Image Encryption Based on Multi-Level Keys on RC5 Algorithm

https://doi.org/10.3991/ijim.v16i17.34335

Abeer Salim Jamil[1](✉), Abdul Monem S. Rahma[2]
[1] Department of Computer Technology Engineering, Al-Mansour University College, Baghdad, Iraq
[2] Computer Science Department, Al-Maarif University College, Baghdad, Iraq
abeer.salim@muc.edu.iq

Abstract—In recent years, the need to develop encryption algorithms has led to an increase in the working and efficiency of algorithms to protect the transmission and reception of information from any security breach. The RC5 type encryption algorithm is the most common and closest to perfection and symmetry algorithms, knowing that it faces many problems in which data collection was limited because it occurs only twice by working on its also, the algorithm is used for only 1 function (XOR) through the encryption process. A research report on digital image development by developing the RC5 algorithm makes that algorithm more secure by adding a new security level (using two keys) and thus increasing the key space. The encryption and decryption process can be done by substituting the XOR operation applied to Sixteen rounds of the algorithm with the new operation (#) based on the use of 2 keys, each of it consisting of 4 states (0,1,2,3) instead of using the traditional key that uses two states (0,1). This development of the RC5 algorithm increases the security and robustness of the hacking methods.

Keywords—RC5 algorithm, 4- state operation, modify RC5 algorithm, encryption and decryption operation, multi-level keys

1 Introduction

to the tremendous progress in electronic technologies and networks in recent years, there have been great developments in communication. Anonymity and image protection are becoming increasingly important. In recent years, image protection has emerged as a critical issue. One of the most important images authentication techniques is image encryption. The data relating to image protection is critical, particularly in medical, military, and industrial sectors. As a result, applying encryption algorithms to electronic data must be to protect it from attackers [1-5]. Generally, cryptography can be categorized into two main fields: asymmetric-key and symmetric-key cryptography. The symmetric key can be classified into stream and block ciphers. Block ciphers encrypt a block of plaintext bits at a time using the same key but encrypt stream ciphers each bit individually by adding part of the mainstream to a plaintext bit [6-8]. Symmetric-key cryptography refers to encryption methods that use the same key for both the sender and the receiver. Symmetric-key cryptography also recognized as public-key cryptography was using two different keys which are related mathematically. To ensure the system's secrecy, each security system contains a set of security functions [9-11]. This set of functions is commonly referred to as the security system's goals. These goals can be characterized into three types (confidentiality, authentication, and integrity). Block cipher should be based on the Feistel network, Horst Feistel invented the Feistel network, which was used in various designs of a block cipher. Feistel network's primary function is to combine rounds number which is required to repeat the same operations [9, 12-14]. The proposed system focuses on the Feistel network implemented in RC5 which is a fast symmetric block cipher and was designed by Ronald Rivest in 1994 [7]." Rivest Cipher" (RC) or "Ron’s Code" (RC). This algorithm is designed to be suitable for both hardware and software implementation. To increase the confidentiality and authentication of employees working in the departments, we can use the proposed system because the image placed in the ID will be encrypted and cannot be subject to alteration or forgery alteration [15, 16]. The study remainder is organized as those items: Section 2 discusses relevant work in the RC5 algorithm and the 4-state operation literature. Section 3 describes the RC5 algorithm and how it can be used with text and images. Section 4 represents the enhanced RC5 algorithm by using the 4-states operation. Section 5 discusses the Experimental Results. Finally, the proposal's conclusion is presented in section 6.

2 Related work

With the growing demand for image encryption, this paper provides an overview of the relevant literature on modifying the Block cipher algorithm to include image encryption [2, 17]. In 2017 [18], researchers presented their findings by proposing a new modification to DES; that would increase the algorithm's security by extending the sizing of bits from 64 -128 bits of each key size and plaintext. This is accrued by multiplying function size, keys, and tables by a factor of two. The "algorithm" will be more resistant to a brute-force attack. In 2010 [19], improve the performance of the DES algorithm, the researchers proposed a new method. The optimization is demonstrated using a two-key operation instead of the predefined XOR operation used by 16 rounds of the standard Feistel algorithm. Instead of the usual two-state keys (0 and 1), the combination of the four states (0,1,2,3) which are using different truth tables is the contents of each key. To determine which of the four tables is used the first key is used, while for encrypt of the algorithm the second key is used. By increasing the algorithm complexity, such replacement will add to counter attackers a new level of security. This proposal was developed by the DES algorithm and more time is required for encryption and decryption. In 2011 [20], the work was presented by the researchers using the RC5 algorithm. First, the contiguous pixels in the RC5 encrypted image are highly correlated. Second, we examined the vulnerability to differential attacks using the pixel exchange rate (NPCR) and unified change intensity (UACI). In 2014 [21], the authors present their findings by proposing a new RC5 modification. Instead of rounds, the F-functions quadrature design will be used in RC5. In order to guarantee better encryption performance, especially for the low entropy images. In 2019 [22], the proposed algorithm by the authors shuffles the video frames alongside the audio, and then RC5 is used to selectively encrypt the sensitive video code word. The video block is first divided into frames in the encryption system, and then these frames are encrypted using block ciphering techniques such as RC5. This method prevents unauthorized viewing of the video file; thus such an algorithm provides a high-security level.

