systems

MDPI

Article

A Hybrid AES with a Chaotic Map-Based Biometric Authentication Framework for IoT and Industry 4.0

Ayman Altameem [1], Prabu P [2], Senthilnathan T [2], Ramesh Chandra Poonia [2] and Abdul Khader Jilani Saudagar [3,*]

[1] Department of Computer Science and Engineering, College of Applied Studies and Community Services, King Saud University, Riyadh 11533, Saudi Arabia
[2] Department of Computer Science, CHRIST (Deemed to be University), Bangalore 560029, India
[3] Information Systems Department, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia
* Correspondence: aksaudagar@imamu.edu.sa

Abstract: The Internet of Things (IoT) is being applied in multiple domains, including smart homes and energy management. This work aims to tighten security in IoTs using fingerprint authentications and avoid unauthorized access to systems for safeguarding user privacy. Captured fingerprints can jeopardize the security and privacy of personal information. To solve privacy- and security-related problems in IoT-based environments, Biometric Authentication Frameworks (BAFs) are proposed to enable authentications in IoTs coupled with fingerprint authentications on edge consumer devices and to ensure biometric security in transmissions and databases. The Honeywell Advanced Encryption Security-Cryptography Measure (HAES-CM) scheme combined with Hybrid Advanced Encryption Standards with Chaotic Map Encryptions is proposed. BAFs enable private and secure communications between Industry 4.0's edge devices and IoT. This work's suggested scheme's evaluations with other encryption methods reveal that the suggested HAES-CM encryption strategy outperforms others in terms of processing speeds.

Keywords: Internet of Things; security; fingerprint authentication; privacy; Biometric Authentication Framework; biometric data; Hybrid AES (Advanced Encryption Standard) with Chaotic Map Encryption; Industry 4.0

check for updates

Citation: Altameem, A.; P, P.; T, S.; Poonia, R.C.; Saudagar, A.K.J. A Hybrid AES with a Chaotic Map-Based Biometric Authentication Framework for IoT and Industry 4.0. *Systems* **2023**, *11*, 28. https://doi.org/10.3390/systems11010028

Academic Editor: Paolo Visconti

Received: 10 November 2022
Revised: 28 December 2022
Accepted: 29 December 2022
Published: 5 January 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

IoT includes many different types of devices, including tablets, smartphones, wearable technology, computers, and PDAs (personal digital assistants). Due to their declining prices, increased mobility, and growing computational power, these devices are used in the daily lives of humans. IoT consists of a wide range of intelligent devices working together to make people's lives more convenient and accessible [1]. IoTs have many advantages; their applications transform how we live and work. Additionally, they create new chances for innovations, expansions, and knowledge exchanges across various businesses. The technological growth of devices has culminated in their usage in the creation of smart homes/cities/grids. They are also employed in many other domains, including agriculture, healthcare, transportation, and many industrial sectors. Deployments of IoTs are depicted in Figure 1 [2].

However, devices for IoTs cannot implement comprehensive security policies due to low power and limited computer capacity limits. Devices for IoTs are widely networked, which encourages attackers to launch more assaults more frequently. These devices for IoTs are turning into a source of possible problems, since device vendors and users are simply too ignorant of the dangers of security in IoT. The devices can proliferate, resulting in water and public electric supply shortages. IoTs linked to homes are also potential targets for attackers [3]. Effective access controls are essential, and leakage of on-device data needs

to be halted given the security issues outlined above [4]. In the early days of IoTs, user identification was only possible through passwords.

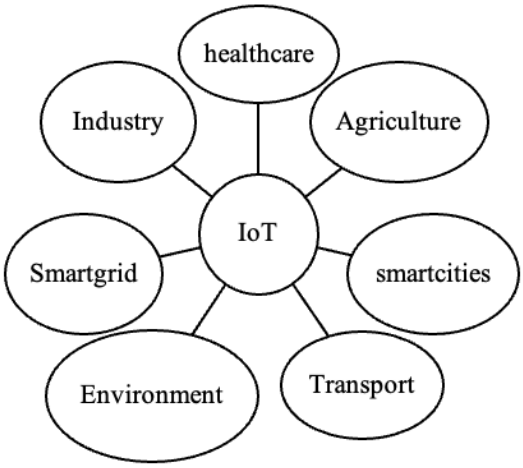

Figure 1. IoT Application.

As a more dependable method of authentication, biometric technology has rapidly spread to practically every aspect of our everyday lives during the past ten years. Biometrics are a part of handheld devices thanks to the prevalence of smartphones, making biometric authentication more generally accepted. Devices for IoTs with biometric modules installed are currently available in the market as separate goods. Human physical characteristics, such as fingerprints and faces, are used in biometric recognition to identify or verify individuals and overcome issues of password-based authentications [5].

Despite the advantages that biometric systems have over conventional authentications, unlike passwords, biometric attributes can be modified or reissued, and hence biometric data residing on databases or handheld devices are insecure. Once biometric template data has been stolen, it is impossible to reverse, and security and privacy breaches are very likely. If an adversary gains access to IoT devices using stolen biometric templates, the sensitive data or records stored on those devices may be compromised and jeopardized [6]. Therefore, there are two justifications for why it is essential to have biometric template data. The user's identity must first be protected to prevent the original biometric data from being recovered. Second, users' sensitive information or private data kept on IoTs should only be accessed by authorized personnel.

The three major pillars of IoT security are protecting the confidentiality of data acquired, employing encrypted communication channels, and implementing user authentication. To safeguard the confidentiality of personal data, user authentication is crucial. IoT user authentication has historically been carried out via pin-based password schemes [7]. However, biometric methods have begun to be employed due to the pin-based password's shortcomings, including the possibility of being forgotten, stolen, or leaked. Biometric descriptors cannot be changed or shared by another person, and they are therefore more difficult to forget. In addition, because biometric information contains personal features that cannot be modified in the event of theft, it poses a major privacy risk [8]. Therefore, biometric data can be secured here using encryption techniques.

This study intends to offer security for IoT devices with fingerprint authentications to prevent unauthorized system access and to safeguard user privacy. Fingerprint captures increase the risks of security and privacy As a result, the BAF framework is suggested for private use and safe communications between IoT devices (Edge Consumer Electronics). The suggested method ensures biometric data's security in transmissions and databases where available standard encryptions are employed. After the approved users' fingerprints have been recorded in the database, BAFs are ready for usage. The following is the work's primary contribution:

- Users send their fingerprints to systems using fingerprint sensors. After executing necessary image processing tasks, Raspberry Pi extracts biometric templates from the sensor's fingerprints.
- These biometric templates are encrypted before transmissions and sent to servers by Raspberry Pi for avoiding hackers. Servers compare the received templates with previously saved database templates of users.
- When fingerprints match in these comparisons, servers grant access, the lack of which results in denial of access to systems.
- Here, the proposed AES algorithm is combined with the chaos system to create the encryption key, which is then used to encrypt the image.

Traditional cryptographic algorithms cannot compare to chaos-based encryption methods in terms of speed, security, reasonable computational overheads, or procedural power. The motivation of this research was to increase the security of fingerprint photographs by combining AES with a chaos-based model. Chaotic maps are mathematical procedures that result in a very random pattern based on the initial seed value. This publication summarizes the usage of chaotic maps to generate pseudo-random numbers and perform encryptions. Even detailed consideration of the algorithm and implementation is not given to cost–benefit analysis. Recent chaos-based algorithms differ from one another in terms of security, since there are no frameworks or standards for security analysis, which is the primary motivation force for this study.

The following is how the paper is set up: The literature is reviewed in Section 2. The basic AES and chaos system as well as the suggested algorithm are thoroughly explained in Section 3. The results analysis, discussion, and comparison of the suggested method with others that were used are all presented in Section 4. Section 5 concludes with recommendations for future work.

2. Related Work

The weakest parts of a system: The resource constraints of IoTs result in using light weighted techniques for security in devices, which increase quickly, and some devices' security can easily go unchecked. Because they have limited control over upgrades, these devices become the IoT network's weakest links. Users frequently have limited awareness of the inner workings of devices for IoTs and insufficient comprehension of how to manage internet updates, creating possibilities for malware to target security. In terms of data protection, IoT networks' smart sensors collect a lot of information from numerous sources, some of which may be connected to users' sensitive personal data [9].

