ISSN: 2182-2069 / E-ISSN: 2182-2077

Cryptography based on Fingerprint Bio Metrics

Zainab Ibrahim Abood Al-Rifaee[1*], Dr. Tarik Z. Ismaeel[2], and Dr. Samir Ibrahim Abood[3]

[1*]Assistant Professor, Department of Electrical Engineering, College of Engineering, University of Baghdad, Baghdad, Iraq. zainab.ibrahim@coeng.uobaghdad.edu.iq, https://orcid.org/0000-0002-4997-3853

[2]Professor, Department of Electrical Engineering, College of Engineering, University of Baghdad, Baghdad, Iraq. tarik.z@coeng.uobaghdad.edu.iq, https://orcid.org/0000-0002-4003-9968

[3]Professor, Electrical and Computer Engineering Department, Prairie View A & M University, USA. siabood@pvamu.edu, https://orcid.org/0000-0002-8976-8221

Received: July 18, 2024; Revised: August 27, 2024; Accepted: September 27, 2024; Published: November 30, 2024

Abstract

Fingerprints remain consistent and stable throughout a human's lifetime. This research exhibits the utilization of fingerprint bio-metrics to generate secured keys for improved security. The main contribution is the generation of 87 keys, achieved by enhancing the fingerprint image and sharpening it with a Laplacian filter. Three types of geometrical shapes chosen arbitrary, such as circle, square, and triangle, are separately drawn on the fingerprint after binarization, morphological operations, and thinning. Each shape is drawn five times on the fingerprint with different radii for each type to increase the number of keys. The end and bifurcation points are extracted as features inside and outside these shapes and these features are considered as keys. Chaotic-Pseudo-Random-Number Generator (CPRNG) technique is used, and the generated keys are merged with those generated from the positions of minutiae (end and bifurcation) points. The process was implemented using MATLAB R2021b. The simulation results demonstrate that it is difficult to crack the keys generated by this technique because the attacker requires a very long time, almost 7.5595e+159 years, to decrypt the encrypted message. Using geometrical shapes and CPRNG) technique increases the number of keys. The contribution of 87 keys is raising the time needed to break the encrypted text to this time, which is greater than the time required to crack the keys generated in some previous research compared to them. Therefore, the proposed technique enhances privacy and security. It can be used via deep learning in fingerprint identification, recognition, and key generation mechanisms and can use any other geometrical shapes.

Keywords: Cryptography, Fingerprint Bio-metrics, Feature Extraction, End Points, Bifurcation Points, Chaotic-pseudo-random-number Generator.

1 Introduction

Digital life has witnessed an increase in data and information security. Notably, the appearance of new technologies has forced data communication and security procedures (Hummady & Morad, 2022). Nowadays, biometric technologies are commonly used for analyzing human characteristics for security purposes. The five most common biometric patterns for security are hand, voice, eye, face, and

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 4 (November), pp. 401-417. DOI: *10.58346/JISIS.2024.I4.025*

*Corresponding author: Assistant Professor, Department of Electrical Engineering, College of Engineering, University of Baghdad, Baghdad, Iraq.

fingerprint. These biometric traits encrypt the original message to generate the ciphered data, and the same thing will be utilized to decrypt it. For securing information, there are many cryptographic algorithms available. The secret key and its length are essential for security (Rashid & Zaki, 2014; Kumari et al., 2021; Zabala-Blanco et al., 2020; Alsharman et al., 2022). Authentication is the earliest step to any security action. Biometric-based authentication can assure higher security to develop secure access (Moradi et al., 2022). A fingerprint is one of the best common biometric modalities utilized for authentication (Barzut et al., 2021; Ogla, 2017). In the fingerprint-based key generation schemes, the key's generation is from the user's biometric features, such as fingerprint minutiae points (Barman et al., 2015).

In (Ibrahim, 2017), a novel technique is introduced, encoding the fingerprint using a quick response code. This innovative approach involves extracting fingerprint minutiae as features. These features are further encrypted using Advanced Encryption Standard (AES). The authors (Hashem & Alibraheemi, 2022) have also pioneered a method of generating a cryptographic key from biometric features, specifically the fingerprint minutiae points and topological information. The authors (Jazi & Kuban Alibraheemi, 2018) have proposed a technique that secures sensitive data by enhances the process in a multi-biometric system which combines fingerprints and faces. In (Rashid & Zaki, 2014), a bio-crypt key generation method is presented, which relies on fingerprint minutiae. These minutiae are then used to generate 1024-bit prime numbers which are utilized in the Rivest-Shamir-Adleman (RSA) cipher algorithm for generating a 2048-bit cryptographic key, ensuring a high level of security. However, (Barman et al., 2014) have proposed an alternative method, generating a cryptographic key from the sender and receiver's cancellable fingerprint templates, further enhancing the security of the system. The authors (Yang et al., 2015) designed fingerprint encryption based on the irreversible transforming function used to transform the minutiae extracted from a thinned fingerprint image; while (Jha et al., 2016) used Hill and Caesar cipher for developing encryption and decryption algorithms to make transmitting messages more secure from eavesdropping.

The author (Esttaifan, 2023) proposed a modified Vigenère method and minutiae positions as features. The key created from fingerprint minutiae depends on the time of cipher-text generation and instantaneous date. To fortify the system against potential hackers, (Zaki, 2015) proposed a robust method of generating a key using fingerprint features (Milind et al., 2024). This technique comprises the EPROM memory part, housing crucial information on enhancement fingerprints and a group of shift registers. The authors (Abundiz-Pérez et al., 2016) presented a fingerprint image encryption technique based on R¨ Ossler map, a highly effective measure to bolster the security of biometric traits, enhance the system's strength, and deter identity theft (Herrera et al., 2023). In (Agrawal et al., 2021) used a fuzzy vault system to combine cryptography and biometric fingerprint images to ensure that no one except authorized users can utilize their PINs and passwords with legal data. However, in (Suresh et al., 2023), they proposed a gray code representation to reduce the not-matched bits between the bit strings generated from two instances at the same fingerprint. In a logistic chaos map (Jerjees et al., 2020) introduced a combination of logistic chaos map and fingerprint biometrics to encrypt a text message and get a robust cipher with brute force attack time of a high value.

This research exhibits the utilization of fingerprint biometrics to generate secured keys for improved security. The main contribution is the generation of 87 keys and three types of geometrical shapes, such as circle, square, and triangle. They are separately drawn on the fingerprint after binarization, morphological operations, and thinning. Also, a CPRNG technique is used and the generated keys are merged with those generated from minutiae (end and bifurcation) points' positions. As a result, it is difficult to crack the keys generated by this technique because the attacker requires time out of a lifetime

to decrypt the encrypted message, and it is greater than that required to crack the keys generated in the previous research. This research organization is as follows: Section 2 presents the proposed materials and methods; Section 3 describes the results and discussion. Finally, section 4 introduced the conclusions and future works.

