Indonesian Journal of Electrical Engineering and Computer Science
Vol. 24, No. 1, October 2021, pp. 452~463
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v24.i1.pp452-463

The security of RC4 algorithm using keys generation depending on user's retina

Huda M. Salih, Raghda Salam Al Mahdawi
Department of Computer Engineering, College of Engineering, University of Diyala, Baqubah, Iraq

Article Info

Article history:

Received May 16, 2021
Revised Jul 30, 2021
Accepted Aug 4, 2021

Keywords:

Average security
RC4
Retina image
RKSA

ABSTRACT

Digital technologies grow more rapidly; information security threats are becoming increasingly dangerous. Advanced and various cyber-attacks and security threats, like targeted emails, and information exploitation, pose a critical threat that basically undermines our trust in the digital society. Rivest cipher 4 (RC4) algorithm is a significant cipher of a stream that could be utilized with protocols of the internet, the advantage of the RC4 algorithm is that it is simple and effective. There are several weak, especially after the pseudo-random generation algorithm (PRGA), PRGA's initially 256 rounds (the amount of the RC4 permutation). Several modified RC4 studies have been published thus far, however, they all face either standard privacy or achievement evaluation issues. This paper proposes a new RC4 algorithm that is based on the user's retina (RC4-Retina), which has solved both of these weak points it was indicated in the standard RC4 algorithm. The novelty of retina key scheduling algorithm (RKSA), which is generated by relying on the user's retina of the algorithm will modify the matrix of permutation used to configure the keys. The efficiency of the improved algorithm was measured by depending on the average security of ciphertext of different keys and different messages, results were good compared to the standard algorithm.

Corresponding Author:

Huda M. Salih
Department of Computer Engineering
University of Diyala
Diyala, Baqubah, 32001 Iraq
Email: alansari.comp@uodiyala.edu.iq, hud.m.salih2020@gmail.com

1. INTRODUCTION

Rivest cipher 4 (RC4) is a significant cipher of the stream that could be found in a wide range of protocols of the internet, including Skype, secure socket layer, transport layer security (SSL/TLS), wireless protected access (WPA), and wired equivalent privacy (WEP) [1], [2]. The speed and clarity of the RC4 algorithm's significant operators have been over such a substantial field of applications; the efficient implementation of both hardware and software has been extremely easy to develop [3]. In comparison to many other encryption algorithms, RC4 is fast and small. The RC4 algorithm encryption procedure was divided into two parts: (1) an assessment of the RC4's initialization, with an emphasis on the key scheduling algorithm's (KSA) initialization, and (2) an evaluation of the keystream generating output, with an emphasis on the pseudo-random generation algorithm (PRGA) round-running process and internal status [4]. Random numbers play an important role in cryptographic processes. Block padding initialization vectors, nonces, obstacles, and the keys are a few of the cryptographic items that involve a series of unpredictable pieces. The related random number generator (RNG) also a cryptographic system that gives bits for any of the

aforementioned. The significant amount of RNG bits are delivered clearly and so a passive intruder has an easy ability to read the RNG performance and may influence any shortcomings contained there [5], [6]. RNGs may be classified into two may categories [7]:

- True random number generators (TRNGs)
- Pseudo-random number generators (PRNGs)

RNGs could be used for cryptographic operational activities, and a discriminating portion of the cryptographic system can be considered on this account [8]. The TRNG produces random numbers using actual physical sources that are uncontrollable and predictable. They are used to generate security system keys. All biometrics can be used as the non-deterministic source of TRNG [9] to produce a unique key directly from the user's biometric information, namely the biometric retina [10]. For several distinct cryptographic structures, chaotic functions are a very useful building block. Their deterministic and aperiodic properties allow the cryptosystems to be analyzed clearly and elegantly. The security of these schemes depends on initial conditions and the parameters of the chaotic systems but not related to the stiffness or the computational bounds [11], [12].

2. RELATED WORK

There is a lot of research that addressed the weaknesses in the RC4 algorithm but it is not without gaps and below is a review of the most important:

Alsharida *et al.* [1] Their paper discusses the RC4 algorithm, RC4D has been improved in this research by amending the first and second sections of the algorithm. In the first section, it raises the usage of key operations to obtain more significant random, while in the second section adds one more random variable and uses the Xor function. Thus, the NIST statistical tests and the statistical analysis of distant-equalities reveal that the RC4D is more robust than the original RC4. Sahib *et al.* [13] They overcome the RC4 algorithm's vulnerability points, there are a variety of mistakes in RC4 's KSA. Based on multi-chaotic maps the research implemented improved RC4 key generation. KSA's new pattern coined as enhanced KSA (IKSA), the S array's permutation modified to depend on the random number generator based on three disorganized maps, and the suggested algorithm outputs are as follows: Output = M XOR generated key XOR random value from IKSA (R3w) The enhanced RC4 with IKSA is proven to be concealed, randomness and consistency over the varying length of the key and various plain text sizes unlike those of the original RC4. Hameed and Mahmood [14], In a quest to increase the RC4's security and get rid of the vulnerability associated with the S array's first permutation and the S array's permutation processes, a new version of KSA is proposed. Fluhrer *et al.* [15], The KSA which derives the initial state from the variable size key was analyzed and two important shortcomings of this process were identified.

3. MOTIVATION

The standard RC4 algorithm has vulnerabilities in the way the keys are created and utilized, which led to the exploitation of these weaknesses and then attack the RC4 algorithm, which caused the researchers to provide various research and studies to address the vulnerabilities, but these researches were not able to fully improve the standard RC4 algorithm. The proposed system in this research, which relies on generating keys using the user's retina, has addressed weaknesses in the generated key, as the keys generated from the user's retina are characterized by randomness and high efficiency.

4. MATERIALS AND METHOD

This paragraph includes a theoretical background to the topics, methods, and tools that will be used in the proposed system.