Users' rights to privacy are violated by the dissemination of these data. Authentications, privacy, reliability, and end-to-end securities are required to overcome the security issues with IoT. A secure communication architecture should be implemented using lightweight technologies, key management systems, policies, and security [10]. It is erroneous to apply security mitigation based on traditional IT network solutions in an IoT environment due to the diversity of devices and communication protocols and the broad range of interfaces and services offered in IoTs. Methods now used in traditional networks for security, such as cryptographically pre-shared keys for authentication, may not be sufficient [11].

Attacks commonly target IoTs with traditional three-layer designs, which include the perception, network, and application levels. Encryption allows IoT personal data to be safeguarded and communicated without any changes. Data encryption and decryption depend on cryptography, which uses private keys. Security concerns such as eavesdropping can be avoided with data encryption. Further discussed are biometric-based authentication systems.

Literature survey: UAKMPs (user authenticated key management protocols) developed by (Wazid et al. [12]) for HIoTNs were brand-new, secure, and portable. The scheme used tri-factor remote user authentications. UAKMPs were based on smart cards, passwords, and the unique biometrics of users. The scheme used the real-or-random model's

formal security conditions, informal security criteria, and formal security verifications with automated validations of Internet security protocols and application tools.

Together with userid, bio-hash codes are computed and saved in an authentication data table (ADT). However, precomputed table attacks can exploit such hashing-based authentication methods. The authentication data table is kept in an untrusted storage server in a revolutionary biometric-based authentication system that protects privacy. Chaotic map, Paillier cryptosystem, and Secure Hash Algorithm-256 are used in the system protocol's architecture. However, this method takes more time in order to fetch and convert the hash code

Fingerprint images are securely stored via DNA sequencing and a chaotic tent map. However, this approach is ineffective against several types of assaults, including man-in-the-middle and known-plaintext analyses (MIMA). Fingerprint images are secured using several chaotic systems. However, this strategy does not effectively combat brute force attacks because each chaotic system differs and has performance issues.

For user authentication, Jiang et al. [13] offered a cancellable biometric approach based on HD-sEMGs (high-density surface electro-myograms) encoded by hand gesture passwords. When users successfully executed preset gesture passwords that collected HD-sEMG signals (256 channels) from their forearm muscles, their biometric tokens were produced; 34 different hand gestures used often in daily life were investigated. Additionally, a password-specific channel mask that was automatically generated was used to lower the number of active channels in devices for IoTs to lessen the strain of data collecting and transmission. As they are also reliable with a lower sampling rate, HD-sEMG biometrics use less power.

HBFs (Hierarchical Bloom Filters) for biometrics were proposed by Shomaji et al. [14]. Their scheme enabled compact storage, tolerance to noises, and quick query processing, even with resource constraints of devices in IoT. The attack methods that could increase the number of false positive non-member authentications and expose soft data on registered members are investigated. Under these explicitly defined attack vectors, quantitative studies evaluated the security of HBF-based biometric systems. Compared to classic Bloom Filters, it was found to be very difficult to penetrate. Additionally, the findings of the experiments demonstrate that soft biometric data are also protected.

New three-factor CSUAC-IoTs were created for IoTs by Mandal et al. (certificateless-signcryption-based user access controls) [15]. The user's password, particular biometrics, and mobile device all function as authentication factors in this technique. Registered users (U), and smart devices (Si) were mutually approved and authenticated through trusted gateway nodes (GN) in IoTs where logins and access controls were based on CSUAC-IoTs. Distinct cells in IoTs had GN and certain counts of devices. The two parties were then able to communicate securely, thanks to their shared session key. CSUAC-IoT also facilitates the introduction of new IoT devices, user revocation, functionality, and capabilities for updating passwords and biometrics.

According to the unique user-authenticated key agreement technique presented by Srinivas et al. [16], only authorized users will be able to access the services offered in the ecosystem with IoTs. The suggested system used fuzzy extractions to validate biometrics where users' smart cards, passwords, and biometrics were examined. The recommended approach included additional devices after their initial deployments, passwords, and biometric update stages along with revocations in emergencies such as misplaced cards.

The recommended strategy also has a simple design. We conducted a formal (mathematical) security study as well as non-mathematical informal security studies of the proposed system. AVISPAs (Automated Validation of Internet Security Protocols and Applications) provided formal security verifications of the proposed approach and suggested unique partial DCT-based CBSs with privacy and security safeguards for a variety of authentication applications in IoTs [17]. The study also suggested session key agreements, data encryptions, and data integrity algorithms to address confidentiality, integrity, and availability concerns during cancellable template enrolment authentications.

The results of the research and experiments revealed that the proposed technique authenticated users with higher accuracy and reduced overhead while safeguarding the confidentiality and privacy of personal cancellable biometric templates and developed light weighted bio-cryptosystems for security while storing or exchanging biometric models [18]. Their proposed bio-crypto architecture had three stages: key creations, confusion, and spreads. A two-dimensional logistic sine map is used for key generation. By using cutting-edge diffusion technology that makes use of DNA encodes and ciphering, it is hypothesized that the encryption process may be made substantially simpler while still maintaining the needed integrity. According to simulations and security analyses, the recommended cryptosystem offers an appropriate degree of security and resilience, requires less computational complexity, and may be able to suit the needs of IoT applications.

The authors presented tri-factor remote user authentications based on ECCs (elliptic curve cryptographies) that operated on smart devices and safeguarded communicating user's privacies and data confidentialities [19]. Numerous cryptographic attacks were examined to bolster our claim, and it was discovered that the suggested scheme is impervious to them. The computation and communication overheads were compared to those of other current protocols to ensure that the suggested system is lightweight. The suggested scheme has undergone a rigorous security study using the AVISPA simulation tool, which confirmed its resistance to relevant security risks.

A three-factor-based authentication strategy (TFASH) that is secure and effective compared to other pertinent techniques was presented by Sahoo et al. for healthcare systems using IoTs and based on ECCs [20]. The suggested TFASH session keys and mutual authentications banked on BAN (Burrows–Abadi–Needham) logic and the Real-Or-Random model. Alzahrani et al. proposed enhancements to lightweight authentications in IoTs [21]. The study's ILAS-IoTs completed the procedure with minimal increases in computation and communication overhead.

The formal and informal security study made it clear that the proposed ILAS-IoTs were resistant to all known attacks as well as stolen verifiers. Golec et al. developed a biometric method known as BioSec in order to provide fingerprint authentication in IoTs connected to edge consumer devices [22]. The study employed common encryptions to protect both transmitted and stored biometric data. The study's suggested BioSec provided discrete and secure communications IoTs using Industry 4.0 edge devices. The study discovered the superiority of 128-bit AES in their comparative evaluations, where AES was the fastest.

Inference: The fingerprint was selected as the biometric authentication method in this study. Sensing fingerprints are less costly than other biometric sensors that gather information on iris or hand geometries. In contrast to other works, this study employed the industry's standard encryption technologies to ensure biometric template secrecy during transmissions and storage. Other investigations, including feature transformations (stenographical encryptions) and biometric cryptosystems (lightweight cryptographies), do not adversely influence performance rates when employed for creating template safeguards. Evaluations of the proposed work scheme with existing encryption techniques show that the proposed HAES-CM encryption scheme beats others in terms of processing speeds.

3. Proposed Methodology

With the help of biometric authentication, this work created the BAF system, which has two layers: client and server. The client part makes use of the Raspberry Pi-4 IoT device. The server component of the system is installed on a computer system. A sensor in the BAF system captures the fingerprints of the user or users who will be registering with the system, and these fingerprint pictures are subsequently sent to the Raspberry Pi device. Fingerprint pictures are turned into a biometric template made up of minute features that may be used for fingerprint identification after passing through the requisite image processing processes on the Raspberry Pi. The friction ridge skin impressions known as minutiae points are thought to be particular to each fingerprint. The biometric template is delivered in encrypted form to protect communication connections between servers and

the Raspberry Pi from hacker attacks. In order to prevent biometric template leaks, the database stores the encrypted biometric templates that were collected in the server portion. In this manner, protection is given against any database hacking, as depicted in Figure 2.

