Performance Comparison of ACM and GRP Methods for Image Permutation

H. OĞRAŞ and Ş. FIDAN

Abstract— **Permutation and substitution processes of an image are most widely used in image encryption algorithms as they are thought to increase system security in cryptography. Permutation is the first process that all pixel positions in an image are shuffled in specific order or randomly in order to break strong correlation between adjacent pixels. Secondly, substitution is used to change pixel values by mixing a secret key in the permutated image. In an ordinary image, adjacent pixels have close values, so they have strong correlation and this correlation needs to be broken effectively before encryption. The degree to which this process is performed, directly affects overall system security. In this paper, performance evaluations for Group (GRP) and Arnold's Cat Map (ACM) methods are analyzed through some numerical results and their performances are compared to figure out which one is better. Experimental results consist of numerical and visual results determined in Matlab R2015a.**

Index Terms— **Image; GRP; Arnold's Cat Map; Confusion; Logistic Map**

I. INTRODUCTION

IN IMAGE cryptosystems, permutation-substitution structure is the most widely used architecture for image encryption algorithms [1-3]. After the first presentation by Fridrich in 1998, lots of studies about this structure have been proposed in image cryptography [4-8]. In most of these studies, it is emphasized that pixel positions of a source image should be replaced to another position before the encryption process for security improvements. In most ordinary image, any given pixel value can be easily predicted from the values of its neighbors. According to the Shannon's requirements, permutation and substitution are two basic processes to obscure high redundancies in an image and strong correlation of pixels in that image [7,9,10]. In order to achieve this situation, researchers use image permutation techniques to enhance security of their encryption algorithms.

Due to simplicity and effectiveness, ACM is one of the most frequently used methods in chaos-based image encryption systems by researchers [11-14].The function of ACM method is that image rotates continuously resulting in a form that is not visible by the naked eye. In addition, it has a characteristic of area-preserving which means that if it is iterated enough times, then the original image reappears. Another permutation method to be examined in this paper is GRP. GRP is an important bit permutation technique in cryptography which changes the position of bits in a given sequence by employing a control bit [15]. Permutation performances between these two methods are compared in detail in this study. In this sense, average moving distance of scrambling (AMDS), number of equal pixel rate (NEPR) and correlation coefficient of adjacent pixels are considered to compare the performance of both permutation methods. The rest of the paper is organized as follows: Section 2 gives the brief overview of GRP and ACM methods. Section 3 introduces chaotic Logistic map that is used to be a control bit generator for GRP. Performance comparison of both methods is analyzed in Section 4. Finally, the conclusions are discussed.

II. MATERIALS AND METHODS

In this section, two mentioned methods for pixel replacement in an image are introduced. Then, some explanations and techniques are given about how to generate control bit from using Logistic map for GRP method. Some mathematical tests of AMDS, NEPR and CCAP are explained briefly which are used to compare performances of both methods.

A. ACM Method

ACM is a simple and invertible discrete system that is defined in (1).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{1}$$

Here, (x, y) is pixel position of the source image sized in NxN and (x', y') refers corresponding pixel position. p and q are control parameters of the system which are positive integers. The inverse of ACM is determined in (2).

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \bmod N \tag{2}$$

ACM can be used as a permutation method for any image. In this technique, permutation process focuses on the position of

HİDAYET OĞRAŞ, is with Vocational School of Technical Sciences, Electronic-Communication Programming, University of Batman, Batman, Turkey, (e-mail: hidayet.ogras@batman.edu.tr).
https://orcid.org/0000-0001-9624-7400

ŞEHMUS FİDAN, is with Vocational School of Technical Sciences, Electronic Programming, University of Batman, Batman, Turkey, (e-mail: sehmus.fidan@batman.edu.tr). https://orcid.org/0000-0002-5249-7245

Manuscript received December 30, 2019; accepted June 03, 2020.
DOI: 10.17694/bajece.667740

pixels not the pixel values in the image. In mathematically, ACM is a linear transformation with simple mod operation.

B. GRP Method

GRP method has two inputs named as data and control bits. In this technique, input data is swapped according to the control bit. Here, input data values are placed in two groups as a left group and a right group. According to the control bit, if bit i of the control bit is 0, then the value of i in data goes to the left group, otherwise it goes to the right group. This process is performed in sequential until all the control bits is checked and relative positions of the input data within the same group do not change. Figure 1 shows as an example of how the GRP instruction works on 8-bit systems.