4.1. RC4 algorithm

Ron Rivest 1987, one of RSA's inventors, introduced the algorithm RC4. RC4 is a “Rivest Cipher 4” acronym, it is also known as “Ron's Code 4.” The algorithm relies on a random permutation being used. The RC4 algorithm is simple to declare, and fairly small [16].

4.2. Retina

The retina may be defined as the following: The optic nerve is in the center of the retina, a circular to oval white region measuring approximately 2 x 1.5 mm in diameter. The main blood vessels of the retina arise from the middle of the optic nerve. Nearly 17 degrees (4.5-5 mm), about two and a half-disk diameter to the left of the disk, the small oval-shaped, vessel-free reddish spot, blood the fovea, can be observed by the

ophthalmologists in the center of the region known as the macula [17], [18]. The retina is the eye's innermost layer which can be seen using suitable appliances like a fundus camera. The two main mechanisms used in the processing of retinal images are the optic disk and blood vessels. The optic disk is the brightest region in the image of the retinal and the blood vessels emerge from the middle [19]. A retina scan shows the layout of blood vessels inside the retina [20]. In contrast with other biometrics, as a biometric, the retina has a set of priorities. It is so safe and allows the use of a reliable physiological function. Spoofing is too difficult. Retinal patterns for left and right eyes are differing. Identical twins, on the other hand, are unique. Additionally, age does not affect retinal patterns [21], [22]. The images will not mark a deceased person on the retina, unlike other biometric characteristics. Because the retina is located inside within the eye of a human, any temporal or environmental factors can seldom affect it. The retina is therefore a significant biometric attribute for the highest security system [23], [24]. Data of biometric could be used to look for biometric data that is random to be used as random number sequences (after encoding in the integer or bit format). Robust random numbers are created by the biometrics data. A figure that shows a cross-sectional human eye with an illustration of a retinal image is mentioned in [25], [26].

4.3. The advantages and application of RC4

The advantages of the RC4 algorithm are that the algorithm is effective, simple, and well-suited for program implementation, which are distinguished by their implementation speed, do not require a great amount of storage space, and has less complexity [1], and it is frequently used in protocols and standards such as Skype, WPA, WEP, and SSL/TLS [14].

5. THE PROPOSED METHOD (RC4-RETINA)

The proposed method consists of four parts (RNG-Retina, Selected keys, improved RKSA, and encryption/decryption), as shown in Figure 1.

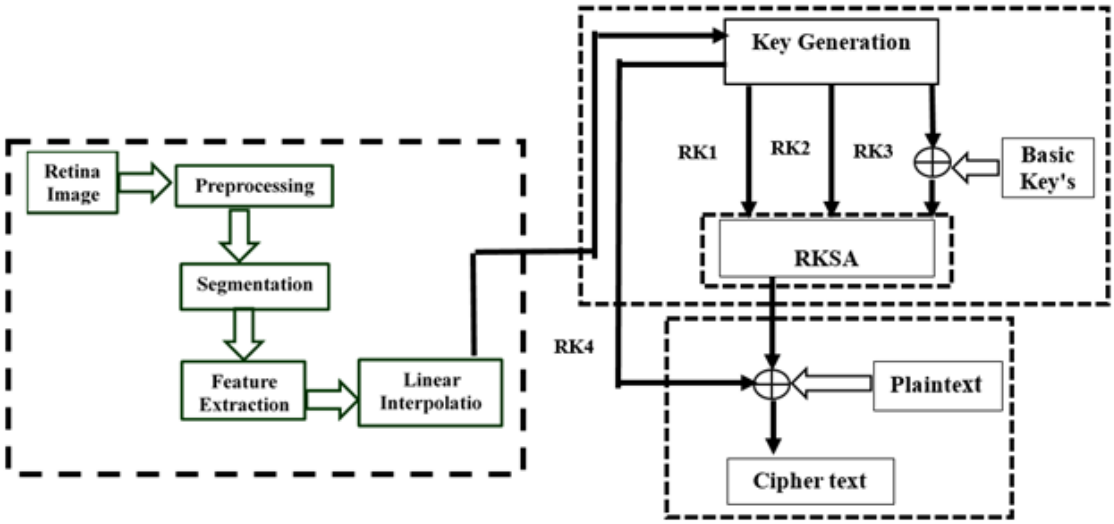


Figure 1. The proposed method

5.1. RNG-retina

This stage consists of several steps that lead to the generation of random keys. Below is an explanation of these steps:

5.1.1. The preprocessing stage for retina image

The retina image is processed improving during the next steps:

– Equalize individual color: When pixel color is a random vector defined by the red, green, and blue colors respectively, and the total density function added to each vector, the histogram of each color would be equalized. This behavior would allow the image's local features to become more visible and clearer than before.

- Grayscale conversion: Because the color image has a three-dimensional structure, the processing of the image is a long and complicated issue. The solution to this issue resides in the conversion of the grayscale. The colored image would be transformed into a grayscale image by measuring the average of each pixel component.
- Classical histogram equalization: It is a method of equalizing the histogram of the entered image to enhance the contrast, such that it is a global operation. The frequency at every gray level occurs from black (0) to white (255) and the histogram is plotted. By taking the gray level of the image pixel as a random vector and imposing the cumulative density function on it, the pixel gray level would be uniformly distributed throughout the image.