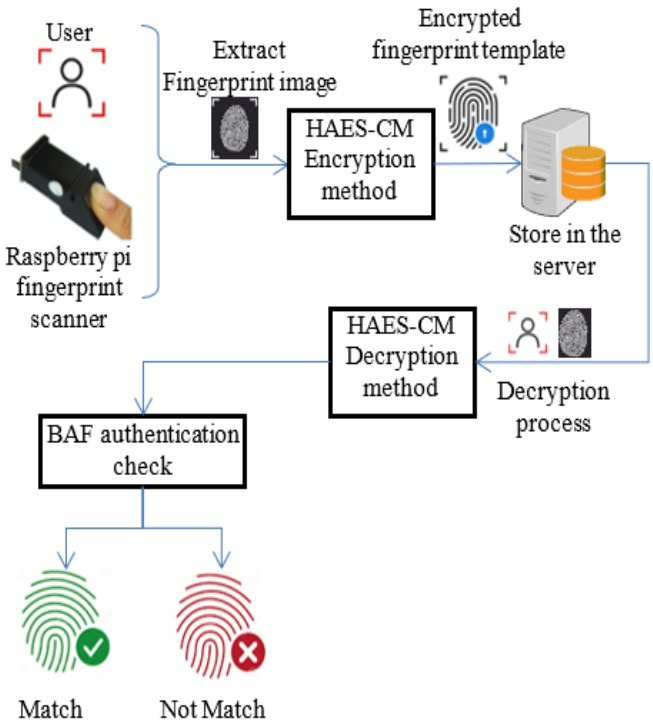

Figure 2. General framework diagram of BAF.

3.1. Fingerprint Enrolment and Client Pat

First, the required pre-processing is applied to the fingerprint pictures of the users who wish to be registered in the system, and feature extraction is used to produce biometric templates. Biometric templates are displayed using the AES-CM variable in this system. These AES-CM data are thereafter encrypted and stored in the database. The encrypted technique was determined to be HAES-CM. There are 80 fingerprint images of 10 individuals in the FVC2004 DB-3 DATABASE folder. Users have different fingerprints (8), which are stored for testing future performances in matches. The remaining images are the stored system's databases. Fingerprints are received from client system buttons using fingerprint sensors attached to the Raspberry Pi. This HAES-CM-encrypted AES-CM data are transmitted to the server across the communication channel.

3.2. Proposed HAES-CM-Based Security Model

The client generates a number in the range of 1 to ES, where E and S are the dimensions of the fingerprint image. The chaotic map's permutation method is used to create the permuted image. The image is next encrypted with a key and the AES method, producing an encrypted image. The receiver uses AES to decrypt the encrypted image after receiving it (using a previous key). Upon receipt of the encrypted images, receivers create random numbers using the same secret parameters. Re-permuted images are then used to produce original texts. The steps of the suggested encryption technique are shown in Algorithm 1.

Algorithm 1. The steps of the encryption algorithm

Input: $E \times S \rightarrow FI$ // Dactylogram input picture and $\mathfrak{X}_0, a$ // confidential attributes
Output: *EFI* //Encrypted Fingerprint picture
Step1: Read Dactylogram picture *FI*
Step2: Algorithm to shift FI based on quadrate chaotic map (2).
Step3: The shifted picture should be encrypted using the AEScryptography technique.
Step4: Publish the encrypted picture *EFI*.

The suggested system combines the necessary statistical properties, chaotic maps dissemination, and the AES encryption algorithm's confounding impact. The proposed model is extended from the existing work by Ashwaq and others [23]. The permutation method based on the chaotic map is shown in Algorithm 2.

Algorithm 2. The steps of the permutation process based on chaotic maps

Input: Dimension $dim \rightarrow E \times S \rightarrow FI$ // Dactylogram input picture and $\mathfrak{X}_0, a$ // confidential attributes
Output: PFI // Shifted Fingerprint picture and original text T
Step1: Let dim $= E \times S$
Step2: Take a random pattern $\mathfrak{X}$ by quadratic map
Let $a = 0.4,\ \mathfrak{X} = 0.15,\ \mathfrak{X}_0 = a \times \mathfrak{X}_0^2$
For $= 1$ *to dim*
$\mathfrak{X}_i = a \times \mathfrak{X}_{i-1}^2$
End
Step3: Mapping the range of chaotic map $\mathfrak{X}$ from $[-0.6\ 0.6]$ to $[1\ dim]$, max $= dim$, min $= 1$

$$T_i = \frac{(Max–Min)}{Max–Min} \times (\mathfrak{X}_i–Max) + Max$$

End
Step4: Convert the PFI from 2D to 1D
Step5: FI's pixel locations should be moved in accordance with T.
Step6: Resize the 1D array to create a PFI dectylogram that is 2D permuted.

There are now several widely used conventional encryption techniques. The majority of them are appropriate for text files. Direct application of these algorithms to photos or videos presents difficulties because to the significant connections between nearby pixels. The level of detail decreases as the correlation between the adjacent pixels decreases. As a first phase, a quadratic map-based technique is used to eliminate the link between pixels and to decrease entropy. For confusion and dispersion, which are essential for confidentiality, AES picture encryption is used. According to the security study results, any modification in the key and encryption solution must be sufficiently comprehensive to defend against brute-force assaults if sensitive encryption and decryption procedures are to be used. AES and chaotic maps, two of the most efficient encryption structures, are combined in a suggested encryption approach to give a comprehensive framework for ciphering fingerprint pictures.

Advanced Encryption Standard: As opposed to the AES algorithm, the Feistel structure is iterative. Encrypting and decrypting data use these two well-known techniques, encryption, substitution, and permutation (SPN). AES can manage 128 bits since it provides a fixed block size of 16 bytes of plaintext and may carry out several mathematical operations concurrently utilizing various cyphers (16 bytes). A 16-bit block is represented as four squares in a four-dimensional matrix in the byte matrix AES uses for encryptions. Additionally, the quantity of rounds N r, which can affect speed, is a crucial component of AES. The quantity of tiny, medium, and large rounds needed will grow if one wants to insert long keys (128, 192, or 256 bits). The approaches employed throughout the entire model describe the various functional combinations depicted in Figure 3.

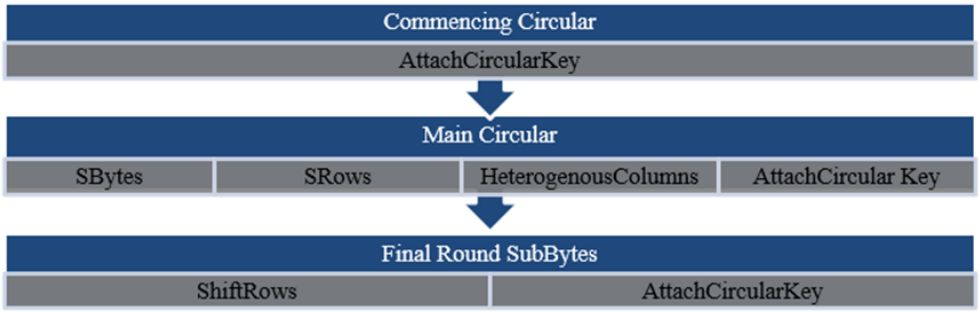

Figure 3. The different combinations of functions in AES.

Substitute Bytes Transformation: Each round begins with a SubBytes transformation stage. The nonlinear S-box is used at this stage to change one state byte to another. Shannon's ideas of dispersion and confusion for designing cryptographic algorithms play a crucial role in achieving significantly greater security [24].

ShiftRows(SRows) Transformation: ShiftRow comes after SubByte in the process of changing the state. The main goal of this phase is to cycle through each row, and instead of row 0, shift the state's bytes to the left. This procedure has no permutation; just the bytes from row zero remain. In the first row, only one byte is transferred to the left in a circular manner. The second row is shifted to the left by two bytes. The final row is enlarged to the left by three bytes. The bytes' condition has changed, but the size of the new state has stayed unchanged at 16 bytes.

HetrogeousColumns Transformation: HetrogenousColumn is another essential stage that the state goes through. The division is conducted outside the state. Multiplying each byte from one row by each value (byte) from the state column is a matrix transformation. In other words, each row of the matrix transformation must be multiplied by the state. The following requires combining these multiplication results using XOR to produce a new set of four bytes:

AttachCircularKey Transformation: The AttachCircularKey phase of the AES algorithm is crucial. A 44-byte matrix is used to organize both the key and the input data, which is sometimes referred to as the state [25]. AttachCircularKey can provide much greater security while encrypting data. The establishment of the connection between the key and the encrypted text forms the basis of this procedure. The encrypted text begins at the earlier step. Users' specified keys precisely impact the AttachCircularKey output [26]. The subkey is also used in the stage, and in conjunction with states in rounds, subkeys are extracted from main keys using Rijndael's key schedules. Both states and subkeys are of equivalent sizes. Subkeys get added by bitwise XORs of state's bytes and their corresponding subkey bytes. The round counts depend on key sizes; for 128-bit keys, AES must use ten rounds, while for 256-bit keys, AES must use 12 rounds plus an additional two rounds. Therefore, Figure 4 shows the initial, intermediate, and final output of the three-stage AES encryption procedure [27].

