

## Cryptography based on retina information

Zainab Ibrahim Abood Alrifae, Tarik Zeyad Ismaeel

Department of Electrical Engineering, College of Engineering, University of Baghdad, Baghdad, Iraq

### Article Info

#### Article history:

Received Mar 20, 2022

Revised Aug 30, 2022

Accepted Sep 12, 2022

#### Keywords:

Cryptography

Diagonal center-end key

Diagonal-radius center-end key

Radius center-end key

Retina feature extraction

Retina information

### ABSTRACT

The security of message information has drawn more attention nowadays, so; cryptography has been used extensively. This research aims to generate secured cipher keys from retina information to increase the level of security. The proposed technique utilizes cryptography based on retina information. The main contribution is the original procedure used to generate three types of keys in one system from the retina vessel's end position and improve the technique of three systems, each with one key. The distances between the center of the diagonals of the retina image and the retina vessel's end (diagonal center-end (DCE)) represent the first key. The distances between the center of the radius of the retina and the retina vessel's end (radius center-end (RCE)) represent the second key. While the diagonal-radius center and the retina vessel's end (diagonal-radius center-end (DRCE)) represent the third key. The results illustrate the process's validity and applicability. Also, improve the time required to decrypt the cipher-text by a brute force attack (BFA) from  $(4.358e+139)$  year in the compared technique to  $(1.3074e+140)$  year for retina3. The BFA time will increase with increasing the number of retina vessels, as in retina1, 2, and 3, which have 24, 53, and 103 retina vessels.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



### Corresponding Author:

Zainab Ibrahim Abood

Department of Electrical Engineering, College of Engineering, University of Baghdad  
Baghdad, Iraq

Email: zainab.ibrahim@coeng.uobaghdad.edu.iq

## 1. INTRODUCTION

Cryptography is the study and practice of mathematical techniques for secure information and related aspects of the data and information security [1], [2]. A secure system should preserve the privacy of data, integrity, and availability [3]. Availability is the capability to access the resources or network data whenever necessary [4]. Data integrity is the resistance to penetration and protection from undetected and unauthorized modification [5]. One way to bolster security in any computer system is to encrypt messages and sensitive records in transmission and storage. The plain-text is the unenciphered text, and enciphering (encryption) is the conversion from a plain-text message to a cipher-text form in which a message can be read-only by the intended receiver [6]. Deciphering (decryption) is the decoding from cipher-text form to plain-text message [5]. Cryptographic algorithms used for encryption and decryption operations [7].

Zainatul *et al.* [8] used a lightweight and secure communication proxy to solve the security problem of the Internet of things (IoT) traffic. (IoT) devices have increased the quantity of information generated in various formats [9]. Omoruyi *et al.* [10] evaluated the ciphering image quality of the Hill-Cipher algorithm. This study has applied three metrics; maximum deviation, entropy of the ciphered image, and color histogram. Mustafa *et al.* [11] presented generating a quick response (QR) code relying on the input message and extracting the features used to generate the key. The features are extracted from QR codes using convolution. Jasmir *et al.* [12] classified the texts of cancer clinical trial documents consisting of unstructured

free texts taken from cancer clinical trial protocols. Numerous human life and skin applications are reviewed in [13], such as classification, detection, blocking, cryptography, localization, identification steganography, tracking, segmentation, and recognition. A review of the image compression technique and formats that use to decrease redundant information in the images, non-visual redundancy, and unnecessary pixels are presented in [14].

Mistry [15] proposed a method for authentication of a medical image using a hybrid algorithm and encryption of a retinal fundus image. Integrity, authentication, and tamper localization at various levels of discrete wavelet transform high-low sub-bands are provided by digital watermarking. Seam *et al.* [2] introduced a method called seam's random number generator. The generated sequences perform the XOR digital operation with a grayscale image to get the encrypted text. Taha *et al.* [16] used hybrid technology consisting of the characteristics of the human retina and functions to generate the keys of high-quality capricious, non-recovery, and unforeseeable. The correlation tests and National Institute of Standards and Technology (NIST) package proved that the keys are random, uncorrelated, and sturdy against different attacks. Tajuddin and Nandini [17] used a robust and large size key that is directly generated from the information of retinal blood vessels and results in delay through encryption/decryption; this creates more complexity for attackers to guess or crack the cryptographic key. George *et al.* [18] proposed a selective image encryption method that encrypts predetermined groups of the input image data to reduce the computational complexity and cryptographic time. Liang *et al.* [19] improved the efficiency by applying permutation with hyperchaotic sequences when using the image encryption method with a public key. At the same time, the elliptic curve cryptography encrypts the hash value. Ma *et al.* [20] introduced unsupervised learning and supervised learning algorithms used as a segmentation algorithm for the retinal blood vessel. Tajuddin and Nandini [21] introduced three retina features; endpoints, islands, and bifurcation points used to generate the secured key to enhancing network security. The problem is how to increase the BFA time to prevent attackers from breaking the encryption.

This paper uses a new technique for encryption/decryption based on retina information. The aim is to generate secured cipher keys from retina information to improve the level of security. The main contribution is the original procedure used to generate three types of keys in one system from the retina vessel's end position and improve the technique of three systems, each with one key. The first is the DCE key, the second is the RCE key, and the third is the DRCE key. As a result, the BFA time is very high and is out of a person's life. Then we compared the BFA time with another technique we have designed for comparing only; called the compared technique, which has three systems, each with an individual key, one with a DCE key, the second with an RCE key, and the third system with a DRCE key. This paper's organization is as follows: section 2 presents an overview and a sequence of explanations of the proposed research method; section 3 describes the testing and evaluation of the implemented results. Finally, section 4 presents the outlines of the conclusion of this paper.

## 2. RESEARCH METHOD

### 2.1. Overview

Cipher algorithms are the rules or instructions for the encryption process. The proposed technique uses retina vessels of three different retina images and MATLAB R2019a. One of the retina images contains 24 retina vessels, the second retina image contains 53 retina vessels, while; the third one has 103 retina vessels. (retina3 taken as a model). Figure 1 shows the three different retina images used for feature extraction. Several preprocessing steps are applied to the retina image before feature extraction is applied to obtain the enhanced gray image output and an original procedure used for retina feature extraction to generate the keys. Figure 2 shows the block diagram of the proposed method.

