Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
Published Online First: February 2021 **E-ISSN: 2411-7986**

DOI: http://dx.doi.org/10.21123/bsj.2021.18.3.0628

An Efficient Image Encryption Using a Dynamic, Nonlinear and Secret Diffusion Scheme

***Rachid RIMANI*[1,2*]** ***Naima HADJ SAID*[1]** ***Adda ALI-PACHA*[1]**
***Juan Antonio López RAMOS*[3]**

[1] Department of Electronics, College of Electrical Engineering, University of Sciences and Technology of Oran, Mohamed Boudiaf, USTOMB – P.O. Box 1505 Oran M'Naouar 31000, ALGERIA
[2] Department of Science and Technology, College of Science and Technology, University Mustapha Stambouli of Mascara – P.O. Box 305 Road of Mamounia, Mascara 29000, ALGERIA
[3] Department of Mathematics, College of Mathematics and Computer Science, University of Almeria, P.O. Box 04120 La Cañada, Almería, SPAIN
[*]Corresponding author: rachid.rimani@univ-usto.dz[*], naima.hadjsaid@univ-usto.dz, a.alipacha@gmail.com, jlopez@ual.es
[*]ORCID ID: https://orcid.org/0000-0002-1923-4312[*] , https://orcid.org/0000-0003-2561-0481 ,https://orcid.org/0000-0003-1828-9562 , https://orcid.org/0000-0002-2263-2178

Received 25/3/2020, Accepted 27/12/2020, Published Online First 21/2/2021

Abstract:

This paper presents a new secret diffusion scheme called Round Key Permutation (RKP) based on the nonlinear, dynamic and pseudorandom permutation for encrypting images by block, since images are considered particular data because of their size and their information, which are two-dimensional nature and characterized by high redundancy and strong correlation. Firstly, the permutation table is calculated according to the master key and sub-keys. Secondly, scrambling pixels for each block to be encrypted will be done according the permutation table. Thereafter the AES encryption algorithm is used in the proposed cryptosystem by replacing the linear permutation of ShiftRows step with the nonlinear and secret permutation of RKP scheme; this change makes the encryption system depend on the secret key and allows both to respect the second Shannon's theory and the Kerckhoff principle. Security analysis of cryptosystem demonstrates that the proposed diffusion scheme of RKP enhances the fortress of encryption algorithm, as can be observed in the entropy and other obtained values.

Key words: Cryptosystem by block, Diffusion scheme, Encrypting images, Permutation table, Round key Permutation

Introduction:

The problem of exchanging secret data has always existed, since the birth of great civilizations. Cryptography is an effective way to protect the secret data and for maintain the confidentiality in the presence of adversaries, especially with the globalization of exchanges (internet, messaging and e-commerce) (1), based on various mediums (sound, image, video).

Encryption techniques can be separated in two main categories: per block or per stream. Block cipher is the most appropriate for encrypting images because of their size. Therefore, it used in the proposed cryptosystem with the substitution-permutation network structure SPN (used in AES). Indeed, the variable structure that depends on the iteration dynamic keys is more difficult to study by the attacker, for this reason, it adopted for the proposed cryptosystem.

The evolution of cryptography is marked by some very important foundational theories like Claude Shannon theory, which consists of using confusion and diffusion for secure encryption system. Encryption methods based on permutation-diffusion has been the subject of numerous studies because of their importance to build a sure encryption system, most of them based on nonlinear permutations for scrambling pixels using a generator of pseudo-random number (for example the chaos). For instance, in (2) proposes a chaotic shuffling-diffusion method for image encryption. In this work, authors generate two chaotic sequence using two logistic map, where the first is for label

the row coordinate of pixels of the scrambled image; and the second is for label the column coordinate of pixels of the scrambled image. Then, a new pixel exchange model is performed by a generated virtual coordinate matrix. For diffusion, they used a matrix of the same size as original image to change the values of the scrambled image according to MOD operation and XOR operation. In(3), researchers propose an efficient image encryption scheme with a self-adaptive permutation–diffusion and DNA random encoding; in this work, the plain image is converted to DNA sequence by a random encoding rules to disarrange the bit distribution of the plaintext, then a self-adaptive permutation–diffusion process is performed. Besides, the intrinsic features of the plaintext disturb the quantization processes of the permutation and diffusion procedures. In(4), proposes an image encryption based on Latin cubes; the permutation scheme in this work is highly plaintext-related with a strong diffusivity of substitution scheme have been constructed by exploiting the excellent cryptographic properties of Latin cubes of high-dimensional form, discreteness, uniformity and 3D attribute. In (5), authors propose an image encryption algorithm, where the image pixel locations is scrambled by a chaotic sequence, and the bit permutation is implemented by butterfly network. Then, the image is coded into a DNA matrix dynamic. In (6), proposed an image encryption scheme using self-adaptive selective permutation and a feedback-based diffusion mechanism, which can act on inter-intra blocks. In (7), researchers generate the permutation and substitution key stream sequences for image data scrambling and mixing by a hyper chaotic Lü system and logistic map, where a pixel swapping mechanism is used for permuting the positions of colored sub pixels in the input image. In (8), proposed a novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, in this work, in the permutation process of image pixel positions, they utilized a generalized Arnold map to generate one chaotic orbit used to get two index order sequences. In (9), proposed a novel encryption algorithm for color image based on Pixel-Level and Bit-Level pseudo-random permutations, while to dispel the redundancy on the entire image, the same permutation function in the ring $\mathbb{Z}/n\mathbb{Z}$ is applied to all pixels in the image, where n is the size of the image. In (10), researchers used a chaotic orbit perturbing mechanism for permutation-diffusion type image cipher with, while the permutation step consists to shuffle pixels in the plain image with a pixel-swapping mechanism, and a chaotic logistic map iteration generate the pseudorandom locations; moreover, a plain pixel related chaotic orbit perturbing mechanism is produced. In (11), proposed a block permutation encryption algorithm for color image, while the block permutation is realized by mixing R.G.B components to strengthen the dependence of each component. In (12), to permute pixels, a chaotic map and deoxyribonucleic acid (DNA) are used, while in the diffusion step a DNA sequence and a DNA operator are performed. In (13), authors propose a strategy of random diffusion for image encryption using a spatiotemporal chaos of the Logistic-dynamic mixed linear-nonlinear coupled map lattices, in this work a pending sequence is generated according to the number of image pixels, and then two index chains are generated combining the conflict handling process. Finally, the cipher image is obtained by random diffusion. In (14), proposes an image encryption using a combination of Grain-128a algorithm and Zaslavsky chaotic map; where a process of bit confusion and diffusion is applied using a sequences generated by the chaotic map. Despite the advantages of algorithms mentioned above, they have a number of inherent limitations. Firstly, the diffusion scheme is static and doen't change along the encryption process. Secondly, transmitter and recipient must share the secret key and some other parameters (for instance in (2,5) the correspondents must share the chaos parameters). Also, when the secret key is changed, the diffusion process does not change, i.e. the diffusion scheme does not have any dependence with the secret key. Taking into account what is mentioned, in this paper, a new diffusion scheme for block cipher algorithm called Round Key Permutation (RKP) is proposed, which makes the diffusion scheme secret and has a direct dependence with the encryption key and subkeys. In addition, it allows the encryption algorithm both to respect Shannon's second theory and Kerckhoffs principle, which means that the security of an encryption system must not reside in the encryption process but in the secret key. Therefore, scrambling pixels of each block will be done with various methods using the permutation table calculated from the master key and round keys. This diffusion technique makes the permutation in each block to be encrypted secret, nonlinear, random and dynamic (changes with the changing of round key).