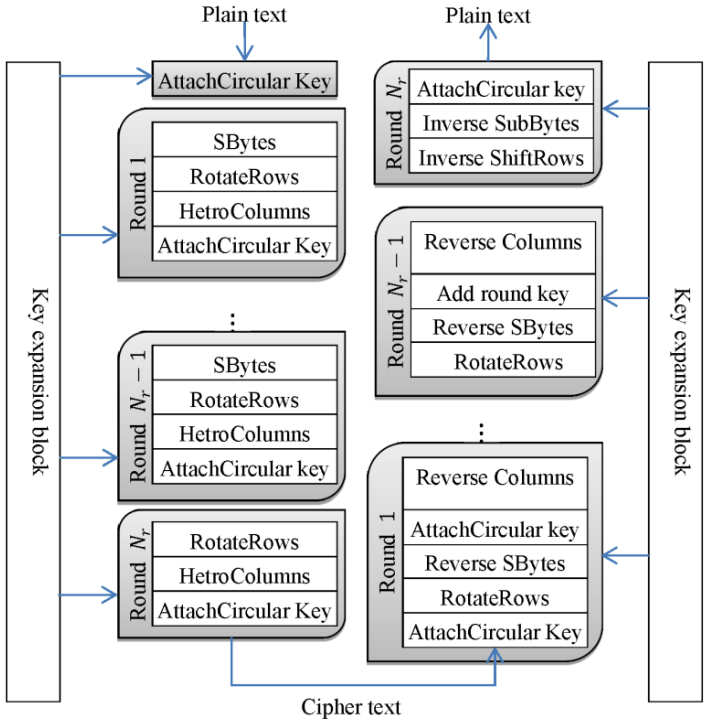

Figure 4. The general framework diagram of cipher and decipher using AES [27].

AES has four main operational blocks [28], and the diagram is given in Figure 5.

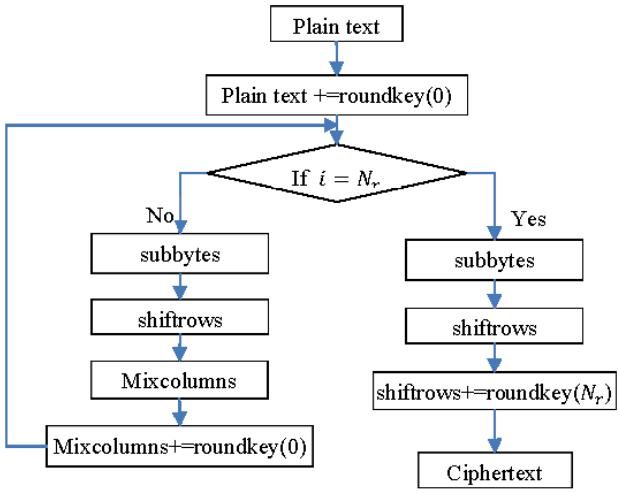

Figure 5. Block diagram of the AES method [28].

- Byte substitution: Each data block's byte is changed to another block using an S-box.
- Row transformation: Depending on where it is in the state matrix, each row is given a cyclic shift to the right side.
- Each column of the state matrix is multiplied by that of the fixed matrix in the mix transformation of columns, which is a matrix multiplication operation.
- Round Key Addition: An XOR operation is carried out between the round key and the new state matrix.

Chaotic System: Compared to classical algorithms, chaos-based encryption has become steadily more important and dominating [29]. Chaotic systems are ergodic, dispersive, and very sensitive to their initial conditions and have many commonalities with cryptography. Chaos-based encryptions and cryptographies have gained importance. Charlie Fridrich

exploited chaotic maps to enhance photo encryption technologies. If image-based chaotic maps are used, studies can exploit the encryption of images using 1D and 2D chaotic maps. Because of their intricate construction and qualities, chaotic maps are frequently utilized for encryption [30].

Compared to chaotic maps in smaller dimensions, 1D chaotic maps show a greater amount of surface structure while having an uneven distribution and discontinuous range. However, these procedures and traits increase the complexity of calculations and the difficulty of implementation [31–33]. Compared to chaotic maps in smaller dimensions, 1D chaotic maps show a greater amount of surface structure while having an uneven distribution and discontinuous range. However, these processes and characteristics make computations more complex and implementation more challenging. A subfield of mathematics called chaos theory studies extraordinarily complex systems. These systems produce large changes in the output when tiny (apparently ignorable) modifications in the input are made [34]. Fingerprint images make extensive use of chaos-based cryptosystems. Many systems fail to achieve a reasonable level of security, and measuring performance and security levels is often highly challenging [35]. Since the Advance Encryption Standard (AES) algorithm's diffusion effect is weak, chaos-based cryptosystems are being presented in the literature to ensure confidentiality for digital images [36].

A chaos system has the following features:

- Sensitivity to the beginning value: Repetitive calculations on a chaotic map with the parameters result in a completely different sequence depending on small initial value changes.
- Sensitivity to the parameters: Repeated calculations on a chaotic map with the input values result in a completely new sequence for small changes in the parameters.
- Randomness: Most of the chaos sequences produced by chaos maps are pseudorandom sequences, and their structures are extremely difficult to anticipate and analyze.
- The attacker cannot predict the chaos sequence without the proper control parameters and beginning values. To put it another way, chaotic systems can increase the security of picture encryption systems.

Generating the round key using the chaos system: The suggested encryption algorithm generates the key K using the Arnold chaos system. Assume that r rounds are required for the encryption and that the original fingerprint picture is of size $M \times N$. As a result, using eq, $r + 2$ arrays of size $N \times M$ are produced (1 and 2). Each array represents the round key of the AES algorithm:

$$\mathfrak{X}1_{r+1} = mod\ (\mathfrak{X}1_r + (a \times \mathfrak{X}2_r), 256) \tag{1}$$

$$\begin{gathered} \mathfrak{X}2_{r+1} = mod\ (b \times \mathfrak{X}1_r + ((a \times b \times 1) \times \mathfrak{X}2_r)),\ 256) \\ K(j,k,i) = floor\big(mod\big((k(j,k,i) * 10^{14})\big), 256 \end{gathered} \tag{2}$$

here, $\mathfrak{X}1$ and $\mathfrak{X}2$ are key values, where $\mathfrak{X}1$ = 0.0215, = 0.5734, $a = 0.4$, and b = 0.

The encryption and decryption processes are identical. The only variation is that some actions are carried out backwards. Arnold's mapping is originally used in the decryption procedure to construct the key, and 10 iterations are specified before the decryption action starts. Only the encrypted image must be XORed with the final key in order to completely eliminate the XOR alterations because the reverse of the XOR operation and XOR operation are interchangeable terms. The suggested encryption method is then reversed, and during this process, the key and the encrypted image are first XORed. The second stage involves transforming the cypher picture using the linear transformation operation's inverse. The next step is the reverse row shift operation, in which a row that was rotated by n units to the right during encryption is rotated by n units to the left during decoding. In the last stage, a condition that selects the last pixel if the number of rounds is odd is checked; otherwise, propagation is carried out. Regardless of the number of rounds, this process is repeated. The initial key is then XORed with the image from the previous phases. The final image is an exact replica of the original.

4. Experimental Results and Discussion

The BioSec system mandates that biometric data be encrypted in both the transmission channel and database to guarantee its security. Evaluation of three different standard encryption algorithms led to the determination of performance times for encryption and decryption.

Figure 6 shows that users have different fingerprints (8) stored for testing future performances in matches.