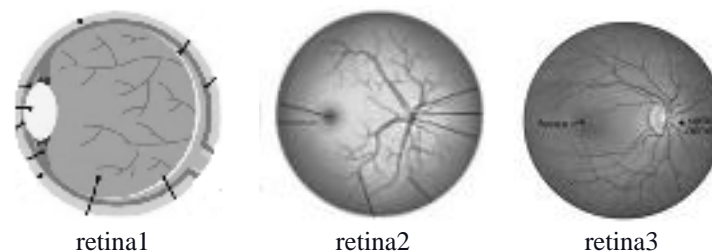


Figure 1. Three different retina images

**2.2. Preprocessing**

In biometrics, the face, retina, and fingerprints are not the same in another person. Therefore, they can be used to generate random keys in cryptographic applications [22]. The original retina color image of any format or size is read as a matrix, and then it is converted to a grayscale form, generally from 0 (black) to 255 (white). After that, the gray image is resized to 256×256 pixels. Figure 3 shows the preprocessed image, where the original color image, grayscale image, and resized image are illustrated in Figure 3(a), Figure 3(b) and Figure 3(c), respectively.

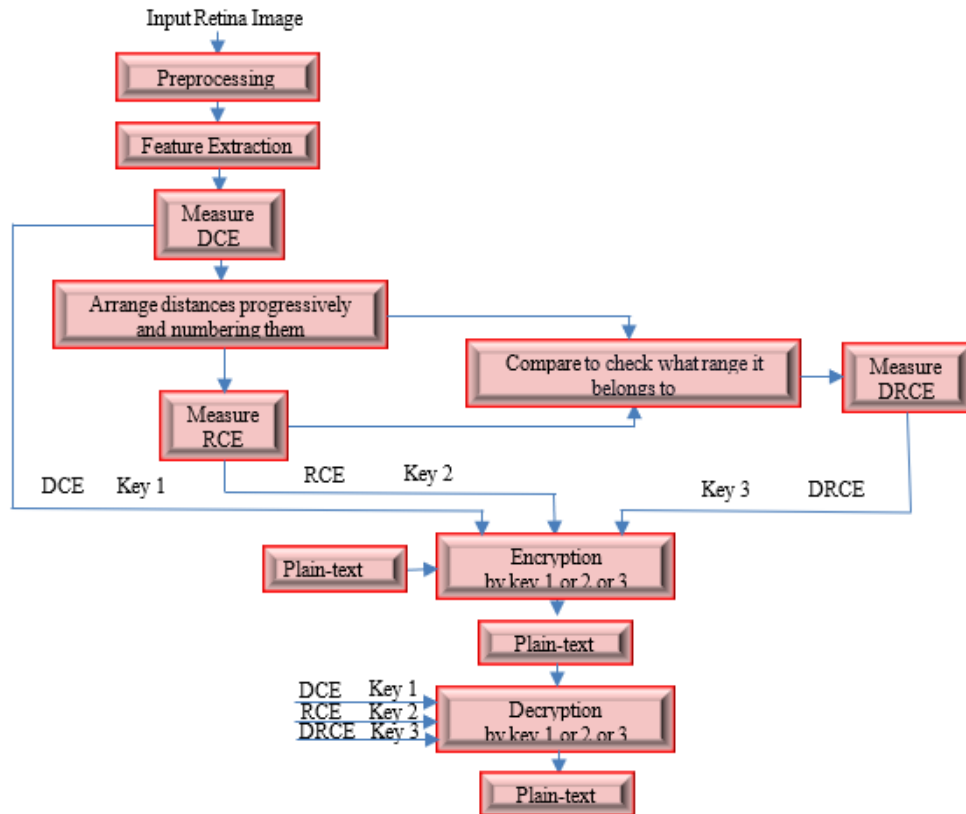


Figure 2. Block diagram of the proposed method

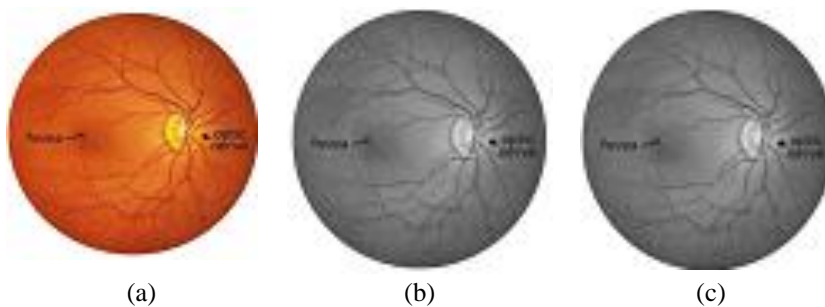


Figure 3. Preprocessed image where (a) original color image (b) grayscale image and (c) resized image

**2.3. Feature extraction**

Feature extraction is an important stage in image processing, computer vision, data mining and image retrieval [23]. The retina is one of the wellsprings of biometric systems which [24] has inherent robustness [22] and give an efficient and reliable method for authentication [24], [25]. The feature extraction of the retina vessels is computing feature vectors to get a compact representation of the original retina [12], [26], [27]. In a retina feature extraction, the retina center's coordinates are calculated by drawing the

diagonals of the retina image; the intersection point of the diagonals is the center of the retina image, which is also the center of the retina. Then the distance between the retina's center and the vessel's end is drawn and measured using Euclidean distance. These distances are the DCE used to encrypt the message as a DCE key. After that, the measured distances are arranged progressively and numbered, starting from one and ahead.

The next step is that; from the center of the retina towards the right-hand side, a horizontal radius of the retina is drawn; then, beginning counterclockwise, measuring the distance between the center of the radius and the retina vessel's end. These distances are used to encrypt the message as an RCE key. Comparing each distance with all distance's lengths in the previous step to check what range it belongs to, then; record its number. This number refers to the number of shifts used to encrypt the message as a DRCE key. Figure 4 shows the feature extraction of the proposed technique. The image with diagonals has been illustrated in Figure 4(a) and the image with diagonals and radius has been illustrated in Figure 4(b). For the values of DCE, RCE, and DRCE, the rounding to the nearest integer number (if not integer) is used using  $\text{round}(x)$  in MATLAB 2019a. Table 1 shows samples of extracted features from retina3, where the (X, Y) are the ending points of the retina vessels.