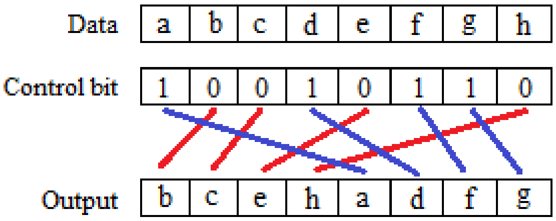

Figure 1. 8-bit GRP operation

C. Logistic Map

Logistic map is a simple non-linear discrete system [16]. It consists of an iterative equation as defined in (3).

$$x_{n+1} = r.x_n(1 - x_n) \tag{3}$$

Here, r is the control parameter and chosen as $0 < r \leq 4$; x_n is state variable of the map. For any initial value under $x_0 \in (0,1)$, the map generates sequence of values in the range of (0,1). Logistic map has very rich dynamic behaviors such as stationary, periodic and chaotic depending on control parameter. When $r \in [3.57, 4]$, then the generated sequence is aperiodic, non-convergent and very sensitive to initial value which leads to chaos and resulting very complicated and unpredictable behavior. Bifurcation diagram of the Logistic map is shown in Figure 2.

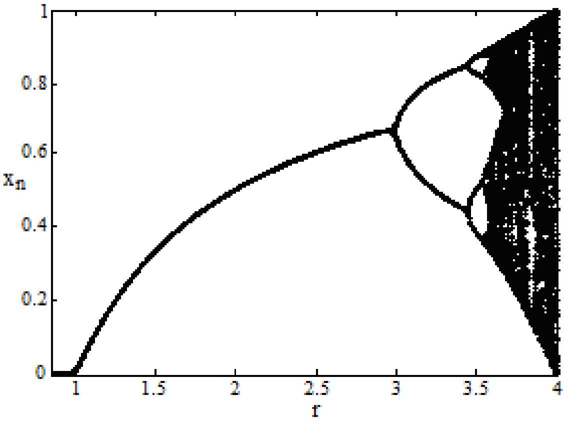

Figure 2. Bifurcation diagram of the Logistic map

D. AMDS Test

In image processing, main purpose of a permutation is to change pixel positions of an image through a specific algorithm so original pixel positions need to be moved to another positions. If a pixel has been moved farther away comparing to its original location, then the degree of permutation is higher [17]. This process can change the visuality of an image although it does not affect pixel values. The average moving distance of scrambling is defined as in (4).

$$AMDS = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \sqrt{(w-i)^2 + (v-j)^2} \tag{4}$$

In (4), (i, j) represents original pixel coordinate in an image with a size of $(M \times N)$ and (w, v) represents permutated pixel coordinate. In ACM method, pixel positions change in diagonal direction so AMDS test can be used to calculate the displacement of pixel positions for this method. On the other hand, in GRP method, pixel positions change in one direction only. Therefore, for each line of the permutated image, position change of the pixels is calculated separately then average distance value is calculated as in (5).

$$ADS = \frac{1}{M} \sum_{l=1}^{M} D_l \tag{5}$$

For instance, means coordinate changes for the pixel address of (1,1:M) between original and permutated image. The larger value of AMDS or average distance of scrambling (ADS) means that less relation between the original image and permutated image and also higher efficiency of the permutation method. For a square image with 256 size, universal mean of the average moving distance for random permutation is 256/3=85.3 [17]. This value can be used as a criterion to compare the efficiency of the permutation for both methods.

E. NEPR Test

NEPR is related to number of the same pixel values found in specific coordinates between the original image and permutated image. It is measured in percent and defined in (6).

$$NEPR(O,S) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left[T\left(O(i,j), S(i,j)\right) \right] \times 100\% \tag{6}$$
$$T\left(O(i,j), S(i,j)\right) = \begin{cases} 1 & , \quad O(i,j) = S(i,j) \\ 0 & , \quad O(i,j) \neq S(i,j) \end{cases}$$

NEPR shows the rate of identical pixel values at the same position between original and permutated images. If NEPR value is high, then efficiency of the scrambling is lower. If NEPR is zero, then no pixel values are equal at the same coordinate.