2 Materials and Methods

The main goal of the proposed approach is to generate encryption keys that are difficult to crack. An excellent biometric is expressed by using a highly unique feature so that the opportunity for two persons to have the same features will be minimal and stable. A person's fingerprint is unique and has been used for over a century (Rashid & Zaki, 2014). Figure 1(a and b) shows the proposed system as a block diagram for encryption and decryption processes respectively.

2.1. Pre-Processing

The pre-processing stage aims to enhance and improve the image quality (Alsharman et al., 2022). Image sharpening is used for enhancing detected edges (Jayapal & Govindan, 2018). The sharpening technique improves the clearness of the image by enhancing the signs of the objects present in the image. This improves their details and borders, giving the image greater depth and neatness (Ganchimeg & Leopold, 2019).

In this work, the original fingerprint image (captured by a ZKTeco U270 device) of size M×N and (png) format is converted to a gray image. Then sharpening the image with a Laplacian filter using MATLAB R2021b. Figure 2 shows the pre-processing, where the original fingerprint, grayscale, and sharpening images are illustrated in Figure 2(a-c), respectively.

2.2. Post-Processing

- **Feature Extraction and Key Generation**

Feature extraction aims to count feature vectors to introduce a compact representation for the input signal (Abood, 2017; Shini et al., 2016). A fingerprint consists of an impression of ridges on the finger, with ridge characteristics known as minutia (Bakheet et al., 2022). The minutiae types are bifurcations and ridge endings (Rashid & Zaki, 2014), as shown in Figure 3, where Figure 3(a) shows ridge endings and Figure 3(b) shows ridge bifurcation (Bakheet et al., 2022). In a fingerprint feature extraction, the centers' coordinates xc and yc of the image are obtained as:

$$xc = M/2$$

$$yc = N/2 \qquad (1)$$

where (xc, yc) considered as the fingerprint diagonals intersection point in eq. (1).

a) Image Binarization

Image binarization is the operation that converts the greyscale image to a binary image. There is no general threshold value for the entire image; however, the threshold value of each pixel is calculated depending on the pixel location (Rashid & Zaki, 2014). The mean value of the intensity of the district pixels block has represented the threshold value. When the pixel's gray value is less than the threshold, it is fixed to black. Otherwise, it is white.

b) Morphological Operations

Erosion and dilation are the basic morphological operations. Erosion eliminates pixels from the object boundaries in an image, while dilation adds pixels to the object boundaries. The number of removed or added pixels depends on the shape and size of a structuring element used for processing the image (Rashid & Zaki, 2014).

c) Thinning

Thinning process is utilized to skeletonize any binary image by slimming all lines to the single pixel thickness (Rashid & Zaki, 2014). This research uses three methods to generate the keys, circle, square, and triangle. Figure 4 shows the key generation, whereas Figure 4(a-c) shows the circle, square, and triangle key generation.

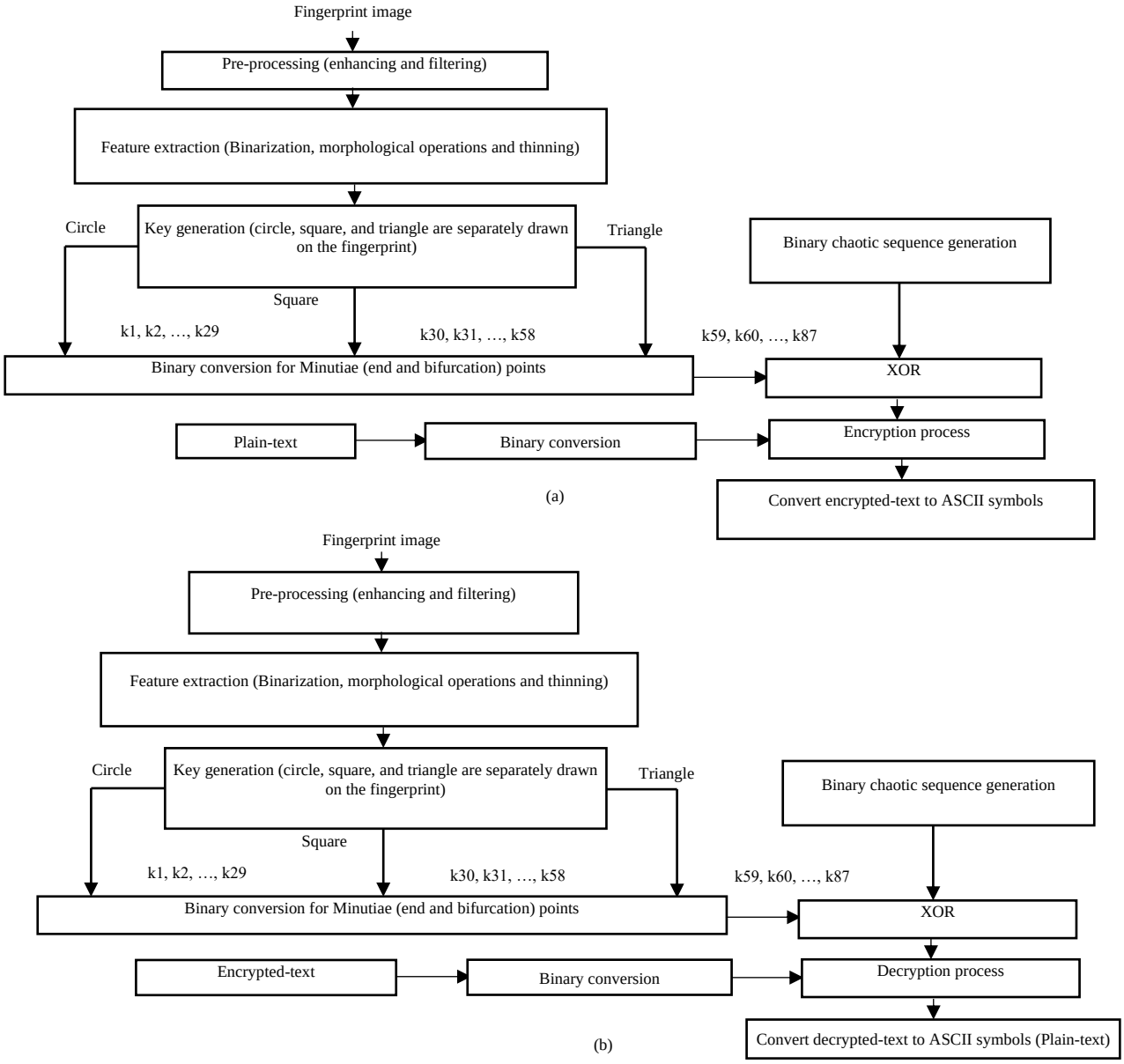
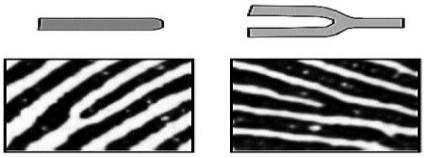


Figure 1: Proposed System Block Diagram a) Encryption b) Decryption

(a) (b) (c)

Figure 2: Pre-processing a) Original Image b) Gray Image c) Sharpened Image



(a) (b)

