Hindawi
Journal of Sensors
Volume 2022, Article ID 4336822, 15 pages
https://doi.org/10.1155/2022/4336822

Research Article

A Real-Time Biometric Encryption Scheme Based on Fuzzy Logic for IoT

Masoud Moradi,[1] Masoud Moradkhani ,[2] and Mohammad Bagher Tavakoli[1]

[1] *Department of Electrical Engineering, Ilam Branch, Islamic Azad University, Ilam, Iran*
[2] *Department of Electrical Engineering, Arak Branch, Islamic Azad University, Arak, Iran*

Correspondence should be addressed to Masoud Moradkhani; moradkhani.m@gmail.com

Received 6 November 2021; Revised 12 January 2022; Accepted 18 January 2022; Published 26 February 2022

Academic Editor: Yanqiong Li

When milliards of smart devices are connected to the Internet using the Internet of Things (IoT), robust security methods are required to deliver current information to the objects. Using IoT, the user can be accessed via smart device applications at any time and any place, which challenges IoT security and privacy. From security point of view, users and smart devices should have secure communication channel and digital ID. Authentication is the first step towards any security action. Biometric-based authentication can ensure higher security for developing secure access. In this paper, fingerprint is used as the biometric factor. After scanning the fingerprint using the cellphone's camera, the image is transmitted to the authentication system. Since the comparison time increases after increasing the database volume, instead of storing the scanned fingerprint image, some key features of the scanned fingerprint are extracted and transmitted to the learning system of the convolutional neural network for detection and authentication and stored in the database. In the user authentication phase, the authentication keys are identified and the passcodes for the user of interest are extracted, and zero code is sent to the forged people; finally, the passcode is examined to check if the user is legal or illegal. In this step, the legal codes for fuzzy encoding of the image and text information are activated, and encryption is carried out in multiple steps depending on the number of members. The final code is compressed using Huffman coding and used for transmission to the network or storage. The proposed method is tested in MATLAB, and the results show that an excellent security is achieved using this cascade encryption method. Conclusively, the proposed hybrid coding technique reduces the information volume by 15.9%.

1. Introduction

Internet of Things (IoT) is a keyword in which all digital devices are connected to exchange information with each other. These devices have captured our daily life, including home appliances, offices, and healthcare. Security is the major concern for IoT. IoT technology can be applied in healthcare services, home monitoring, smart home/cities (for security and monitoring purposes), and oil platform as a control platform. With IoT deployment on the cloud (as Cloud of Things) and the society becoming digital, the volume, diversity, and validity of data (for example, big data) are increasing considerably. Authentication is required whenever the devices are connected to ensure secure connection. Therefore, gateway authentication is secure for a communication system. The existing vulnerabilities in IoT devices make them prone to collusion and forgery. The device authentication problem, or the question that if the device's ID is the same as what is being claimed, is a major problem. Therefore, biometric methods are used for authentication. A comprehensive architecture for biometric IoT and big data requires three challenges: (1) IoT devices have hardware and cannot process the encryption protocols that require resources. (2) The biometric devices introduce the data content of multimedia due to various biometric traits. (3) Fast growth of biometric-based devices and IoT contents generates a large volume of data for computational processing [1].

Biometric system is a set of technologies that extract data from biological or behavioral patterns of an individual (or other biological organisms) to identify it. The biometric systems rely on specific biological patterns. Data is executed through algorithms to achieve a specific result, which is associated with positive identification of another user or individual.

Compared to passwords, biometric is a biological measurement technology that employs the unique nature of some physical or behavioral traits of the humans for verification/identification. Unlike conventional authentication methods like passwords and tokens, biometric technology uses physical devices for authentication [2]. The fact that the biometric traits cannot be forgotten or lost and are difficult to forge makes them more secure than conventional authentication. Many biometric traits can be defined from the human body. Examples of biometric traits include fingerprint, face, iris, and voice. In general, they can be classified into two classes of physiological and behavioral traits, as shown in Figure 1. The above classes have their own pros and cons and play a unique role in specific applications [3, 4].

Among all biometric identification systems, fingerprint identification systems have more applications. Patterns of ridges and valleys on the surface of the fingertip are determined in the first few months; even identical twins have different fingerprints [2]. The detection performance of fingerprint detection systems, measured with equal error rate (EER) [6], has been reported to be excellent [6].

Mobile devices like smart phones are not just to make phone calls or send short messages, they have become very strong, and more people, especially adults, tend to have a smart phone, like iPhone, and use it almost all throughout the day. With the development of wireless network technology to 4G and LTE, faster data transmission and network stability can be provided. Consumers can purchase their required items with a tap on their mobile device. Also, various applications can be installed on mobile phones, making its applications wider. In this context, an application captures fingerprint images, enabling the user to transmit biometric information of the fingerprint to different systems at any time. Accordingly, this paper presents a biometric encryption technique using fingerprint that creates new and different information codes of the original information through cascade fuzzy encoding and uses Huffman coding to compress the new information and send it to the Internet for storage or transmission.

This paper is focused on designing a fingerprint-based encrypted biometric system used for various smart applications. The proposed biometric system considers security of private data and smart information compression. Also, the proposed scheme balances security and performance.

In the security dimension, in the proposed method, a cascaded fuzzy encryption is used, which, while changing the information for each text, has created a unique code for compression and spreading information. In the compression dimension, the proposed method with two steps of compression during encryption is reduced to more information for storing or sending. Therefore, in this paper, we have been able to achieve good results for different text and image information with the help of a new biometric cryptographic approach with fingerprint. A significant point in this work is the real-time authentication with the help of fingerprints for transferring and storing confidential information as soon as possible. In these circumstances, each person by registering fingerprint image at any moment is able to store and send their private information.

The rest of this paper is organized as follows. Section 2 reviews previous studies in the context of biometric encryption and compares them. Section 3 presents the biometric encryption system based on cascade fuzzy logic capable of information compression. Section 4 provides the empirical results and security analysis results. Finally, the paper is concluded and future suggestions are given in Section 5.

2. Related Work

Ensuring security through biometric authentication is a major challenge for network designers. The biometric information is very valuable and should be protected against fraud, especially during remote authentication and data exchange in wireless mesh networks like IoT. In [7], a secure biometric encryption has been presented for IoT based on fuzzy commitment that is suitable due to its ability to process and protect data against devices connected to the network. This paper, which is based on fingerprint methods, can be divided into two sections. First, on the transmitter side, a biometric trait vector is extracted using DWT, and then, data is encrypted to be transferred via the Internet. Second, on the receiver side, an authentication protocol is used to authenticate and decrypt the received data.

The authors have proposed a framework for ASIoT using biometric as an application [1]. The proposed biometric IoT includes seven layers to handle challenges of biometric applications and decision-making. In the rest of the paper, the design of the biometric IoT has been discussed from 4 points of view: (1) calculating parallel division and capture, (2) computational complexity, (3) device security, and (4) effectiveness of the algorithms. The empirical results have been presented to validate the effectiveness of the D&C method.

The IoT measurement abilities are now accessible as a public service. This new model that is called sensing as a service (S2aaS) allows the owners to sell/exchange data with the consumers interested in large markets. However, the service industry being open makes the S2aaS model subject to destructive attacks. In [8], a simple, efficient, and secure consensus scheme has been presented for the IoT-based S2aaS model. The users of the proposed system can access public services via a simple website, not a smart card, fast and securely. The fuzzy extraction algorithms, Diffie-Hellman elliptic curve, symmetric encryption, and hash functions have been used to develop a secure key consensus and data exchange session. Heavy processes are avoided in the critical and repeated intervals.

The authors of [9] have studied device fingerprinting (DFP) using interarrival time (IAT). IAT is the interval between two packets received subsequently. It has been observed that IAT is unique for a device because of the employed hardware and software. The works existing in the context of DFP employ statistical techniques to analyze IAT and generate more information using unique devices. This study presents a new idea of DFP by plotting IAT curves for the packets, 100 IATs in each diagram, and processing the resultant diagrams for device identification. This approach increases device DFP identification due to accessing deep learning libraries in image processing. In this study, two

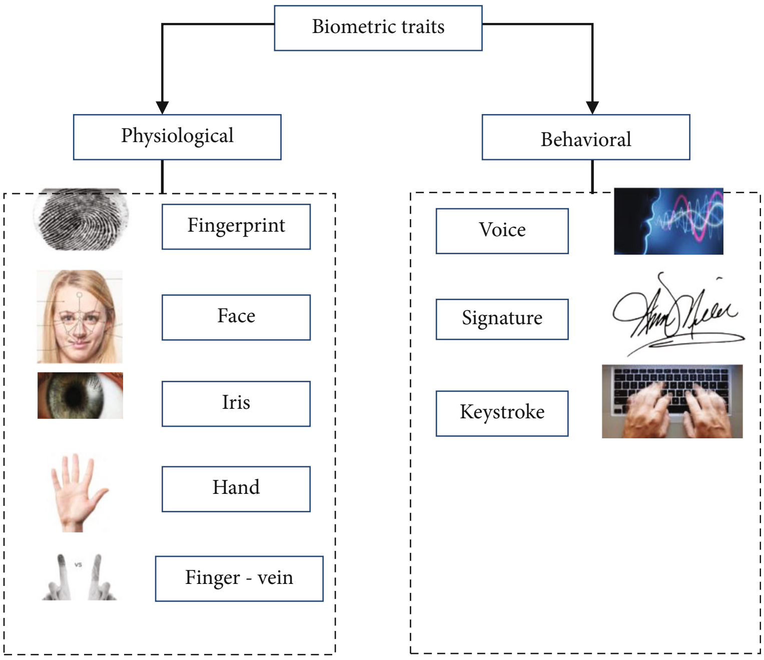


Figure 1: Classification of biometric traits (adapted from [5]).