5.1.2. Segmentation using gray-scale morphology

The purpose of the segmentation of the image is to obtain the main features which are obvious in the image. The usage of morphological processes with grayscale is then used to segment the image and to gain blood vessels in the retina. The key morphological operations are dilatation, erosion opening, and closing; in this research, opening and top and hitting operations are used with the structural element of the diamond form and the scale 5×5. Opening action eliminates tiny items from the foreground of the image and puts them in the background. Since these blood vessels are dark-gray in color, morphological top-hat and image subtraction operations are done to acquire white-colored blood vessels as a foreground. The opening can be described by the structuring element N as the dilation of the erosion of image H. The image in grayscale H is a function where the domain is a two-dimensional digitized space subset Z × Z. To every point q ∈ Z × Z, the translation of H by q is described by:

$$(H)q=\{s+q|\ \forall s\in H\} \tag{1}$$

and dilation and erosion are offered by (the structuring element N) respectively [27].

$$H\ominus N=\min\{(Hq)\}\,|q\in N\}=\min_{q\in N}(H)q \tag{2}$$

$$H\oplus N=\text{Max}\ \{(H)q\,|q\in N=\max_{q\in N}(H)q \tag{3}$$

The white top-hat transform is a variation of some structuring element between the input image and its opening.

5.1.3. Pixel entropy feature extraction using two dimensions' maximum entropy threshold method

The 2D maximum entropy threshold method will be performed for following the processing and segmentation of the retina image. This will extract a pixel entropy feature which will be used for future procedure for generating keys at the stage of linear interpolation. A first step of the 2D entropy thresholding approach is to construct a 2D histogram by calculating the frequency incidence of each pair of the gray level of each pixel and its neighborhood's average gray-level value. The second step is to calculate 2D entropy using (4).

Assume mi refers to the number of pixels that the gray value is i. The gray probability is described by the (4). The fij refers to the number of pixels, the gray value being i and the average gray value being j.

$$M=\sum_{i=0}^{L-1} mi.\ q_{ij=\,f_{ij}\,/\,M} \tag{4}$$

Suppose that g is a pixel grey value. T is a pixel average-gray value. The computation of information entropy is described by (5) to a pair of values (g, t) [28].

$$\emptyset(g.t)=\ln\Big(\sum_{i=0}^{g}\sum_{j=0}^{t} q\,ij\Big)+\ln\Big(\sum_{i=g+1}^{L-1}\sum_{j=t+1}^{L-1} qij\Big)-\frac{\sum_{i=0}^{g}\sum_{j=0}^{t} pij\ \ln pij}{\sum_{i=0}^{g}\sum_{j=0}^{t} pij}-\frac{\sum_{i=g+1}^{L-1}\sum_{j=t+1}^{L-1} pij\ \ln pij}{\sum_{i=g+1}^{L-1}\sum_{j=t+1}^{L-1} pij} \tag{5}$$

5.1.4. Determination of retina center

The conventional Canny edge detection achieves even in highly distorted images to detect edges. Using a Gaussian filter mask to create a smooth image. An algorithm for adaptable canny could be described by transforming the color image to a grayscale image, detecting edges using a 2D Gaussian gradient edge detector by using the equation where the sigma 1=2 and segma2=2 and performing thinning by using the location of the threshold parameter as alpha=0.7 to decide the last collection of pixels. The black pixels represent the significant spots in the image on the retina vessels. Through having a maximum of x, y; a

minimum of x, y; and implementing linear interpolation between them, the resulting x, y will represent the midpoint and the middle of the retina grid will be it is coordinate.

5.1.5. Linear interpolation implementation

The linear interpolation technique is implemented between the position of the retina core and to obtain new points of entropy whose coordinates locate the major values. This step is done to increase the number of points on the processed retina image and thereby to increase the length of the generated key. The RNG-Retina is to generate true random numbers (TRN), Each iteration (number of iterations n=0 to 255) is used of 24 bits (RK2, RK3, and RK4 every have 8 bits in order). And the number of bits to RK1 depends on the length of the basic key (BK).

5.2. Selected keys

From the previous step, both were selected RK1, RK2, RK3, and RK4. RK1 = 8 bits, RK2 = 8 bits, RK3 = 8 bits, RK1= its length depends on the length of the basic key Improved basic key (IBK) = BK Å RK1.

5.3. Improved key scheduling (IKSA)

The IKSA was invented as an improvement for KSA, and the permutation of S was changed to based on truly random values RK2, RK3, and lBK.

Algorithm 1. (RC4–Retina Algorithm)

```
Input: Message M, LBk
Output: Cipher text
Step 1: /Initialize /
for j = 0 to 255
S[j] = j
T[j] = lK[j mod LBK];
Next j
Step 2: / Do IP of S /
For w=0 to 255
RK2w = Location: generate from the RNG-Retina
RK3w = Location: generate from the RNG-Retina
i = (RK3w + S [ RK2w] + T [ RK2w]) mod255
Swap (i, S (RK2w])
Next w
Step 3: /Stream Generation/
Set [j, i] = 0
While (true)=0
j = (j + 1) mod 256;
i = (i + S[j]) mod 256;
Swap (S[i], S[j]);
t = (S[j] + S[i]) mod 256;
lk = S[t];
RK4: produced from RNG-Retina
Step 4:/ Encryption, Decryption /
C = (M ⊕ LK ⊕ RK4) mod256
Decryption M= (C⊕LK ⊕ RK4) mod 256
Step 5:/End
```

6. RESULTS AND TESTING

6.1. Key generation

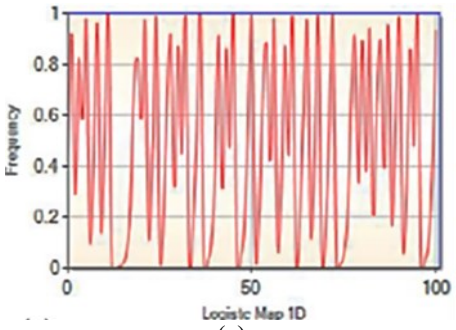
Random keys are generated using the RNG-Retina generator, as shown by some results below, as shown in Figure 2. Figure 2 illustrates the results of the crypto-key generation by using matrix 64 X 64 filled with the values of a one-dimensional logistic function with a starting value of x=0.1 and 2=4 as shown in Figures 2(a) and (b) and the coordinates of the points of the retina determine the key values of the chaotic matrix used for encryption afterward. Figure 3 illustrates the effects of key generation by using matrix 64 X 64 filled with sequential numbers. In the matrix of consecutive numbers, the retina points coordinates find the key values, as shown in Figure 3(a).