Figure 3: Minutiae Types a) Ridge Ending b) Ridge Bifurcation

d) Circle (c)

A circle of specified center coordinates (xc, yc) with a radius r = 60 is drawn, as shown in Figure 4(a). The ends and bifurcations of the fingerprint inside the circle are extracted separately, and their points are recorded. These ends and bifurcations are considered as keys of circle1 (c1), but for the taken fingerprint, there are no bifurcation points inside c1, so there is no bifurcation key. With the exact center coordinates, but with r = 110, circle2 (c2) is drawn. The ends and bifurcations inside c2 but at the same time outside c1 are extracted separately as (c2-c1) keys. With the exact center coordinates, but with r = 160, circle3 (c3) is drawn. The ends and bifurcations inside c3 but at the same time outside c2 are extracted separately as (c3-c2) keys. And so on for r = 210 and 250, the ends and bifurcations are extracted separately as (c4-c3) and (c5-c4) keys. The other keys, either for ends or bifurcations, are found as follows:

c1 = c1

c2 = (c2-c1) + c1

c3-c1= (c3-c2) + (c2-c1)

c3 = c2 + (c3-c2)

c4-c2 = (c3-c2) + (c4-c3)

c4-c1= (c4-c2) + (c2-c1)

c4 = c3 + (c4-c3)

c5-c3 = (c4-c3) + (c5-c4)

c5-c2 = (c3-c2) + (c5-c3)

c5-c1 = (c5-c2) + (c2-c1)

c5 = c4 + (c5-c4)

In Figure 1, the keys: k1, k2, …, k29 refer to c1, c2-c1, …, c5 for circle end and bifurcation points.

e) Square (s)

A square of specified center coordinates (xc, yc) with radius rs = 60 is drawn from the center point to the top-left corner, top-right corner, bottom-right corner, and bottom-left corner, as shown in Figure 4(b):

$$x1 = xc-rs$$
$$y1 = yc-rs \qquad (2)$$

Where (x1, y1) is a bottom-left corner point in eq. (2).

The ends and bifurcations of the fingerprint inside the square are extracted separately, and their points are recorded. These ends and bifurcations are considered as keys of square1 (s1), but for the taken fingerprint, there are no bifurcation points inside s1, so there is no bifurcation key. With the exact center coordinates, but with rs = 110, square2 (s2) is drawn. The ends and bifurcations inside s2 but at the same time outside s1 are extracted separately as (s2-s1) keys and so on for rs=160, 210, and 250. The other keys, either for ends or bifurcations, are found as in the circle. In Figure 1, the keys: k30, k31, …, k58 refer to s1, s2-s1, …, s5 for square end and bifurcation points.

f) Triangle (t)

A triangle of specified center coordinates (xc, yc) with rt = 80 is drawn from the center point to the top-left corner, top-right corner, and bottom corner, as shown in Figure 4(c):

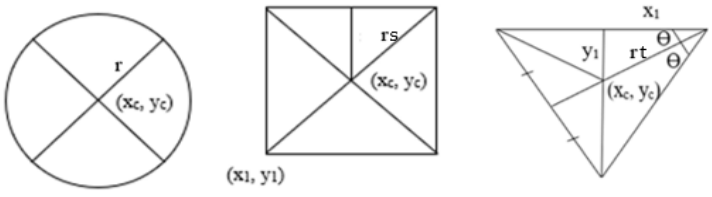
$$x1 = rt \cos \Theta$$
$$y1 = rt \sin \Theta$$
$$\Theta = 30° \qquad (3)$$

The ends and bifurcations of the fingerprint inside the triangle are extracted separately, and their points are recorded. In eq. (3) shows these ends and bifurcations are considered as keys of triangle1 (t1), but for the taken fingerprint, there are no bifurcation points inside t1, so there is no bifurcation key. With the exact center coordinates, but with rt = 110, triangle2 (t2) is drawn. The bifurcations and ends inside t2 but at the same time outside t1 are extracted separately as (t2-t1) keys. And so on for rt = 160, 250, 330, and 430. The other keys, either for ends or bifurcations, are found as in the circle. Note that rt values in the triangle have different values from those in the circle and square to cover the maximum area of the fingerprint and ensure an appropriate distance between the triangles. In this case, one can ensure that the ends and bifurcations are present at these distances. In Figure 1, the keys: k59, k60, …, k87 refer to t1, t2-t1, …, t5 for triangle end and bifurcation points. Table 1 shows the key number (key no.) and key name for circle, square, and triangle end and bifurcation points.

k1, k2, …, k15 and k16, k17, …, k29 refer to end and bifurcation keys for circle.

k30, k31, …, k44 and k45, k46, …, k58 refer to end and bifurcation keys for square.

k59, k60, …, k73 and k74, k75, …, k87 refer to end and bifurcation keys for triangle.



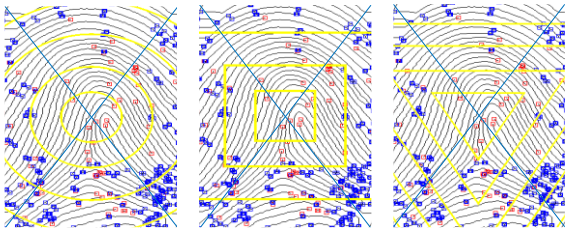
(a) (b) (c)

Figure 4: Methods of Key Generation (a) Circle; (b) Square; (c) Triangle

Table 1: Key no. and Key Name for Circle, Square and Triangle End and Bifurcation Points

Key no.	Key name	Key no.	Key name	Key no.	Key name	Key no.	Key name
K1	c1	K23	c4-c1	K45	s2-s1	K67	t4-t1
K2	c2-c1	K24	c4	K46	s2	K68	t4
K3	c2	K25	c5-c4	K47	s3-s2	K69	t5-t4
K4	c3-c2	K26	c5-c3	K48	s3-s1	K70	t5-t3
K5	c3-c1	K27	c5-c2	K49	s3	K71	t5-t2
K6	c3	K28	c5-c1	K50	s4-s3	K72	t5-t1
K7	c4-c3	K29	c5	K51	s4-s2	K73	t5
K8	c4-c2	K30	s1	K52	s4-s1	K74	t2-t1
K9	c4-c1	K31	s2-s1	K53	s4	K75	t2
K10	c4	K32	s2	K54	s5-s4	K76	t3-t2
K11	c5-c4	K33	s3-s2	K55	s5-s3	K77	t3-t1
K12	c5-c3	K34	s3-s1	K56	s5-s2	K78	t3
K13	c5-c2	K35	s3	K57	s5-s1	K79	t4-t3
K14	c5-c1	K36	s4-s3	K58	s5	K80	t4-t2
K15	c5	K37	s4-s2	K59	t1	K81	t4-t1
K16	c2-c1	K38	s4-s1	K60	t2-t1	K82	t4
K17	c2	K39	s4	K61	t2	K83	t5-t4
K18	c3-c2	K40	s5-s4	K62	t3-t2	K84	t5-t3
K19	c3-c1	K41	s5-s3	K63	t3-t1	K85	t5-t2
K20	c3	K42	s5-s2	K64	t3	K86	t5-t1
K21	c4-c3	K43	s5-s1	K65	t4-t3	K87	t5
K22	c4-c2	K44	s5	K66	t4-t2		

Figure 5 shows feature extraction and key generation, where Figure 5(a-c) shows the ends in a red color and bifurcations in a blue color for circle, square and triangle, respectively.