The proposed diffusion technique is applied to the advanced encryption standard algorithm (AES); because it is the ultimate secure choice for block cryptosystem, besides its use is very practical and has many advantages compared with other algorithms (based on a variable structure of substitution-permutation network and a dynamic

key in each iteration). Also another algorithm which had a dynamic encryption key can be used like the algorithm proposed in (15), in this paper the authors showed that rekeying increase security, extend the lifetime of the master key effectively and bringing significant, provable security gains in practical situations. This propriety of rekeying allows us by applying the RKP to increase the security level and the dependence between the encryption scheme and master key (sub-keys). The cryptosystem used consists to replace the linear permutation of Shift-Rows step in AES algorithm by the proposed diffusion technique RKP which is a nonlinear, random, secret and dynamic permutation. The test of complexity of the proposed cryptosystem (AES with Round Key Permutation) and a comparative study is presented thereafter with the AES and other encryption algorithm by tests of statistical, differential analysis and the sensitivity of the secret key.

Structure of AES:

The AES (Advanced Encryption Standard) is a symmetric encryption algorithm that processes data blocks of 128, 196 or 256 bits and the size of the typically key used is 128 bits with variants of 192 and 256 bits. The data blocks and the key are stored in a table as shown in Fig.1; the number of columns depends on the blocks size and the key (16,17).

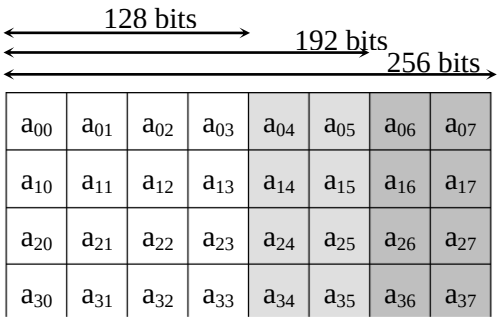


Figure 1. State table block

AES is based on a succession of rounds; the rounds number varies depending on the block size and the key size. The proposed cryptosystem use the AES algorithm of 128 bits block size with 128 bits key size and a rounds number r equal to 10.

The AES algorithm in the encryption mode consists of 3 steps:

- The first is an " exclusive or" operation between the plaintext block and the secret key K.
- The second step is a set of 9 rounds each executing 4 operations: SubBytes, ShiftRows, MixColumns and AddRoundKey.
- The last step is a round in which the MixColumns operation is not performed.

All the encryption operations are invertible. Therefore, in order to decrypt a block, operations are applied reversely.

Contribution: Image Encryption by AES Algorithm with RKP:

Image encryption is provided by the AES algorithm replacing the linear permutation of ShiftRows step by the proposed diffusion technique, which permute pixels of each block according to the permutation table calculated from the encryption key and sub-keys through the following procedure:

Marking the 1st minimum (or maximum) in the matrix of the encryption key by 1, the 2nd by 2 and so on until reaching 16 (the key size). In case of equality, always takes the reference from left to right and from top to bottom (according to the order of appearance). (Figs. 2, 3).

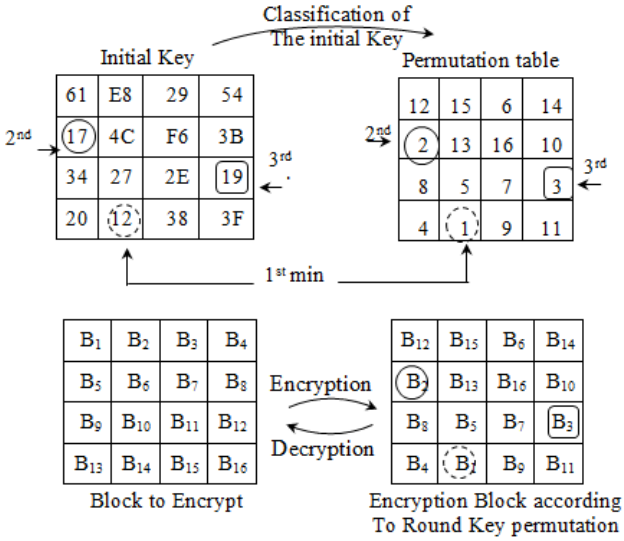


Figure 2. Calculating procedure of the permutation table and encryption/ decryption block

To decrypt a block, the same procedure is applied reversely.

When the image contains homogeneous areas, all identical blocks will also be identical after encryption. In this case, the ciphered image contains textured areas and the entropy of the image is not maximal. To solve this problem, the CBC mode is applied on the proposed algorithm; this allows on one hand to increase the level of complexity and on the other hand satisfies second Shannon's theory of diffusion.