Generation Point	Cryptography	
No 100	Xo 0.10	L 4
Logistic Map ID		
No	X	
0	0.36	
1	0.9216	
2	0.28901376	
3	0.82193922612265	
4	0.585420538734197	
5	0.970813326249436	
6	0.113339247303761	
7	0.401973649297512	
8	0.961563495113613	
9	0.147836559913285	
10	0.503923645865164	
11	0.999938420012499	
12	0.000246304781624125	
13	0.000964976462324709	
14	0.00393602513473358	

(a)

1	2	3	4	5	6	7	8	9	10	11	12	13
0.36	.0.9	0.2	0.8	0.5	0.9	0.1	0.4	0.9	0.14	0.50	0.99	0.00
0.5	0.9	0.1	0.4	0.9	0.0	0.1	0.5	0.9	0.00	0.01	0.05	0.20
0.5	0.9	0.0	0.3	0.9	0.3	0.8	0.3	0.9	0.27	0.79	0.65	0.90
0.0	0.0	0.2	0.6	0.8	0.4	0.9	0.0	0.3	0.86	0.45	0.99	0.03
0.3	0.9	0.3	0.8	0.3	0.9	0.2	0.7	0.6	0.89	0.39	0.95	0.18
0.1	0.5	0.9	0.0	0.0	0.1	0.5	0.9	0.1	0.38	0.94	0.20	0.66
0.5	0.9	0.1	0.3	0.9	0.2	0.7	0.7	0.7	0.69	0.84	0.52	0.99
0.0	0.0	0.2	0.7	0.8	0.5	0.9	0.1	0.3	0.94	0.19	0.63	0.92
0.1	0.5	0.9	0.0	0.1	0.4	0.9	0.0	0.3	0.84	0.52	0.99	0.01
0.0	0.1	0.5	0.9	0.0	0.1	0.5	0.9	0.0	0.15	0.53	0.99	0.01
0.0	0.3	0.8	0.5	0.9	0.0	0.0	0.2	0.7	0.78	0.66	0.88	0.40
0.9	0.0	0.1	0.6	0.9	0.1	0.6	0.9	0.2	0.72	0.79	0.65	0.90
0.4	0.9	0.0	0.1	0.4	0.9	0.1	0.3	0.9	0.19	0.63	0.92	0.27
0.4	0.9	0.0	0.1	0.4	0.9	0.0	0.0	0.0	0.33	0.89	0.38	0.94
0.0	0.0	0.3	0.8	0.5	0.9	0.0	0.0	0.0	0.02	0.08	0.32	0.87

(b)



(c)

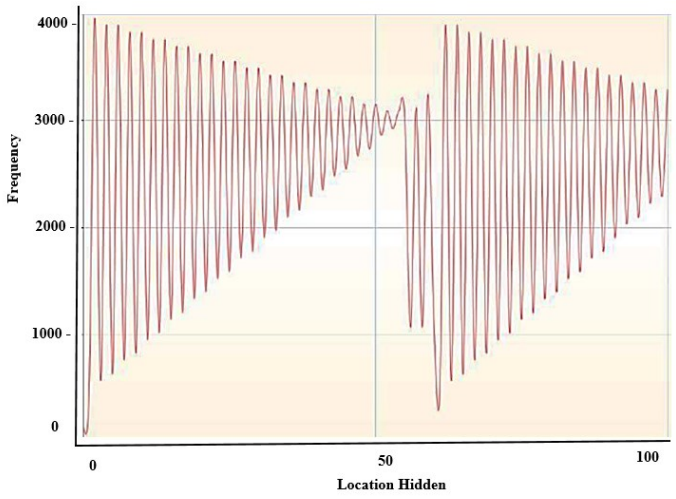
Generation Key			100	
#	i	j	Value	BIN
1	2	5	0.3407784	111110101011101111
2	2	6	0.8985939	111111110011010101
3	2	7	0.3644916	111110101110101001
4	2	8	0.9265499	111111110110111001
5	3	8	0.3189449	111110101000111001
6	3	9	0.8688763	111111101111011011
7	3	10	0.4557212	111110111010011010
8	3	11	0.9921576	111111111110111111
9	3	12	0.03112378	111100111111101111
10	4	12	0.1823176	111110111010101100
11	4	13	0.5963116	111111110001010011
12	4	14	0.9628963	111111111011010000
13	4	15	0.1429079	111110100101010110
14	5	15	0.9348741	111111110111110100
15	5	16	0.343538	111110111100111000

(d)

Figure 2. The crypto-keys generated; (a) the table shows the numbers obtained at the beginning of the logistic function conditions, (b) matrix 64 X 64 filled with ID logistic function values, (c) a graph shows the behavior and the random number distribution generated with the use of the chaotic function system above and (d) the coordinates of the retina points, in contrast to the key values of the chaotic matrix

#	i	j	location
1	2	5	133
2	2	6	445
3	2	7	3960
4	2	8	573
5	3	8	3895
6	3	9	636
7	3	10	3893
8	3	11	761
9	4	11	3828
10	4	12	827
11	4	13	3826
12	4	14	955
13	5	14	3761
14	5	15	1018
15	5	16	3759
16	5	17	1146
17	6	17	3694
18	6	18	1209
19	6	19	3692
20	6	20	1337

(a)



(b)

Figure 3. The keys generated; (a) In a chaotic matrix, locate key values by the retina point coordinates and (b) a chart illustrates the behavior and distribution of the keys

6.2. Encryption

Two sets of messages are encoded volumes (1024, 2048, 4096, 8192, and 16384), using two sets of keys in length (128, 256, 512, 1024, and 2048), and using the standard RC4 algorithm and the proposed algorithm (improve RC4 – Retina). So that the encryption process is done according to:

– Different messages-fixed keys.
– Different keys-fixed messages.