3 RC5 algorithm

In 1994, Ronald Rivest created RC5, a fast symmetric block cipher [23]. RC is an abbreviation for "Rivest Cipher," as opposed to "Ron's Code." This algorithm is intended for both hardware and software implementation. The extensive use of data-dependent rotation in RC5 is a novel feature. It is the algorithm parameterized with the variable block size, rounds number, and the length key. That allows for a great deal of flexibility in terms of two characteristics of performance and security. The RC5- w/r/b algorithm is a specific RC5 algorithm. The bits number in a word, w, RC5 is structure repetition with an inconstant rounds number. However, the round number, r, is the second parameter of RC5. a secret key will be used by RC5 with a variable-length, b. Below is a summary of these parameters [22, 23]:

w: The word bit size. 32 bits is a standard value, while the other values such as 64; 32; & 16 are also acceptable. RC5 encrypts 2-word blocks, thus the plaintext and ciphertext were both two words long [12].

r: The rounds number. Furthermore, allowable r values are (0, 1, 2..., 255), and the table of key expanded of S includes t = 2[24] words.

b: Specify the number of bytes for the secret key. K. b values range from 0 - 255. K: b - byte secrete key; K {0}sa, K {1} ... K {b 1}. simplicity is one of the RC5 design features, It makes it easy to implement. The other RC5 encryption distinguishing feature is its data-dependent rotation extensive use. The usefulness of this feature in preventing both linear cryptanalysis and differential analysis [3]. The following three primitive operations will be used by these algorithms:

1. Adding the complementary words of the two, represented by the "+" sign, adding to the words modulo 2w.
2. Bitwise- XOR (Words).
3. <<< SYMBOL OF ROTATION (ROTATION ON LEFT): CYCLIC ROTATION OF WORD X LEFT BY Y BITS IS DENOTED X <<< Y.

RC5 consists of three elements:

a) Key Expansion [23]

Algorithm Key expansion, expands a user key K to populate the expanded key table S, so that S represents an array of random binary words t = 2 {r +1} defined by K. It uses 2- words {magic constants size}, Qw, & Pw which are defined for any w, as shown below [6]:

$$Pw = Odd\ \{(e - 2)2w\} \tag{1}$$

$$Qw = Odd\ \{(\varphi - 1)2w\} \tag{2}$$

where the constants are:
φ = {1 +√5}/2 = 1. 61803.. (golden ratio).
e = 2.71828 … {Natural logarithms base}.
Odd(x) is the odd integer nearest to x.
The steps expansion algorithm key is [19]:

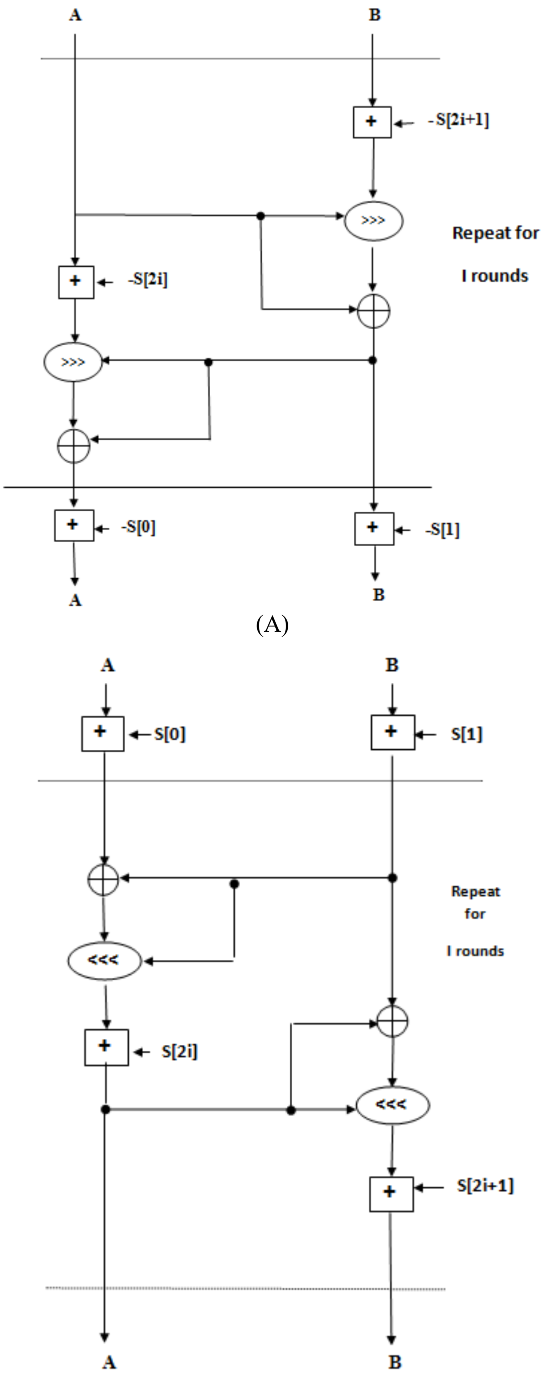
Step 1: Convert the key secrete from bytes- to words. The key secret K {0 ... b-1} is copied into an array L {0...c-1} and the value of c={b/u} words, where u = w/8 represents a number of bytes / word.

Step 2: This step expansion key involves initializing the array (S) into fixed pseudo-random bit pattern (key independent) using the 2w arithmetic progression criterion defined by magic Pw and Qw. Since Qw is an odd number, the progression calculation has a period of 2w.

Step 3: The secret key users are shuffled in 3 passes over the arrays (S) & (L) in this step. Because of possible size differences between (S) & (L), the larger array will be processed three times, while the other array can be processed three times more.

b) Encryption and Decryption [21, 22]

The encryption process begins with plain text and ends with ciphertext. The key expansion process should have been completed prior to this process. The process of decryption accepts cipher text as the input & returns plaintext as the output. Generally, when the same key is used, the same plaintext block will always be encrypted to a same ciphertext in a block of cipher, while the same plaintext is encrypted to different ciphertext in the stream cipher. Figure 1 depicts the RC5 traditional architecture.



(A)

(B)

Fig. 1. (A) RC5 algorithm encryption structure & (B) RC5 algorithm decryption structure

4 Proposed 4-states operation to enhance RC5 algorithm

The proposed work presents an image encryption method. A good encryption algorithm should resist attacks that try to hack the system, such as fixed, differential, and brute force attacks. Since attack resistance is a good measure of a system's cryptographic performance, it is often used to evaluate those systems. The method proposed in this section is to encrypt digital images using multi-level keys of the RC5 algorithm after modifying the RC5 algorithm by replacing XOR operation with a 4-state operation. Our proposed technology increases the efficiency of the encryption technology and reduces the encryption time due to image encryption. Moreover, a new method for generating multi-keys has been developed. The proposed RC5 modification work is divided into two sections.

4.1 4-States # operation (multi-level keys)

When the key space and the security are increased, so is making more double the encryption algorithms to intruders, the new manipulation bit process is added using the manipulated bit process variable truth table, which operates on four states {0, 1, 2, 3}, whereas the old traditional binary operation {XOR} works only on {0, 1} bits. The symbol (#) was used to indicate the performing of the operator, this operation using the 4-state truth tables as shown in Figure 2 [25, 26].

#0	0	1	2	3
0	3	2	1	0
1	2	3	0	1
2	1	0	3	2
3	0	1	2	3

#1	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

#2	0	1	2	3
0	2	3	0	1
1	3	2	1	0
2	0	1	2	3
3	1	0	3	2

#3	0	1	2	3
0	1	0	3	2
1	0	1	2	3
2	3	2	1	0
3	2	3	0	1

Fig. 2. A 4- States tables for (#) operator [20]

The operation of 4-states requires (3) inputs. The first to specify the number of the tables that must be used to calculate the score between the (4) tables. The other (2) entries specify the column & row number of table that has been given, where the result is provided by crossing point between them. Figure 3 illustrates this. The examples below demonstrate how to implement a 4-state table depended on block bits and select one of them.