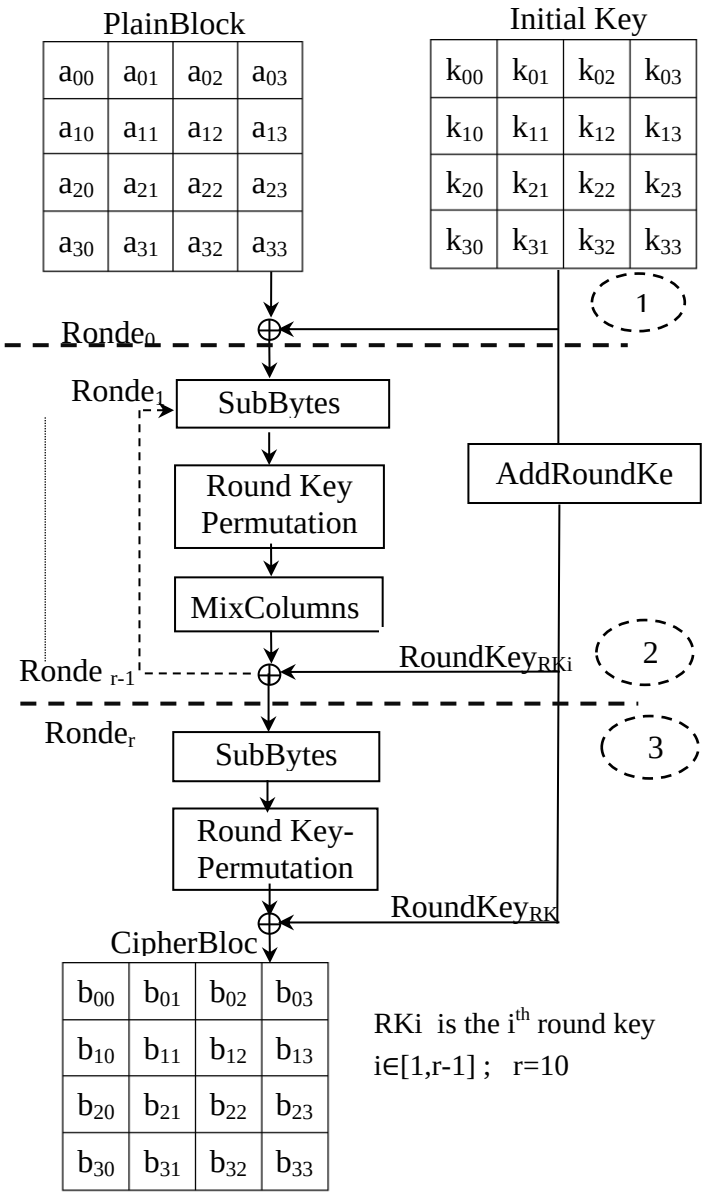


Figure 3. AES with Round Key Permutation in Encryption mode

Security Analysis of Proposed Cryptosystem and Experimental Results:

After the encryption of an image, it is necessary have an independence (low correlation) between pixels of the plain image and that of the ciphered image. This independence can be seen by simple viewing of the ciphered image, but the visual inspection remains insufficient to judge the encryption of an image. The metrics for evaluating the degree of encryption can be classified into statistical analysis, differential analysis and sensitivity analysis of the secret key.

Statistical Analysis

To resist the statistical attack, the ciphered image histogram must be very close to a uniform distribution. To measure this uniformity, two tests are applied, the first test is entropy and the second test is chi-square.

Histogram

The histogram of image is an important feature in analyzing of statistical performance in the encryption process. The histogram of an image is a discrete function that maps the number of pixel for each intensity simply by counting the number of pixel having certain intensity in the image (18), so the histogram illustrates how the gray levels pixels in an image are distributed. Therefore, it can be displayed as probability density function.

Figure 4 shows the results of Lena's image 224x224, encrypted by the AES algorithm with Round Key Permutation in CBC mode. The encrypted image is not at all visible; also the plain image histogram is changed tremendously comparing with the encrypted image histogram and the gray level occurrence probabilities is uniformly distributed in the encrypted image (Fig.4e).

Baghdad Science Journal
P-ISSN: 2078-8665
E-ISSN: 2411-7986

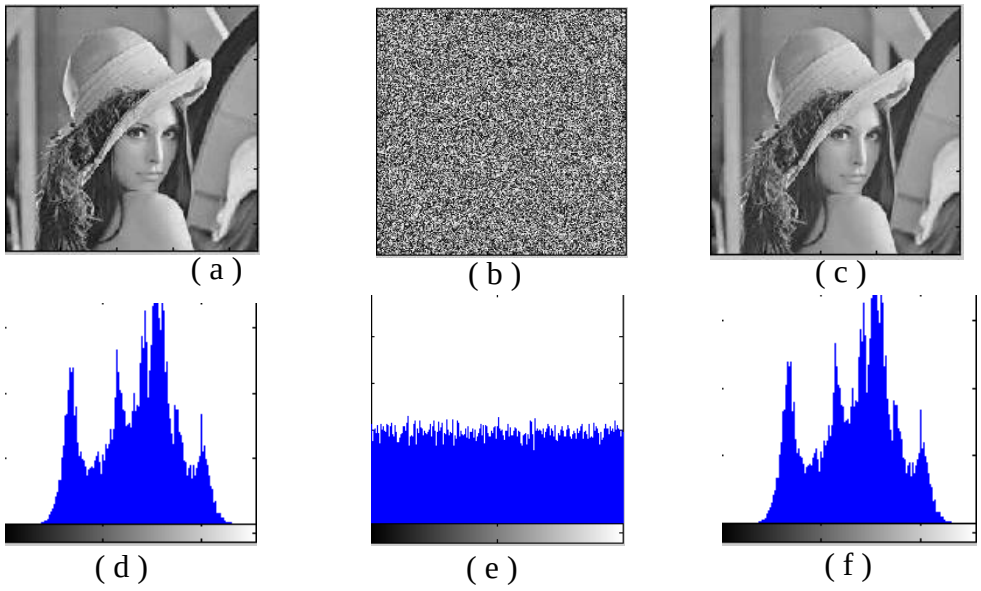


Figure 4. Encryption and decryption image by AES algorithm with Round Key Permutation in CBC mode

a) Plain image
b) Ciphered image
c) Decrypted image
d) Histogram of image (a)
e) Histogram of image (b)
f) Histogram of image (c)

Entropy Test

Entropy is the amount of information released or encompassed by a source of information. The entropy test of an image M is given by equation 2:

$$H(M) = \sum_{i=0}^{Q-1} p_i log_2 \frac{1}{p_i} = -\sum_{i=0}^{Q-1} p_i log_2 p_i \quad (1)$$

$Q=2^8=256$ represents the number of gray level, pi the probability of having an intensity i

More an image is complex, more its entropy is large. The uniform distribution is obtained, when the entropy $H(M)$ is maximum and is given by equation 3 :

$$H_{max} = log_2(Q) = 8 \quad (2)$$

The obtained entropy value of the encrypted image is 7.9967; this results is very close to H_{max}, it means that the source data has a nearly uniform distribution and the cryptosystem providing such data can withstand to the statistical attack.