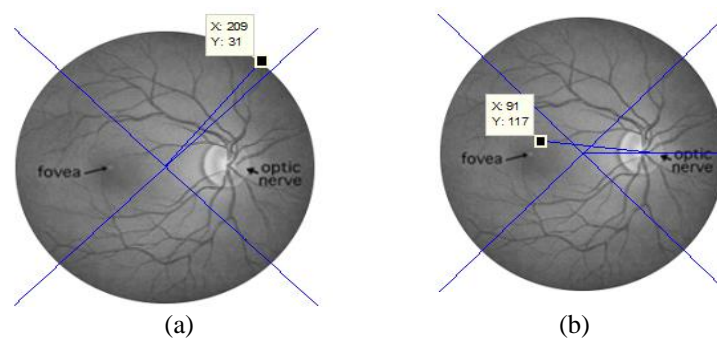


Figure 4. Feature extraction of the proposed system image with (a) diagonals and (b) diagonals and radius

Table 1. samples of extracted features from Retina3

Retina vessel's number	DCE value	RCE value	DRCE value	(X, Y) points
1	26	89	30	(109, 146)
2	34	85	28	(118, 160)
3	35	83	27	(117, 161)
4	35	69	20	(119, 162)
5	36	72	20	(105, 100)
6	39	66	19	(91, 117)
7	40	48	10	(126, 88)
8	41	37	5	(120, 88)
9	47	62	18	(112, 172)
10	47	60	18	(100, 166)
11	49	55	15	(107, 84)
12	49	55	15	(79, 132)

#### 2.4. Cryptography Algorithms

Cryptographic algorithms are: i) symmetric encryption: used to hide the contents of streams or blocks of data of whatever size, including messages, encryption keys, files, and passwords; ii) asymmetric encryption: used to hide small data blocks, such as hash function values and encryption keys, used in the digital signatures [28]; iii) data integrity algorithms: used to protect the blocks of data, like messages, from alteration [28], [29] and iv) authentication protocols: these schemes depend on cryptographic algorithms to authenticate the entities' identity [28].

There are many key-based cryptographic schemes; symmetric keys and asymmetric keys are the two-standard key-based encryption techniques [3]. Symmetric key cryptography uses the same key for encryption and decryption, while; Asymmetric key cryptography uses two different keys, one for encryption and the other for decryption [7]. Equations (1) and (2) express the algorithms of the encryption and decryption, respectively:

$$e(x) \equiv (x + k) \bmod n \quad (1)$$

$$d(y) \equiv (y - k) \text{ mod } n \tag{2}$$

where x and y are the plain-text and cipher-text character’s numbers, k and n are a shift key and modulus, respectively [28]. When the systems use encryption, cipher-text should be challenging to decipher the text without knowing the key to increasing the confidence of systems’ integrity [3].

**2.4.1. Lookup table**

In the encryption approach, a lookup table is to map one math symbol or letter with the other one according to the operation used in converting between them. The construction of a lookup table is from (26) English small and (26) capital letters, (71) math symbols, and space. All of these are numbered from one to 124. Table 2 shows the suggested Lookup table used in the encryption and decryption in this research. The abbreviations (ch.) mean “character” and (ch. no.) mean “character number”.

Table 2. Lookup table

Ch.	Ch. no.	Ch.	Ch. no.	Ch.	Ch. no.	Ch.	Ch. no.	Ch.	Ch. no.	Ch.	Ch. no.	Ch.	Ch. no.	Ch.	Ch. no.	Ch.	Ch. no.
A	1	P	16	e	31	t	46	>	61	°	76	+	91	↔	106	∛	121
B	2	Q	17	f	32	u	47	<<	62	°F	77	–	92	∴	107	∜	122
C	3	R	18	g	33	v	48	>>	63	°C	78	φ	93	¬	108	∓	123
D	4	S	19	h	34	w	49	≤	64	Δ	79	α	94	:	109	…	124
E	5	T	20	i	35	x	50	≥	65	∇	80	β	95	∴	110		
F	6	U	21	j	36	y	51	≠	66	∃	81	γ	96	∴	111		
G	7	V	22	k	37	z	52	≅	67	τ	82	δ	97	⊗	112		
H	8	W	23	l	38	space	53	≈	68	∈	83	ε	98	⊃	113		
I	9	X	24	m	39	=	54	≡	69	∋	84	ε	99	■	114		
J	10	Y	25	n	40	≠	55	√	70	±	85	θ	100	ρ	115		
K	11	Z	26	o	41	×	56	∂	71	√	86	ϑ	101	σ	116		
L	12	a	27	p	42	÷	57	∩	72	~	87	μ	102	ω	117		
M	13	b	28	q	43	!	58	∩	73	∞	88	π	103	∫	118		
N	14	c	29	r	44	∞	59	∅	74	·	89	→	104	↑	119		
O	15	d	30	s	45	<	60	%	75	*	90	↓	105	←	120		

**2.4.2. Encryption algorithm**

Encryption is the method of encoding plain-text into cipher-text before transmitting it through channel for avoiding thieving of confidential data [16]. Encryption has been implemented through shifting operation to the right (forward) using the corresponding key. This key is represented by the retina vessel’s end position and from (1):

Encryption at DCE points:

$$e_{kD}(x) \equiv (x+k_D) \text{ mod } 124$$

Encryption at RCE points:

$$e_{kR}(x) \equiv (x+k_R) \text{ mod } 124$$

Encryption at DRCE points:

$$e_{kDR}(x) \equiv (x+k_{DR}) \text{ mod } 124$$

where  $x \in Z_{124}$  and it is the plain-text character number.  
 $k_D$ =position of DCE point+value of DCE at the same point  
 $k_R$ =position of RCE point+value of RCE at the same point  
 $k_{DR}$ =position of DRCE point+value of DRCE at the same point

**2.4.3. Decryption algorithm**

Decryption is converting the cipher-text to the original plain-text using a secret key. It has been implemented through shifting operation to the left (Backward) using a key that is represented by the retina vessel's end position and from (2):