Let:

- Input 1(table no.) :(011100001001100111) ===Convert to decimal no. ➔ (130021213)

- Input 2(row no.): (101110000110010101)=== Convert to decimal no. ➔ (232012111)
- Input 3(col. no.): (0001000110101110001) === Convert to decimal no. ➔(010122321)
- Result : (231210031)=== Convert to Binary no. ➔ (101101100100001101)

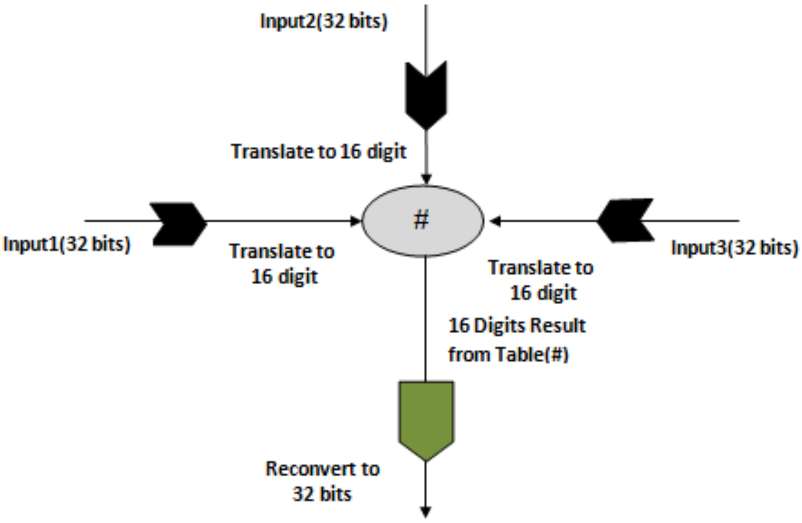


Fig. 3. Proposed of # operation in RC5 algorithm

4.2 Proposed RC5 algorithm

This paper proposed a new RC5 algorithm improvement. The proposed improvement uses the new, predefined process (description of 4-states operation). The operation (#) will be used during the original RC5 algorithm in each round. When another key is required to perform this operation, it can be in binary form then converted to a 4-state key, as shown in Figure 4.

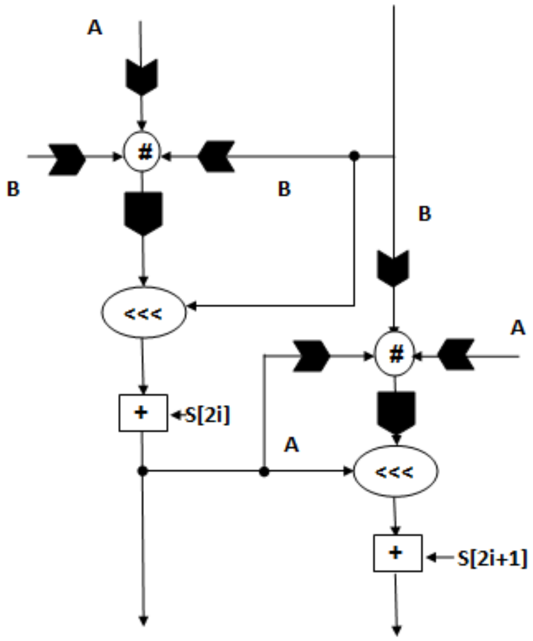


Fig. 4. Proposed of RC5 flowchart

As a result, each round of the original RC5 algorithm will use multiple inputs. The first input to the # operation in equation (2.3) is the value of A, the second input is B, and the third input is A, and the same operation is used in equation (2.4).in Figure 8, three 32-bit inputs are fed into the # operation, and the output is also 32 bits. These three inputs should first be converted from 32 bits to 16 digits, with each two bits converted to their decimal digit equivalents. Following that, the # operation would be used to generate the new 16-digit value which are must be reconverted to the 32 bits before being input into the second round. Figure 5 depicts the modified RC5 algorithm.

```
Input: Image(Original)
Output: image Encryption
Step 1: Begin
Step 2: read image
Step 3: Divided the input to two blocks: A(32 bits) and B(32 bits)
Step 4: Generate the key (section 2.1)
Step 5: Convert each blocks (A and B) from 32 bits to blocks of 2 bits (4-stses) by:
            If 00 then 0
            If 01 then 1
            If 10 then 2
            If 11 then 3
Step 6: Initial the value of A and B by :-  A= A+S[0]
                                            B=B+S[1]
Step 7: for i=1 to 12 do the following     Begin
          A=(A#B#B) <<<B)+S[2*i]// used # operation table
          B=(B#A#A) <<<A)+S[2*i+1]//used # operation table   End
Step 8: Brows the image encryption
Step 9: End
```