Table 1 indicates that the entropy of the AES algorithm with Round Key Permutation is large compared to the AES algorithm; also the entropy of the AES algorithm with Round Key Permutation in CBC mode is high compared to the algorithm without CBC mode, so the CBC mode adds complexity to the proposed cryptosystem.

Table 1. Comparison of entropy between AES encryption algorithm and Round Key Permutation with and without CBC mode

Algorithm	Entropy Plain	Entropy Cipher
AES	7.2353	7.9950
AES with RKP	==	7.9953
AES with RKP in CBC mode	==	7.9967

Chi-square Test

The chi-square is a similarity measure of two categorical probability distributions. The chi-square value is 0 if the two distributions are identical; if the distributions are very different, some higher number will result. The chi-square test is given by the following formula:

$$X^2_{exp} = \sum_{i=0}^{Q-1} \frac{(O_i - e_i)^2}{e_i} \quad (3)$$

$Q=2^8=256$ is the number of gray level

O_i represents the observed occurrence frequency of each gray level $i \in [0,255]$ in the histogram of encrypted image, and e_i represents the theoretical occurrence frequency of the uniform distribution

$e_i = T_0/Q$ where T_0 is the size of image in bytes

The distribution of the histogram is uniform if it satisfies the following condition:

$X^2_{exp} < X^2_{th\ Q-1,\ \alpha} = 273,12$ for a threshold α fixed at 0.05 in our experiment.

X^2_{exp}=225.6633 using the proposed cryptosystem.

Correlation Coefficient of Adjacent Pixels

The calculation of the correlation coefficient between the pixels allows evaluating the encryption quality of cryptosystem. Generally, in an original image, each pixel is strongly correlated with its adjacent pixels in the three directions horizontal, vertical and diagonal. In the case of ideal cryptosystem, the encrypted image doesn't have any correlation between adjacent pixels.

To test the correlation between adjacent pixels; 5300 pairs of two adjacent pixels are taken from the original image and those encrypted in the three directions horizontal, vertical and diagonal as follows:

For each selected pixel (at the number 5300) of coordinates *(i, j)*, 4 vectors V, V_H, V_V, V_D containing the gray levels of the pixels are formed, which are found at the positions *(i, j), (i+1, j), (i, j+1), (i+1, j+1)* respectively. The correlation coefficients in the three directions are C_{VH}, C_{VV}, C_{VD}.

Table 2 groups the correlation coefficients for the following algorithms: the proposed algorithm AES with Round Key Permutation, ECKBA proposed in (19); the algorithm proposed by Mansour et al (20). The correlation coefficients measured for the original image are close to 1, while the correlation coefficients for the encrypted images of different algorithms are close to 0, it is also deduced that the encryption has considerably attenuated the correlation between pixels of encrypted images.

Table 2. Correlation coefficient of adjacent pixels

Direction	Correlation coefficient		
	Horizontal	**Vertical**	**Diagonal**
Plain image	0.9244	0.9588	0.8948
AES with RKP	-0.0111	0.0066	0.0069
ECKBA	0,0760	0,0227	-0,0012
Mansour et al	0,0479	-0,0414	-0,0416

The graph in Fig.5 represents the correlation coefficients in absolute value of the adjacent pixels of the encrypted images of each algorithm for comparing the performances of the proposed cryptosystem with ECKBA and Mansour et al algorithm. For the horizontal and vertical direction, Round Key Permutation performance has exceeded the other two algorithms; with the exception of the ECKBA algorithm which has a value of diagonal adjacent pixels lower than the proposed algorithm.