Decryption at DCE points:

$$d_{kD}(y) \equiv (y - k_D) \pmod{124}$$

Decryption at RCE points:

$$d_{kR}(y) \equiv (y - k_R) \pmod{124}$$

Decryption at DRCE points:

$$d_{kDR}(y) \equiv (y - k_{DR}) \pmod{124}$$

where  $y \in Z_{124}$ , and it is the cipher-text character number

### 3. TESTING AND EVALUATING THE RESULTS

For testing and evaluating the performance of the proposed technique, ten tables show the details of the results when using various keys of retina vessels for retina 1, 2, and 3. Table 3 shows the encryption process using DCE key with a plain-text (Simulation) and resulting cipher-text for retina3. According to the lookup table, the plain text letter S mapping into the character number of the value 19. The DCE has the value of 64 at that number after arranging the measured distances progressively and numbering them; i.e., the distance between the retina's center and the vessel's end of a coordinate (88, 78). Therefore, the plain - text; (Simulation) is encrypted to a cipher-text ( $A \div \equiv < G : m > NU$ ) depending on shifting to the right. Tables 4 and 5 show the encryption of the plain-text; (Simulation) but using RCE and DRCE. The encrypted texts are ( $\alpha ! \nabla \text{Mod} \cdot \cdot \text{h}\omega$ ) and ( $L \leftarrow \nabla x l E i \gamma > \ll$ ) respectively. The encryption by using DCE, RCE, and DRCE results in different cipher-text when using the same plain-text.

Table 3. Encryption using DCE key with a plain-text (simulation)

Plain-text	Character no.(C)	DCE value	DCE (X, Y)	$(C + DCE + (X + Y)) \pmod{124}$	Cipher-text
S	19	64	(88, 78)	$249 \pmod{124} = 1$	A
i	35	97	(32, 141)	$305 \pmod{124} = 57$	÷
m	39	104	(26, 148)	$317 \pmod{124} = 69$	≡
u	47	107	(222, 180)	$556 \pmod{124} = 60$	<
l	38	101	(191, 49)	$379 \pmod{124} = 7$	G
a	27	81	(67, 182)	$357 \pmod{124} = 109$	:
t	46	107	(22, 112)	$287 \pmod{124} = 39$	m
i	35	125	(145, 252)	$557 \pmod{124} = 61$	>
o	41	104	(133, 232)	$510 \pmod{124} = 14$	N
n	40	105	(198, 50)	$393 \pmod{124} = 21$	U

Table 4. Encryption using RCE key with a plain-text (simulation)

Plain-text	Character no.(C)	RCE value	RCE (X, Y)	$(C + RCE + (X + Y)) \pmod{124}$	Cipher-text
S	19	122	(88, 78)	$307 \pmod{124} = 59$	$\alpha$
i	35	98	(32, 141)	$306 \pmod{124} = 58$	!
m	39	115	(26, 148)	$328 \pmod{124} = 80$	$\nabla$
u	47	184	(222, 180)	$633 \pmod{124} = 13$	M
l	38	135	(191, 49)	$413 \pmod{124} = 41$	o
a	27	126	(67, 182)	$402 \pmod{124} = 30$	d
t	46	179	(22, 112)	$359 \pmod{124} = 111$	$\cdot \cdot$
i	35	98	(145, 252)	$530 \pmod{124} = 34$	h
o	41	82	(133, 232)	$488 \pmod{124} = 116$	$\sigma$
n	40	77	(198, 50)	$365 \pmod{124} = 117$	$\omega$

Suppose the plain-text is a sentence such as (What a nice car!). Tables 6, 7, and 8 show the encryption of the same message for different keys of retina vessels; DCE, RCE, and DRCE leading to a different cipher-text for each key. In the encryption using the DCE key, the three times repetition of the (space) in the plain-text have the same character number (53) according to the lookup table and its encryption to  $\gg$ ,  $\cdot \cdot$ , and  $\in$  in the first, second, and third case, respectively. Encryption to three different values is because of the variation in values and (X, Y) points of the DCE at these spaces. Also, the repetition of the letters a

and c in the plain-text; are three times and two times, respectively. Encrypted to different values in DCE, RCE, and DRCE; this will increase the proposed technique's ambiguity.

Table 5. Encryption using DRCE key with a plain-text (simulation)

Plain-text	Character no.(C)	DRCEvalue	DRCE (X, Y)	(C+DRCE+(X+Y)) mod124	Cipher-text
S	19	75	(88, 78)	260 mod 124=12	L
i	35	36	(32, 141)	244 mod 124=120	←
m	39	57	(26, 148)	270 mod 124=22	V
u	47	103	(222, 180)	552 mod 124=56	×
l	38	103	(191, 49)	381 mod 124=9	I
a	27	101	(67, 182)	377 mod 124=5	E
t	46	103	(22, 112)	283 mod 124=35	i
i	35	36	(145, 252)	468 mod 124=96	γ
o	41	27	(133, 232)	433 mod 124=61	>
n	40	22	(198, 50)	310 mod 124=62	<<

Table 6. Encryption using DCE key with a plain-text (what a nice car!)

Plain-text	Character no. (C)	DCE value	DCE (X, Y)	(C+ DCE+(X+Y)) mod124	Cipher-text
W	23	77	(100, 200)	400 mod 124=28	b
h	34	95	(78, 209)	416 mod 124=44	r
a	27	81	(67, 182)	357 mod 124=109	:
t	46	107	(22, 112)	287 mod 124=39	m
	53	109	(130, 19)	311 mod 124=63	>>
a	27	83	(72, 67)	249 mod 124=1	A
	53	124	(223, 207)	607 mod 124=111	·
n	40	105	(198, 50)	393 mod 124=21	U
i	35	97	(32, 141)	305 mod 124=57	÷
c	29	86	(44, 146)	305 mod 124=57	÷
e	31	93	(60, 192)	376 mod 124=4	D
	53	104	(26, 148)	331 mod 124=83	€
c	29	86	(101, 210)	426 mod 124=54	=
a	27	111	(216, 196)	550 mod 124=54	=
r	44	106	(155, 25)	330 mod 124=82	τ
!	58	116	(52, 215)	441 mod 124=69	≡

Table 9 shows encryption of a plain-text (Simulation), using DCE, RCE, and DRCE for retina1, 2, and 3. The suffix 1 in DCE<sub>1</sub> refers to retina1, the suffix 2 in DCE<sub>2</sub> refers to retina2, the suffix 3 in DCE<sub>3</sub> refers to retina3, and the same for RCE and DRCE. For each retina, different keys used to encrypt the same message and cipher-text are different for each key because each retina has different values and lengths of DCE, RCE, and DRCE from the other retina. Table 10 shows the encryption using DRCE for retina1, 2, and 3 with a plain-text (What a nice car!). Each retina has a different DRCE key, so when encrypting the same message, the cipher-text obtained differs from one retina to another.