(A)

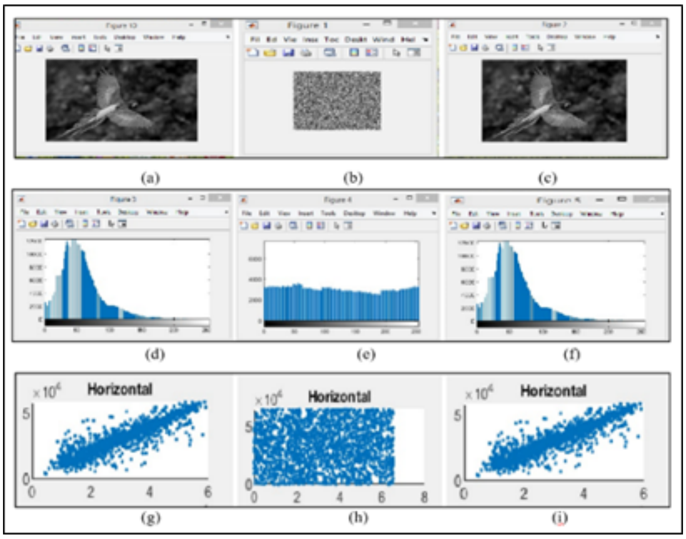
```
Input: Image Encryption
Output: Image(Original)
Step 1: Begin
Step 2: Read image
Step 3: Divided the input (cipher image) to two blocks:A(32 bits) and B (32 bits)
Step 4: Generate the key (section 2.1)
Step 5: Convert each blocks (A and B) from 32 bits to blocks of 2 bits (4-stses) by:
If 00 then 0
If 01 then 1
If 10 then 2
If 11 then 3
Step 6: Initial the value of A and B by :-A= A+S[0]
                                          B=B+S[1]
Step 7:   for i=12 down to 1 do the following Begin
         B=((B-S[2*i+1])>>>A) #A#A// # operation
        A=((A-S[2*i])>>>B) #B#B// # operation      End
B=B-S[1]
A=A-S[0]
Step 8: Brows the image
Step 9: End
```

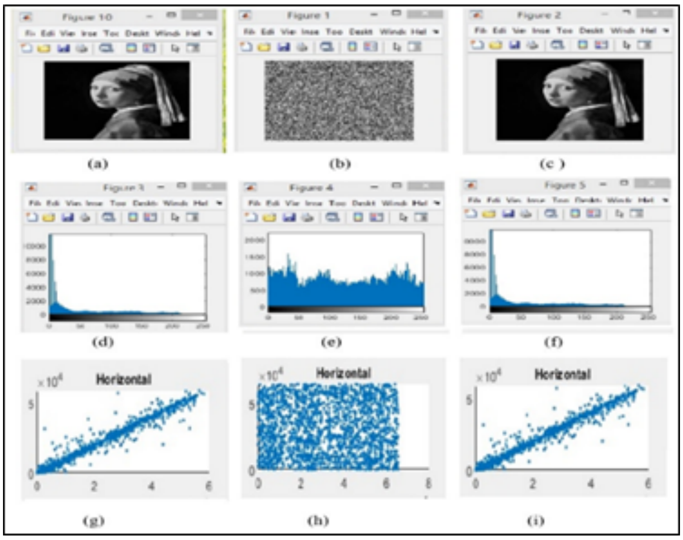
(B)

Fig. 5. The proposed RC5 algorithm: (A) Encryption operation and (B) Description operation

5 Result of experimental

Through the proposed method, color images of any size or type can be encoded. The proposed technique was applied to four samples of color images, as shown in Figure 6.