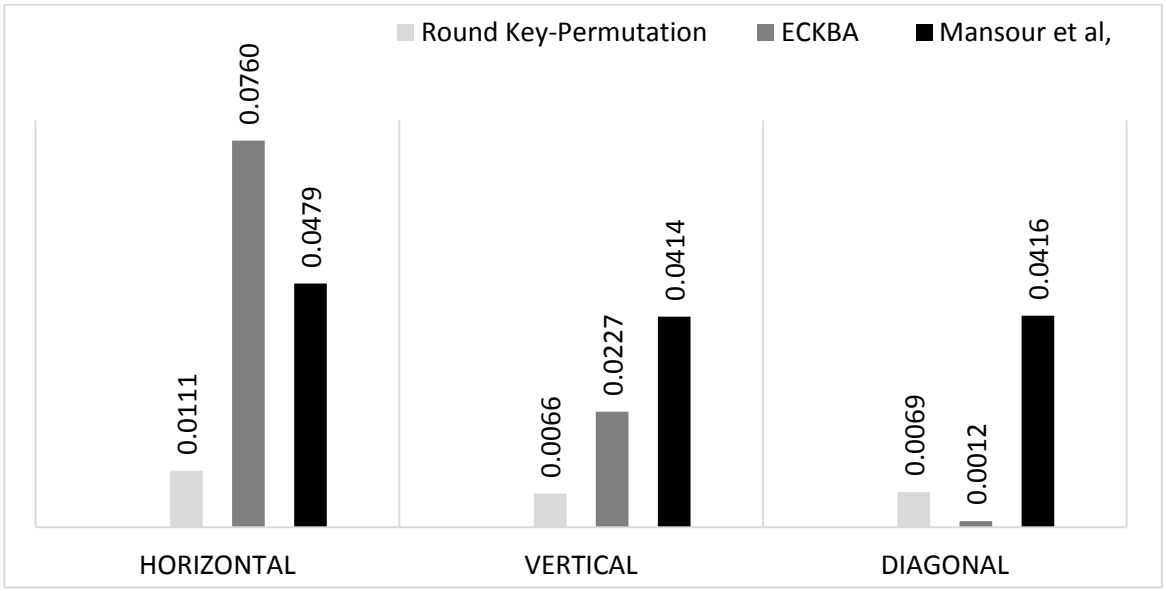
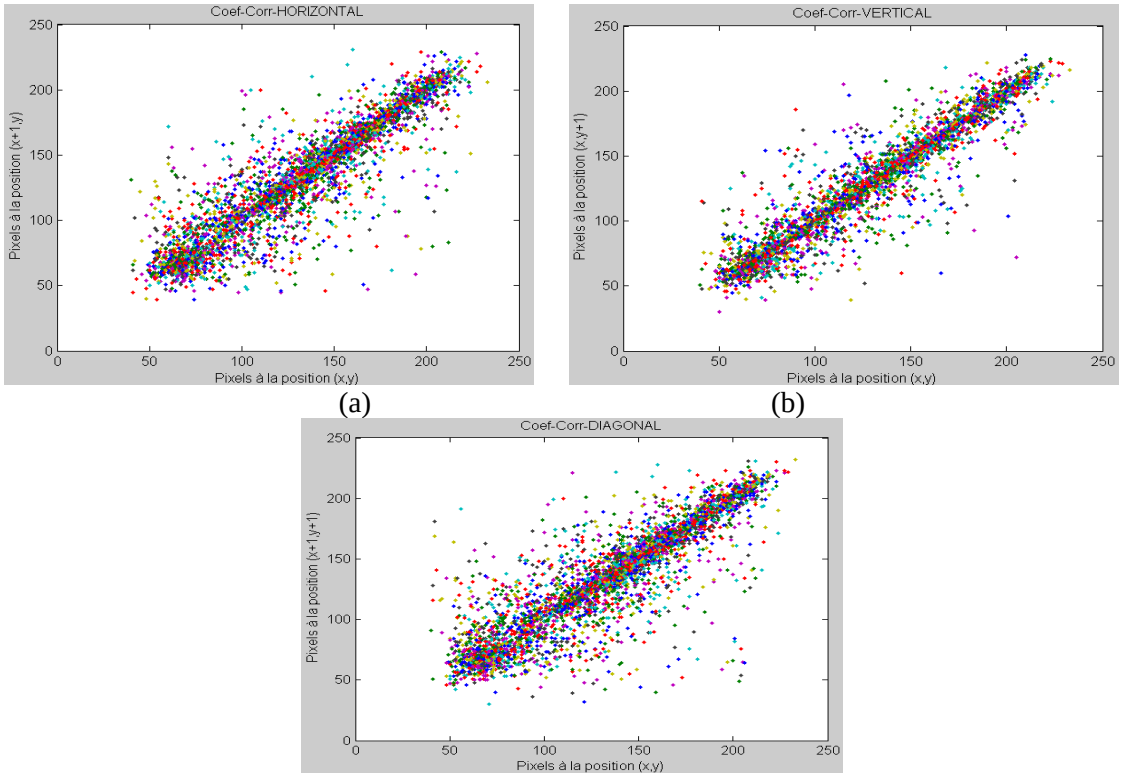


Figure 5. Correlation coefficient comparison of adjacent pixels for different algorithms

Figure 6 represents the correlation distributions of the horizontal, vertical and diagonal adjacent pixels in the plain image. The pixel intensity distribution is focused on the diagonal. Therefore, the pixels are then strongly correlated.

Baghdad Science Journal
P-ISSN: 2078-8665
E-ISSN: 2411-7986

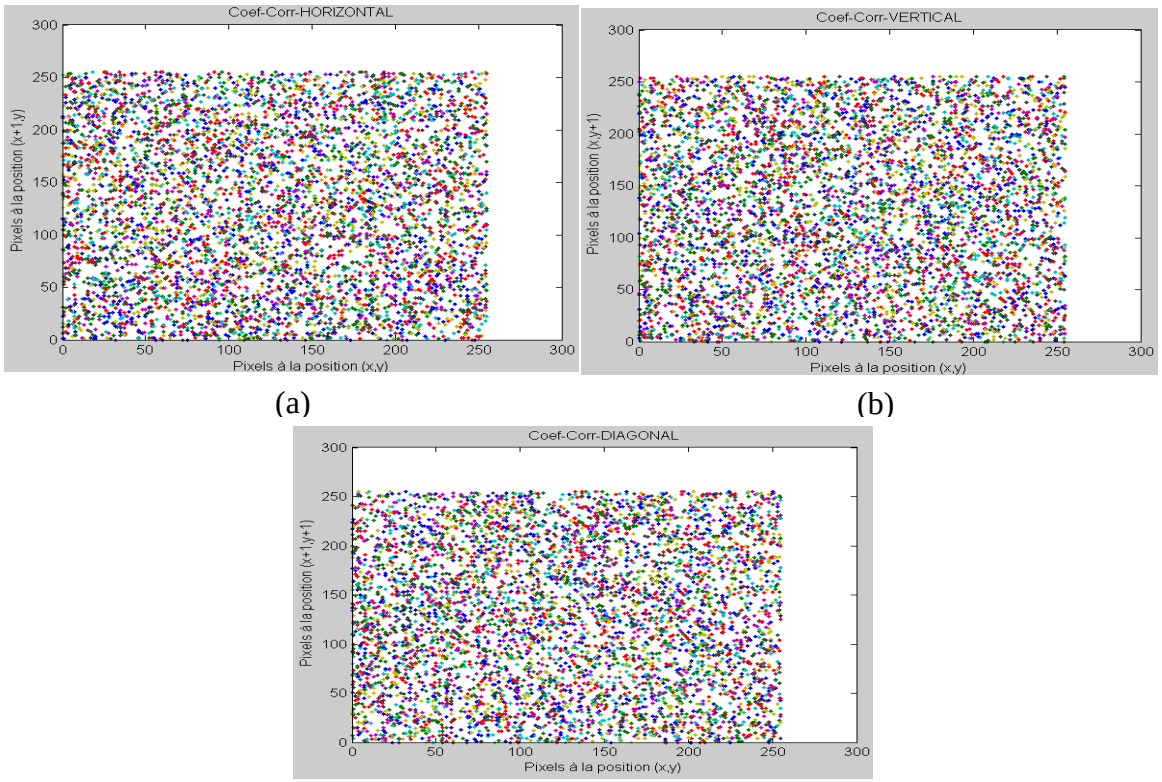


(a) (b)

(c)

Figure 6. Correlation distribution of peers of adjacent pixels in the original image: a) Horizontally, b) Vertically, c) Diagonally)

Figure 7 represents the correlation distributions of the horizontal, vertical and diagonal adjacent pixels in the encrypted image. The pixel intensity distributions are uncorrelated and they have a uniform distribution.