Table 7. Encryption using RCE key with a plain-text (what a nice car!)

Plain-text	Character no. (C)	RCE value	RCE (X, Y)	(C+RCE+(X+ Y)) mod124	Cipher-text
W	23	79	(100, 200)	402 mod 124=30	d
h	34	102	(78, 209)	423 mod 124=51	y
a	27	126	(67, 182)	402 mod 124=30	d
t	46	179	(22, 112)	359 mod 124=111	·
	53	113	(130, 19)	315 mod 124=67	≅
a	27	133	(72, 67)	299 mod 124=51	y
	53	115	(223, 207)	598 mod 124=102	μ
n	40	77	(198, 50)	365 mod 124=117	ω
i	35	98	(32, 141)	306 mod 124=58	!
c	29	125	(44, 146)	344 mod 124=96	γ
e	31	95	(60, 192)	378 mod 124=6	F
	53	115	(26, 148)	342 mod 124=94	α
c	29	145	(101, 210)	485 mod 124=113	⊔
a	27	132	(216, 196)	571 mod 124=75	%
r	44	91	(155, 25)	315 mod 124=67	≅
!	58	143	(52, 215)	468 mod 124=96	γ

The cipher-text is converted to the original plain-text efficiently using the proposed decryption process, which illustrates the validity and applicability of the process. Table 11 shows decryption results using DRCE for retina3 to reconstruct the original message (what a nice car!).

Table 8. Encryption using DRCE key with a plain-text (what a nice car!)

Plain-text	Character no. (C)	DRCE value	DRCE (X, Y)	$(C+DRCE+(X+Y)) \text{ mod } 124$	Cipher-text
W	23	24	(100, 200)	$347 \text{ mod } 124=99$	ε
h	34	38	(78, 209)	$359 \text{ mod } 124=111$	∴
a	27	101	(67, 182)	$377 \text{ mod } 124=5$	E
t	46	103	(22, 112)	$283 \text{ mod } 124=35$	i
a	53	57	(130, 19)	$259 \text{ mod } 124=11$	K
	27	102	(72, 67)	$268 \text{ mod } 124=20$	T
n	53	57	(223, 207)	$540 \text{ mod } 124=44$	r
	40	22	(198, 50)	$310 \text{ mod } 124=62$	<<
i	35	36	(32, 141)	$244 \text{ mod } 124=120$	←
c	29	97	(44, 146)	$316 \text{ mod } 124=68$	≈
	31	34	(60, 192)	$317 \text{ mod } 124=69$	≡
e	53	57	(26, 148)	$284 \text{ mod } 124=36$	j
	29	103	(101, 210)	$443 \text{ mod } 124=71$	∂
a	27	102	(216, 196)	$541 \text{ mod } 124=45$	s
r	44	30	(155, 25)	$254 \text{ mod } 124=6$	F
!	58	103	(52, 215)	$428 \text{ mod } 124=56$	×

Table 9. Encryption using DCE, RCE and DRCE for retina1, 2, and 3 with a plain-text (simulation)

Plain-text	Cipher-text DCE <sub>1</sub>	Cipher-text RCE <sub>1</sub>	Cipher-text DRCE <sub>1</sub>	Cipher-text DCE <sub>2</sub>	Cipher-text RCE <sub>2</sub>	Cipher-text DRCE <sub>2</sub>	Cipher-text DCE <sub>3</sub>	Cipher-text RCE <sub>3</sub>	Cipher-text DRCE <sub>3</sub>
S	∂	n	<<	C	n	ε	A	α	L
i	S	μ	ε	p	≠	κ	÷	!	←
m	e	∩	∴	Z	L	∅	≡	∇	V
u	d	≤	°C	C	b	α	<	M	×
l	±	°	Y	W	A	≡	G	o	I
a	γ	∩	°	G	·	ε	:	d	E
t	÷	%	¬	≅	¬	H	m	∴	i
i	U	M	↔	≠	∓	ρ	>	h	γ
o	π	∂	q	J	D	τ	N	σ	>
n	≡	β	Q	τ	θ	d	U	ω	<<

Table 10. Encryption using DRCE for retina1, 2, and 3 with a plain-text (what a nice car!)

Plain-text	DRCE/Retina	Cipher-text
What a nice car!	DRCE <sub>1</sub>	$= \downarrow \circ \neg \text{CNyQ} \in \text{e}\mu\text{jbrBE}$
What a nice car!	DRCE <sub>2</sub>	$\cap \varphi\sqrt{H} \omega \sim \varphi d\kappa \uparrow < K : \text{°FWW}$
What a nice car!	DRCE <sub>3</sub>	$\epsilon \cdot \cdot \text{E i K T r} \ll \leftarrow \approx \equiv \text{j } \partial \text{sF } \times$

Table 11. Decryption using DRCE for retina3 with a plain-text (what a nice car!)

Cipher-text	Ciphered letter's no.	DRCE value	DRCE (X, Y)	$(\text{Ciphered letter's no.} - (\text{DRCE} + (X+Y)) \text{ mod } 124)$	Plain-text
ε	99	24	(100, 200)	$-225 \text{ mod } 124=23$	W
∴	111	38	(78, 209)	$-214 \text{ mod } 124=34$	h
E	5	101	(67, 182)	$-345 \text{ mod } 124=27$	a
i	35	103	(22, 112)	$-202 \text{ mod } 124=46$	t
K	11	57	(130, 19)	$-195 \text{ mod } 124=53$	a
T	20	102	(72, 67)	$-221 \text{ mod } 124=27$	
r	44	57	(223, 207)	$-443 \text{ mod } 124=53$	n
<<	62	22	(198, 50)	$-208 \text{ mod } 124=40$	
←	120	36	(32, 141)	$-89 \text{ mod } 124=35$	i
≈	68	97	(44, 146)	$-219 \text{ mod } 124=29$	c
≡	69	34	(60, 192)	$-217 \text{ mod } 124=31$	e
j	36	57	(26, 148)	$-195 \text{ mod } 124=53$	c
∂	71	103	(101, 210)	$-343 \text{ mod } 124=29$	
s	45	102	(216, 196)	$-469 \text{ mod } 124=27$	a
F	6	30	(155, 25)	$-204 \text{ mod } 124=44$	r
×	56	103	(52, 215)	$-314 \text{ mod } 124=58$	!