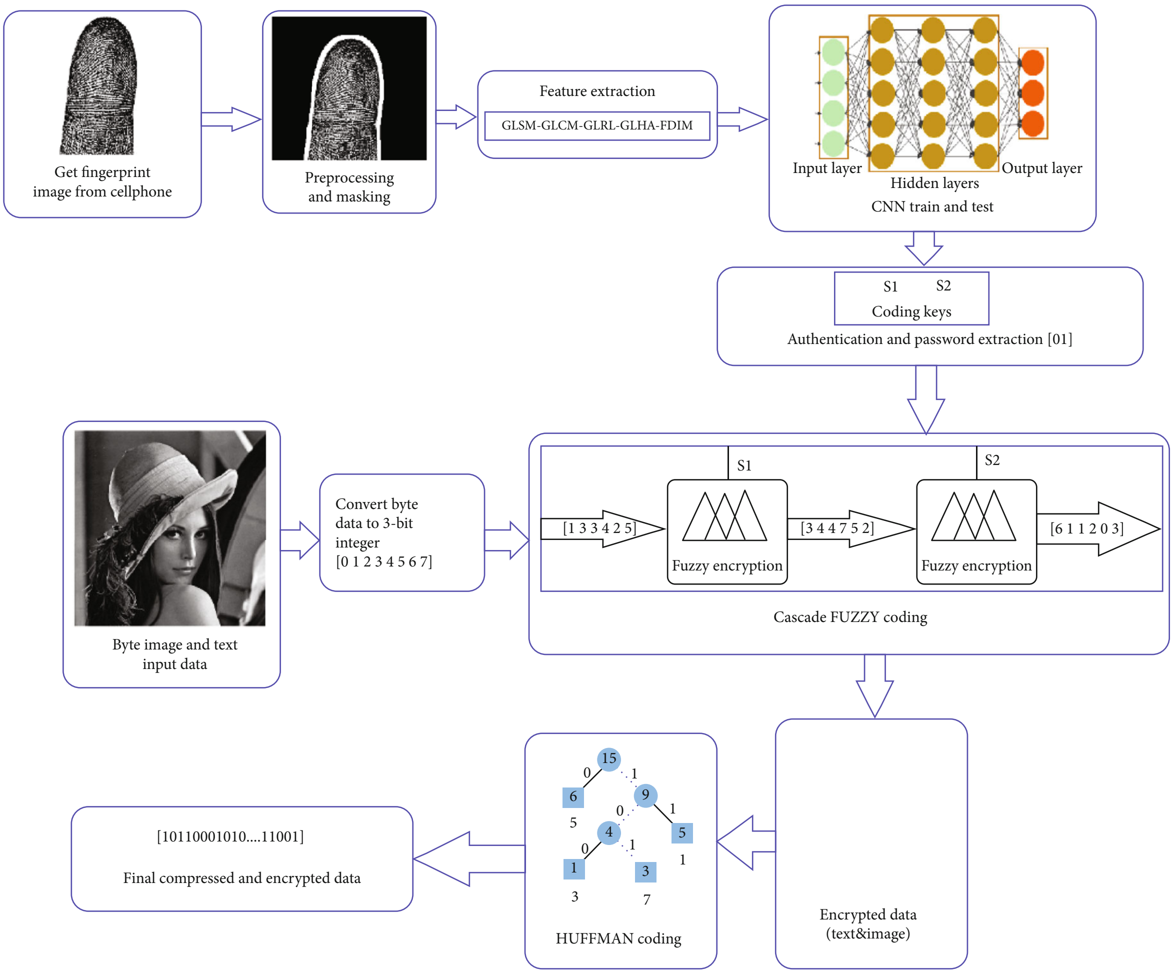


Figure 2: Flowchart of the proposed biometric encryption algorithm.

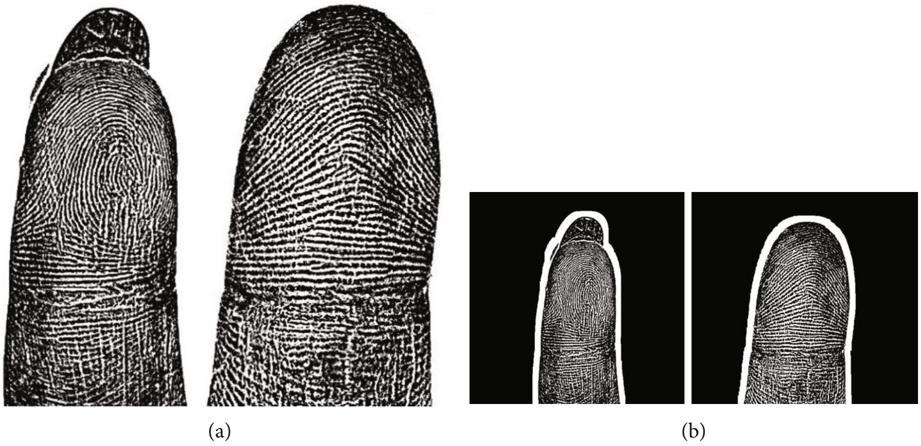


Figure 3: (a) Main fingerprint images. (b) Preprocessing and masking fingerprint images.

devices including iPad4 and iPhone 7 plus are connected to a router and the IAT diagrams are plotted; CNN is used to identify the devices, and an accuracy of 86.7% has been obtained.

Authentication with text passwords is still used widely, but it is insecure. Therefore, it is a major concern that is investigated using biometric authentication. In [10], the concept of securing the IoT network using biometric authentication through iris identification has been presented. In [11], the existing approaches for behavioral fingerprinting have been discussed generally, and their application on IoT devices has been evaluated.

In [12], a new software based on Java GUI has been presented for comparative fingerprint and iris biometric analysis. The first part is implemented using Java programming language in the GUI framework, called swing, while the rest of the paper discusses the advantages and disadvantages of both biometric methods and presents scientific data about the time of using fingerprint and iris detection for creating high-level security.

A new scheme, called human to object (H2O) has been presented for problem of sharing data and services in IoT [13]. The proposed approach is capable of continuous authentication of an entity in the network and presents the reliability assessment mechanism based on behavioral fingerprint. Accurate security analysis evaluates robustness of the proposed protocol.

In the context of essential urban infrastructures, trusting IoT data is of great importance, while most technology stacks provide a tool for authentication and encoding the device to cloud traffic. Currently, there is no mechanism to reject physical manipulation in IoT device sensors. To fill this gap, the authors of [14] have introduced a new method for hardware fingerprint extraction of an IoT sensor that can be used for identity authentication without being hidden. The proposed approach is detected by the behavior of analog circuits that apply an AC current with fixed frequency to the sensor while recording its output voltage.

In [15], a novel algorithm has been proposed for detecting people identity based on the image of the handwritten signatures. The proposed work combines textural and statistical features extracted from the images of the signature. Local binary platform (LBP) and histogram of oriented gradient (HOG) features represent texture. The authors are classified regarding gender using machine learning techniques. The proposed technique is evaluated based on a dataset of 4790 signatures, and an incentive accuracy of 96.17, 98.72, and 100% is obtained for k-nearest-neighbor (kNN), decision tree, and support vector machine (SVM) classifiers.