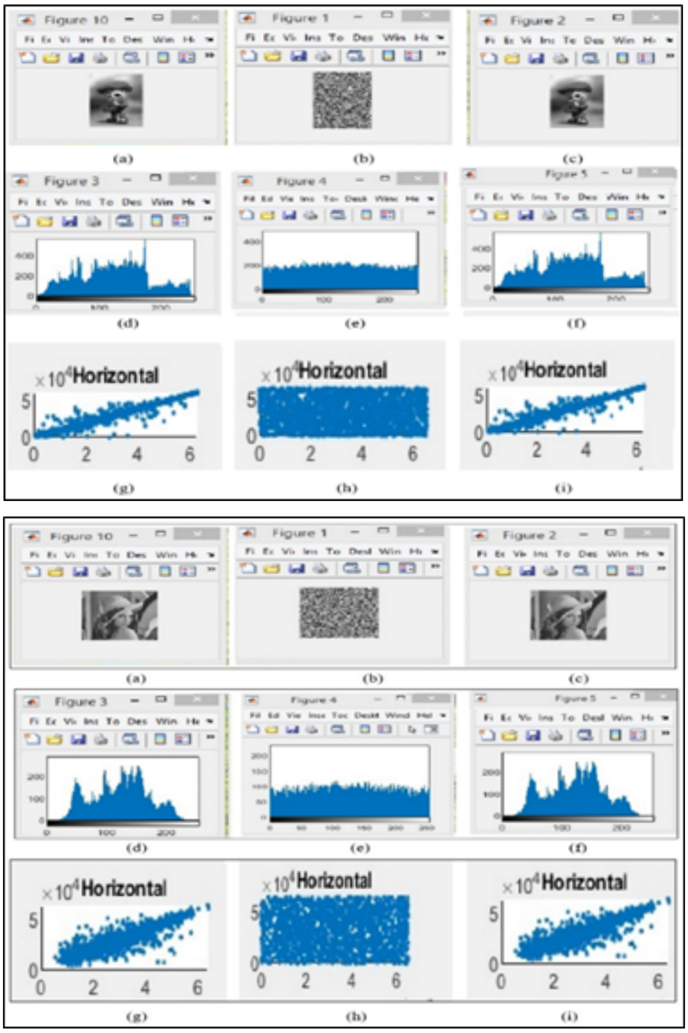


Fig. 6. The result of four sample of images; (a) the original image, (b) the encryption image, (c) the decryption image, (d)Histogram of original image, (e) Histogram of encryption (f), Histogram of decryption, (g) Correlation of original image, (h) Correlation of encryption image (i), Correlation of decryption image

Many metrics are used to evaluate the performance of the proposed RC5 algorithm, including correlation of adjacent pixels in equation 1, time of encryption for color images, Peak Signal to Noise Ratio (PSNR) as defined by equation (8) [27], and the Equation of Entropy Coefficient as defined in (9) [28].

$$Rxy = \frac{cov(x,y)}{\sqrt{D(x)\sqrt{D(Y)}}} \tag{3}$$

Where:

$$E(x) = 1/N \sum_{k=0}^{n} x(k) \tag{4}$$

$$D(x) = \frac{1}{N} \sum_{k=0}^{n} \ (xk - E(x))\verb|^|2 \tag{5}$$

$$\mathrm{cov(x, y)} = 1/\mathrm{N} \sum_{\mathrm{i=1}}^{\mathrm{N}} \big(\mathrm{xi} - \mathrm{E(x)})(\mathrm{yi} - \mathrm{E(y)}\big) \tag{6}$$

The Peak Signal to Noise Ratio (PSNR) and Entropy can be calculated using the following formulas:

$$\mathrm{MSE} = 1/\mathrm{p} \sum_{\mathrm{i=1}}^{\mathrm{p}} (\mathrm{Yi} - \mathrm{Y'i})^2 \tag{7}$$

Where: P is number of squared error, Yi is observed value and Y′i is predicated values.

$$PSNR10 \times log10 \lceil M \times N2552 \sum m - 1\ M \sum |\int\ (m,n) - \int d(m,n)|\ N\ 2\ n1 \rceil \tag{8}$$

Where: f{m, n}: Original image & fd{m, n}: Decrypted image.

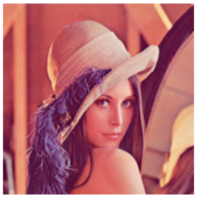
$$Entropy\ = \sum\{p(i))\ (log\ 1\ p(i)\} \tag{9}$$

Where: P{i}: represent the prob. of a count of an ith value of image gray.

Table 1 displays a correlation of adjacent pixels, encryption time, PSNR, MSE, for Encryption & Decryption images, & entropy value of different image encryption variances samples.