F. CCAP Test

In an ordinary image, an arbitrarily chosen pixel is strongly correlated with its adjacent pixels either they are vertically, horizontally or diagonally oriented.

$$cc = \frac{\sum_{i=1}^{N}(x_i - \bar{x}).(y_i - \bar{y})}{\sqrt{\left(\sum_{i=1}^{N}(x_i - \bar{x})^2\right)\left(\sum_{i=1}^{N}(y_i - \bar{y})^2\right)}} \quad (7)$$

This correlation needs to be broken after permutation process. Consequently, in the case of high-performance permutation methods, correlation coefficients of adjacent pixels are expected to be close to zero. The formula of the correlation coefficient is defined in (7).

The formula given in (7) returns a value between -1 and 1. Correlation coefficient of 1 means a strong positive relationship between two variables. Correlation coefficient of -1 indicates that for every positive increase in one variable, there is a negative decrease of proportion in the other. 0 means no relationship between two variables.

G. *Generating Control Bit*

GRP method uses a sequential control bit for data replacement. In this study, chaotic Logistic map is used to generate control bit for GRP method. In order to get a sequential bit, a map equation in (8) is utilized.

$$control\_bit = \begin{cases} 0 \ , & x_n < 0.5 \\ 1 \ , & x_n \geq 0.5 \end{cases} \quad (8)$$

Using (8), a control bit value of '1' or '0' is generated for each $x_n$which is the output of Logistic map. For instance, generated bit values are listed in Table 1, when the system parameters are selected as x_0=0.1234 and r=4.

TABLE I

GENERATING BIT VALUES USING LOGISTIC MAP

Log. Map Output	0.4327	0.981	0.0712	0.2644	0.7781	0.6907	0.8545	0.4974
Output of the (8)	0	1	0	0	1	1	1	0

III. Experimental Results

In this section, test image of 'Peppers' with different size is used for the performance evaluation of both permutation methods. Since both permutation methods depend on pixel positions rather than pixel values, the meaning of the test image does not have much importance. However, the size of the test images may affect results of the performance analysis for both methods. In some analysis, test images with different size are taken into consideration for the performance comparison. The performances of the both methods are also compared with different iterations of permutation operation.

A. *Visual Analysis*

'Peppers' test image with 256x256 size is used for visual analysis. Figure 3 shows the results of ACM method applied on the test image for different number of iteration (n) with randomly selected parameters of p=5 and q=4.

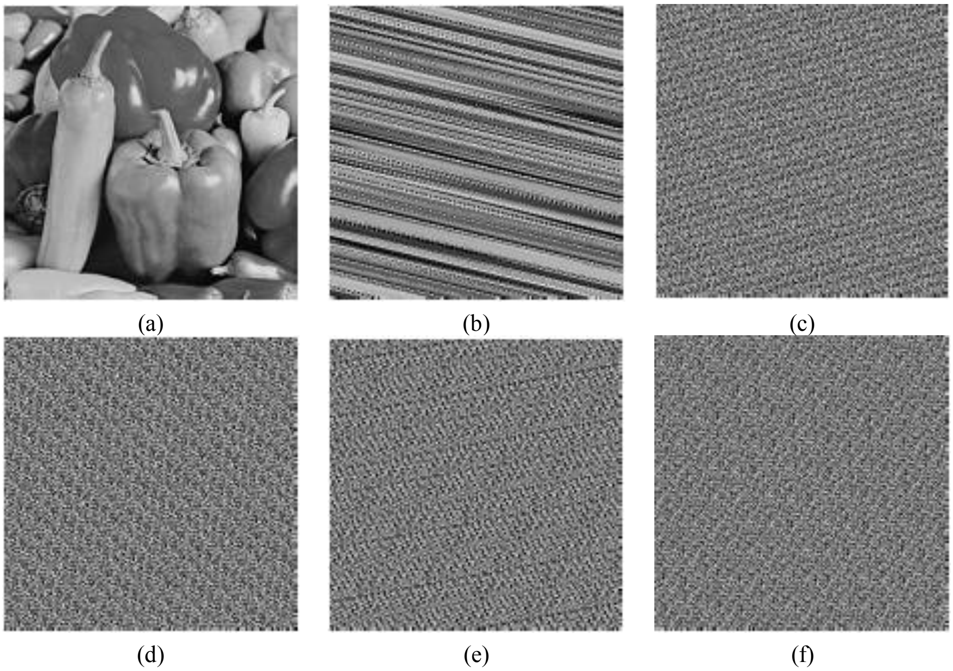

Figure 3. Results of ACM for 'Peppers' image with different number of iterations: (a) n=0 (b) n=1 (c) n=3 (d) n=8 (e) n=15 (f) n=40

Figure 4 shows the results of applying GRP-256 bit method on the ‘Peppers’ image for different number of n.