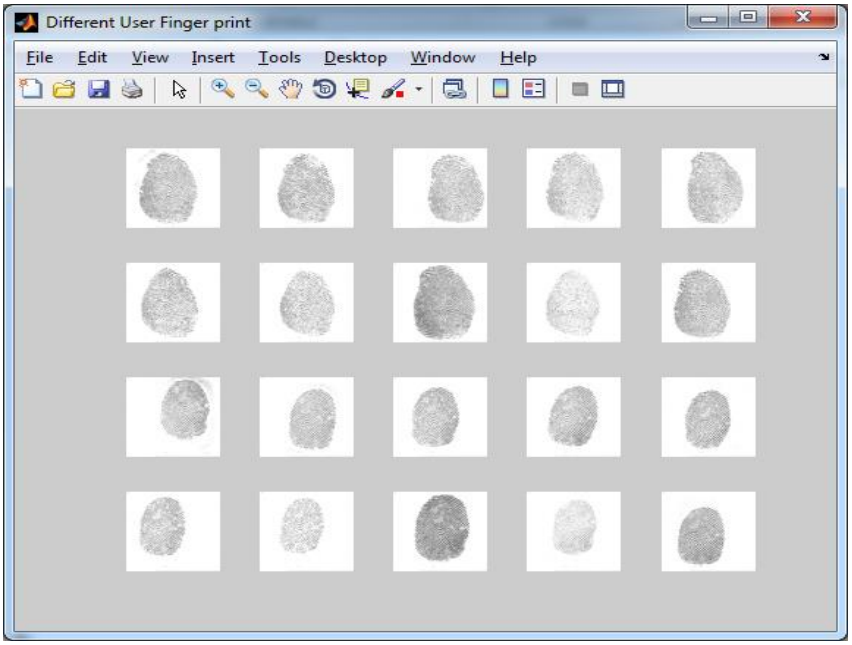

Figure 6. User fingerprint image.

Figure 7 shows that the encrypted technique was determined to be HAES-CM.

Figure 7. Extract fingerprint image.

Figure 8 shows the HAES-CM scheme, which combines Hybrid Advanced Encryption Standards with Chaotic Map Decryptions. The performance metrics used by QILV to compare it to ECC and AES (quality index-based local variance) are SSIMs (structural similarity indices), precision, sensitivity, f-measure, PSNR, MSE, encryption correctness, and computing time.

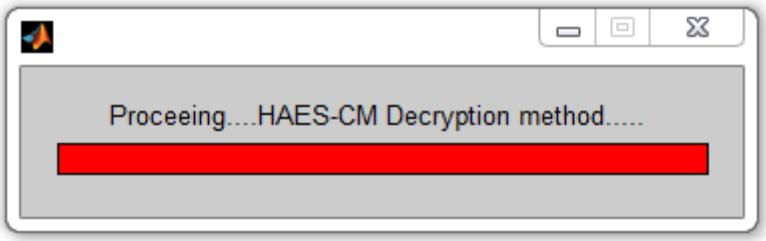

Figure 8. Extract fingerprint image.

Figure 9 shows the Biometric Authentication Frameworks to enable authentications in IoTs coupled with fingerprint authentications on edge consumer devices and ensure biometric securities in transmissions and databases.

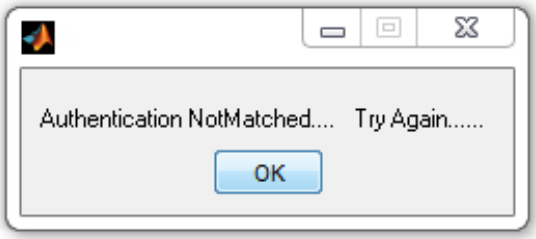

Figure 9. Extract fingerprint image.

Table 1 shows the performance timings for the three encryption methods with varied key lengths. This system uses HAES-CM-128 bit, which is still considered a safe algorithm at a time when processing speed is vital. Based on performance criteria such as SSIMs (structure similarity indices), QILV compares it against ECC and AES (quality index based local variance), precision, sensitivity, f-measure, PSNR, MSE, encryption accuracy, and computational time.

Table 1. Performance timings for the three encryption methods.

Methods	SSIM	QILV	Precision (%)	Sensitivity (%)	F-Measure (%)	PSNR (dB)	MSE	Accuracy (%)	Computation Time (s)
ECC	0.8241	0.8992	0.856	0.826	0.848	62.12	3.9	82.65	6.5
AES	0.8564	0.9042	0.869	0.853	0.876	65.32	3.5	89.23	5.7
HAES-CM	0.8896	0.9098	0.879	0.894	0.912	68.23	3.2	93.48	3.5

SSIM: The parameter is calculated to determine whether the decrypted signal and the encrypted image S_{enc} are similar. Its value ought to fall in the range [0,1]. A higher value indicates a better-deciphered signal.

$$SSIM = \frac{\left(2\mu_{S_{enc}}\mu_{S_{dec}} + v_1\right)\left(2\sigma_{S_{enc}}\mu_{S_{den}} + v_2\right)}{\left(\mu^2_{S_{enc}} + \mu^2_{S_{den}} + v_1\right)\left(\mu^2_{S_{enc}} + \mu^2_{S_{den}} + v_2\right)} \quad (3)$$

QILV: This compares the decrypted image's local variance distribution to that of the plain signal. A higher index value indicates better signal quality.

$$QILV = \frac{2\mu_{S_{enc}}\mu_{S_{dec}}}{\mu_{S_{enc}}^2 + \mu_{S_{dec}}^2} \cdot \frac{2\sigma_{S_{enc}}\sigma_{S_{dec}}}{\sigma_{S_{enc}}^2 + \sigma_{S_{dec}}^2} \cdot \frac{\sigma_{S_{enc}*c}}{\sigma_{I_{enc}}\sigma_{S_{dec}}} \tag{4}$$

Sensitivity: The fraction of actual positive values that are correctly encrypted and calculated as in Equation (3) is what is measured by sensitivity:

$$sensitivity/recall = \frac{TP}{TP + TN} \tag{5}$$

Precision: The ratio of correctly encrypted positive samples to the total number of positive predictions on samples is computed as in Equations (3) and (5).

$$Precision = \frac{TP}{FP + TP} \tag{6}$$

F-measure: It is the harmonic mean of precision and recall, also called F_1-score, and is calculated as in Equations (7).

$$F - measure = \frac{2 * (Recall \ * \ Precision)}{(Recall + Precision)} \tag{7}$$

PSNR: The PSNR is used to find the deviation of the encrypted image and from the ground truth image as represented in Equation (8).

$$PSNR = 10 \log_{10} \frac{R^2}{MSE} \tag{8}$$

where R stands for max fluctuations in input image data types, while R represents the double precision data type and 255 for the 8-bit unsigned data type.

MSE: It is the error metric used to compare image encryption quality. The lower the value of MSE, the lower the error and the better the quality of encryption. MSE is calculated as in Equation (9)

$$MSE = \sum_{M,N} \frac{[I_1(M,N) - I_2(M,N)]^2}{M * N} \tag{9}$$

Accuracy: Accuracy is the ratio of correctly encrypted samples to the total sample count, as in Equation (10):

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{10}$$

4.1. SSIM Comparison Results

The results of the SSIM methods for the number of photos are shown in Figure 10. ECC, AES, and the HAES-CM technique were used in the process. The suggested method's SSIM rate is 0.8896, while the DSC values for known methods such as ECC and AES are 0.8241 and 0.8564, respectively. From this graph, it can be seen that when compared to earlier methods, the suggested method offers superior SSIM, which improves encryption standards. This technique is not impacted by lower contrast edges, which are caused by noise and may result in local minima and inaccurate energy minimization methods.

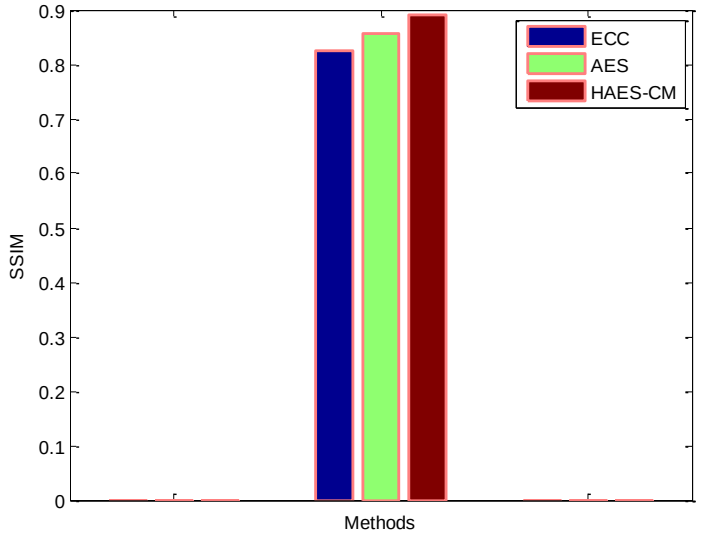

Figure 10. SSIM comparison results between the existing and proposed methods.