Table 1. Display time of encryption, correlation value, value of entropy, MSE value, and value of PSNR for encryption and decryption

Samples of Images	Encryption Time Full Image(second)	Correlation value	Entropy (Encrypted Image)	MSE (Image Encryption)	PSNR (Image Encryption)	PSNR (Image Decryption)
	1.075	-0.000367	7.995	64.7	19.2	96.6
	2.411	-0.0013	7.97	65.4	21.1	90 .8

	3.315	-0.000635	7.9942	67.5	19.7	95.74
	5.100	-0.0051	7.9903	70.50	20.2	98.3

6 Conclusion

Individual privacy protection is a topic in the security and surveillance fields. Encryption of Colour images becomes important. Increasing security using RC5 encryption to encrypt images is the purpose of this paper. This paper shows that until very recently RC5 is one of the most popular encryption algorithms used, and because of its many weaknesses, RC5 is considered unsafe for many applications. However, for example, these weaknesses include 1- single function, 2-length of key, 3- having fewer randomness, etc. Therefore, to increase the security level of this algorithm, it is necessary to add multiple levels of security to mentioned algorithm. Where an additional key has been added, the old XOR has been replaced by a new process known as "4-state of # operation," and more truth tables has been used also. Modifying the RC5 algorithm made this paper more robust against any attack type, using keys of multi-level instead of a single key to increase the reliability per round which increases the security algorithm. However, this would reduce the possibilities of penetration versus differential analysis from brute force attacks and increase encryption efficiency. The result of the encryption was more efficient and secure. Table 1 shows that a proposed algorithm has a very effective in increasing the value of security and decreasing the time of encryption, also more accurate through increasing the complexity of key computation while saving time and achieving lower PSNR and time between the original and encrypted images.

7 References

[1] A. S. J. Raghad Abdulaali Azeez, Ayad Al-Adhami, Nidaa Flaih Hassan "Multibiometric System with Runs Bits Permutation for Creating Cryptographic Key Generation Technique," *Iraqi Journal of Science,* vol. 64, no. 1, 2023.

[2] M. Y. Rhee, *Internet security: cryptographic principles, algorithms and protocols*. John Wiley & Sons, 2003.

[3] A. E. Earle, *Wireless security handbook*. Auerbach Publications, 2005. https://doi.org/10.1201/9780849333781

[4] I. A. Aljazaery, and A. H. M. Alaidi, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *International Journal of Online Biomedical Engineering,* vol. 18, no. 3, pp. 101-113, 2022. https://doi.org/10.3991/ijoe.v18i03.28021

[5] M. S. Shareef, T. Abd, and Y. S. Mezaal, "Gender voice classification with huge accuracy rate," *TELKOMNIKA,* vol. 18, no. 5, pp. 2612-2617, 2020. https://doi.org/10.12928/telkomnika.v18i5.13717

[6] S. Kandar, D. Chaudhuri, A. Bhattacharjee, and B. C. Dhara, "Image encryption using sequence generated by cyclic group," *Journal of information security applications,* vol. 44, pp. 117-129, 2019. https://doi.org/10.1016/j.jisa.2018.12.003

[7] R. A. Azeez, M. K. Abdul-Hussein, M. S. Mahdi, and H. T. S. ALRikabi, "Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique," *Periodicals of Engineering Natural Sciences,* vol. 10, no. 1, pp. 178-187, 2022. https://doi.org/10.21533/pen.v10i1.2577

[8] I. A. Aljazaery, and M. R. Aziz, "Combination of Hiding and Encryption for Data Security," *International Journal of Interactive Mobile Technologies,* vol. 14, no. 9, pp. 34-47, 2020. https://doi.org/10.3991/ijim.v14i09.14173

[9] M. S. Mahdi, R. A. Azeez, and N. F. Hassan, "A proposed lightweight image encryption using ChaCha with hyperchaotic maps," *Periodicals of Engineering Natural Sciences,* vol. 8, no. 4, pp. 2138-2145, 2020.

[10] H. T. ALRikabi and H. T. Hazim, "Enhanced Data Security of Communication System Using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[11] N. Alseelawi, and H. T. Hazim, "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT," *International Journal of Online Biomedical Engineering,* vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28011

[12] M. F. Mushtaq, S. Jamel, A. H. Disina, Z. A. Pindar, N. S. A. Shakir, and M. M. Deris, "A survey on the cryptographic encryption algorithms," *International Journal of Advanced Computer Science Applications,* vol. 8, no. 11, 2017. https://doi.org/10.14569/IJACSA.2017.081141

[13] T. H. Obaida, A. S. Jamil, and N. F. Hassan, "A Review: Video Encryption Techniques, Advantages And Disadvantages," *Webology,* vol. 19, no. 1, 2022.

[14] Y. S. Mezaal, D. A. Hammood, and M. H. Ali, "OTP encryption enhancement based on logical operations," in *2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC)*, 2016, pp. 109-112: IEEE. https://doi.org/10.1109/ICDIPC.2016.7470801

[15] D. Singh and R. Priyadharshini, "Performance analysis of data encryption algorithms for secure data transmission," *International Journal for Science Advance Research in Technology,* vol. 2, no. 12, 2016.