A valuable classification of security attacks is active attacks that attempt to affect system resources or alter their operation and passive attacks which attempt to learn or use the system's information without affecting system resources [2]. There are many kinds of code-breaking attacks. One of them is a cipher-text attack when an opponent has only the cipher-text. The known plain-text problem happens when the opponent has some matched parts of the plain-text and the cipher-text. The most significant risk is the chosen plain-text problem, in which the attackers [30] can encrypt parts of plain-text. Brute-force is the eventual attack on the cipher, testing all the possible keys until the right one is encountered [3] uses trial and error algorithm [31]. Various ways were researched and developed for limiting or mitigating brute-force attacks [32]–[36]. Brute force technique used in various fields of authentication schemes such as mail servers and web servers [37]. A timing attack is the only one in which the information about the plain-text or the key is obtained by watching how long it takes for the implementation to run out of decryption on different cipher-texts. A timing attack [28], [38] utilizes encryption and decryption algorithms and sometimes takes various amounts of time for different inputs [28]. A compared technique; another technique we have designed for comparing only and it has three systems. Each system with an individual key, one with a DCE key, the second with an RCE key while the third system with a DRCE key. Figure 5 shows a compared technique with a DCE key, RCE key, and DRCE key. Figures 5(a)-(c) shows the compared technique with a DCE key, RCE key, and DRCE key respectively.

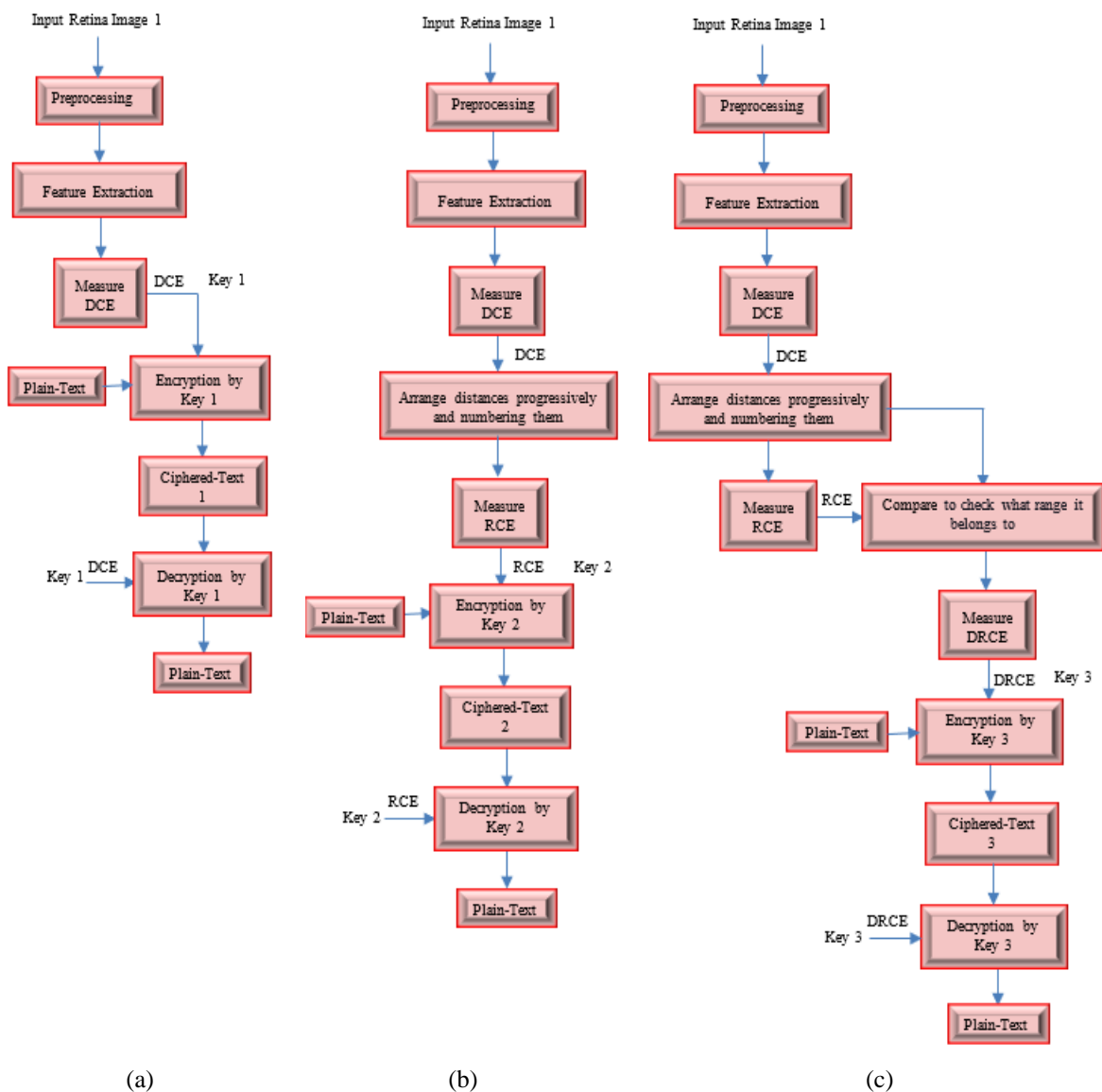


Figure 5. A compared technique with (a) DCE key, (b) RCE key, and (c) DRCE key

The BFA time to discover the key found by (3):

$$\text{BFA}_{\text{time}} = \left( \frac{3 \times (\text{Number of retina vessels})!}{2^{56}} \right) \text{sec.} \quad (3)$$

where 3 refers to DCE, RCE and DRCE and  $2^{56}$  is the number of deciphering operations per second. No. of seconds in one year =  $365 \times 24 \times 60 \times 60 = 31536000$  sec.

$$\text{BFA}_{\text{time}} = \left( \frac{3^{(103)!}}{2^{56}} \right) / 31536000 \text{ year}$$

$$\text{BFA}_{\text{time}} = 1.3074\text{e}+140 \text{ year}$$

Table 12 shows a comparison between the proposed technique and compared technique for retina1, 2, and 3 according to the number of retina vessels and BFA time. A BFA uses trial and error algorithms to decode the encrypted data, so; the choice of the BFA represents a suitable type of attack. retina3 has the most considerable BFA time to find the key than retina1 and retina2 because they have the lowest number of retina vessels compared with retina3. Also, the comparison between the BFA time of retina1, 2, and 3 in the proposed technique is three times that in the compared technique because the last one has three systems, each with one key. The suffix prop. in Variables<sub>prop.</sub> refers to variables in the proposed technique and the suffix comp. in Variables<sub>comp.</sub> refers to the variables in compared technique.