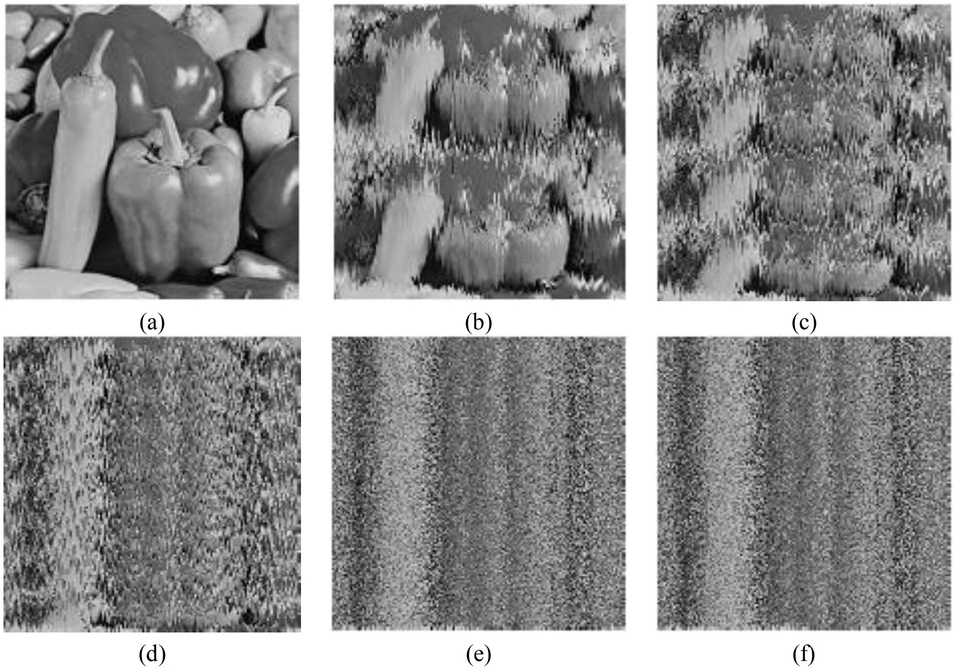

Figure 4. Results of GRP-256 bit for Peppers image with different number of iterations: (a) n=0 (b) n=1 (c) n=2 (d) n=3 (e) n=15 (f) n=40.

According to the results of Figure 3, in ACM method the test image becomes meaningless after the first iteration. This provides sufficient and effective permutation with only one iteration of the test image. On the other hand, GRP-256 bit method makes the test image meaningless completely at the end of the 3th iteration, so in GRP method, iterations must be done several times for enough complexity. It is concluded that for visual analyses, ACM shows better performance than the GRP-256 bit method.

B. AMDS Analysis

Test images with different size are used to determine AMDS values for ACM and GRP methods. AMDS values are calculated for different number of iterations for ACM and the results are listed in Table 2.

TABLE II

AMDS VALUES FOR ACM METHOD

Image size	ACM (p=1; q=1)	Number of iterations				
		n=1	n=2	n=3	n=4	n=5
128x128	AMDS	69.2	67.3	66.9	66.7	66.7
256x256	AMDS	**138.5**	**134.6**	**133.8**	**133.5**	**133.4**
512x512	AMDS	277.0	269.2	267.7	267.0	266.9

TABLE III

ADS VALUES FOR GRP METHOD

Image size	GRP	Number of iterations				
		n=1	n=2	n=3	n=4	n=5
128x128	ADS	37.1	39.2	40.4	41.8	43.0
256x256	ADS	63.6	78.1	81.7	83.9	**87.2**
512x512	ADS	127.9	156.0	159.8	163.2	167.1

ADS values are calculated for test images with different sizes and number of iterations for GRP method. Results are listed in Table 3.

According to the Table 2 results, AMDS values decrease slightly as the number of iterations increases in ACM method. However, the calculated values (written in bold) are significantly higher than the critical level. This indicates a sufficient permutation of the ACM method. On the other hand, according to the Table 3, the values obtained from GRP are much lower than the ACM values for all iterations. Furthermore, if the number of iteration increases, then ADS value also increases significantly. Hence, enough number of iterations is needed for effective permutation in GRP method. For instance, an image with a size of 256x256 requires 5 iterations for ADS to be greater than the critical value of 85.3. In addition, as the size of the test images increases, both AMDS and ADS values also increase proportionally. As a result, in ACM method, the degree of displacement of pixel positions is much better than the GRP method.