[16] T. H. Obaida, A. S. Jamil, and N. F. Hassan, "Real-time face detection in digital video-based on Viola-Jones supported by convolutional neural networks," *International Journal of Electrical Computer Engineering,* vol. 12, no. 3, 2022. https://doi.org/10.11591/ijece.v12i3.pp3083-3091

[17] Y. S. Mezaal, H. A. Hussein, F. A. Alfatlawy, Z. J. Abdulkareem, and L. N. Yousif, "Investigation of PAPR Reduction Technique Using TRC-SLM Integration," *Int J Simul Syst Sci Technol,* vol. 19, no. 6, pp. 34.1-34.6, 2018.

[18] B. F. Cruz, K. N. Domingo, F. E. De Guzman, J. B. Cotiangco, and C. B. Hilario, "Expanded 128-bit data encryption standard," *Int. J. Comput. Sci. Mob. Comput,* vol. 68, no. 8, pp. 133-142, 2017.

[19] R. F. Hassan, "New Approach for Modifying DES Algorithm Using 4-States Multi-keys," *J world,* vol. 4, p. 5, 2010.

[20] A. Mohamed, G. Zaibi, and A. Kachouri, "Implementation of rc5 and rc6 block ciphers on digital images 2011 8th international multi-conference on systems, signals and devices (SSD)," ed: IEEE, 2011. https://doi.org/10.1109/SSD.2011.5767447

[21] A. T Hashim, R. F. Nathim, and G. Saeed Mahdi, "Modification of RC5 Algorithm for Image Encryption," *IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL SYSTEMS ENGINEERING,* vol. 14, no. 2, pp. 62-71, 2014.

[22] A. Sharma and H. Sharma, "RC5 Algorithm for Video."

[23] R. L. Rivest, "RC5 Encryption Algorithm," *Dr Dobbs Journal,* vol. 226, pp. 146-148, 1995. https://doi.org/10.1007/3-540-60590-8_7

[24] M. Rajput and M. Deshmukh, "Secure (n, n+ 1)-multi secret image sharing scheme using additive modulo," *Procedia Computer Science,* vol. 89, pp. 677-683, 2016. https://doi.org/10.1016/j.procs.2016.06.034

[25] H. B. AbdulWahab and A. M. S. Rahma, "Proposed new quantum cryptography system using quantum description techniques for generated curves," in *The 2009 International conference on security and management, SAM2009*, 2009.

[26] S. M. Kareem and A. M. S. Rahma, "New modification on feistel DES algorithm based on multi-level keys," *International Journal of Electrical Computer Engineering,* vol. 10, no. 3, p. 3125, 2020. https://doi.org/10.11591/ijece.v10i3.pp3125-3135

[27] S. E. Umbaugh, Digital image processing and analysis: human and computer vision applications with CVIPtools. CRC press, 2010. https://doi.org/10.1201/9781439802069

[28] D. Salomon, *Data compression: the complete reference*. Springer Science & Business Media, 200.

8 Authors

Assist. Prof. Dr. Abeer Salim Jamil received the MSc. and PhD. in Computer Science from University of Technology, Iraq, 2004 and 2015 respectively. She has around 24 years of teaching experience and 11 years teaching in Cisco Network Academic (CISCO). Her areas of interests are Digital Image Processing, Video Processing, Security, software Engineering, Networking and artificial intelligence applications. She can be contacted at email: abeer.salim@muc.edu.iq.

Prof. Abdul Monem S. Rahma has an extensive background in the field of Cryptography and Information Security. In 1984, he received his PhD in Computer Science from the Loughborough University of Technology in the United Kingdom, and become a professor in Computer Science since 2008. his main work experience involves teaching at Iraqi universities and supervising postgraduate students. Also he was the Deputy Dean of the Department of Computer Science, University of Technology, Baghdad, Iraq from 2005 to 2013; and then from 2013 to 2015 become the Dean of the department. Now Prof. Rahma the head of the Department of Computer Science, Al-Maarif University College, Iraq. Prof. Rahma published 240 Papers, 4 Books in the field of Computer Science; supervised 41 PhD and 76 M.Sc. He can be contacted at email: monem.rahma@uoa.edu.iq.

Article submitted 2022-06-31. Resubmitted 2022-08-01. Final acceptance 2022-08-02. Final version published as submitted by the authors.