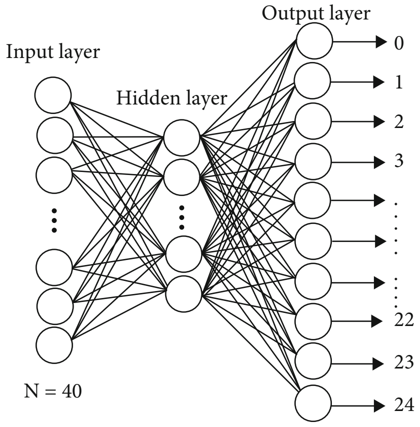
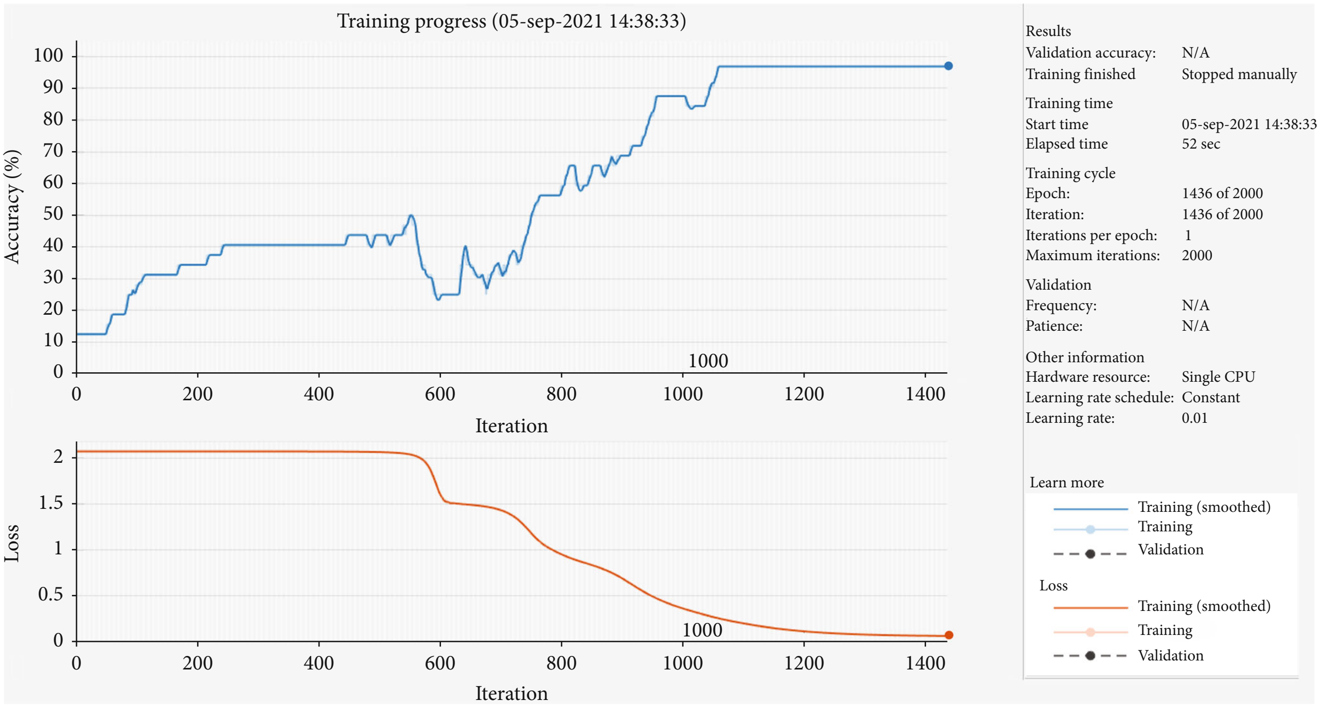


Figure 4: Structure of the studied CNN.

In [16], a multilayer biometric identification system has been presented with a small computational complexity, which is proper for IoT devices. Also, due to hardware and software cooperation in realizing this system in a chain structure, locating and providing alternative paths for the system flow in case of attack is easier. To analyze security of this system, one of the elements of this system called advanced encryption system (AES) has been contaminated by four hardware Trojans that target different parts of this module. The target of these Trojans is to destroy the biometric data being processed by the biometric identification system. All hardware and software of this system are implemented using MATLAB and Verilog HDL.

In [17], a new identity authentication method for IoT based on electromagnetic noise has been presented. The main advantage of electromagnetic noise is that each electronic



Results
Validation accuracy: N/A
Training finished Stopped manually

Training time
Start time 05-sep-2021 14:38:33
Elapsed time 52 sec

Training cycle
Epoch: 1436 of 2000
Iteration: 1436 of 2000
Iterations per epoch: 1
Maximum iterations: 2000

Validation
Frequency: N/A
Patience: N/A

Other information
Hardware resource: Single CPU
Learning rate schedule: Constant
Learning rate: 0.01

Figure 5: Block diagram of object classification.

device generates electromagnetic noise during normal operation. Some features of the electromagnetic propagation and machine learning algorithms are extracted for identifying devices based on these features. The proposed method achieves an accuracy of 77% while identifying the devices among a set of seven devices.

In [18], constraints of the IoT-based authentication scheme that has been introduced recently have been discussed for cloud computing. Also, an advanced three-step identity authentication scheme using chaos map has been presented. The cipher key is developed based on Diffie-Hellman key exchange based on Chebyshev chaos. Also, the cipher key is a long-term pass. It is ensured that the proposed scheme is secure against all attacks that might target the cipher key. Also, the proposed scheme can update the user's cipher key locally. The proof of Burrows-Abadi-Needham verifies that the proposed method presents mutual authentication and cipher key agreement. In [19], a light encryption system that can be implemented on limited IoT devices has been presented. This algorithm is mainly based on the advanced encryption standard (AES) and a new chaotic S-box.

In [20], a tested and reliable scheme that provides AE through reinforcing mapping of a plain text to elliptic curve cryptography (ECC) has been presented. It withstands multiple cryptographic attacks like chosen plaintext attack (CPA) and chosen ciphertext attack (CCA). In [21], a novel approach using Huffman coding and wavelet decomposition for multispectral fingerprint biometric system has been presented. The technique promises to template the database as well as compressed templates. The compressed templates

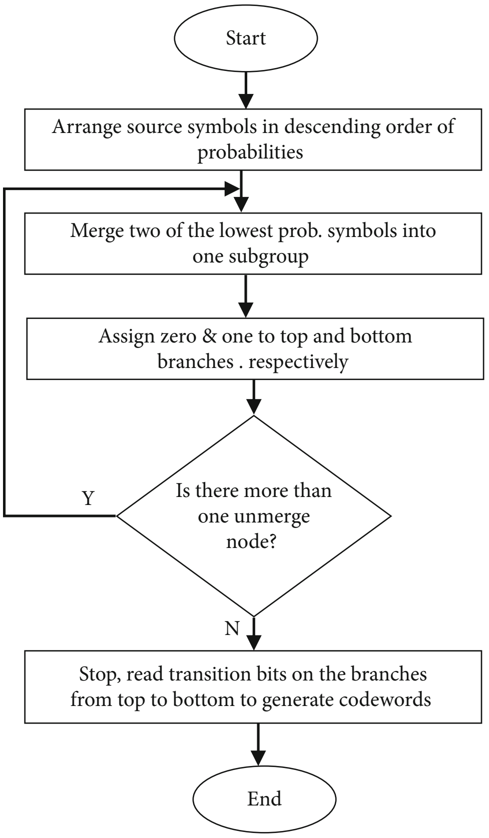

Start
Arrange source symbols in descending order of probabilities
Merge two of the lowest prob. symbols into one subgroup
Assign zero & one to top and bottom branches . respectively
Y
Is there more than one unmerge node?
N
Stop, read transition bits on the branches from top to bottom to generate codewords
End

Figure 6: The flowchart of Huffman algorithm [28].

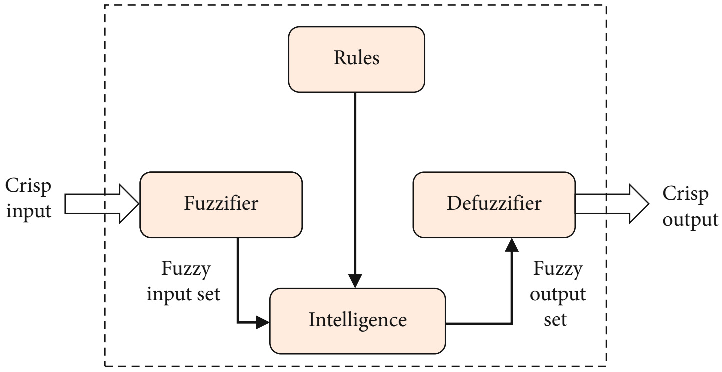


Figure 7: Block diagram of the fuzzy logic [25].

Table 1: Fuzzy rules of mapping.

Input (W)	0	1	2	3	4	5	6	7
Low	7	6	5	4	3	2	1	0
Mid	3	2	1	0	7	6	5	4
High	7	3	1	5	4	2	0	6

result in faster matching during authentication phase of the fingerprint biometric system. Moreover, the presented technique results in low revocability but high security to mitigate the effect of masquerade attacks.