6.3. Average secrecy of cipher

Table 1 and the figures of charts as shown in Figures 4-8, show the proposed RC4-Retina algorithm has higher average secrecy than the traditional RC4-KSA algorithm and RKSA with enhanced RC4 algorithm (RC4 – Retina) using various messages sizes (2^{10}, 2^{11}, 2^{12}, 2^{13}, and 2^{14} bits), as well as a set fixed key length for each step (2^{7}, 2^{8}, 2^{9}, 2^{10}, and 2^{11} bits).

Table 1. Average secrecy of cipher-different message size, fixed keys length

Keys length / Bits	Messages Size / Bits	Average Secrecy of Cipher	
		Standard RC4 with KSA	Proposed Method RC4-Retina
128	1024	0.329	0.6999
	2048	0.197	0.7796
	4096	0.295	0.755
	8192	0.247	0.7661
	16384	0.177	0.5838
256	1024	0.418	0.7812
	2048	0.214	0.5221
	4096	0.333	0.7939
	8192	0.143	0.7887
	16384	0.448	0.6625
512	1024	0.532	0.7125
	2048	0.448	0.7992
	4096	0.504	0.6998
	8192	0.523	0.4963
	16384	0.601	0.7901
1024	1024	0.132	0.7523
	2048	0.52	0.6989
	4096	0.433	0.7321
	8192	0.502	0.692
	16384	0.189	0.5881
2048	1024	0.612	0.7992
	2048	0.119	0.6999
	4096	0.402	0.7808
	8192	0.502	0.5621
	16384	0.618	0.7911

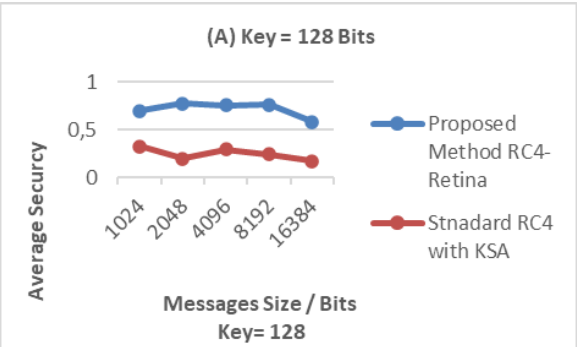


Figure 4. Key=128 bits

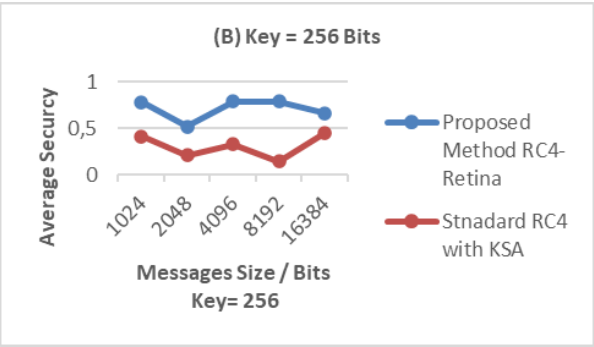


Figure 5. Key=256 bits

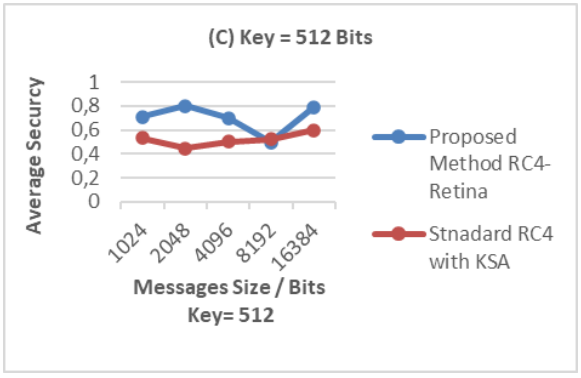


Figure 6. Key=512 bits

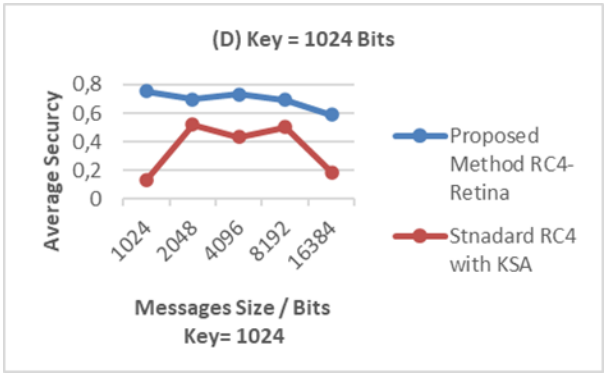


Figure 7. Key=1024 bits

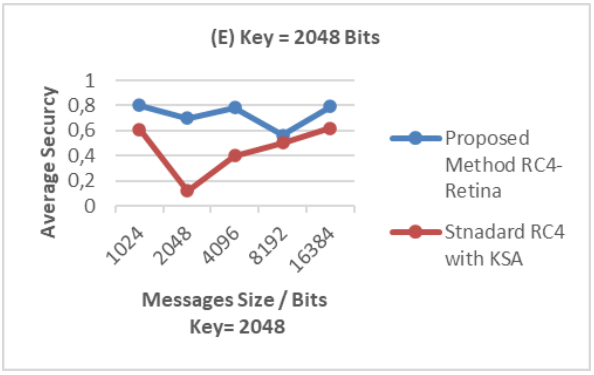


Figure 8. Key=2048 bits

6.3.1. Different message size, fixed keys

The variable message size is encrypted with a fixed-length key using the standard RC4 algorithm and improves RC4-Retina (proposed method).