(a) (b)

(c)

Figure 7.Correlation distribution of peers of adjacent pixels in the encrypted image: a) Horizontally, b) Vertically, c) Diagonally

All results show that the cryptosystem used reveals good properties and resists against statistical attacks.

Differential Analysis

To ensure the security of an image encryption scheme against differential analysis, two quantitative measures are used: the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) defined by the following equation:

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} D(i,j)}{M * N} * 100 \qquad (4)$$

Where *M* and *N* are the width and height of image I_1 and I_2 respectively and *D(i, j)* is a matrix of the same size as I_1 and I_2 such that:

$$D(i,j) = \begin{cases} 1 & if\ I_1(i,j) \neq I_2(i,j) \\ 0 & else \end{cases}$$

$$UACI = \frac{1}{M * N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{|I_1(i,j) - I_2(i,j)|}{255} * 100 \qquad (5)$$

Table 3 indicates that the NPCR / UACI score between original image and encrypted image by AES with Round Key Permutation algorithm is large compared to that of AES; by applying the CBC mode, the NPCR of the algorithm increases. Also the NPCR of the proposed algorithm is large compared to the ECKBA encryption algorithm and the algorithm proposed by Mansour et al. The UACI of the proposed algorithm is better than the other tested algorithms.

Table 3. NPCR and UACI values between the original image and the encrypted image

Algorithm	NPCR (%)	UACI (%)
AES	99.5556	15.2373
AES with RKP	99.5775	15.3656
AES with RKP in CBC mode	99.5974	15.3048
ECKBA	99.5625	13.4146
Mansour et al	99.5937	13.0731

Another test is performed between two encrypted images (LENA 224*224) that differ from the original image by a single pixel, the NPCR and UACI values are shown in Table 4.

The UACI value of AES with Round Key Permutation algorithm is better compared to the AES, but the NPCR value is the same. Also, the NPCR of the ECKBA algorithm reaches the maximum value but its UACI value remains lower than the proposed algorithm.

Table 4.NPCR and UACI values between two encrypted images having one pixel different at the origin

Algorithm	NPCR (%)	UACI (%)
AES	0.0319	0.0091
AES with RKP	0,0319	0,0110
AES with RKP in CBC mode	77.4932	26.0442
ECKBA	100	15.9849
Mansour et al	0.0156	0.0059

Sensitivity of the Secret Key

To test the sensitivity of the key on the proposed cryptosystem and their reliability; two different tests are performed:

- The first test is to encrypt the same image by two keys slightly different; the used keys are different only by a single bit at the initial condition.

K1=[9 17 43 74;36 20 85 13; 41 7 16 54;21 47 63 **95**] 0**1**011111

K2=[9 17 43 74;36 20 85 13; 41 7 16 54;21 47 63 **31**] 0**0**011111

Figure 8 contains the histograms of Lena's image (80x80) encrypted by the two keys K1 and K2.

Baghdad Science Journal
P-ISSN: 2078-8665
E-ISSN: 2411-7986

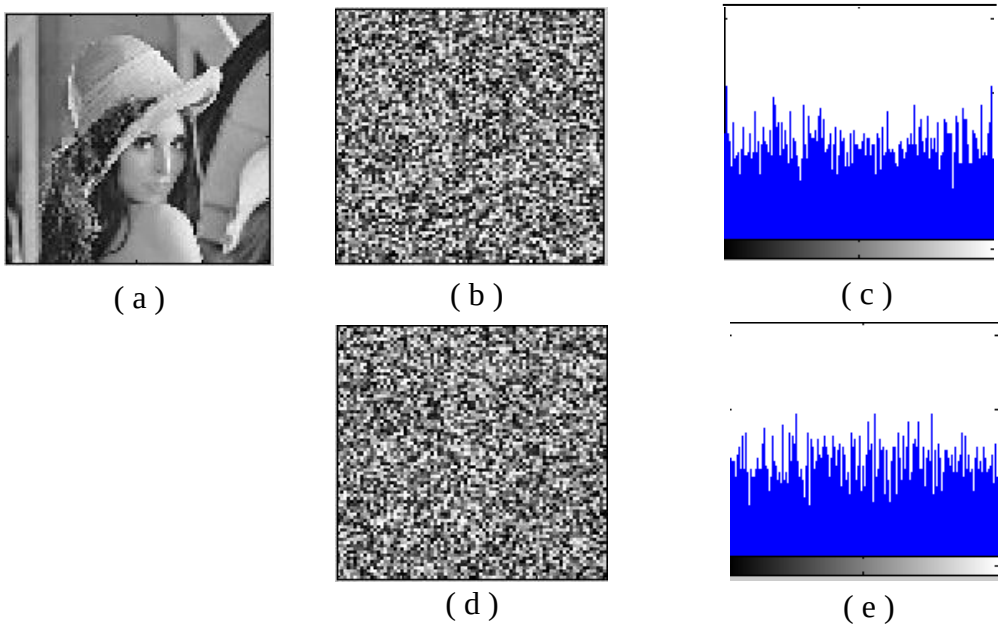


Figure 8. Image encrypt by two slightly different keys K1 and K2
a) Plain image, b) Ciphered image with K1, d) Ciphered image with K2
c) Histogram of image (b), e) Histogram of image (d)

Changing a single bit in the encryption key then gives two completely different histograms with a very low correlation coefficient between the two encrypted images (corrcoef = 0.0090). Therefore, the two encrypted images are completely independent from each other.