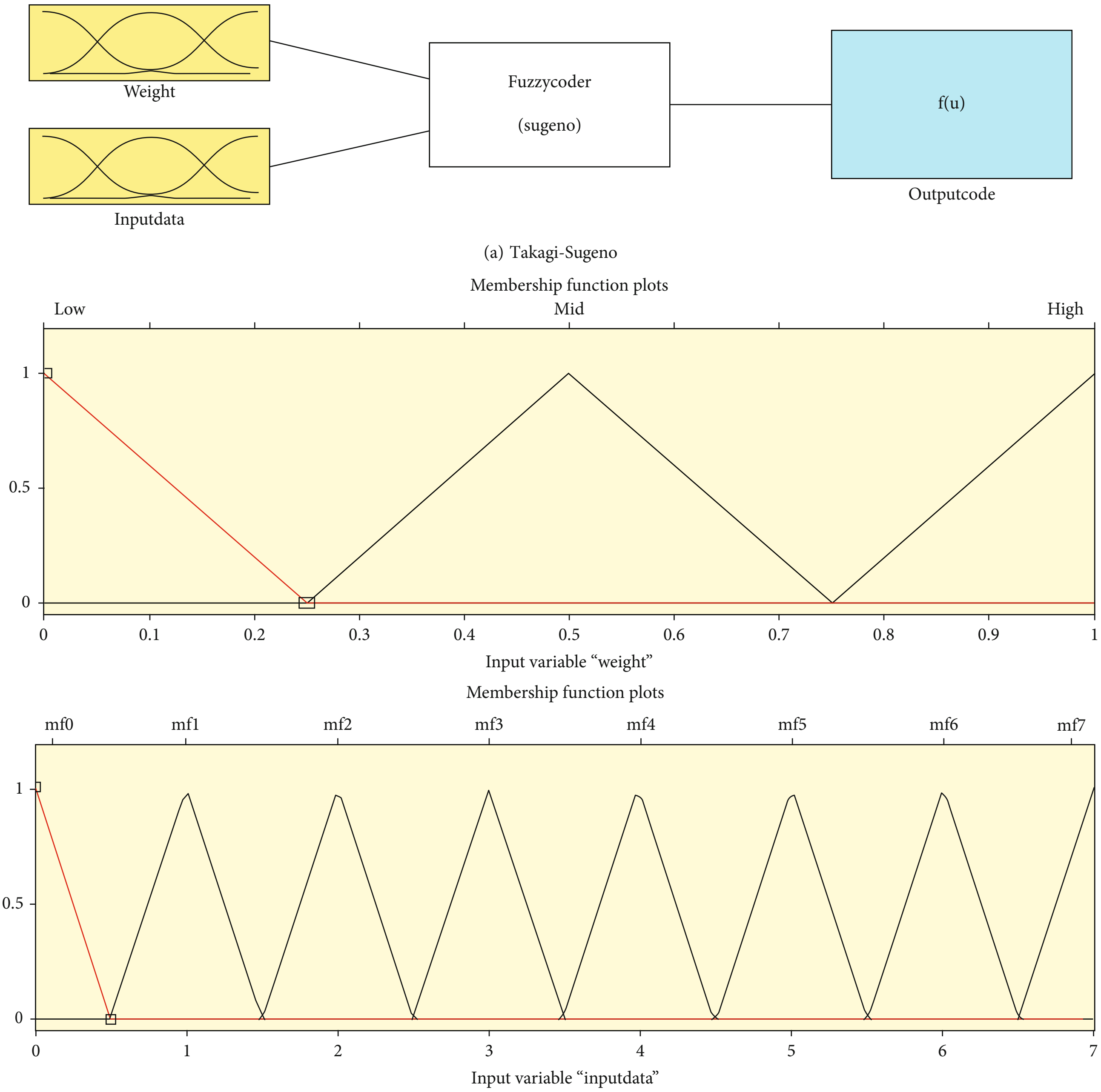
Fuzzy fingerprint biometric-based key security (FFBKS) scheme is introduced by utilizing feature extraction, in [22]. Extracted feature vectors securely produce private key for user. This key is sent to every sensor node, and then, private key among sensor nodes is produced by pseudorandom number and user key. Then, adaptive possibilistic C-means clustering (APCMC) is initiated for nodes grouping based on distance and identifier among nodes. Here, group key is produced based on fuzzy membership function from prime numbers, and it is utilized for estimation of security. After grouping is formed, data transmission is carried out among group key by fuzzy membership, and sensor nodes are carried out by biometric-based private key. Cluster group keys are diverse from one cluster to another. Also in [23], an optical selective encryption scheme for the medical image based on the fast and robust fuzzy C-means clustering (FRFCM) algorithm and face biometric has been proposed.

In [24], a new chaff generation algorithm for encryption which is computationally fast and viable for hardware acceleration by employing simple arithmetic operations has been proposed. Complexity study shows that the algorithm has a complexity of O(n2), which is a significant improvement over the existing method that exhibits O(n3) complexity. With the new chaff generation algorithm, it becomes much more amenable to implement the fuzzy vault scheme in the resource-constrained environment of system-on-chip.

The literature review reveals that biometric encryption is one of the essential issues for IoT security. Among various biometric structures, fingerprint has more applications in encryption due to easier access and possibility of scanning using smart phones. In this paper, this method is used along with authentication using a CNN to present a smart encryption based on cascade fuzzy logic and develop a secure encryption. To this end, Huffman coding is used for compression to achieve a lossless and asymmetric encryption. According to this structure, a private key is generated for each individual using the features extracted from the fingerprint image. The length of the passkey increases considering the number of subscriptions for the cascade fuzzy encoding structure and increasing number of cascade stages. This work is superior because the cipher keys are selected for each individual through selecting a set of analog keys for each stage. Also, the security of the proposed encryption is higher because the cipher keys depend on authenticating identities using fingerprint.

3. The Proposed Method

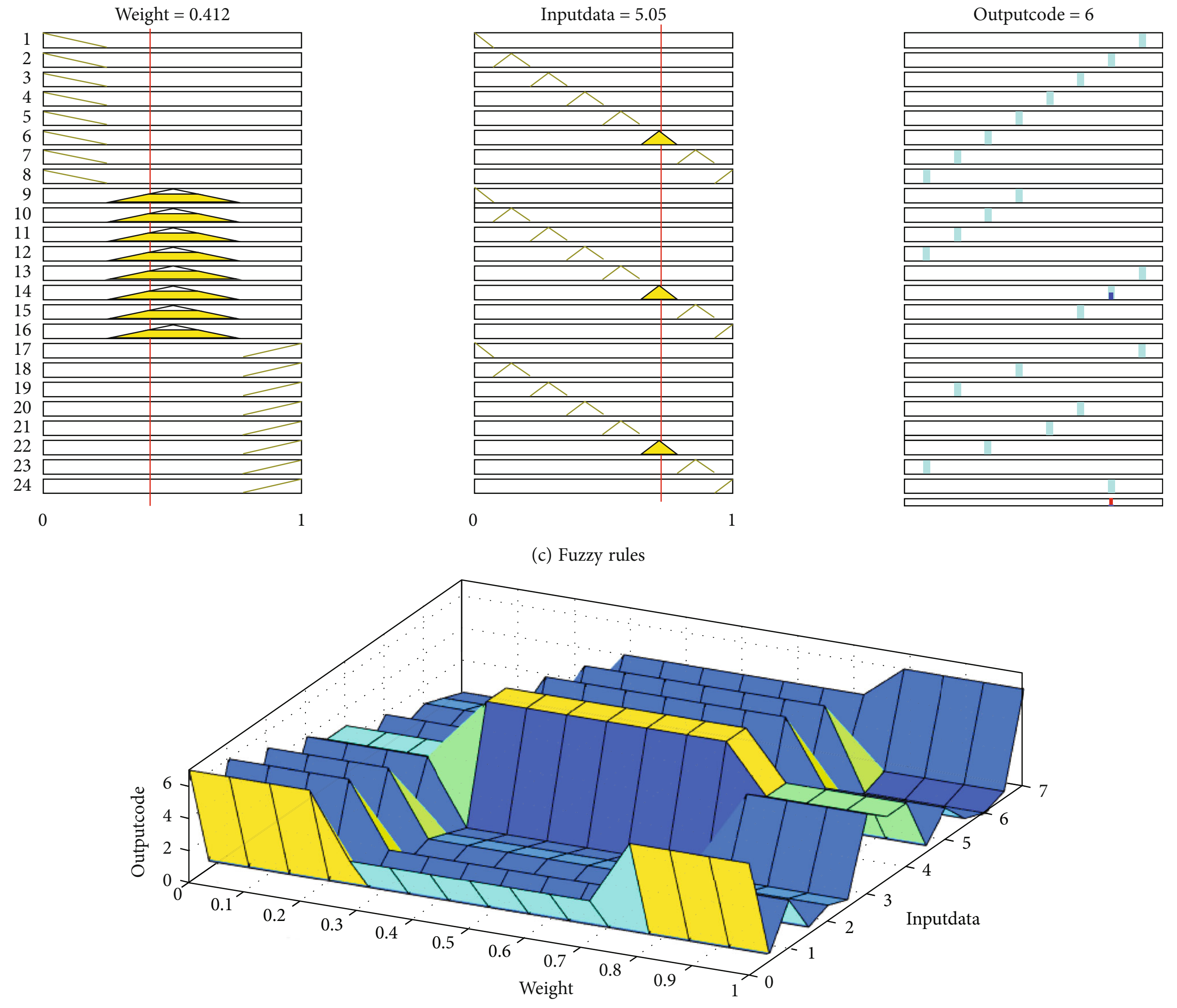
Fingerprint is unique for each individual and can be used as the signature of each individual to authenticate its identity. Most well-known apps of this type are used in criminology. However, today, demand for automatic fingerprint comparison is increasing. Among applications of this system, the followings can be mentioned: physical location access control, computer, network, resources, and bank accounts. There are ridges in the fingerprint images that are different from one individual to another. In this paper, a set of features is extracted for fingerprint images. These features represent the characteristics and position of the fingerprint ridges. First, the primary processes are applied to the images to show off the original finger images along with the ridges, and then, various conventional features on the masked fingerprint image, including geometrical and statistical features, GLSM, GLCM, GLRL, GLHA, and FDIM, are extracted. These features are extracted and stored as the fingerprint information of the individuals instead of the original fingerprint image. In the next step, this information is transmitted to different individuals for authentication. In this work, the fingerprint information that is defined for 25 different individuals using phones is given to CNN for training. Figure 2 shows a schematic of the proposed approach for biometric encryption based on fuzzy cascade encryption. After authentication, the analog passcodes S1 and S2 that are initialized in the range of zero