(a) (b) (c)

Figure 5: Feature Extraction and Key Generation a) Circle b) Square c) Triangle

- **Chaotic System**

A Chaotic system is vastly used with cryptography, while the researchers developed chaos maps several years ago. A pseudo-random bit generator is generated based on a chaotic system and used for stream-cipher cryptography (Jerjees et al., 2020). For more security and to produce a vital encryption key, a Chaotic-Pseudo-Random-Number Generator technique will be used. The keys generated by CPRNG are merged with those generated from minutiae (end and bifurcation) points' positions. The authors (Jerjees et al., 2020) used two Logistic maps but in this research three Logistic maps with different system parameters and initial conditions are used to achieve better randomness bits sequence:

$$X1(n+1) = I1 \times X1(n) \times (1 - X1(n))$$
$$X2(n+1) = I2 \times X2(n) \times (1 - X2(n))$$
$$X3(n+1) = I3 \times X3(n) \times (1 - X3(n)) \quad (4)$$

where I1, I2 and I3 are iteration factors. X1(n), X2(n), and X3(n) are the initial values in eq. (4).

Pseudo-random bit b(n) is generated from the logistic map after (n) iterations and obtained by comparing the mean value of the outputs of three logistic maps $(\bar{x})$ with the output of every map as in equation 5 (Jerjees et al., 2020).

$$b(n) = \begin{cases} 0 \; if \; x(n) \leq \bar{x} \\ 1 \; if \; x(n) > \bar{x} \end{cases} \quad (5)$$

where $\bar{x}$ is the mean value in eq. (5).

2.3. Encryption and Decryption Algorithms

Cryptography is a science that uses mathematical principles to encrypt and decrypt messages. It enables anyone to transmit sensitive information or store it across insecure networks such as the internet in order to be read by the intended recipient only and cannot be read by others (Jha et al., 2016; Sarkar & Noel, 2020; Alrifaee & Ismaeel, 2022; Younis et al., 2016; Al-Hassani, 2022). A cryptosystem is also referred to as a cipher system (Tyagi & Dixit, 2018). Data or messages that can be understood and read without special measures are called clear or plain-text. The process of hiding the plain-text substance or disguising it; is called encryption. The cipher-text is the unreadable gibberish results from the encryption process. The process of decoding the cipher-text to its original plain-text using a secure key is called decryption (Sarkar & Noel, 2020; George et al., 2020; Krishna & Kareem, 2021; Ibraheem et al., 2018). Encryption-based biometrics became more suitable to meet cryptographic demands by applying fingerprint images to generate the crypto-biometric key (Jerjees & Ismaeel, 2018).

Cryptography is symmetric or asymmetric; in symmetric, the same key is used in encryption and decryption algorithms. In asymmetric, two unlike keys are used: the public key to encrypt the plain-text and the private key to decrypt the cipher-text into plain-text (Barman et al., 2015; Rabee & Abdullah, 2020). The same plain-text encrypts to different cipher-text using different keys. The security of the encrypted data is dependent on the key secrecy and the algorithms' strength (Sarkar & Noel, 2020; Tyagi & Dixit, 2018; Al-Lehiebe, 2015). Encryption and decryption algorithms are expressed in equations (6) and (7):

$$e(i) \equiv (i + n) \bmod m \quad (6)$$
$$d(j) \equiv (j - n) \bmod m \quad (7)$$

where i and j are the plaintext and ciphertext letters' numbers, n is a shift key point, and m is a modulus in eq. (6) – (7).

The end and bifurcation coordinate points (x, y) values are sufficient to give randomness in data, so in this work, they have been considered as minutiae points of the fingerprint images for both sender and receiver. Table 2 shows a lookup table with 26 capital letters, space, and point designed with modulus m=28. Each letter (Let.) has a corresponding mapped number (No.) while (.) and (space) have the numbers 27 and 28, respectively.

Table 2: Lookup Table

Let.	No.	Let.	No.	Let.	No.	Let.	No.	Let.	No.	Let.	No.	Let.	No.
A	1	E	5	I	9	M	13	Q	17	U	21	Y	25
B	2	F	6	J	10	N	14	R	18	V	22	Z	26
C	3	G	7	K	11	O	15	S	19	W	23	.	27
D	4	H	8	L	12	P	16	T	20	X	24	Space	28

3 Results and Discussion

The key and algorithm control the operation on the plain-text and cipher-text (Tyagi & Dixit, 2018). Keys are crucial as ciphers without changing keys are simply breakable; therefore, fingerprint features are used in this paper as security keys. Table 3 shows the encryption and decryption process using the end key c1 with r = 60 and a plain-text (THANK YOU). The letter T has the end point (202, 216), when it is mapped onto the lockup table, it has a number of 20. In the encryption process using cipher shift right with mod28, the resulting number $No_{en.}$ = 18 (where $No_{en.}$ = (No. + (X+ Y)) mod28), which has a mapped letter R on the lockup table. When this ciphered letter R is decrypted using cipher shift left with an encrypted number No_{en} = 18 and mod28, the resulting number is the decrypted number ($No_{dec.}$) which is equal to 20 (where $No_{dec.}$ = ($No_{en.}$ - (X+ Y)) mod28), which has a mapped letter T on the lookup table and so on for other letters in the plain-text. The plain-text is encrypted then the cipher-text is decrypted to retrieve the plain-text. Some end points such as (202, 216), (200, 237), and (182, 263) in the table are repeated because the plain-text has nine letters and the end points inside c_1 are only six; so only these three points are repeated. There are no bifurcation points inside c1. Table 4 shows the processes of encryption and decryption using the ending points' key of c2 with r=110. Despite the same plain-text and No., the cipher-text differs in Tables 3 and 4 because the points differ.