4.2. QILV Comparison Results

The comparison results for the normalized graph cut method, ECC, AES, and proposed HAES-CM approaches are shown in Figure 11. When the quantity of photos increased, the QILV value grew linearly. This graph demonstrates the effectiveness of the proposed technique, which had a high QILV of 0.9098. The ECC and AES produced low Jaccard values of 0.8992 and 0.9042, respectively. These were typically caused by backdrop markers that were either too loosely defined or too tightly defined.

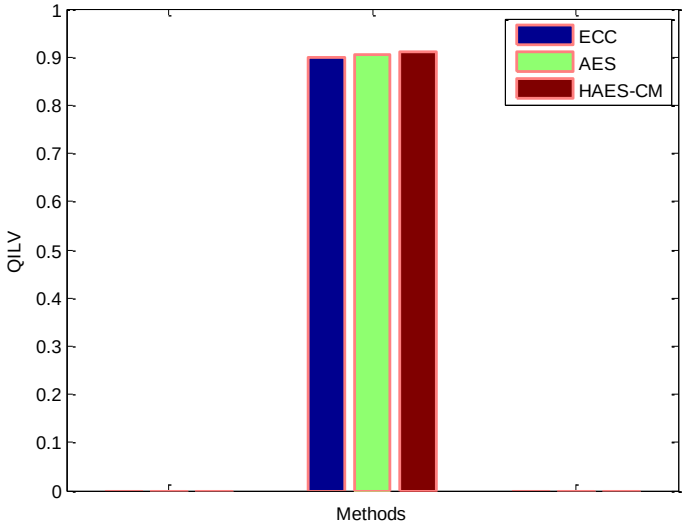

Figure 11. QILV comparison results between the existing and proposed methods.

4.3. Precision Comparison Results

The precision coefficient comparison findings for the ECC, AES, and suggested HAES-CM approaches are shown in Figure 12. When there were more photos, the precision value increased linearly as the number of images increased. This graph shows that the suggested method successfully encrypted the image with a high degree of precision of 0.879 percent. The ECC and AES produced low precision values of 0.856 percent and 0.869 percent, respectively. The watershed algorithm always recognized a contour in that region, even if there were no distinct borders between the markers. As a result, the proposed method's picture encryption procedure achieved a high precision rate.

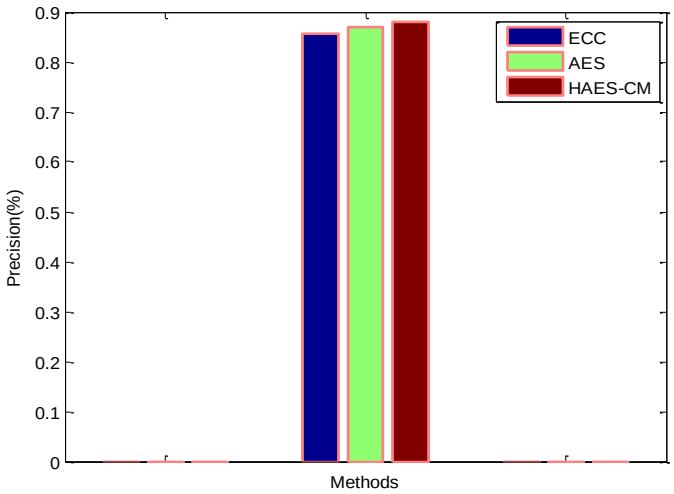

Figure 12. Precision comparison results between the existing and proposed methods.

4.4. Sensitivity Comparison Results

The sensitivity of the approaches for the amount of photos is seen in Figure 13. ECC, AES, and the HAES-CM technique were used in practice. The suggested method's sensitivity rate was 0.894 percent, compared to the sensitivity rates of existing methods such as ECC and AES, which were 0.826 percent and 0.853 percent, respectively. According to the findings, the proposed approach for fingerprint encryption is more efficient and increases privacy rates.

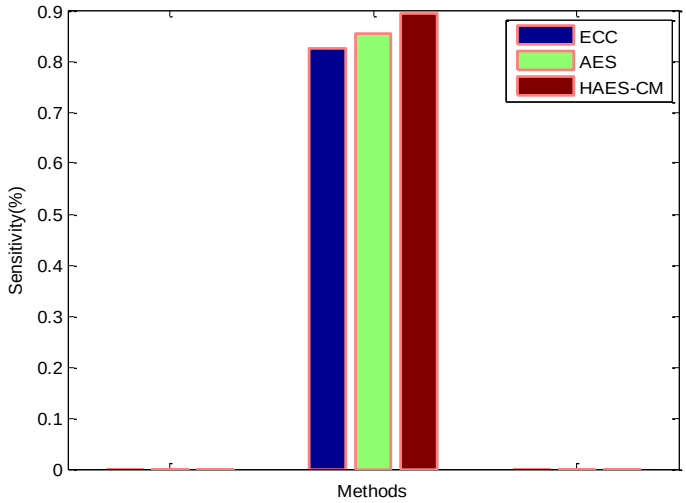

Figure 13. Sensitivity comparison results between the existing and proposed methods.

4.5. F-Measure Comparison Results

The F-measure findings of approaches for the number of photos are shown in Figure 14. The ECC, AES, and HAES-CM techniques were used in practice. The suggested method's F-measure rate was 0.912 percent, compared to the F-measure rates of existing methods such as ECC and AES, which were 0.848 percent and 0.876 percent, respectively. Based on the findings, it was found that fingerprint encryption may be improved.

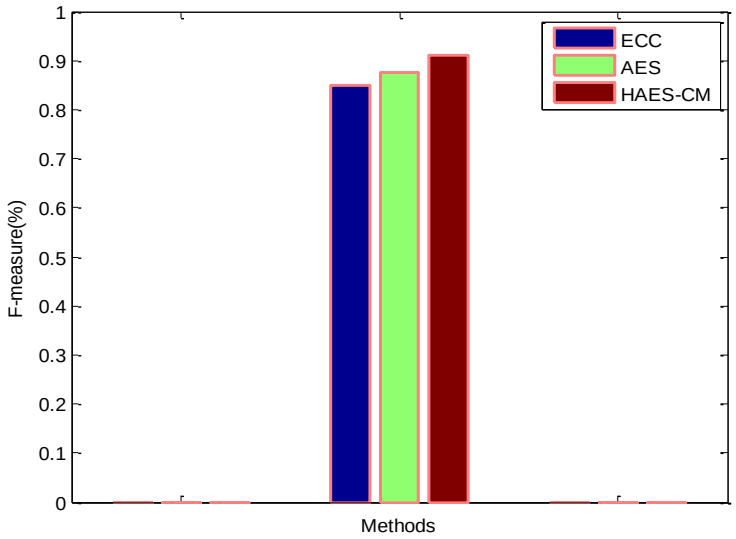

Figure 14. F-measure comparison results between the existing and proposed methods.

4.6. PSNR Comparison Results

Figure 15 compares the PSNR for the proposed HAES-CM method, ECC, and AES. When the number of pictures was increased, the PSNR rose linearly. The suggested method efficiently encrypted the fingerprint image with a high PSNR of 68.23 dB, as seen in the graph. The ECC and AES produced low PSNR values of 62.12 and 65.32 dB, respectively. Finding all mass candidates was the aim of the proposed encryption stage, even if some false positives resulted in strong PSNR findings.

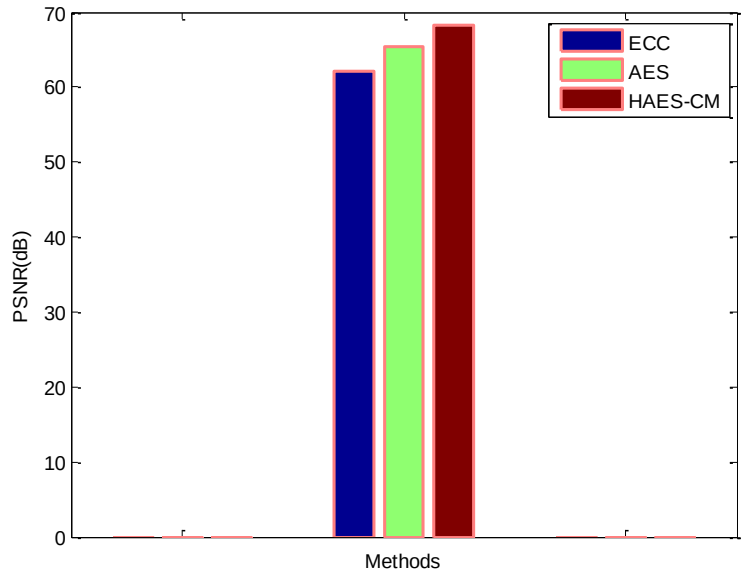

Figure 15. PSNR comparison results between the existing and proposed methods.