(a) Takagi-Sugeno

(b) Input membership functions

Figure 8: Continued.



(c) Fuzzy rules

(d) Input-output characteristics

Figure 8: Fuzzy logic block of the fuzzy encoder for determining different maps based on the private key.

and one are bicoded, and the information of the image or text of interest is encrypted in two fuzzy coding steps as shown in Figure 2. In the final step, the encrypted codes for 0, 1, 2, 3, 4, 5, 6, and 7 are compressed using the Huffman coding method so that the main code is not accessed easily. Now, the extracted binary codes are transmitted to the network to be stored or transmitted.

When decrypting the information of the stored or received data, fingerprint is used to restore the cipher keys. Then, the compressed information is retrieved for Huffman expansion, and the main information is retrieved for cascade fuzzy encoding using S1 and S2 keys. In the following, the proposed scheme, Huffman theory, and the proposed fuzzy logic are described.

3.1. Receiving the Input Information.

First, the fingerprint image is received via a smart phone for identity authentication and identification. In this paper, the fingerprint images of 25 individuals taken from the left index finger in 4 steps are used to encrypt a set of information, including image or text. Three fingerprint images are selected to train the CNN, and one image is used for the test.

3.2. Preprocessing and Feature Extraction.

First, the fingerprint image of the individual is transmitted in accordance with Figure 3(a). After receiving the input frames, the Gaussian noise removal algorithm is applied to each fingerprint image to increase accuracy (in Figure 3(b). After applying this filter, a polished image is obtained; thus, it is expected that feature points are extracted satisfactorily. In this step, a masking operation is applied to highlight the fingerprint image and its ridges to obtain more accurate information of the fingerprint image.

After masking, 40 different features, including geometrical and unique features, are introduced for object detection (GLSM, GLCM, GLRL, GLHA, and FDIM).

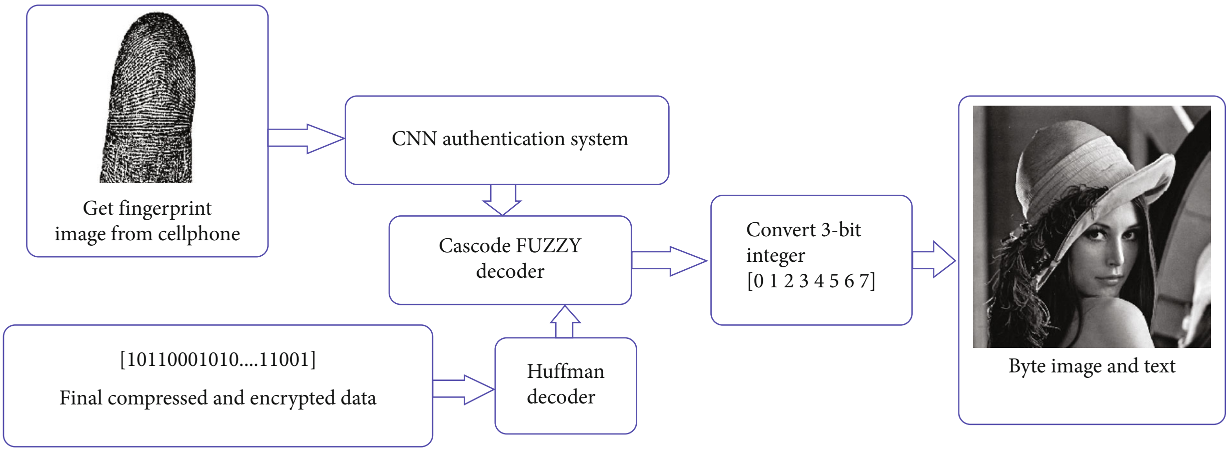
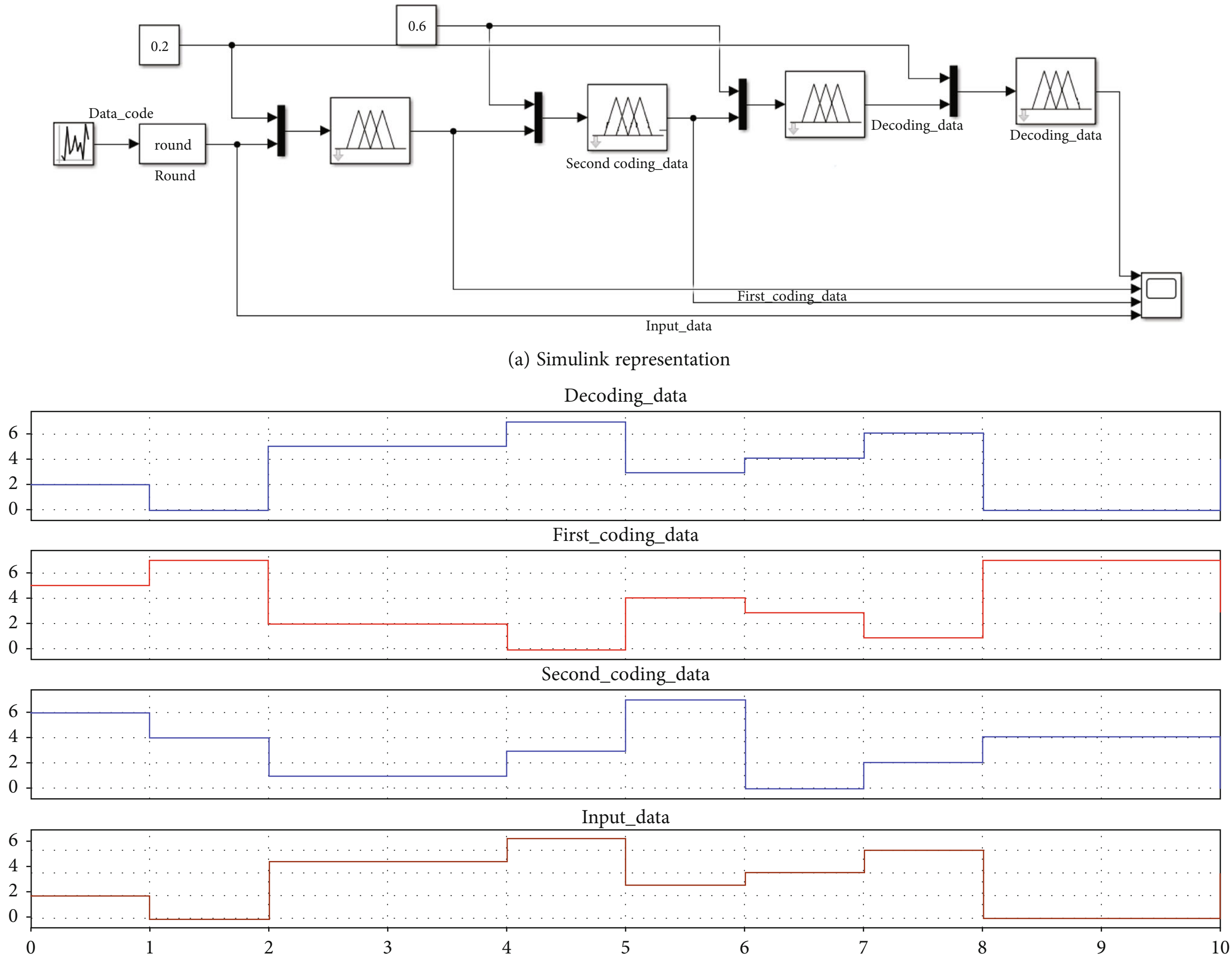