Table 3: Encryption and Decryption using End Key c1 with r=60

Plain-text	No.	(X, Y)	$No_{en.}$	Cipher-text	$No_{dec.}$	Plain-text
T	20	(202, 216)	18	R	20	T
H	8	(200, 237)	25	Y	8	H
A	1	(182, 263)	26	Z	1	A
N	14	(173, 252)	19	S	14	N
K	11	(165, 297)	25	Y	11	K
	28	(134, 228)	26	Z	28	
Y	25	(202, 216)	23	W	25	Y
O	15	(200, 237)	4	D	15	O
U	21	(182, 263)	18	R	21	U

Table 4: Encryption and Decryption Using Bifurcation Key c2 with r=110

Plain-text	No.	(X, Y)	$No_{en.}$	Cipher-text	$No_{dec.}$	Plain-text
T	20	(78, 213)	9	I	20	T
H	8	(65, 255)	24	X	8	H
A	1	(167, 335)	3	C	1	A
N	14	(154, 351)	13	M	14	N
K	11	(78, 213)	28		11	K
	28	(65, 255)	16	P	28	
Y	25	(167, 335)	27	.	25	Y
O	15	(154, 351)	14	N	15	O
U	21	(78, 213)	10	J	21	U

Tables 5 and 6 show the encryption and decryption process using end and bifurcation points of various c keys with a plain-text (SHE IS VERY HAPPY.). The abbreviation (En.) refers to the cipher-text when the plain-text is encrypted using the related keys c1 or c2-c1 ..., etc. or in other terms

k1 or k2 ..., etc., and (Dec. text) refers to the plain-text when the cipher-text is decrypted using any of these keys. c1 has no bifurcations, which means no bifurcation point inside c1. In Table 5, using equations (6) and (7), the plain-text is encrypted by the key k1 to the encrypted text (QFBEWHZKJWKQFRMUKY). While by using key k2, the encrypted text will be (GI ZUVMJF MWLKNDQTY). For each key in Table 5, the encrypted text is not the same as for the other keys. In Tables 6, using bifurcation points, the encrypted text is not the same as for the other keys but it is the same only when the plain-text is encrypted by the keys k16 and k17 because k16 is c2-c1 while k17 is c2 as mentioned in Table 1 and c1 has no bifurcations which leads to c2-c1=c2.

Tables 7 and 8 show the encryption and decryption process using end points of various s and t keys, respectively. In these tables and Table 5, all the letters in the plain-text have different representations in the encrypted text, even if the letters are repeated in the message. s1 and t1 have no bifurcations, that means no bifurcation points inside s1 and t1.

Table 5: Encryption and Decryption Using End Points of Various c Keys

Plain-text	No.	En. k1	En. k2	En. k3	En. k4	En. k5	En. k6	En. k7	En. k8	En. k9	En. k10	En. k11	En. k12	En. k13	En. k14	En. k15	Dec. text
S	19	Q	G	G	Z	Z	G	A	Z		G	J	J	Z	Z	G	S
H	8	F	I	F	N	I	N	Q	Q	I	Q	A	Q	Q	I	A	H
E	5	B						G				X	X				E
	28	E	Z	E	T	Z	T	T	T	Z	T	U	T	T	Z	U	
I	9	W	U	U	Z	Z	U	S	Z	Z	U			Z	Z	U	I
S	19	H	V	H	I	V	I			V		L			V	L	S
	28	Z	M	M	X	X	M	B	X	X	M	S	S	X	X	M	
V	22	K	J	K		J		N	N	J	N	O	N	N	J	O	V
E	5	J	F	F	X	X	F	O	X	X	F	X	X	X	X	F	E
R	18	W	M	W	O	M	O	.	.	M	.	K	.	.	M	K	R
Y	25	K	W	W	U	U	W	.	U	U	W	P	P	U	U	W	Y
	28	Q	L	Q	G	L	G	T	T	L	T	U	T	T	L	U	
H	8	F	K	K	N	N	K	R	N	N	K	.	.	N	N	K	H
A	1	R	N	R	X	N	X	J	J	N	J	V	J	J	N	V	A
P	16	M	D	D	L	L	D	R	L	L	D	G	G	L	L	D	P
P	16	U	Q	U	V	Q	V	H	H	Q	H	I	H	H	Q	I	P
Y	25	K	T	T	O	O	T	G	O	O	T	P	P	O	O	T	Y
.	27	Y	Y	Y	W	Y	W	H	H	Y	H	T	H	H	Y	T	.

Table 6: Encryption and Decryption Using Bifurcation Points of Various c Keys

Plain-text	No.	En.c1	En. k16	En. k17	En. k18	En. k19	En. k20	En. k21	En. k22	En. k23	En. k24	En. k25	En. k26	En. k27	En. k28	En. k29	Dec. text
S	19		H	H	D	D	H	A	D	D	H	D	A	D	D	H	S
H	8		X	X	T	X	T	T	T	X	T	E	E	T	X	E	H
E	5		G	G	B	B	G	B	B	B	G	K	B	B	B	G	E
	28		.	.	V	.	V	L	L	.	L	J	J	L	.	J	
I	9		Z	Z	Y	Y	Z	F	Y	Y	Z	V	F	Y	Y	Z	I
S	19		G	G	X	G	X	A	A	G	A	P	P	A	G	P	S
	28		B	B	P	P	B	J	P	P	B	U	J	P	P	B	
V	22		U	U	C	U	C	D	D	U	D	D	D	D	U	D	V
E	5		V	V	.	.	V	Q	.	.	V	R	Q	.	.	V	E
R	18		F	F	C	F	C	O	O	F	O	O	O	O	F	O	R
Y	25		.	.	D	D	.	I	D	D	.	Z	I	D	D	.	Y
	28		.	.	D	.	D	Y	Y	.	Y	J	J	Y	.	J	
H	8		Y	Y	K	K	Y	R	K	K	Y	Y	R	K	K	Y	H
A	1		Q	Q		Q		K	K	Q	K	Z	Z	K	Q	Z	A
P	16		R	R	A	A	R	Z	A	A	R	I	Z	A	A	R	P
P	16		O	O		O				O		Z	Z		O	Z	P
Y	25		N	N	V	V	N	B	V	V	N	J	B	V	V	N	Y
.	27		O	O	U	U	U	K	K	O	K	X	X	K	O	X	.

Table 7: Encryption and Decryption Using End Points of Various s Keys

Plain-text	No.	En. k30	En. k31	En. k32	En. k33	En. k34	En. k35	En. k36	En. k37	En. k38	En. k39	En. k40	En. k41	En. k42	En. k43	En. k44	Dec. text
S	19	Q	G	G	Y	Y	G	A	Y	Y	G	J	A	Y	Y	G	S
H	8	Y	I	Y	C	I	C	Q	Q	I	Q	.	.	.	I	.	H
E	5	B			L	L		G	L	L		X	G	L	L		E
	28	E	Z	E	R	Z	R	O	O	Z	O	S	S	S	Z	S	
I	9	W	U	U	E	E	U	B	E	E	U		B	E	E	U	I
S	19	Q	V	Q	Y	V	Y	A	A	V	A	J	J	J	V	J	S
	28	Z	M	M	Y	Y	M	I	Y	Y	M	S	I	Y	Y	M	
V	22	G	N	G	R	N	R	X	X	N	X	M	M	M	N	M	V
E	5	B	V	V	Y	Y	V	T	Y	Y	V	X	T	Y	Y	V	E
R	18	W	I	W	X	I	X	K	K	I	K	I	I	I	I	I	R
Y	25	K	M	M	T	T	M	G	T	T	M	P	G	T	T	M	Y
	28	Z	A	Z	W	A	W	B	B	A	B	S	S	S	A	S	
H	8	F	C	C	O	O	C	W	O	O	C	.	W	O	O	C	H
A	1	R	.	R	S	.	S	V	V	.	V	T	T	T	.	T	A
P	16	M			L	L		Z	L	L		G	Z	L	L		P
P	16	U	S	U	V	S	V	Y	Y	S	Y	G	G	G	S	G	P
Y	25	K	J	J	V	V	J	F	V	V	J	P	F	V	V	J	Y
.	27	Y	S	Y	W	S	W	A	A	S	A	R	R	R	S	R	.