- The second test consists on using the key K1 to encrypt an image (LENA 80x80), and using the key K2 in the decryption phase (Fig. 9)

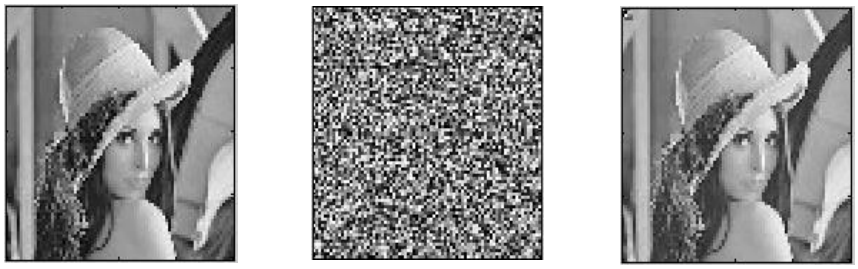


Figure 9. a) Plain image, b) Image decrypted by K2, c) Image decrypted by K1

The decryption process failed when the secret key is slightly changed and the decrypted image is completely blurred (Fig 9b).

With these two tests, the conclude is that the AES algorithm with Round Key Permutation is extremely sensitive to small changes of the secret key, so the proposed approach guarantees security against brute force attacks.

Avalanche Criterion:

Any function that satisfies this criterion must have a change with a probability of one-half of the output bits, if only one bit at the input changes; the output will then be uniformed and no statistical prediction can take place; this criterion is measured by calculating of hamming distance.

The Hamming distance is the number of different bits between two binary sequences C1 and C2, which will be noted dH(C1, C2). This criterion measures the avalanche effect and it is defined by the equation 6:

$$d_H(C_1, C_2) = \sum_{i=0}^{n-1} |C_1(i), C_2(i)| \quad (6)$$

Two binary sequences E1 and E2 are encrypted, which differ by a single bit by our algorithm AES with Round Key Permutation, then the Hamming distance is calculated between the two resulting encrypted sequences C1 and C2, by changing each time the position of the bit to be changed for plain text sequences. Figure 10 shows

the percentage of the Hamming distance in bits given by equation 7:

$$pd_H(j) = \frac{d_H(j)}{L_b} * 100 \quad (7)$$

The size of the binary sequences tested is Lb = 128 bits and j represents the different bit position. 81.25% pairs of encrypted sequences have a Hamming distance greater than 46%, and 18.75% pairs have a distance less than 46%; the average value of the Hamming distance obtained for our algorithm is 50.2563 (Fig. 10); indeed whatever the position of the changed bit, this provided almost 50% of difference between the bits of two concerned sequences. So the avalanche property is reached by the algorithm AES with Round Key Permutation.

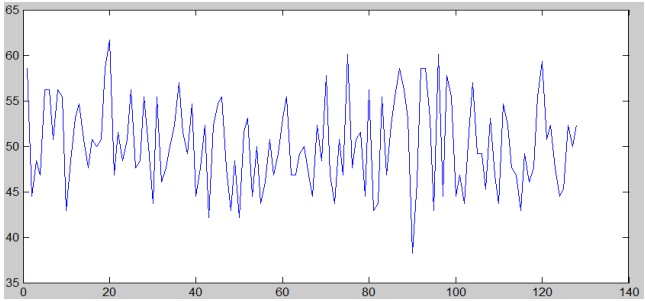


Figure 10. Percentage in bits of the Hamming distance according to the positions of the changed bits for pairs of encrypted texts by AES with Round Key Permutation

Comparison of the Execution Time:

The execution time was evaluated by MATLAB 7.6.0 (R2008a). The experiments were conducted using an Intel Core i3 processor with a frequency of 2.4 GHz.

The execution time required for each algorithm: AES and Round Key Permutation to encrypt a Lena's image of different size (40x40, 80x80, 120x120, 160x160, 240x240, 320x320 and 400x400) is provided in Fig. 11. If the size of the image increases, the two methods have almost the same execution time with a difference of a few milliseconds.

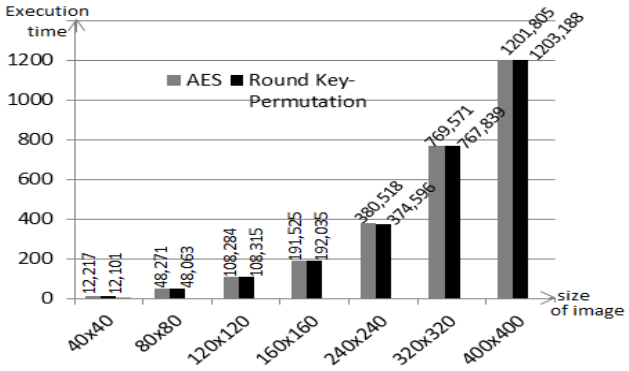


Figure 11.Execution time between AES and Round Key Permutation according to the size of the image

The proposed diffusion technique RKP does not improve the execution time and its application remains limited to the block encryption algorithm.

Conclusion:

This work presents a new diffusion technique depending on the secret key and the sub-keys; this technique is tested thereafter with the AES encryption algorithm by replacing the linear permutation of the ShiftRows step with the proposed technique Round Key Permutation which is random, dynamic and nonlinear (a new permutation for each Round). Another drawback in ShiftRows step is the public permutation; on the other hand, in the proposed approach, the permutation procedure is secret and depends on the secret key; this means that the security in the Round Key Permutation method is not based on the encryption scheme, but on the confidentiality of the key (Kerckhoff principle).

The proposed diffusion technique is suitable for encryption algorithm by block; and if the size of the key is changed , the encryption/ decryption procedure does not change; it is sufficient to modify the size of the permutation table and the size of the encryption blocks.

The AES encryption algorithm has been used as an example for testing the proposed technique Round Key Permutation, but if necessary, it can replaced by another encryption algorithm, which have best cryptographic properties. In conclusion, the modification made on the AES algorithm does not have any influence in its efficiency, but also enhances its fortress as can be observed in the entropy and other values obtained.

Authors' declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours,

have been given the permission for re-publication attached with the manuscript.

- Ethical Clearance: The project was approved by the local ethical committee in University Mustapha Stambouli of Mascara.