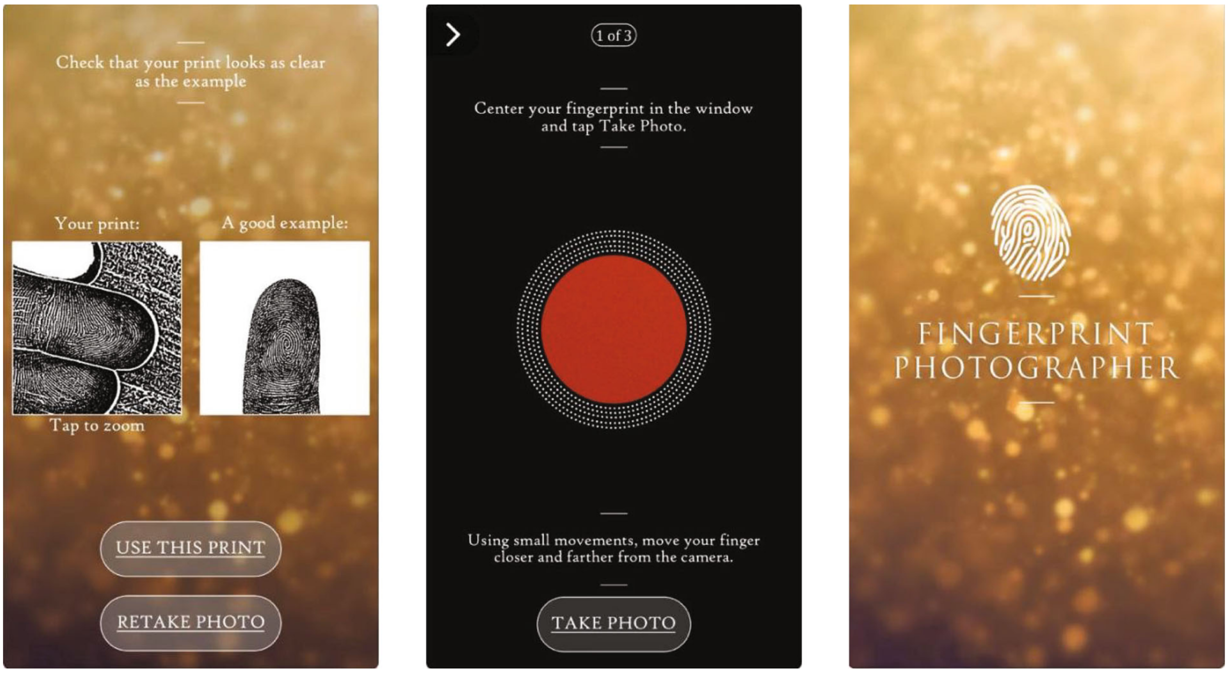
Figure 9: Block diagram of the proposed biometric encryption.



(a) Simulink representation

(b) Decoding and decryption for $w = 0.2$ and 0.6

Figure 10: Output of the cascade encoder and decoder.


Check that your print looks as clear as the example

Center your fingerprint in the window and tap Take Photo.

Using small movements, move your finger closer and farther from the camera.

Figure 11: The software used for fingerprint images.

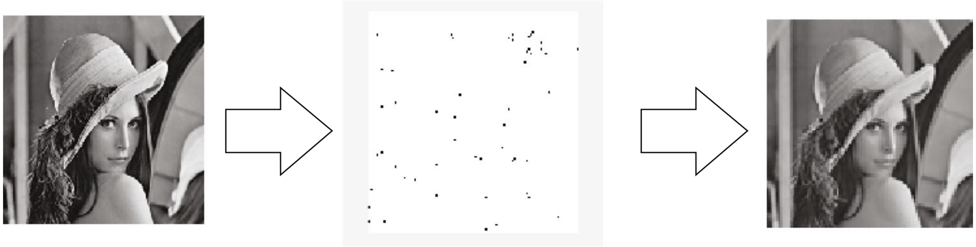

A. Original image B. Encoded image C. Deecoded image

Figure 12: Performance of the proposed biometric encryption scheme.

3.3. CNN Classification. The input layer of the network contains neurons that code the values of the input features. Our training data includes 32∗32 pixel images of the fingerprint image dataset; thus, the input layer includes 40 neurons equivalent to various features.

The second layer is a hidden layer. The number of neurons in this layer is represented by n, and different values are tested for n. The given example represents a small hidden layer including $n = 158$ neurons.

The output layer includes 25 neurons, representing 25 types of image labels. The output neurons are numbered from 0 to 24, and the neuron with maximum activation value is selected as the prediction result. Figure 4 shows the general structure of the CNN. Figure 5 shows the results of one test and training round. In general, the accuracy means that the model predicts the output correctly. In this work, the accuracy size is determined by dividing the number of correct authentication specimens from fingerprint to total image samples. According to this result, accuracy is 96.87%.

3.3.1. Huffman Coding Theory. Huffman programming in computer science and information theory that was developed by David Huffman in 1952 [25] is a technique to compress lossless data [26] based on coding of variable length source code proportional with the possibility of emergence, or in other words, it is expressed in image processing for image compression—with the possibility of repeating the color degree in the image array.

The Huffman coding theory depends on the two following laws [27]:

(A) The symbols that occur frequently are represented with shorter code words compared to the symbols that occur rarely

Table 2: Display coding results in different stages.

Main data code.												
7	6	2	6	5	7	3	7	6	7	5	5	6
	7	3	6	7	7	7	7	7	7	7	7	7
	7	7	7	7	0	4	1	0	0	0	0	0
	0	3	4	2	4	4	4	2	0	0	4	5
	7	2	2	0	6	0	0	5	3	1	1	0
	0	0	1	3	7	0	2	1	7	1	7	7
	4	0	1	6	7	2	5	0	2	0	0	1
	6	2	0	5	0	4	5	2	1	0	1	2
	2	2	6	5	6	2	5	0	1	5	4	6
	7	1	2									
First data encrypted code.												
0	1	5	1	2	0	4	0	1	0	2	2	1
	0	4	1	0	0	0	0	0	0	0	0	0
	0	0	0	0	7	3	6	7	7	7	7	7
	7	4	3	5	3	3	3	5	7	7	3	2
	0	5	5	7	1	7	7	2	4	6	6	7
	7	7	6	4	0	7	5	6	0	6	0	0
	3	7	6	1	0	5	2	7	5	7	7	6
	1	5	7	2	7	3	2	5	6	7	6	5
	5	5	1	2	1	5	2	7	6	2	3	1
	0	6	5									
Second data encrypted code.												
3	2	6	2	1	3	7	3	2	3	1	1	2
	3	7	2	3	3	3	3	3	3	3	3	3
	3	3	3	3	4	0	5	4	4	4	4	4
	4	7	0	6	0	0	0	6	4	4	0	1
	3	6	6	4	2	4	4	1	7	5	5	4
	4	4	5	7	3	4	6	5	3	5	3	3
	0	4	5	2	3	6	1	4	6	4	4	5
	2	6	4	1	4	0	1	6	5	4	5	6
	6	6	2	1	2	6	1	4	5	1	0	2
	3	5	6									
Huffman Binary code (323 bit).												
1	0	0	0	0	0	0	0	1	0	0	0	0
	0	0	0	1	1	0	0	1	0	1	1	0
	0	0	0	0	1	0	0	0	0	1	0	0
	0	1	0	0	0	0	1	0	0	1	0	1
	0	0	0	0	1	0	1	0	1	0	1	0
	1	0	1	0	1	0	1	0	1	0	1	0
	1	0	1	0	1	0	1	1	0	1	0	0
	0	1	1	1	1	1	1	1	1	1	1	1
	1	1	1	0	1	0	1	0	1	0	0	0
	0	1	0	1	0	0	0	1	0	0	0	1
	0	0	0	0	1	1	1	1	1	0	1	0
	0	0	0	0	1	1	0	0	0	1	0	0
	1	1	1	0	0	0	0	1	1	1	1	0
	0	0	1	0	1	0	1	0	1	1	0	1

Table 2: Continued.