Table 8: Encryption and Decryption Using End Points of Various t Keys

Plain-text	No.	En. k59	En. k60	En. k61	En. k62	En. k63	En. k64	En. k65	En. k66	En. k67	En. k68	En. k69	En. k70	En. k71	En. k72	En. k73	Dec. text
S	19	P	Q	Q	G	G	Q	J	G	G	Q	A	J	G	G	Q	S
H	8	M	Y	M	F	Y	F	N	N	Y	N	R	R	R	Y	R	H
E	5	S	F	F	Y	Y	F	L	Y	Y	F	O	L	Y	Y	F	E
	28	Z	L	Z	X	L	X	R	R	L	R	J	J	J	L	J	
I	9	D	L	L	O	O	L	F	O	O	L	S	F	O	O	L	I
S	19	P	D	P	O	D	O			D		A	A	A	D	A	S
	28	E	Q	Q	T	T	Q	B	T	T	Q	J	B	T	T	Q	
V	22	H	Q	H	M	Q	M	I	I	Q	I	D	D	D	Q	D	V
E	5	C	C	C	U	U	C	Z	U	U	C	O	Z	U	U	C	E
R	18	M	G	M	P	G	P	I	I	G	I				G		R
Y	25	V	Z	Z	Q	Q	Z	C	O	O	Z	G	C	Q	Q	Z	Y
	28	E	L	E	X	L	X	G	G	L	G	J	J	J	L	J	
H	8	V	K	K	N	N	K	Z	N	N	K	R	Z	N	N	K	H
A	1	.	R	.	Y	R	Y	Z	Z	R	Z	K	K	K	R	K	A
P	16	K	K	K	H	H	K	Y	H	H	K	Z	Y	H	H	K	P
P	16	M	K	M	G	K	G	R	R	K	R	Z	Z	Z	K	Z	P
Y	25	B	N	N	M	M	N	E	M	M	N	G	E	M	M	N	Y
.	27	M	V	M	Y	V	Y	T	T	V	T	I	I	I	V	I	.

Using equation (4) with I1=3.7, I2=3.9, and I3=4 and initial values, X1(0) =0.61, X2(0) =0.5, and X3(0) =0.6 to achieve better randomness bits sequence. To generate the binary key used for encryption, CPRNG technique generated keys merged with those generated from minutiae (end and bifurcation) points' positions. So, binary bits of minutiae positions are XORed with the binary bits generated from CPRNG. Then, this key is XORed with the binary bits of the plain-text to produce the cipher-text, which is converted to ASCII symbols. In the decryption process, the recipient gets the key in random text, which contains the encrypted text too. This key is a guide used in the encryption process. Tables 9 and 10 show the encryption and decryption of the proposed system.

Table 9: Encryption of the Proposed System

Encryption Process	Operation
Plain-text	SHE IS VERY HAPPY.
Encoded plain-text using ASCII	01010011, 01001000, 01000101, 00100000, 01001001, 01010011, 00100000, …
Minutiae points	(202,216), (200,237), (173,252), (78,213), (65,255), (107,135), (54,151), …
Minutiae key	11001010, 11011000, 11001000, 11101101, 10101101, 11111100, 01001110, …
Binary chaos key	11101001, 11110100, 11011010, 10001011, 01101100, 10011000, 00011101, …
Minutiae binary key XORed by chaos key	00100011, 00101100, 00010010, 01100110, 11000001, 01100100, 01010011, …
Cipher-text (plain-text XORed with the key)	01110000, 01100100, 01010111, 01000110, 10001000, 00110111, 01110011, ...
Decoding of cipher-text using ASCII	pdWFˆŽ§Ga/(h&?)…

Table 10: Encryption of the Proposed System

Decryption Process	Operation
Encoded cipher-text to binary using ASCII	01110000, 01100100, 01010111, 01000110, 10001000, 00110111, 01110011, ...
Minutiae points	(202,216), (200,237), (173,252), (78,213), (65,255), (107,135), (54,151), …
Minutiae key	11001010, 11011000, 11001000, 11101101, 10101101, 11111100, 01001110, …
Binary chaos key	11101001, 11110100, 11011010, 10001011, 01101100, 10011000, 00011101, …
Minutiae binary key XORed by chaos key	00100011, 00101100, 00010010, 01100110, 11000001, 01100100, 01010011, …
Plain-text (cipher-text XORed with the key)	01010011, 01001000, 01000101, 00100000, 01001001, 01010011, 00100000, …
Decoding of plain-text using ASCII	SHE IS VERY HAPPY.

Cryptanalysis is breaking and analyzing secure communication (Sarkar & Noel, 2020). There are many attacks in a biometric system to recover and steal the biometric trait of the user. One of the powerful attacks is the extracting of fingerprint patterns when transmitted over communication lines lying between modules (Salman et al., 2020; Bakheet et al., 2022; Jassim et al., 2022). Identification of a human is the most pivotal step today to reduce identity theft and fraud. Fingerprints are the unique and most important thing; the ridges assist people in keeping things. Brute-force attacks include different hacking techniques that use password guessing in order to access a system (Abdulrezzak & Sabir, 2023). A timing attack uses encryption/decryption algorithms and occasionally takes different time values for various inputs (Krishna & Kareem, 2021). Brute-force attack time (Alrifaee & Ismaeel, 2022). Using geometrical shapes and CPRNG) technique increases the number of keys. The contribution of 87 keys is rising the BFA time:

BFA time/sec. = [((no. of keys' type) × (number of keys in each type)) × ((no. of fingerprint features' type) × (number of end and bifurcation points))!) / (deciphering operations' number per second)] (8)

To convert BFA time from second to year, it must be divided by ($60\times 60 \times 24 \times 365$), which is equal to 31536000:

BFA time/year = 3×29× (((2×56)!) / (2^56)) / 31536000 = 7.5595e+159 year

where 3 refers to the three types of keys: circle, square, and triangle

29 is the number of keys in each type

2 is the type of fingerprint features; ends and bifurcations

56 is the number of end and bifurcation points

2^56 is the deciphering operations' number per second

Table 11 shows the proposed technique as compared with other techniques. Several features and keys in (Alrifaee & Ismaeel, 2022) which uses the retina vessel's end as features are 103 and 3, respectively. While in the proposed technique, which uses ends and bifurcations, is 112 and 87, respectively. Reference (Jerjees et al., 2020) used a hybrid ciphering method with two chaos logistic maps, while the proposed technique used three chaos logistic maps. A BFA time/year in the proposed technique is 7.5595e+159, which is more significant than that in (Alrifaee & Ismaeel, 2022) and (Jerjees et al., 2020). It means that when the number of keys, features, and logistic chaos map increases, the BFA time will increase, and the technique will be more protected from attackers.

