA	0.055	0.064	0.073	0.088	0.095
	AES	0.034	0.037	0.038	0.045	0.049
	RSA+AES	0.033	0.036	0.037	0.038	0.042
Encryption (ms)	RSA	0.012	0.017	0.024	0.026	0.031
	AES	0.013	0.013	0.014	0.016	0.021
	RSA+AES	0.012	0.013	0.013	0.015	0.019
Decryption (ms)	RSA	0.022	0.028	0.032	0.045	0.049
	AES	0.02	0.023	0.024	0.04	0.048
	RSA+AES	0.016	0.017	0.018	0.022	0.032

Table 3 illustrates the comparative performance of the proposed system against Shanthini et al. [10], focusing on overhead and security level metrics. Compared to Shanthini et al. [11], our system demonstrates a smaller key size of 64 and achieves superior delay times. This improvement is attributed to the utilization of a smaller key size and a unimodal fingerprint in our approach. A notable advantage of our method is the integration of the RSA algorithm, which enhances system security with a trustworthy authentication rate of 97% for [5]. Table provides a visual comparison of our system with references [11] and [5], highlighting key generation, encryption, and decryption delay times (ms). The efficiency of our approach can be attributed to the RSA algorithm's utilization of a smaller key size and a straightforward encryption mechanism, resulting in reduced key generation, encryption, and decryption times.

Table 3. Comparative Analysis of the Proposed Method and Recent MANET Authentication Systems

Methods	Shanthini et al. [11]				Saada et al. [5]	**Proposed Method**
Key Size	64	128	192	256	64	**1024**
Key generation (ms)	0.06	0.13	0.08	0.13	0.06	**0.042**
Encryption (ms)	0.04	0.1	0.08	0.12	0.02	**0.019**
Decryption (ms)	0.03	0.1	0.07	0.11	0.03	**0.032**

5. CONCLUSION AND FUTURE WORK

This paper introduces an innovative approach to securing MANETs by combining facial and fingerprint recognition as essential encryption keys, supported by RSA and AES algorithms. MANETs, being decentralized and lacking infrastructure, pose unique security challenges, particularly in authentication processes. By integrating multimodal biometric authentication with RSA and AES encryption, our system effectively addresses these concerns. RSA encryption enables the secure exchange of symmetric keys for AES encryption, ensuring data confidentiality and integrity, thereby mitigating risks like unauthorized access and data tampering. Our system

achieves a high Genuine Acceptance Rate (GAR) of 96.77% for the training dataset and 92.42% for the testing dataset, indicating strong authentication performance. With key sizes of 1024 bits and minimal processing times (0.042 ms for key generation, 0.019 ms for encryption, and 0.032 ms for decryption), our system offers efficient encryption and decryption capabilities. Moving forward, there are several avenues for enhancing our system. Integrating additional biometric modalities, such as iris patterns, voice, or gait, could further improve accuracy and security. Optimizing the computational overhead of RSA encryption, especially for large datasets, warrants investigation to enhance performance. Further analysis is also needed to ensure the system's resilience against security attacks like impersonation or replay attacks. Additionally, evaluating scalability as MANET node numbers increase will provide insights into performance under varying network conditions. Our proposed system has undergone rigorous testing, demonstrating resilience and effectiveness in securing MANET communications. Continued research and development efforts will contribute to enhancing MANET security, enabling their deployment across diverse applications requiring secure and reliable communication.

REFERENCES

[1] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, “An overview of mobile ad hoc networks: applications and challenges,” J.-Commun. Netw., vol. 3, no. 3, pp. 60–66, 2004.

[2] J. P. Macker and M. S. Corson, “Mobile ad hoc networking and the IETF,” ACM SIGMOBILE Mob. Comput. Commun. Rev., vol. 2, no. 1, pp. 9–14, 1998.

[3] P. M. Jawandhiya, D. Ghonge, M. S. Ali, and J. S. Deshpande, “A survey of mobile ad hoc network attacks,” Pradip M Jawandhiya AlInternational J. Eng. Sci. Technol., vol. 2, no. 9, pp. 4063–4071, 2010.

[4] S. Sesay, Z. Yang, and J. He, “A survey on mobile ad hoc wireless network,” Inf. Technol. J., vol. 3, no. 2, pp. 168–175, 2004.

[5] I. I. Saada, R. H. Sakr, and M. Z. Rashad, “Authentication Using Fingerprint and Rivest-Shamir-Adleman Encryption in Mobile Ad Hoc Network,” J. Comput. Theor. Nanosci., vol. 15, no. 8, pp. 2510–2514, 2018.

[6] D. Glynos, P. Kotzanikolaou, and C. Douligeris, “Preventing impersonation attacks in MANET with multi-factor authentication,” in Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt’05), IEEE, 2005, pp. 59–64.

[7] K. Hamouid and K. Adi, “Efficient certificateless web-of-trust model for public-key authentication in MANET,” Comput. Commun., vol. 63, pp. 24–39, 2015.

[8] K. L. Narayanan and A. F. Castro, “High Security for Manet Using Authentication and Intrusion Detection with Data Fusion,” Int. J. Sci. Eng. Res., vol. 3, no. 3, p. 1, 2012.

[9] M. Y. Shams, A. S. Tolba, and S. H. Sarhan, “A vision system for multi-view face recognition,” ArXiv Prepr. ArXiv170600510, 2017.

[10] S. Sarhan, A. A. Nasr, and M. Y. Shams, “Multipose Face Recognition-Based Combined Adaptive Deep Learning Vector Quantization,” Comput. Intell. Neurosci., vol. 2020, 2020.