1	1	1	1	1	1	1	0	1	1	0	1
0	1	1	0	1	1	0	0	1	0	1	1
1	0	0	1	1	1	0	1	0	0	1	0
0	1	1	0	1	1	0	0	0	0	1	0
0	0	1	0	0	0	1	1	1	0	0	1
1	1	1	1	0	1	1	0	0	0	0	0
0	1	1	1	0	0	0	1	1	1	0	1
0	0	0	0	0	1	0	0	1	0	1	1
1	1	0	1	1	0	0	1	0	0	1	0
0	1	0	0	0	0	0	0	0	1	0	0
0	0	0	0	1	0	0	0	1	1	1	0
1	1	0	0	0	1	0	1	0	0	0	0
0	0	1	0	0	1	1	0	0	1		

(B) Code words of the two symbols that are less frequent are the same

3.3.2. Huffman Algorithm. Implementation of the Huffman coding algorithm can be represented by the following steps:

(i) Step 1. Sort the pixel values based on their probability values

(ii) Step 2. Merge the two values with minimum probability; label one of them with zero and the other one with one

(iii) Step 3. Add their probabilities

(iv) Step 4. Specify two subsequent sets of the current set of singular values or pair of values

(v) Step 5. Go to step 2 and continue until another root is obtained

3.3.3. Huffman Flowchart. The Huffman coding algorithm can be described using the flowchart shown in Figure 6:

3.3.4. Classification and Labeling Items Based on Fuzzy Logic

(1) Fuzzy Logic Theory. Fuzzy logic theory is widely used to model the concepts of human thinking and refers to unreliability of the existing information for decision-making based on various measures. Substitution competency is described against measures, and their significant weight associated with the mentioned linguistic values is broadcast in numbers. In the fuzzy set, the linguistic variables are used to describe the fuzzy conditions and convert the linguistic variables to numerical variables, and the real logical values with unit distances are substituted in the decision-making process [29]. Therefore, mathematically, a set is defined as a limited, unlimited, or countable unlimited set of elements. In each case, each element is either a member of the set or not. However, in fuzzy systems, the element might be a part of the set or outside the set. Therefore, the answer to the question X "member of a set A" has no certain correct or incorrect answer. Figure 7 shows block diagram of the fuzzy logic.

(1)1. Fuzzy Set. A fuzzy set A is defined in the global discourse that is specified by a membership function: $\mu\mathrm{A} : \mathrm{U} \longrightarrow [0, 1]$ which is given in Eq. (1).

$$A = \left\{ (x, \mu A(x)) | x \int U \Lambda \mu A(x) \int [0, 1] \right\} \tag{1}$$

For each x member of set A, $\mu A(x)$ represents the relationship degree of x in A.

$$x \int (A, \mu) \Leftrightarrow x \int A \Lambda \mu(x) \neq 0 \tag{2}$$

In addition, using the membership function, each element x, which is a member of U describes a degree of relationship in each set A, expressing how much the element x belongs to the set A. Thus, an element with a relationship degree of zero indicates that this element is not included in the set, while an element with a relationship degree of one is completely included in the set.

(1)2. Fuzzification. Considering the application domain of the current study, the triangular membership function is used. A triangular fuzzy number A can be adjusted using three numbers (a, b, and c) with an adaptive function as in Eq. (3).

$$\mu A(x) = \begin{cases} 0, \ \mathrm{se}\, x < a\,; \\ (x - a)/(b - a), \mathrm{se}\, a \leq x \leq b\,; \\ (c - x)/(c - b) \ \mathrm{se}\, b \leq x \leq c\,; \\ 0, \ \mathrm{se}\, c < x. \end{cases} \tag{3}$$

(1)3. Fuzzy Inference. Defuzzification is a process that generates the quantitative value and magnitude in the fuzzy logic; that is, the fuzzy numbers are converted to a unit number based on different methods, which describes the average maximum weight as in Eq. (4).

Table 3: Comparison of the proposed method to some state-of-the-art methods using biometric encryption.

Reference	Key point	Accuracy
[30]	It extracted 57 geometric features from hand (lengths, areas, angles, and ratios) and used Euclidean distance for classification.	93%
[31]	It used morphological operations (e.g., thinning) in order to create the line edge map and implement the Hausdorff distance for classification. Research was performed on the own database.	95%
[32]	It implemented various features extractors (e.g., CompCode, OLOF, and RLOC) and various matching methods (e.g., SVM and kNN). Research was performed on 5 different mobile devices.	56% -81%
[33]	Lightweight verification schema based on fusion of the features presented in this work.	91%
[7]	Characteristic vectors have to be extracted from the gray scale image using filtering or transformation techniques such as oriented field flow curves (OFFC), Gabor filter, discrete wavelet transform (DWT), fast Fourier transform (FFT), discrete cosine transform (DCT), and principal component analysis (PCA).	90%
[21]	Wavelet feature extracted.	98.9%
This work	40 different features, including geometrical and unique features, are introduced for object detection (GLSM, GLCM, GLRL, GLHA, and FDIM).	99.1%

$$Z0 = \frac{\sum \mu(x)i \times wi}{\sum \mu(x)i}. \tag{4}$$

According to Eq. (4), Z_0 is the output of the defuzzifier, $\mu(x)i$ is the relationship degree with the fuzzy set, and wi is the output fuzzy weight.

3.4. Encryption under Fuzzy Mapping. After determining a weight for elements 0 to 7 for compression, it is time to present a method to encrypt information based on a complex encryption. Therefore, in this section, a mapping is introduced that changes the octal codes with their real value. In this section, two numerical keys are defined as the private keys, which are developed using the authentication codes in the previous steps. In this case, the fuzzy coding system is defined that introduces unidentifiable maps in the range of [0,1] for this system. Table 1 represents the governing equations of this structure. Figure 8 shows the fuzzy structure of the fuzzy encoder for Takagi-Sugeno type and the input membership functions.

The important point in the proposed encryption method is changing the private key for private key characteristics of S1 and S2, such that the transmitter generates the private keys using fingerprint. In this paper, three ranges are selected for the private key value; by increasing the number of ranges, the number of maps can be increased to increase the security level. The important point in this study is that selecting the number change mapping or number mapping is arbitrary and provided by a nonlinear and unpredictable model, where the number of nonlinear mappings can be increased by increasing the private key range.

In this section, with the development of maps, the encryption complexity is further increased and smaller processes are required. After this step, the coded data is transmitted to the destination based on the defined path, and the received code is decrypted according to Figure 9. As can be seen in this figure, the inverse procedure of the encryption process is carried out to obtain the information packet. Therefore, in this structure, the received data along with the information of weights and cipher key are processed according to the steps shown in the above figure to obtain the code of the original data. In this set, to obtain the main key, the authentication condition and fingerprint are used. In these blocks in the fuzzy and Huffman sections, decoding and decryption are used. As examples of correcting the data encryption and decryption, as shown in Figure 10, different private key weights are examined and simulated for different inputs. After decryption, the code is obtained in the octal basis; in the last section, conversion block is used to convert it to the binary basis to calculate different values. The output code is the binary code of the original data, which is finally converted to the original data values, including image or text, using inverse conversion. In this paper, two cascade stages are used for fuzzy encoding and decryption to the number of authenticated individuals.

4. Experimental Results and Analysis

For this experiment, we used a database including 25 individuals, with four different fingerprints for each individual. The fingerprint images are taken using mobile phones using fingerprint photographer and transmitted to the proposed identifier system as shown Figure 11. Each individual has four fingerprints (samples), 3 cases are used for training, and 1 case is used for test; it can be said the 75% of data is for training and 25% is for test.

This system is implemented using Apple iPhone SE. The program is deployed on a router with IOS as Wi-Fi connection point connected to the LAN of a wired network that executes Ethernet services, and the images are transmitted to the authentication system using MATLAB2017b. After authentication, in case of identification, the code of the authenticated individual is extracted and the results are transmitted to the fuzzy encoder. Due to the limited number of subjects, two fuzzy stages are used for encoding and decoding; but as the number of cascade stages increases, more individuals can be covered. Finally, the encrypted code is compressed for 0-7 samples with a good compression coefficient for storage or transmission to the network under Huffman coding. The images are considered vertically for the left index finger.

After sending the fingerprint image to the authentication system, if the individual is identified, the private keys are transmitted to the output, and if the information is fake, the cipher key returns zero. Next, the extracted key is tested for two types of text and image data, where the results are described in the following.

4.1. Text Data. Here, the selected text includes the following sentence:

"hello, I am a good student. This new EEG DATA."

In the first phase, the octal number codes of the text data are as follows, and the encoding results are as follows after two cascade fuzzy encoding steps with private keys of S1 = 0.2 and S2 = 0.6. In this study, the text includes 48 characters that occupy 384 bits of the memory by assigning 8 bits of memory to each character. For the final code, the volume of the encoded file using cascade fuzzy encoding is 323 bits. Therefore, compression with a coefficient of 0.841 decreases to total volume of the text. Table 2 shows these steps.