References:

1. Daria L, Alexander P. Applying Correlation and Regression Analysis to Detect Security Incidents in the Internet of Things. IJCNIS. 2015 Dec; 7(3):131-137.
2. Xingyuan W, Siwei W, Yingqian Z, Kang G. A novel image encryption algorithm based on chaotic shuffling method. Inf. Secur. J. 2017 Feb; 26 (1):7-16.
3. Chen J, Zhu Zhi-liang, Zhang Li-bo, Zhang Y, Yang Ben-qiang. Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption. Signal Process.; 2018; 142: 340-353
4. Ming X, Zihong T. A novel image cipher based on 3D bit matrix and latin cubes. Inf. Sci. 2019; 478:1-14
5. Xuncai Z, Feng H, Ying N. Chaotic Image Encryption Algorithm Based on Bit Permutation and Dynamic DNA Encoding. Computational Intelligence and Neuroscience. Volume 2017, Article ID 6919675, 11 pages.
6. Dong-dai L, Wei Z, Hai Y, Zhi-liang Z. An image encryption scheme using self-adaptive selective permutation and inter-intra-block feedback diffusion. Signal Process.. 2018 Oct; 151: 130-143. Available from: https://doi.org/10.1016/j.sigpro.2018.05.008
7. Chong F, Gao-yuan Z, Mai Z, Zhe C, Wei-min L. A New Chaos-Based Color Image Encryption Scheme with an Efficient Substitution Keystream Generation Strategy. Secur. Commun. Netw. 2018 Feb; 2018:1-13. Available from: https://doi.org/10.1155/2018/2708532
8. Ruisong Y. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Opt. Commun. 2011; 284(22): 5290-5298.
9. Hraoui S, Gmira F, Abbou FM, Jarrar AO, Jarjar A. A Chaotic Cryptosystem for Color Images Using Pixel-Level and Bit-Level Pseudo-Random Permutations. In:The Proceedings of the Third International Conference on Smart City Applications 2018 Oct 10 (pp. 481-491). Springer, Cham.
10. Jun-xin C, Zhi-liang Z, Chong F, Hai Y. An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism. Opt. Express. 2013; 21(23): 27873-27890.
11. Guangfeng C, Chunhua W, Hua C. A Novel Color Image Encryption Algorithm Based on Hyperchaotic System and Permutation-Diffusion Architecture. Int J Bifurcat Chaos . 2019; 29(09): 1950115.
12. Rasul E, Abdul HA, Ismail F I, Ayman A, Malrey L. Image encryption using a synchronous permutation-diffusion technique. Opt Lasers Eng. 2017; 90: 146-154.
13. Xingyuan W, Hongyu Z, Le F, Xiaolin Y, Hao Z. High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices. Opt Lasers Eng. 2019; 122:225-238. Available from: https://doi.org/10.1016/j.optlaseng.2019.04.005
14. Nawel B, Zahir A, Aissa B, Selma B. Image encryption using a combination of Grain-128a algorithm and Zaslavsky chaotic map. IET Image Processing. 2020; 14(6): 5-11. DOI: 10.1049/iet-ipr.2019.0671.
15. Abdalla M, Mihir B. Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-keying Techniques. ASIACRYPT 2000. Lecture Notes in Computer Science book series. Springer-Verlag, 2000 Dec; 1976: 546-559.
16. TownSendSecurity.com. Introduction to AES Encryption: White Paper, 2016. (online) Available at https://townsendsecurity.com/sites/default/files/AES_Introduction.pdf.
17. William s. Cryptography and network security principles and practice. Pearson. United States of America, 2011, p. 900.
18. Chen G, Mao Y, Chui CK. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons and Fractals. 2014; 21:749–761.
19. Socek D, Li S, Magliveras SS, Furht B. Short paper: Enhanced 1-d chaotic key-based algorithm for image encryption. InFirst International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05) 2005 Sep 5 (pp. 406-407). IEEE.
20. Mansour I, Chalhoub G, Bakhache B. Evaluation of a fast symmetric cryptographic algorithm based on the chaos theory for wireless sensor networks. In2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications 2012 Jun 25 (pp. 913-919). IEEE.

Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
Published Online First: February 2021 **E-ISSN: 2411-7986**

تشفير فعال للصور باستخدام مخطط خلط ديناميكي وغير خطي

رشيد ريماني[1،2*] نعيمة حاج سعيد[1] عدة علي باشا[1] جوان انتونيو لبز رموس[3]

[1] قسم الإلكترونيات ، كلية الهندسة الكهربائية ، جامعة العلوم والتكنولوجيا بوهران ، محمد بوضياف ، - USTOMBص 1505 .وهران منوار 31000 ، الجزائر.
[2] قسم العلوم والتكنولوجيا ، كلية العلوم والتكنولوجيا ، جامعة مصطفى ستامبولي - معسكر - ص.ب .ب 305 طريق المامونية ، معسكر 29000 ، الجزائر
[3] قسم الرياضيات، كلية الرياضيات والاعلام الالي، جامعة ألميريا – صندوق بريد 04120 لكانيادا، ألميريا، إسبانيا

الخلاصة:

تقدم هذه الورقة مخطط نشر سري جديد يسمى نظام التشفير بالمجموعة (RKP) والذي يرتكز على أساس التقليب غير الخطي، الديناميكي والعشوائي لتشفير الصور حسب الكتلة، حيث تعتبر الصور بيانات معينة بسبب حجمها ومعلوماتها، والتي هي ذات طبيعة ثنائية الأبعاد وتتميز بالتكرار العالي والارتباط القوي. أولاً، يتم حساب جدول التقليب وفقًا للمفتاح الرئيسي والمفاتيح الفرعية. ثانيًا، سيتم إجراء خلط وحدات البكسل لكل كتلة سيتم تشفيرها وفقًا لجدول التقليب. بعد ذلك، نستخدم خوارزمية تشفير AES في نظام التشفير عن طريق استبدال التقليب الخطي لمرحلة تحول الصفوف، بالتناوب غير الخطي والسري لمخطط RKP؛ هذا التغيير يجعل نظام التشفير يعتمد على المفتاح السري ويسمح لكلاهما باحترام نظرية شانون الثانية ومبدأ كيرشوف. يوضح تحليل الأمان لنظام التشفير أن مخطط الانتشار المقترح لـ RKP يعزز حصن خوارزمية التشفير، كما يمكن ملاحظته في الانتروبيا والقيم الأخرى التي تم الحصول عليها.

الكلمات المفتاحية: نظام التشفير بالمجموعة، تقنية الخلط، تشفير الصور، جدول التقليب، مفتاح التقليب في كل شوط