6.3.2. Different keys length, fixed message size

The fixed message size is encrypted with a variable key length using the standard RC4-algorithm and improved RC4-Retina. Table 2 and the figures of charts as shown in Figures 9-13, show the proposed RC4-Retina algorithm offers better average secrecy than both the regular RC4-algorithm with KSA and the enhanced RC4 algorithm (RC4-Retina) with RKSA, which uses a separate key length for each phase (2^7, 2^8, 2^9, 2^{10}, and 2^{11} bits), and fixed messages sizes (2^{10}, 2^{11}, 2^{12}, 2^{13}, and 2^{14} bits).

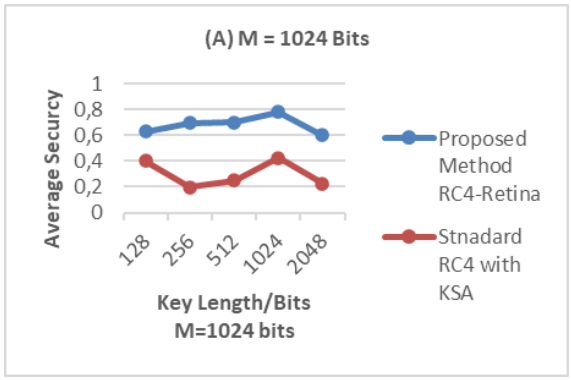


Figure 9. M=1024 bits

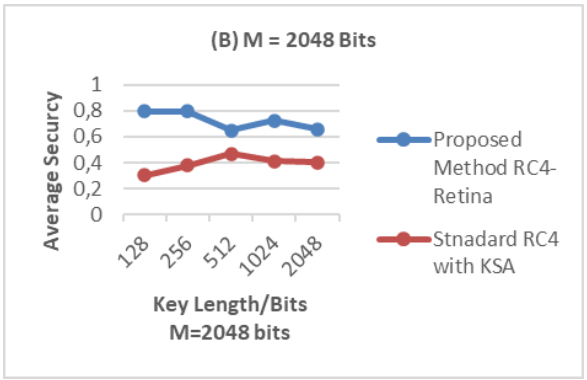


Figure 10. M=2048 bits

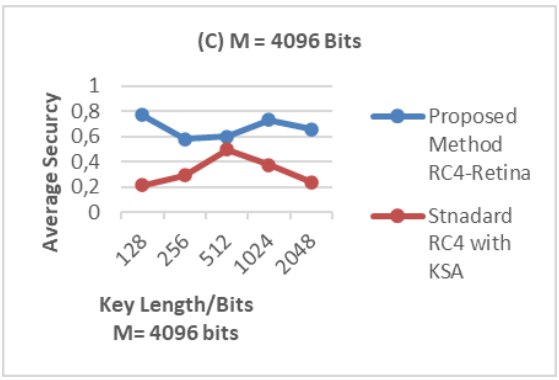


Figure 11. M=4096 bits

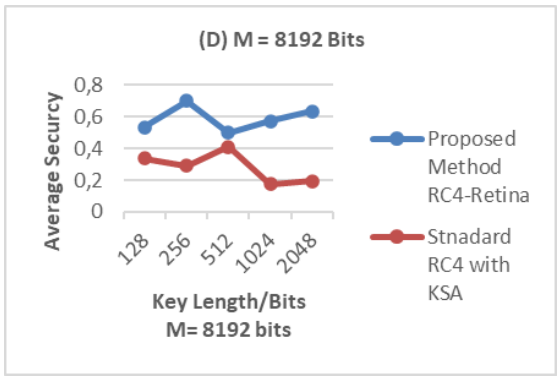


Figure 12. M=8192 bits

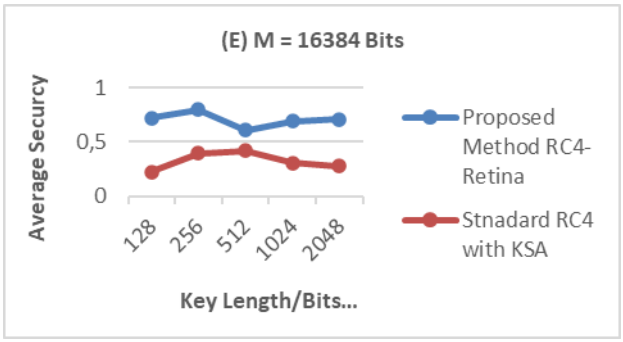


Figure 13. M=16384 bits

Table 2. Average secrecy of cipher- different keys length, fixed message size

Keys length / Bits	Messages Size / Bits	Average Secrecy of Cipher	
		Standard RC4 with KSA	Proposed Method RC4-Retina
1024	128	0.4035	0.6298
	256	0.1999	0.6965
	512	0.2501	0.7001
	1024	0.4235	0.7789
	2048	0.2256	0.5988
2048	128	0.3005	0.7932
	256	0.3765	0.7955
	512	0.4677	0.6501
	1024	0.4123	0.7229
	2048	0.3998	0.6587
4096	128	0.2137	0.7718
	256	0.2925	0.5809
	512	0.5001	0.5996
	1024	0.3762	0.7352
	2048	0.239	0.6608
8192	128	0.3373	0.5358
	256	0.2886	0.7001
	512	0.412	0.4999
	1024	0.1762	0.5721
	2048	0.1957	0.6339
16384	128	0.223	0.7221
	256	0.3981	0.7992
	512	0.4222	0.6111
	1024	0.3073	0.6929
	2048	0.2811	0.7092

6.4. The execution time

The time of obtaining the ciphertext from the plaintext according to the proposed improved algorithm compared to the standard algorithm is shown in Table 3 and graphs of data of different sizes and keys of different lengths, as shown in Figures 14 and 15.