Table 12. No. of retina vessels and BFA for retina 1, 2, and 3

Variables <sub>prop.</sub>	Retina1	Retina2	Retina3	Variables <sub>comp.</sub>	Retina1	Retina2	Retina3
No. of retina vessels	24	53	103	No. of retina vessels	24	53	103
BFA <sub>time</sub> /Year	0.8191	5.6436e+45	1.307e+140	BFA <sub>time</sub> /Year	0.2730	1.8812e+45	4.358e+139

#### 4. CONCLUSION

This research aims to generate secured cipher keys from retina information to increase the level of security. Original procedure used to generate three types of keys in one system from the retina vessel's end position. The results show that for different keys of retina vessels such as DCE, RCE and DRCE used to encrypt the same message, word, or text, the cipher-text differs for each key and each retina, i.e., the same plain-text encrypted to a different cipher-text. A decryption process efficiently converts the cipher-text to the original plain-text, illustrating the process's validity and applicability, and the secret keys are robust against various attacks. The cipher-text is challenging to be broken because the time required to decrypt the cipher-text by a BFA is very high, almost (1.3074e+140) year for retina 3, which has 103 retina vessels. When the number of retina vessels decreases, the BFA time will also be decreased as in retina1 and retina2 because they have 24 and 53 retina vessels, respectively; the BFA time increases with increasing the length of the secret key, which is preferable in the cryptography. Also, the BFA time of retina 1, 2, and 3 in the proposed technique is three times that in the compared technique, which has BFA time (4.358e+139) year for retina3, because the last one has three systems each with one key. It is now possible to conclude that the proposed technique is highly secure and efficient for cryptography. For the future works, using the process of image encryption with the proposed system and design a technique of generating secured keys from the fingerprint with image or text encryption.

#### REFERENCES





- [1] P. K. Das, P. Kumar, and M. Sreenivasulu, "Image cryptography: a survey towards its growth," *Advance in Electronic and Electric Engineering*, vol. 4, no. 2, pp. 179–184, 2014.
- [2] M. S. I. Seam, M. M. Islam, M. B. A. Miah, B. K. Paul, M. S. Uddin, and K. Ahmed, "Proposal of a new method for image encryption and decryption technique," in *2019 IEEE International Conference on Signal Processing, Information, Communication & Systems (SPICSCON)*, Nov. 2019, pp. 126–129. doi: 10.1109/SPICSCON48833.2019.9065013.
- [3] Z. P. Buba and G. M. Wajiga, "Cryptographic algorithms for secure data communication," *International Journal of Computer Science and Security*, vol. 5, no. 2, pp. 227–243, 2011.
- [4] J. Polpong and P. Wuttidittachotti, "Authentication and password storing improvement using SXR algorithm with a hash function," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, pp. 6582–6591, Dec. 2020, doi: 10.11591/ijece.v10i6.pp6582-6591.
- [5] Z. K. Obaid and N. F. H. Al Saffar, "Image encryption based on elliptic curve cryptosystem," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 2, pp. 1293–1302, Apr. 2021, doi: 10.11591/ijece.v11i2.pp1293-1302.
- [6] A. M. M., "Implementation of full-parallelism AES encryption and decryption," *International Journal of Electronics and Communication Engineering*, vol. 1, no. 8, pp. 1–5, Oct. 2014, doi: 10.14445/23488549/IJECE-V11I8P103.