4.7. MSE Comparison Results

The comparative outcomes for MSE for ECC, AES, and HAES-CM are displayed in Figure 16. The MSE value decreased linearly as the number of photos rose in accordance with it. This graph shows that the suggested approach successfully and efficiently encrypted the image with a low MSE of 3.2. The ECC and AES produced high MSE values of 3.9 and 3.5, respectively. The suggested technique was quite successful in locating images under all settings, leading to successful fingerprint encryption results with low MSE. This is because the proposed encryption is based on pixel density fluctuation present in all mass photos.

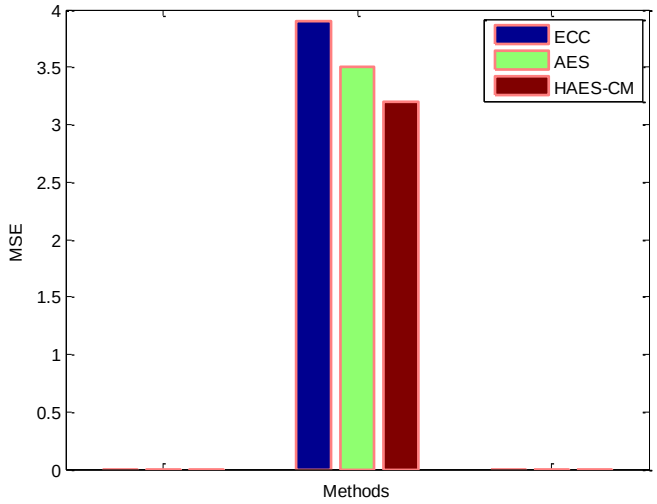

Figure 16. MSE comparison results between the existing and proposed methods.

4.8. Accuracy Comparison Results

Figure 17 compares the encryption accuracy for the three methods of encryption: ECC, AES, and the newly suggested HAES-CM. According to the encryption, the accuracy value decreased linearly as the number of photos increased. This graph shows that the proposed method successfully and accurately encrypted the image with a rate of 93.48 percent. Low accuracy was produced by the ECC and AES, at 82.65 and 89.23 percent, respectively. Based on the findings, it can be said that the suggested is very suitable for efficient fingerprint image encryption.

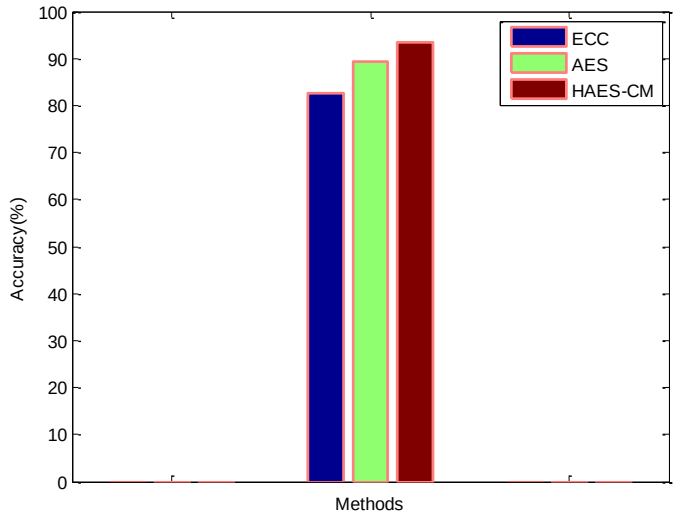

Figure 17. Accuracy comparison results between the existing and proposed methods.

4.9. Computation Time Comparison

When compared to the proposed ECC and AES methods, which required computation times of 6.5 s and 5.7 s, respectively, for encryption, the proposed algorithm's computation time was relatively low, reaching a value of 3.5 s, as shown in Figure 18. Different brain images were investigated for brain MR image encryption. ECC, AES, and the proposed HAES-CM encryption scheme were used in the encryption trials. The accompanying Figure 13 displays the computation time measurements for the existing and proposed methods. The primary drawback of most chaotic encryption algorithms is their reliance on floating-point calculations, which makes classical cyphers such as AES and DES, which

only work with integer values, more efficient and simpler to implement in software or hardware. The floating point calculation accuracy improved in the proposed model.

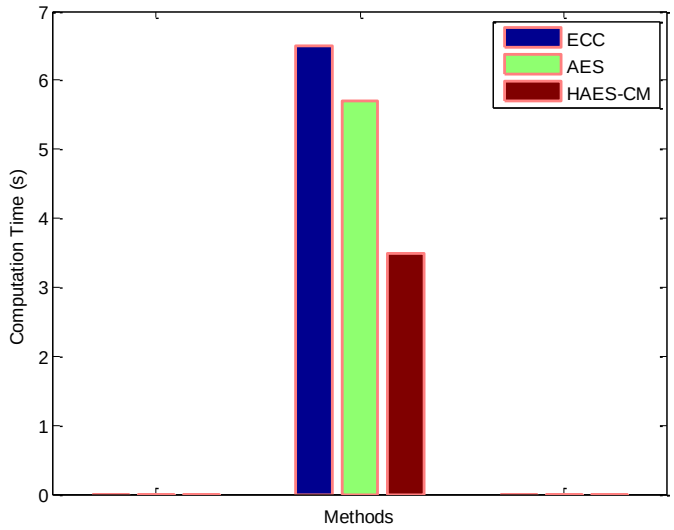

Figure 18. Computation time comparison results between the existing and proposed methods.

5. Conclusions and Future Work

For private and secure communication among edge devices in IoTs and Industry 4.0, a biometric authentication system called BioSec is recommended in this article. The security of IoTs was further improved by applying encryption techniques to protect the biometric data utilized. The system's database and data transmission pipelines securely safeguard the biometric data supplied there by using the encryption method. The chaotic sequence and the AES algorithm are combined to create a unique picture encryption algorithm that is detailed in this work. This technique generates the encryption key using a random sequence. The modified AES method is then used to implement the round keys produced by the chaotic system, encrypting the original picture. The updated AES has ten rounds of encryption and uses linear conversion and pixel value summarization in place of the column substitution and integration processes. These procedures make the method less time-complex and capable of dispersion, making the HAES-CM algorithm's encrypted images more resistant to differential attacks. The proposed method's key space is sufficiently large to fend off brute-force attacks. Because of how sensitive this approach is to the initial settings and input image, even tiny changes in these values can have a large impact on the encrypted image. Additionally, this feature stops unauthorized individuals from decrypting the encrypted image. The quickest algorithm is employed for encryption in this system after three alternative encryption techniques are applied to compare processing times. By strengthening the BAF work, the system can be significantly more secure. Since the system employs symmetric encryption techniques, the security of biometric data is likewise jeopardized if the encryption key is lost or stolen. As a result, the security of the entire system may be compromised. Evaluations of the proposed work scheme with existing encryption techniques show that the proposed HAES-CM encryption scheme beats others in terms of processing speeds.

Despite its relevance, research into biometrics for IoT security is still relatively young, as seen by the modest number of publications published [31]. Given the resource restrictions of IoT devices, as well as the issue of user acceptance and/or ease in collecting biometrics, lightweight authentication systems, preferably with features such as template data protection or key management, are required to improve system security. Another crucial element for promoting public adoption of biometrics in IoTs is a user-friendly strategy. We think that finding the ideal mix of ease and privacy will be crucial for the mainstream adoption of biometric technologies in IoTs.

Author Contributions: Datasets Preproceesing and investigation, A.A.; Algorithm Implementation, P.P.; Methodology and Validation, S.T.; Experimental and analysis of methodlogy, R.C.P.; Result Analysis, A.K.J.S. All authors have read and agreed to the published version of the manuscript.

Funding: Project number (RSP2023R498), King Saud University, Riyadh, Saudi Arabia.