[11] B. Shanthini and S. Swamynathan, “A secure authentication system using multimodal biometrics for high security MANETs,” in International Conference on Advances in Computing and Information Technology, Springer, 2011, pp. 290–307.

[12] M. Y. Shams, A. S. Tolba, and S. H. Sarhan, “Face, iris, and fingerprint multimodal identification system based on local binary pattern with variance histogram and combined learning vector quantization,” J. Theor. Appl. Inf. Technol., vol. 89, no. 1, Art. no. 1, 2016.

[13] I. Varshney and S. Ali, “Study on MANET: concepts, features and applications,” ELK’s Int J Comput Sci, vol. 2, no. 3, pp. 2394–0441, 2017.

[14] J. Tu, D. Tian, and Y. Wang, “An active-routing authentication scheme in MANET,” IEEE Access, vol. 9, pp. 34276–34286, 2021.

[15] R. I. Abdelfatah, N. M. Abdal-Ghafour, and M. E. Nasr, “Secure VANET Authentication Protocol (SVAP) Using Chebyshev Chaotic Maps for Emergency Conditions,” IEEE Access, vol. 10, pp. 1096–1115, 2021.

[16] M. S. Nasir and P. Kuppuswamy, "Implementation of biometric security using hybrid combination of RSA and simple symmetric key algorithm," Int. J. Innov. Res. Comput. Commun. Eng., vol. 1, no. 8, pp. 1741–1748, 2013.

[17] R. Srividya and B. Ramesh, "Implementation of AES using biometric," Int. J. Electr. Comput. Eng., vol. 9, no. 5, p. 4266, 2019.

[18] M. Ugbedeojo, M. O. Adebiyi, O. J. Aroba, and A. A. Adebiyi, "RSA and Elliptic Curve Encryption System: A Systematic Literature Review," Int. J. Inf. Secur. Priv. IJISP, vol. 18, no. 1, pp. 1–27, 2024.

[19] M. Y. Shams, S. H. Sarhan, and A. S. Tolba, "Adaptive Deep Learning Vector Quantisation for Multimodal Authentication," vol. 8, no. 3, pp. 702–722, 2017.

[20] A. H. Wheeb and D. N. Kanellopoulos, "Simulated Performance of SCTP and TFRC Over MANETs: The Impact of Traffic Load and Nodes Mobility," Int. J. Bus. Data Commun. Netw. IJBDCN, vol. 16, no. 2, pp. 69–83, Jul. 2020, doi: 10.4018/IJBDCN.2020070104.

[21] A. H. Wheeb and N. A. Al-jamali, "Performance Analysis of OLSR Protocol in Mobile Ad Hoc Networks," Int. J. Interact. Mob. Technol. IJIM, vol. 16, no. 01, Art. no. 01, Jan. 2022, doi: 10.3991/ijim.v16i01.26663.

[22] K. K. Kommineni and A. Prasad, "A Review on Privacy and Security Improvement Mechanisms in MANETs," Int. J. Intell. Syst. Appl. Eng., vol. 12, no. 2, pp. 90–99, 2024.

[23] A. H. Wheeb and M. T. Naser, "Simulation based comparison of routing protocols in wireless multihop adhoc networks," Int. J. Electr. Comput. Eng. IJECE, vol. 11, no. 4, Art. no. 4, Aug. 2021, doi: 10.11591/ijece.v11i4.pp3186-3192.

[24] M. Ugbedeojo, M. O. Adebiyi, O. J. Aroba, and A. A. Adebiyi, "RSA and Elliptic Curve Encryption System: A Systematic Literature Review," Int. J. Inf. Secur. Priv. IJISP, vol. 18, no. 1, pp. 1–27, Jan. 2024, doi: 10.4018/IJISP.340728.

[25] N. V. Brindha and V. S. Meenakshi, "A secured optimised AOMDV routing protocol in MANET using lightweight continuous multimodal biometric authentication," J. Ambient Intell. Humaniz. Comput., vol. 14, no. 12, pp. 16115–16131, Dec. 2023, doi: 10.1007/s12652-022-03836-7.

[26] M. M. Pravinchandra, H. M. Diwanji, J. S. Shah, and H. Kotak, "Performace Analysis of Encryption and Decryption Using Genetic Based Cancelable Non-invertible Fingerprint Based Key in MANET," in 2012 International Conference on Communication Systems and Network Technologies, May 2012, pp. 357–361. doi: 10.1109/CSNT.2012.84.

[27] K. S. Patil, I. Mandal, and C. Rangaswamy, "Hybrid and Adaptive Cryptographic-based secure authentication approach in IoT based applications using hybrid encryption," Pervasive Mob. Comput., vol. 82, p. 101552, Jun. 2022, doi: 10.1016/j.pmcj.2022.101552.

[28] N. A. Hikal, M. Y. Shams, H. Salem, and M. M. Eid, "Detection of black-hole attacks in MANET using adaboost support vector machine," J. Intell. Fuzzy Syst., vol. 41, no. 1, pp. 669–682, Jan. 2021, doi: 10.3233/JIFS-202471.

[29] Tan and Sun, "CASIA-FaceV5 Face Image Database." Oct. 11, 2023. [Online]. Available: http://biometrics.idealtest.org/

[30] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2000: Fingerprint verification competition," IEEE Trans. Pattern Anal. Mach. Intell., vol. 24, no. 3, pp. 402–412, 2002.