4.2. Image Data. Here, an image, shown in Figure 12, is used as the personal information. The results after encryption and decryption are shown in Figures 12(b) and 12(c). As can be seen for a 103∗103 image, despite reducing volume from 84872 bits to 79136 bits and compressing the image with a coefficient of 93.2%, the image in Figure 12(b) is an obscure image of the original image being encrypted.

4.3. Comparison. In this section, we compare articles in the field of biometrics and information security with the help of hands, irises, and fingerprints. Table 3 shows the important points and the accuracy of each and is finally compared with our proposed technique. As can be seen, due to the uncertain complexity defined in the proposed encryption, we have been able to improve information security well. The compression provided along with the proposed encryption also helps to store information, which can increase the importance of this encryption.

5. Conclusion

In this study, we presented a reliable encryption scheme for the IoT that considers security requirements and material constraints of the connected objects. The purpose of this encryption scheme is to protect the authentication information (biometric of the user and object identities) and data exchange (approved after one session). The basis is the biometric fuzzy commitment and illustrating the security requirements at each step. Selection, encoding, features vector, quantitative code, and compression code techniques based on the Huffman coding are all without security threat. For encryption, the fuzzy encoding technique is used due to its low computational complexity. To extract the features vector, an analog code technique was used for the private cipher key, which increased the complexity of selecting the cipher key for fuzzy encoding, and the fuzzy stages generate a heterogeneous and unpredictable value for each numerical value of the cipher key. In the proposed cryptographic method, nested semantic cryptographic structure is introduced by determining the fingerprint-based key code, which is decoded and decrypted according to the fuzzy key processes of confidential information. In addition to increasing security for encryption, this leads to an increase in compression and is an important benefit of the proposed method compared to biometric-based cryptographic methods. In the proposed method, we encounter the complexity of the Hoffman coding method that in the future we plan to expand its method for other codes. According to the classification results, an EER of 3.12% is obtained for fingerprint images of different individuals.

Data Availability

The data will be shared only at the request of the esteemed editor for review by the Reviewers.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] K. L. Ang and K. P. Seng, "Biometrics-based Internet of Things and Big data design framework," *Mathematical Biosciences and Engineering*, vol. 18, no. 4, pp. 4461–4476, 2021.

[2] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics*, Springer-Verlag New York, Inc, USA, 2008.

[3] W. Ahmed, A. Rasool, J. Nebhen et al., *Security in Next Generation Mobile Payment Systems: A Comprehensive Survey*, 2021, https://arxiv.org/abs/2105.12097.

[4] W. Yang, J. Hu, C. Fernandes, V. Sivaraman, and Q. Wu, "Vulnerability analysis of iPhone 6," in *2016 14th Annual Conference on Privacy, Security and Trust (PST),*, pp. 457–463, Auckland, New Zealand, 2016.

[5] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics for Internet-of-Things security: a review," *Sensors*, vol. 21, no. 18, p. 6163, 2021.

[6] G. Borghi, E. Pancisi, M. Ferrara, and D. Maltoni, "A double Siamese framework for differential morphing attack detection," *Sensors*, vol. 21, no. 10, p. 3466, 2021.

[7] A. Bentahar, A. Meraoumia, H. Bendjenna, S. Chitroub, and A. Zeroual, "Biometric cryptosystem scheme for Internet of Things using fuzzy commitment principle," in *2018 International Conference on Signal, Image, Vision and their Applications (SIVA)*, pp. 1–6, Guelma, Algeria, 2018.

[8] A. Bentahar, A. Meraoumia, L. Bradji, and H. Bendjenna, "Sensing as a service in Internet of Things: efficient authentication and key agreement scheme," *Journal of King Saud University-Computer and Information Sciences*, vol. 17, 2021.

[9] S. Aneja, N. Aneja, and M. S. Islam, "IoT device fingerprint using deep learning," in *2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS)*, pp. 174–179, Bali, Indonesia, 2018.

[10] G. Meena and S. Choudhary, "Biometric authentication in internet of things: a conceptual view," *Journal of Statistics and Management Systems*, vol. 22, no. 4, pp. 643–652, 2019.

[11] B. Bezawada, I. Ray, and I. Ray, "Behavioral fingerprinting of Internet-of-Things devices," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 11, no. 1, article e1337, 2021.

[12] K. G. Lalović and M. Z. Bogdanoski, "Java GUI application for comparing the levels of biometric security: Fingerprint vs. iris,"

Vojnotehnički glasnik/Military Technical Courier, vol. 69, no. 3, pp. 676–686, 2021.

[13] M. Ferretti, S. Nicolazzo, and A. Nocera, “H2O: secure interactions in IoT via behavioral fingerprinting,” *Future Internet*, vol. 13, no. 5, p. 117, 2021.

[14] F. Lorenz, L. Thamsen, A. Wilke et al., “Fingerprinting analog IoT sensors for secret-free authentication,” in *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, pp. 1–6, Honolulu, HI, USA, 2020.

[15] S. S. Gornale, S. Kumar, A. Patil, and P. S. Hiremath, “Behavioral biometric data analysis for gender classification using feature fusion and machine learning,” *Frontiers in Robotics and AI*, vol. 8, 2021.

[16] S. Taheri and J.-S. Yuan, “A cross-layer biometric recognition system for mobile IoT devices,” *Electronics*, vol. 7, no. 2, p. 26, 2018.

[17] A. Souza, I. Carlson, H. S. Ramos, A. A. Loureiro, and L. B. Oliveira, “Internet of Things device authentication via electromagnetic fingerprints,” *Engineering Reports*, vol. 2, no. 8, article e12226, 2020.

[18] F. Wang, G. Xu, G. Xu, Y. Wang, and J. Peng, “A robust IoT-based three-factor authentication scheme for cloud computing resistant to session key exposure,” *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 3805058, 15 pages, 2020.

[19] B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, and A. Alzamil, “Implementing a symmetric lightweight cryptosystem in highly constrained IoT devices by using a chaotic S-box,” *Symmetry*, vol. 13, no. 1, p. 129, 2021.

[20] H. AlMajed and A. AlMogren, “A secure and efficient ECC-based scheme for edge computing and internet of things,” *Sensors*, vol. 20, no. 21, p. 6158, 2020.

[21] A. Sharma, S. Arya, and P. Chaturvedi, “A novel image compression based method for multispectral fingerprint biometric system,” *Procedia Computer Science*, vol. 171, pp. 1698–1707, 2020.

[22] B. Nivedetha and I. Vennila, “FFBKS: fuzzy fingerprint biometric key based security schema for wireless sensor networks,” *Computer Communications*, vol. 150, pp. 94–102, 2020.

[23] Y. Shen, C. Tang, M. Xu, and Z. Lei, “Optical selective encryption based on the FRFCM algorithm and face biometric for the medical image,” *Optics & Laser Technology*, vol. 138, p. 106911, 2021.

[24] M. Khalil-Hani, M. N. Marsono, and R. Bakhteri, “Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm,” *Future Generation Computer Systems*, vol. 29, no. 3, pp. 800–810, 2013.

[25] D. Huffman, “A method for the construction of minimum-redundancy codes,” *Proceedings of the IRE*, vol. 40, no. 9, pp. 1098–1101, 1952.

[26] B. O’Hanen and M. Wisan, *JPEG Compression*, 2005.

[27] P. Kaur, *Compression using fractional Fourier transform, a thesis submitted in the partial fulfillment of requirement for the award of the degree of master of engineering in electronics and communication*Deemed University.

[28] A. Odat, M. Otair, and M. Al-Khalayleh, “Comparative study between LM-DH technique and Huffman coding,” *International Journal of Applied Engineering Research*, vol. 10, no. 15, pp. 36004–36011, 2015.

[29] H. M. Alabool and A. K. Mahmood, “Trust-based service selection in public cloud computing using fuzzy modifed VIKOR method,” *Australian Journal of Basic and Applied Sciences*, vol. 7, no. 9, pp. 211–220, 2013.

[30] S. Barra, M. De Marsico, M. Nappi, F. Narducci, and D. Riccio, “A hand-based biometric system in visible light for mobile environments,” *Information Sciences*, vol. 479, pp. 472–485, 2019.

[31] M. Trik, S. Pour Mozaffari, and A. M. Bidgoli, “Providing an Adaptive Routing along with a Hybrid Selection Strategy to Increase Efficiency in NoC-Based Neuromorphic Systems,” *Computational Intelligence and Neuroscience*, 2021.

[32] A. S. Ungureanu, S. Thavalengal, T. E. Cognard, C. Costache, and P. Corcoran, “Unconstrained palmprint as a smartphone biometric,” *IEEE Transactions on Consumer Electronics*, vol. 63, no. 3, pp. 334–342, 2017.

[33] A. Giełczyk, M. Choraś, and R. Kozik, “Lightweight verification schema for image-based palmprint biometric systems,” *Hindawi, Mobile Information Systems*, vol. 2019, article 2325891, 2019.