- [7] M. A. Almaiah, Z. Dawahdeh, O. Almomani, A. Alsaaidah, A. Al-Khasawneh, and S. Khawatreh, "A new hybrid text encryption approach over mobile ad hoc network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, pp. 6461–6471, Dec. 2020, doi: 10.11591/ijece.v10i6.pp6461-6471.
- [8] Z. Y. M. Yusoff, M. K. Ishak, and L. A. Rahim, "A java servlet based transaction broker for internet of things edge device communications," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 11, no. 1, pp. 488–497, Feb. 2022, doi: 10.11591/eei.v11i1.3455.
- [9] A. H. Ali, M. N. Abbod, M. K. Khaleel, M. A. Mohammed, and T. Sutikno, "Large scale data analysis using MLlib," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 19, no. 5, pp. 1735–1746, Oct. 2021, doi: 10.12928/telkomnika.v19i5.21059.
- [10] O. Omoruyi, C. Okereke, K. Okokpujie, E. Noma-Osaghae, O. Okoyeigbo, and S. John, "Evaluation of the quality of an image encryption scheme," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 6, pp. 2968–2974, Dec. 2019, doi: 10.12928/telkomnika.v17i6.10488.
- [11] R. A. Mustafa, A. A. Maryoosh, D. N. George, and W. R. Humood, "Iris images encryption based on QR code and chaotic map," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 1, pp. 289–300, Feb. 2020, doi: 10.12928/telkomnika.v18i1.13293.
- [12] J. Jasmir, S. Nurmaini, R. F. Malik, and B. Tutuko, "Bigram feature extraction and conditional random fields model to improve text classification clinical trial document," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 19, no. 3, pp. 886–892, Jun. 2021, doi: 10.12928/telkomnika.v19i3.18357.
- [13] H. A. H. Al Naffakh, R. Ghazali, N. K. El Abbadi, and A. N. Razzaq, "A review of human skin detection applications based on image processing," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 10, no. 1, pp. 129–137, Feb. 2021, doi: 10.11591/eei.v10i1.2497.
- [14] A. J. Qasim, R. Din, and F. Q. A. Alyousuf, "Review on techniques and file formats of image compression," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 9, no. 2, pp. 602–610, Apr. 2020, doi: 10.11591/eei.v9i2.2085.
- [15] S. K. Mistry and Z. Mizwan, "Encryption of retinal fundus image using digital watermarking," *International Journal of Scientific Progress & Research (IJSPR)*, vol. 49, no. 149, pp. 115–118, 2018.
- [16] M. A. Tah, N. M. Sahib, and T. M. Hasan, "Cryptographic key generation using retina biometric parameter," *International Journal of Computer Science and Mobile Computing*, vol. 8, no. 9, pp. 172 – 181, 2019.
- [17] M. Tajuddin and C. Nandini, "Cryptographic key generation using retina biometric parameter," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 3, no. 1, pp. 53–56, 2013.
- [18] L. E. George, E. K. Hassan, S. G. Mohammed, and F. G. Mohammed, "Selective image encryption based on DCT, hybrid shift coding and randomly generated secret key," *Iraqi Journal of Science*, vol. 61, no. 4, pp. 920–935, Apr. 2020, doi: 10.24996/ijs.2020.61.4.25.
- [19] H. Liang, G. Zhang, W. Hou, P. Huang, B. Liu, and S. Li, "A novel asymmetric hyperchaotic image encryption scheme based on elliptic curve cryptography," *Applied Sciences*, vol. 11, no. 12, pp. 1–23, Jun. 2021, doi: 10.3390/app11125691.
- [20] Y. Ma, Z. Zhu, Z. Dong, T. Shen, M. Sun, and W. Kong, "Multichannel retinal blood vessel segmentation based on the combination of matched filter and U-Net network," *BioMed Research International*, vol. 2021, pp. 1–18, May 2021, doi: 10.1155/2021/5561125.
- [21] M. Tajuddin and C. Nandini, "Secured crypto biometric system using retina," *International Advanced Research Journal in Science, Engineering and Technology*, vol. 2, no. 1, pp. 28–32, Jan. 2015, doi: 10.17148/IARJSET.2015.2104.
- [22] A. N. Mazher and J. Waleed, "Retina based glowworm swarm optimization for random cryptographic key generation," *Baghdad Science Journal*, vol. 19, no. 1, pp. 179–188, 2022, doi: 10.21123/BSJ.2022.19.1.0179.
- [23] A. O. Salau and S. Jain, "Feature extraction: a survey of the types, techniques, applications," in *2019 International Conference on Signal Processing and Communication (ICSC)*, Mar. 2019, pp. 158–164. doi: 10.1109/ICSC45622.2019.8938371.
- [24] P. Panchal, R. Bhojani, and TP, "An algorithm for retinal feature extraction using hybrid approach," *Procedia Computer Science*, vol. 79, pp. 61–68, 2016, doi: 10.1016/j.procs.2016.03.009.
- [25] V. Kakkad, M. Patel, and M. Shah, "Biometric authentication and image encryption for image security in cloud framework," *Multiscale and Multidisciplinary Modeling, Experiments and Design*, vol. 2, no. 4, pp. 233–248, Dec. 2019, doi: 10.1007/s41939-019-00049-y.
- [26] A. H. Shini, Z. I. Abood, and T. Z. Ismaeel, "Hybrid techniques-based speech recognition," *International Journal of Computer Applications*, vol. 139, no. 10, pp. 12–18, 2016.
- [27] Z. Ibrahim Abood and A. H. Al-sudani, "3-Level techniques comparison-based image recognition," *International Journal of Computer Applications*, vol. 97, no. 11, pp. 19–25, Jul. 2014, doi: 10.5120/17052-7241.
- [28] W. Stallings, "Computer and network security concepts I, introduction to number theory II, classical encryption techniques III, block ciphers and the data encryption standard IV," in *Cryptography and network security: principles and practice*, Pearson Edu. Lim, 2017, pp. 1–766.
- [29] E. N. Witanto, Y. E. Oktian, and S.-G. Lee, "Toward data integrity architecture for cloud-based AI systems," *Symmetry*, vol. 14, no. 2, pp. 1–41, Jan. 2022, doi: 10.3390/sym14020273.
- [30] M. Jasimridha and A. H. Fadil, "Retina image and bat-inspired algorithm for artificial key generation," *Medico-Legal Update*, vol. 20, no. 2, pp. 583–591, Apr. 2020, doi: 10.37506/mlu.v20i2.1173.
- [31] S. K. Wanjau, G. M. Wambugu, and G. N. Kamau, "SSH-brute force attack detection model based on deep learning," *International Journal of Computer Applications Technology and Research*, vol. 10, no. 01, pp. 42–50, 2021, doi: 10.7753/ijcatr1001.1008.
- [32] F. Ayankoya and B. Ohwo, "Brute-Force attack prevention in cloud computing using one time password and cryptographic hash function," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 17, no. 2, pp. 7–19, 2019.
- [33] S. Saito, K. Maruhashi, M. Takenaka, and S. Torii, "TOPASE: detection and prevention of brute force attacks with disciplined IPs from IDS logs," *Journal of Information Processing*, vol. 24, no. 2, pp. 217–226, 2016, doi: 10.2197/ipsjip.24.217.
- [34] E. Dogruluk, J. Macedo, and A. Costa, "A countermeasure approach for brute-force timing attacks on cache privacy in named data networking architectures," *Electronics*, vol. 11, no. 8, pp. 1–20, Apr. 2022, doi: 10.3390/electronics11081265.
- [35] L. Bosnjak, J. Sres, and B. Brumen, "Brute-force and dictionary attack on hashed real-world passwords," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, May 2018, pp. 1161–1166. doi: 10.23919/MIPRO.2018.8400211.
- [36] C. Tezcan, "Key lengths revisited: GPU-based brute force cryptanalysis of DES, 3DES, and PRESENT," *Journal of Systems Architecture*, vol. 124, Mar. 2022, doi: 10.1016/j.sysarc.2022.102402.





- [37] A. V. Arzhakov and D. S. Silnov, "Analysis of brute force attacks with Ylmf-pc signature," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 6, no. 4, pp. 1681–1684, Aug. 2016, doi: 10.11591/ijece.v6i4.10320.
- [38] M. Kepkowski, L. Hanzlik, I. Wood, and M. A. Kaafar, "How not to handle keys: timing attacks on FIDO authenticator privacy," *Proceedings on Privacy Enhancing Technologies*, vol. 2022, no. 4, pp. 705–726, Oct. 2022, doi: 10.56553/popets-2022-0129.

## BIOGRAPHIES OF AUTHORS



**Zainab Ibrahim Abood Alrifaa**     received the 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, and Information Security. She can be contacted at email: zainab.ibrahim@coeng.uobaghdad.edu.iq.



**Prof. Dr. Tarik Zeyad Ismaeel**     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. He can be contacted at email: tarik.z@coeng.uobaghdad.edu.iq.