Table 3. Execution time/ms, key length 1024 & 2048

Data Size / KB	Keys Length / Bits	Execution Time / µs RC4-Standard	Execution Time / µs RC4-Retina
20	1024	1005.1	936.8
40		1133.2	872.1
60		1180.9	890.6
80		1127.6	801.3
100		1205.8	884.4
20	2048	1126.2	914.7
40		1209.8	924.8
60		1318.5	952.9
80		1423.9	961.3
100		1602.1	980.8

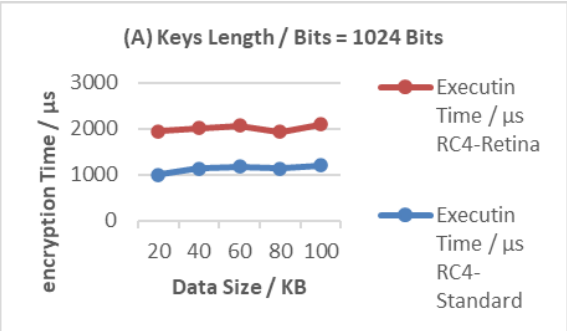


Figure 14. Keys length/bits=1024 bits

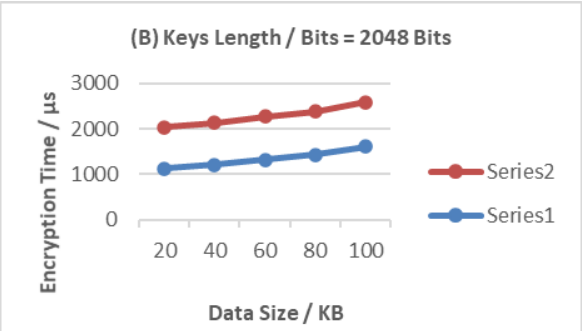


Figure 15. Keys length/bits=2048 bits

7. COMPARISON WITH OTHER RESEARCH

In the section below, we present a comparison between the proposed method in this research (RC4-Retina) and among one of the researches [12] that were covered in the section of related works, where the comparison was made through, the fixed message size is encrypted with a variable key length as shown in the Table 4, also the message size is encrypted with a fixed- key length using the improved RC4-Retina (proposed method) as shown in Table 5. It is clear from the tables that the average secrecy of cipher is the highest in the proposed method.

Table 4. Compare some value of the secrecy of cipher-different message size, fixed keys length

		Algorithms	
Keys length / Bits	Messages Size / Bits	Improvement RC4 with IKSA [12]	Proposed Method RC4-Retina
128	1024	0.5033	0.6999
256	1024	0.4551	0.7812

Table 5. Compare some value of the secrecy of cipher-different keys length, fixed message size

		Algorithms	
Messages Size / Bits	Keys length / Bits	Improvement RC4 with IKSA [12]	Proposed Method RC4-Retina
1024	128	0.5033	0.6298
	256	0.4551	0.6965

8. CONCLUSION

Within this paper, the following is proposed and achieved by the RC4-Retina Algorithm: Solve Standard RC4 algorithm weakness as well as patterns that were presented. Enhances the algorithm's productivity and improves and enhances its average secrecy through increasing efficiency and increasing the encryption time, i.e., RC4-Retina algorithm gave better results in terms of speed and execution time compared with another previous RC4 algorithm. A modern, secure system is constructed with unpredictability and unique keys based on retina images. The approach uses the advantage of the speeds of computer processing, a chaotic map, and biometric data to generate robust cipher keys without needing complicated sequences to memorize that could be stolen, or perhaps anticipated to be lost. In this study, the improved RC4 algorithm with RKSA based on logistic maps is proposed (RC4-Retina algorithm). This algorithm overcomes the weakness of the original RC4 with KSA. The average secrecy for the proposed

algorithm is best than the original algorithm. A suggestion has been made to improve the standard RC4 algorithm based on the generation of random keys generated by the user's retina. This led to an increase in the security of the new proposed algorithm RC4-Retina compared with the old standard algorithm, after calculating the Average secrecy and evaluating performance with a set of different messages and keys.

REFERENCES

[1] R. Alsharida, M. Hammood, M. A. Ahmed, B. Thamer, and M. Shakir, "RC4D: A New Development of RC4 Encryption Algorithm," in *the 12th International Networking Conference, INC 2020*, 2021, pp. 19-30, doi: 10.1007/978-3-030-64758-2_2.

[2] O. K. Hamid, R. B. Abduljabbar, and N. J. Alhyani, "Fast and robust approach for data security in communication channel using pascal matrix," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 19, no. 1, pp. 248-256, July 2020, doi: 10.11591/ijeecs.v19.i1.pp248-256

[3] F. S. Roozbahani and R. Azad, "Security Solutions against Computer Networks Threats," *Int. J. Advanced Networking and Applications*, vol. 7, no. 1, pp. 2576-2581. 2015.

[4] A.Y. Pyrkova and Z.E. Temirbekova, "Compare encryption performance across devices to ensure the security of the IOT," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 20, no. 2, pp. 894-902, Nov. 2020, doi: 10.11591/ijeecs.v20.i2.pp894-902.

[5] A. W. Altaher and A. H. Hussein, "Intelligent security system detects the hidden objects in the smart grid," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 19, no. 1, pp. 188-195, July 2020, doi: 10.11591/ijeecs.v19.i1.pp188-195.

[6] Ayushi, "A Symmetric Key Cryptographic Algorithm," *International Journal of Computer Applications*, vol. 1, no. 15, pp. 1-4, 2010.

[7] I. E. Hanouti, H. E. Fadili, W. Souhail and F. Masood, "A Lightweight Pseudo-Random Number Generator Based on a Robust Chaotic Map," *2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS)*, 2020, pp. 1-6, doi: 10.1109/ICDS50568.2020.9268715.

[8] B. Craincu, "On Invariance Weakness in the KSA Algorithm," *Procardia Technology*, vol. 19, pp. 850-857, 2015, doi: 10.1016/j.protcy.2015.02.122.