Table 11: Comparison between the Proposed Technique and Other Techniques

Parameters	**Hybrid ciphering method (Jerjees et al., 2020)**	**Retina vessel's end (Alrifaee & Ismaeel, 2022)**	**Proposed technique**
No. of features	-	103	112
No. of keys	-	3	87
Chaos logistic maps	2	-	3
BFA time / year	5.9e+129	1.3074e+140	7.5595e+159

4 Conclusions

The proposed technique improves security by generating 87 secured keys from fingerprint biometrics. These keys are generated in a method that is difficult enough to guess. The generation is achieved by enhancing the fingerprint image and sharpening it with a Laplacian filter. Circles, squares, and triangles are drawn on the fingerprint separately after binarization, morphological operations, and thinning. Then, the end and bifurcation points are extracted inside and outside these shapes to generate secured keys. A CPRNG technique is used, and the generated keys are merged with those generated from the positions of minutiae (end and bifurcation) points. After the encryption and decryption processes, it was found that the attacker required time of almost 7.5595e+159 years to decrypt the encrypted message, which is more than that required to crack the keys generated in the previous researches. Also, it is proved that by separately drawing three types of geometrical shapes on the fingerprint and with different radii, the plain-text can be reconstructed after encryption using keys generated from end and bifurcation points. That means drawing any geometrical shape with any radius can be used in this technique. Therefore, the proposed technique can enhance privacy and security. The technique can be used in fingerprint identification, recognition, and retrieval for future works. Also, it can be used in key generation mechanisms via deep learning.

Authors' Contribution: All authors contributed equally.

Funding Statement: This research article earned no external funding.

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

References

[1] Abdulrezzak, S., & Sabir, F. (2023). An empirical investigation on Snort NIDS versus supervised machine learning classifiers. *Journal of Engineering*, *29*(02), 164-178. https://doi.org/10.31026/j.eng.2023.02.11

[2] Abood, Z. I. (2017). Composite techniques based color image compression. *Journal of Engineering*, *23*(3), 80-93.

[3] Abundiz-Pérez, F., Cruz-Hernández, C., Murillo-Escobar, M. A., López-Gutiérrez, R. M., & Arellano-Delgado, A. (2016). A fingerprint image encryption scheme based on hyperchaotic Rössler map. *Mathematical Problems in Engineering*, *2016*(1), 2670494. https://doi.org/10.1155/2016/2670494

[4] Agrawal, R., Singh, B. K., & Sharma, L. (2021). Cryptography based internet security ATM system using fingerprint for securing PIN. *Journal of University of Shanghai for Science and Technology*, *23*(10), 369-380. http://doi.org/10.51201/JUSST/21/10717

[5] Al-Hassani, M. D. (2022). A novel technique for secure data cryptosystem based on chaotic key image generation. *Baghdad Science Journal*, *19*(4), 905-913.

[6] Al-Lehiebe, A.A. (2015). Ciphered text hiding in an image using RSA algorithm. *Journal of College of Education for Women*, *26*(3), 879-884.

[7] Alrifaee, Z. I. A., & Ismaeel, T. Z. (2022). Cryptography based on retina information. *Indonesian Journal of Electrical Engineering and Computer Science*, *28*(3), 1697-1708. https://doi.org/10.11591/ijeecs.v28.i3

[8] Alsharman, N., Saaidah, A., Almomani, O., Jawarneh, I., & Al-Qaisi, L. (2022). Pattern mathematical model for fingerprint security using bifurcation minutiae extraction and neural network feature selection. *Security and Communication Networks*, *2022*(1), 4375232. https://doi.org/10.1155/2022/4375232

[9] Bakheet, S., Alsubai, S., Alqahtani, A., & Binbusayyis, A. (2022). Robust fingerprint minutiae extraction and matching based on improved SIFT features. *Applied Sciences*, *12*(12), 6122. https://doi.org/10.3390/app12126122

[10] Barman, S., Chattopadhyay, S., & Samanta, D. (2014, December). Fingerprint based symmetric cryptography. In *2014 International Conference on High Performance Computing and Applications (ICHPCA)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICHPCA.2014.7045306

[11] Barman, S., Samanta, D., & Chattopadhyay, S. (2015). Fingerprint-based crypto-biometric system for network security. *EURASIP Journal on Information Security*, *2015*, 1-17. https://doi.org/10.1186/s13635-015-0020-1

[12] Barzut, S., Milosavljević, M., Adamović, S., Saračević, M., Maček, N., & Gnjatović, M. (2021). A novel fingerprint biometric cryptosystem based on convolutional neural networks. *Mathematics*, *9*(7), 730. https://doi.org/10.3390/math9070730

[13] Esttaifan, B. A. (2023). A modified Vigenère Cipher based on time and Biometrics features. *Journal of Engineering*, *29*(06), 128-139. https://doi.org/10.31026/j.eng.2023.06.10

[14] Ganchimeg, G., & Leopold, H. (2019). Fingerprint image enhancement using filtering techniques. *International Journal of Advanced Research*, *7*(5), 637-645. https://doi.org/10.21474/IJAR01/9084

[15] George, L. E., Hassan, E. K., Mohammed, S. G., & Mohammed, F. G. (2020). Selective image encryption based on DCT, hybrid shift coding and randomly generated secret key. *Iraqi Journal of Science*, 920-935. https://doi.org/10.24996/ijs.2020.61.4.25

[16] Hashem, M. I., Alibraheemi, K. (2022). Cryptographic key generation from fingerprint image based on minutiae neighborhood information. *International Journal of Mechanical Engineering*, *7*(1), 6517-6522.

[17] Herrera, J. A. Q., Limo, F. A. F., Tasayco-Jala, A. A., Vargas, I. M., Farias, W. B., Inga, Z. M. C., & Palacios, E. L. H. (2023). Security Issues in Internet Architecture and Protocols Based on Behavioural Biometric Block Chain-Enhanced Authentication Layer. *Journal of Internet Services and Information Security*, *13*(3), 122-142. https://doi.org/10.58346/JISIS.2023.I3.008

[18] Hummady, M. M., & Morad, A. H. (2022). Enhancement of System Security by Using LSB and RSA Algorithms. *Al-Khwarizmi Engineering Journal*, *18*(1), 26-37. https://doi.org/10.22153/kej.2022.03.001.

[19] Ibraheem, Z., Mohammed, S. A., Tawfiq, N. J., & Jassim, A. A. (2018). Performance study for mixed transforms generated by tensor product in image compression and processing. *Association of Arab Universities Journal of Engineering Sciences*, *25*(3), 155-168.