Data Availability Statement: The data presented in this study are available upon request from the corresponding author.

Acknowledgments: Researchers supporting project number (RSP2023R498), King Saud University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Miranda, J.; Mäkitalo, N.; Garcia-Alonso, J.; Berrocal, J.; Mikkonen, T.; Canal, C.; Murillo, J.M. From IoTs to the Internet of People. *IEEE Internet Comput.* **2015**, *19*, 40–47. [CrossRef]
2. Lohiya, R.; Thakkar, A. Application Domains, Evaluation Data Sets, and Research Challenges of IoT: A Systematic Review. *IEEE Internet Things J.* **2020**, *8*, 8774–8798. [CrossRef]
3. Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security threats and issues in automation IoT. In Proceedings of the 2017 IEEE 13th Inter national Workshop on Factory Communication Systems (WFCS), 31 May 2017–2 June 2017; pp. 1–6.
4. Alferidah, D.K.; Jhanjhi, N.Z. A review on security and privacy issues and challenges in internet of things. *Int. J. Comput. Sci. Netw. Secur. IJCSNS* **2020**, *20*, 263–286.
5. Li, C.-T. Secure smart card based password authentication scheme with user anonymity. *Inf. Technol. Control* **2011**, *40*, 157–162. [CrossRef]
6. Yang, W.; Wang, S.; Zheng, G.; Yang, J.; Valli, C. A Privacy-Preserving Lightweight Biometric System for Internet of Things Security. *IEEE Commun. Mag.* **2019**, *57*, 84–89. [CrossRef]
7. Xu, T.; Wendt, J.B.; Potkonjak, M. November. Security of IoT systems: Design challenges and opportunities. In Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, USA, 2–6 November 2014; pp. 417–423.
8. Goel, A.K.; Rose, A.; Gaur, J.; Bhushan, B. July. Attacks, countermeasures and security paradigms in IoT. In Proceedings of the 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, India, 5–6 July 2019; Volume 1, pp. 875–880.
9. Sandeep, C.H. Security Challenges and Issues of the IoT System. *Indian J. Public Health Res. Dev.* **2018**, *9*, 744–753. [CrossRef]
10. Lin, H.; Bergmann, N.W. IoT Privacy and Security Challenges for Smart Home Environments. *Information* **2016**, *7*, 44. [CrossRef]
11. Grabovica, M.; Popic, S.; Pezer, D.; Knezevic, V. Provided security measures of enabling technologies in Internet of Things (IoT): A survey. In Proceedings of the 2016 Zooming Innovation in Consumer Electronics International Conference (ZINC), Novi Sad, Serbia, 1–2 June 2016; pp. 28–31. [CrossRef]
12. Wazid, M.; Das, A.K.; Odelu, V.; Kumar, N.; Conti, M.; Jo, M. Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks. *IEEE Internet Things J.* **2017**, *5*, 269–282. [CrossRef]
13. Jiang, X.; Liu, X.; Fan, J.; Ye, X.; Dai, C.; Clancy, E.A.; Farina, D.; Chen, W. Enhancing IoT security via cancelable HD-sEMG-based biometric authentication password, encoded by gesture. *IEEE Internet Things J.* **2021**, *8*, 16535–16547. [CrossRef]
14. Shomaji, S.; Ghosh, P.; Ganji, F.; Woodard, D.; Forte, D. An Analysis of Enrollment and Query Attacks on Hierarchical Bloom Filter-Based Biometric Systems. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 5294–5309. [CrossRef]
15. Mandal, S.; Bera, B.; Sutrala, A.K.; Das, A.K.; Choo, K.-K.R.; Park, Y. Certificateless-Signcryption-Based Three-Factor User Access Control Scheme for IoT Environment. *IEEE Internet Things J.* **2020**, *7*, 3184–3197. [CrossRef]
16. Srinivas, J.; Das, A.K.; Wazid, M.; Kumar, N. Anonymous Lightweight Chaotic Map-Based Authenticated Key Agreement Protocol for Industrial Internet of Things. *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 1133–1146. [CrossRef]
17. Punithavathi, P.; Geetha, S. Partial DCT-based cancelable biometric authentication with security and privacy preservation for IoT applications. *Multimed. Tools Appl.* **2019**, *78*, 25487–25514. [CrossRef]
18. Sujarani, R.; Manivannan, D.; Manikandan, R.; Vidhyacharan, B. Lightweight Bio-Chaos Crypt to Enhance the Security of Biometric Images in Internet of Things Applications. *Wirel. Pers. Commun.* **2021**, *119*, 2517–2537. [CrossRef]
19. Sadhukhan, D.; Ray, S.; Biswas, G.P.; Khan, M.K.; Dasgupta, M. A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. *J. Supercomput.* **2020**, *77*, 1114–1151. [CrossRef]
20. Sahoo, S.S.; Mohanty, S.; Majhi, B. A secure three factor based authentication scheme for health care systems using IoT enabled devices. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *12*, 1419–1434. [CrossRef]
21. Alzahrani, B.A.; Chaudhry, S.A.; Barnawi, A.; Xiao, W.; Chen, M.; Al-Barakati, A. ILAS-IoT: An improved and lightweight authentication scheme for IoT deployment. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *13*, 5123–5135. [CrossRef]
22. Priyadharshini, T.C.; Geetha, D.M. Efficient Key Management System Based Lightweight Devices in IoT. *Intell. Automtion Soft Comput.* **2021**, *31*, 1793–1808. [CrossRef]
23. Ashwaq, T.; Amira, K.; Qussay, F. Medical Image Encryption based of AES Chaptic Map. *J. Phys. Conf. Ser.* **2021**, *1937*, 012037.

24. Moafimadani, S.S.; Chen, Y.; Tang, C. A New Algorithm for Medical Color Images Encryption Using Chaotic Systems. *Entropy* **2019**, *21*, 577. [CrossRef]
25. Hashim, A.T.; Jalil, B.D. Color image encryption based on chaotic shit keying with lossless compression. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 5736–5748. [CrossRef]
26. Wadi, S.M.; Zainal, N. High Definition Image Encryption Algorithm Based on AES Modification. *Wirel. Pers. Commun.* **2014**, *79*, 811–829. [CrossRef]
27. Hashim, A.T.; Jabbar, A.K.; Hassan, Q.F. Medical Image Encryption Based on Hybrid AES with Chaotic Map. *J. Phys. Conf. Ser.* **2021**, *1973*, 12037. [CrossRef]
28. Loaiza, J.H.; Cloutier, R.J. Analyzing the Implementation of a Digital Twin Manufacturing System: Using a Systems Thinking Approach. *Systems* **2022**, *10*, 22. [CrossRef]
29. Zhang, G.; Jiang, J. Multimedia Security: A Survey of Chaos-Based Encryption Technology. In *Multimedia-A Multidisciplinary Approach to Complex Issues*; IntechOpen: London, UK, 2012. [CrossRef]
30. Arab, A.; Rostami, M.J.; Ghavami, B. An image encryption method based on chaos system and AES algorithm. *J. Supercomput.* **2019**, *75*, 6663–6682. [CrossRef]
31. Golec, M.; Gill, S.S.; Bahsoon, R.; Rana, O. BioSec: A Biometric Authentication Framework for Secure and Private Communication among Edge Devices in IoT and Industry 4.0. *IEEE Consum. Electron. Mag.* **2022**, *11*, 51–56. [CrossRef]
32. Vinod, F.; Brindha, M. Privacy preserving biometric authentication using Chaos on remote untrusted server. *Measurement* **2021**, *177*, 109257.
33. Nezhad, S.Y.D.; Safdarian, N.; Zadeh, S.A.H. New method for fingerprint images encryption using DNA sequence and chaotic tent map. *Optik* **2020**, *224*, 165661. [CrossRef]
34. Hung, H.I.; Junghsi, L. Fingerprint images cryptography based multiple chaotic systems. *Signal Process.* **2015**, *113*, 169–181.
35. Gonzalo, Z.; Shujun, L. Some basic cryptographic requirements for chaos based cryptosystems. *Int. J. Bifurc. Chaos* **2006**, *16*, 2129–2151.
36. Murillo-Escobar, M.A.; Meranza-Castillón, M.O.; López-Gutiérrez, R.M.; Cruz-Hernández, C. Integral Analysis for Chaos-Based Image Cryptosystems. *Entrophy* **2019**, *21*, 815. [CrossRef] [PubMed]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.