[9] P. Kohlbrenner and K. Gaj, "An embedded true random number generator for FPGAs," *12th international symposium on Field pro-grammable gate arrays,* Feb. 2004, pp. 71-78, doi: 10.1145/968280.968292.

[10] S. A. Tuncer and T. Kaya, "True Random Number Generation from Bioelectrical and Physical Signals," *Computational and Mathematical Methods in Medicine*, vol. 2018, 2018, doi: 10.1155/2018/3579275.

[11] 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. 54-56, 2013.

[12] G. Ablay, "A Chaotic Random Bit Generator with Image Encryption Applications," *International Journal of Computing Academic Research (IJCAR)*, vol. 5, no. 4, pp. 207-214, Aug. 2016.

[13] N. M. Sahib, A. H. Fadel and N. S. Ahmed, "Improved RC4 Algorithm Based on multi-chaotic Maps," *Research journal of Applied Sciences, Engineering and Technology*, vol. 15, no. 1, pp. 1-6, 2018, doi: 10.19026/rjaset.15.5285.

[14] S. M. Hameed, and I. N. Mahmood, "A Modified Key Scheduling Algorithm of RC4," *Iraqi Journal of Science*, vol. 57, no. 1A, pp. 262-267, 2016.

[15] S. Fluhrer, I. Mantin and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4", *International Workshop on Selected Areas in Cryptography*, 2001, pp. 1-24, doi: 10.1007/3-540-45537-X_1.

[16] P. Yankanchi and S. Angadi, "Biometric Steganography: A New Approach Using Hand Geometry," *International Journal of Recent Trends in Engineering &Research (IJRTER)*, vol. 2, no. 9, pp. 96-104, 2016.

[17] M. A. Taha, N. M. Sahib and T. M. Hasan, "Retina Random Number Generator for Stream Cipher Cryptography," *International Journal of Computer Science and Mobile Computing*, vol. 8, no. 9, pp. 172-181, Sep. 2019.

[18] S. Koduru, P. V. G. D. P. Reddy and P. Preethi, "A novel key exchange algorithm for security in internet of things," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 16, no. 3, pp. 1515-1520, Dec. 2019, doi: 10.11591/ijeecs.v16.i3.pp1515-1520.

[19] M. W. Patil and A. J. Patil, "Iris Recognition by Using Blood Vessel Segmentation for High Resolution Dastaset," *International Refereed Journal of Engineering and Science (IRJES)*, vol. 5, no. 8, pp. 40-50, 2016.

[20] K. Saraswathi, B. Jayaram and R. Balasubramanian, "Retinal Biometrics based Authentication and Key Exchange System," *International Journal of Computer Applications*, vol. 19, no. 1, pp. 1-7, 2011, doi: 10.5120/2329-3026.

[21] S. E. Borujeni and M. S. Ehsani, "Modified Logistic Maps for Cryptographic Application," *Applied Mathematics*, vol. 6, no. 5, pp. 773-782, 2015, doi: 10.4236/am.2015.65073.

[22] M. F. El-Santawy and A. N. Ahmed, "On Comparing Different Chaotic Maps in Differntial Evolutionary Optimization," *Anale. Seria Informatica*, vol. 10, no. 1, pp. 25-28, 2012.

[23] O. F. Mohammad, M. S. M. Rahim, S. R. M. Zeebaree and F. Y. H. Ahmed, "A Survey and Analysis of the Image Encryption Methods," *International Journal of Applied Engineering Research*, vol. 12, no. 23, pp. 13265-13280, 2017.

[24] C. Yu, J. Li, X. Li, X. Ren and B. B. Gupta, "Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram," *Multimedia Tools and Applications*, vol. 77, pp. 4585-4608, 2018, doi: 10.1007/s11042-017-4637-6.

[25] C. A. Montes, "Automatic Pixel-Parallel Extraction of the Retinal Vascular Tree: Algorithm Design, On-Chip Implementation and Applications," *PhD Thesis, Universidade da Coruna*, Advisor: Manuel G. Penedo and David L. Vilariño, 2008.
[26] F. Arena and G. Pau, "An overview of big data analysis," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 9, no. 4, pp. 1646-1653, Aug. 2020, doi: 10.11591/eei.v9i4.2359.
[27] O. Deforges, N. Normand and M. Babel, "Fast Recursive Grayscale Morphology Operators: from the Algorithm to the Pipeline Architecture," *Journal of Real-Time Image Processing*, vol. 8, pp. 143-152, 2013, doi: 10.1007/s11554-010-0171-8.
[28] L. Zheng, G. Li and Y. Bao, "Improvement of Grayscale Image 2D Maximum Entropy Threshold Segmentation Method," *2010 International Conference on Logistics Systems and Intelligent Management (ICLSIM)*, 2010, pp. 324-328, doi: 10.1109/ICLSIM.2010.5461410.

BIOGRAPHIES OF AUTHORS

Huda Mohammed Salih, she received her bachelor's degree from the University of Baghdad in 2001, she obtained a master's degree in computer sciences from the University of Baghdad in 2005, she participated in many local and international conferences, and participated in many training courses, including the IT course from the University of Berlin/Germany, and the CCNA1 course. She is currently working as a lecturer in the Computer Engineering Department/College of the Engineering/University of Diyala. Her research interests are mainly: Computer Networks and Information Technology, Cryptography and Information Security, Image Processing, Linux Open-Source System, Database management System, and Data Compression.

Raghda Salam Al Mahdawi obtained B. Sc in the Departement of Computer Engineering from the college of Engineering., University of Diyala, Iraq in 2007. Also carried out master degree in computer applid technology, University of Huazuing University for Science and Technology (HUST), China, 2016. The Research interest are computer networks, Image processing, Software Engineering, computer applid technology