[20] Ibrahim, M. F. (2017). A Method to Encode the Fingerprint Minutiae Using QR Code. *Journal of the College of Basic Education*, *23*(99), 17-28. https://doi.org/10.35950/cbej.v23i99.6761

[21] Jassim, M. F., Hamzah, W. M. S., & Shimal, A. F. (2022). Biometric iris templates security based on secret image sharing and chaotic maps. *International Journal of Electrical and Computer Engineering (IJECE)*, *12*(1), 339-348. http://doi.org/10.11591/ijece.v12i1.pp339-348

[22] Jayapal, R., & Govindan, P. (2018). Biometric encryption system for increased security. *Systemics, Cybernetics and Informatics*, *16*(1), 75-80.

[23] Jazi, A. H., & Kuban Alibraheemi, K. H. (2018). Hiding Fingerprint Minutiae in Face Features. *Journal of College of Education for Pure Science*, *8*(3). https://doi.org/10.32792/utq.jceps.08.03.09

[24] Jerjees, S. A., & Ismaeel, T. Z. (2018). New data security method based on biometrics. *Journal of Engineering and Applied Sciences*, *13*(21), 9269-9276. http://dx.doi.org/10.3923/jeasci.2018.9269.9276

[25] Jerjees, S. A., Esttaifan, B. A., & Ismaeel, T. Z. (2020). Hybrid ciphering method based on chaos logistic map and fingerprint information. *Journal of Engineering Science and Technology*, *15*(5), 3013-3024.

[26] Jha, D. P., Kohli, R., & Gupta, A. (2016, February). Proposed encryption algorithm for data security using matrix properties. In *2016 International conference on innovation and challenges in cyber security (ICICCS-INBUSH)* (pp. 86-90). IEEE. https://doi.org/10.1109/ICICCS.2016.7542316

[27] Krishna, A., & Kareem, S. (2021). A survey on fingerprint authentication using various cryptographic techniques. *International Research Journal of Engineering and Technology (IRJET)*, *8*(4), 5109-5113. http://www.irjet.net

[28] Kumari, V., peerzade, M.U., Nayak, S., Bhagya, V., & Senbagavalli, M. (2021). Biometric auth-entication system using visual cryptography. *International Research Journal of Engineering and Technology (IRJET)*, *8*(2), 662-669.

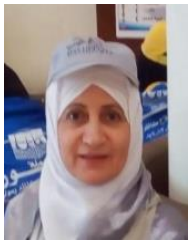
[29] Milind, B. B., Shivaprakasha, K. S., Meenakshi, R. P., & Lalita, S. A. (2024). Fingerprint Reconstruction: Approaches to Improve Fingerprint Images. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *15*(1), 75-87. http://doi.org/10.58346/JOWUA.2024.I1.006

[30] Moradi, M., Moradkhani, M., & Tavakoli, M. B. (2022). A Real-Time Biometric Encryption Scheme Based on Fuzzy Logic for IoT. *Journal of Sensors*, *2022*(1), 4336822. https://doi.org/10.1155/2022/4336822

[31] Ogla, R. A. A. S. (2017). A Hybrid Algorithm to Protect Computer Networks Based on Human Biometrics and Computer Attributes. *Ibn AL-Haitham Journal for Pure and Applied Science*, *29*(3), 209-221.

[32] Rabee, E. H., & Abdullah, M. N. (2020). Hybrid security framework based on biometrics features. *International Journal of Engineering Research & Technology (IJERT)*, *9*(8), 685-688, http://www.ijert.org
[33] Rashid, M., & Zaki, H. (2014). RSA Cryptographic key generation using fingerprint minutiae. *Iraqi Journal for Computers and Informatics*, *41*(1), 66-69.
[34] Salman, D. D., Azeez, R. A., & Hossen, A. M. J. (2020). Key generation from multibiometric system using meerkat algorithm. *Engineering and Technology Journal*, *38*(3B), 115-127. https://doi.org/10.30684/etj.v38i3B.652
[35] Sarkar, P., & Noel, S. (2020). Cipher: encryption & decryption. *International Research Journal of Engineering and Technology (IRJET)*, *7*(10), 731-737.
[36] Shini, A. H., Abood, Z. I., & Ismaeel, T. Z. (2016). Hybrid Techniques based Speech Recognition. *International Journal of Computer Applications*, *139*(10), 12-18.
[37] Suresh, K., Pal, R., & Balasundaram, S. R. (2023). A stable cryptographic key generation from fingerprint biometrics using Gray code for secure data storage. *International Journal of Information and Computer Security*, *20*(3-4), 366-398. https://doi.org/10.1504/IJICS.2023.128829
[38] Tyagi, H., & Dixit, S. (2018). Development of biometric cryptosystem using finger-print authentication. *International Journal of Electronics Engineering*, *10*(1), 350-358, http://www.cssjjourrnallss.com
[39] Yang, Y., Yu, J., Zhang, P., & Wang, S. (2015). A fingerprint encryption scheme based on irreversible function and secure authentication. *Computational and mathematical methods in medicine*, *2015*(1), 673867. http://dx.doi.org/10.1155/2015/673867
[40] Younis, M. I., Fadhil, H. M., & Jawad, Z. N. (2016). Acceleration of the RSA Processes based on Parallel Decomposition and Chinese Remainder Theorem. *International Journal of Application or Innovation in Engineering & Management*, *3*(1), 12-23. https://www.ijaiem.org
[41] Zabala-Blanco, D., Mora, M., Barrientos, R. J., Hernández-García, R., & Naranjo-Torres, J. (2020). Fingerprint classification through standard and weighted extreme learning machines. *applied sciences*, *10*(12), 4125. https://doi.org/10.3390/app10124125
[42] Zaki, H. A. (2015). Cryptographic key generation using fingerprint biometrics. *Journal Thi-Qar Science*, *5*(2), 74-79. https://www.researchgate.net/publication/321278086

Authors Biography



Zainab Ibrahim Abood Al-Rifaee, Assistant professor, received her B.Sc. and M.Sc. degree in Electrical Engineering from College of Engineering, University of Baghdad, Iraq. She has been a faculty member since 2009 and is currently an Assistant Professor at the Department of Electrical Engineering, University of Baghdad, Iraq. Her research interest includes digital signal and image processing, communication, electronics, information security, and research methodology.

Dr. Tarik Zeyad Ismaeel, Professor, has been a faculty member at a University of Baghdad, College of Engineering, Electrical Engineering Department since 1994. His research interest includes communication, information security, digital signal and image processing.

Dr. Samir Ibrahim Abood, Professor, received his B.S. and M.S. from the University of Technology, Baghdad, Iraq, in 1996 and 2001; respectively, he got his Ph.D. in the Electrical and Computer Engineering Department at Prairie View A & M University. From 1997 to 2001, he worked as an engineer at the University of Technology. From 2001 to 2003, he was a professor at the University of Baghdad and Al-Nahrain University. From 2003 to 2016, Mr. Abood was a professor at Middle Technical University / Baghdad-Iraq. From 2018 to the present, he has worked at Prairie View A & M University/ Electrical and Computer Engineering Department. He is the author of 30 papers and ten books. His main research interests are sustainable power and energy systems, microgrids, power electronics and motor drives, digital PID Controllers, digital methods for electrical measurements, digital signal processing, and control systems.