C. *NEPR Test*

After an effective permutation process, number of equal pixels for the same pixel coordinates between original and permutated images should be very low. NEPR test is applied for ACM method for different iterations of the permutated version of the image and results are listed in Table 4.

TABLE IV
NEPR VALUES FOR ACM METHOD

Image size	**ACM (p=1; q=1)**	**Number of iterations**				
		n=1	n=2	n=3	n=4	n=5
128x128	NEP	83	93	108	109	112
	Rate (%)	**0.51**	0.57	0.66	0.66	0.68
256x256	NEP	345	367	417	396	404
	Rate (%)	0.53	0.56	0.64	0.60	0.62
512x512	NEP	1802	1811	2003	2157	2059
	Rate (%)	0.69	0.69	0.76	0.82	0.78

TABLE V
NEPR VALUES FOR GRP METHOD

Image size	**GRP**	**Number of iterations**				
		n=1	n=2	n=3	n=4	n=5
128x128	NEP	537	578	603	649	592
	Rate (%)	3.28	3.53	3.68	3.96	3.61
256x256	NEP	1714	1696	1794	1859	1759
	Rate (%)	2.62	2.59	2.74	2.84	2.68
512x512	NEP	5953	5812	5792	6067	5825
	Rate (%)	2.27	2.22	**2.21**	2.31	2.22

NEPR values are calculated for test images having different sizes for GRP method. Results are listed in Table 5.

According to the NEPR results for both methods, the overall performance of ACM is better than the GRP. For ACM method, the minimum NEPR value occurs in the first iteration of a 128x128 image, while in GRP method, the minimum NEPR value occurs in the third iteration of the 512x512 test image. This confirms that ACM method has a great permutation effect on the test image for small number of iterations. In addition, GRP requires several times of iteration for sufficient permutation of the test image. All NEPR results in GRP are significantly bigger than the results of ACM for all sizes and number of iterations.

D. *CCAP Test*

In a good permutated image, an arbitrarily chosen pixel is weakly correlated with its adjacent pixel. Correlation coefficient value between original and permutated images should be small in an effective permutation. ACM and GRP methods are applied to the test image of ‘Peppers’ and then CCAP test is performed in vertical (V), horizontal (H) and diagonal (D) directions to compare the performance of both methods. The average results are listed in Table 6 and Table 7. Minimum values of CCAP are written in bold.

TABLE VI

CCAP VALUES FOR ACM METHOD

Image size	ACM (p=1; q=1)	Direction	Number of iterations				
			n=1	n=2	n=3	n=4	n=5
128x128	CCAP	V	-0.3243	-0.1071	0.1582	-0.0452	0.1299
		H	0.0164	-0.3370	**0.0091**	0.2463	0.1251
		D	-0.1144	-0.2151	-0.1077	-0.0674	**-0.0496**
256x256	CCAP	V	-0.3116	-0.1112	0.1744	-0.0647	0.0838
		H	**0.0323**	-0.3386	-0.0688	0.1711	0.0741
		D	-0.1289	-0.1891	-0.1400	**-0.0983**	-0.1035
512x512	CCAP	V	-0.3569	0.1041	0.0535	-0 0301	**0.0195**
		H	0.0318	0.0613	-0.1473	**0.0132**	-0.0568
		D	-0.1123	**-0.0082**	-0.1317	-0.0546	-0.0856

TABLE VII

CCAP VALUES FOR GRP METHOD

Image size	GRP	Direction	Number of iterations				
			n=1	n=2	n=3	n=4	n=5
128x128	CCAP	V	0.1319	-0.1014	**0.0389**	0.0410	-0.1776
		H	0.0858	0.3265	0.4179	0.3992	0.2571
		D	0.3420	0.2472	0.0983	0.1953	0.0776
256x256	CCAP	V	0.1082	-0.0977	**-0.0292**	0.1042	0.1088
		H	0.1296	0.0899	0.1784	0.2803	0.3324
		D	0.3142	0.1473	0.1153	0.2484	0.1846
512x512	CCAP	V	0.2721	-0.1169	-0.1040	-0.0513	0.0552
		H	0.1240	0.1160	0.1616	0.1838	0.2292
		D	0.4996	0.2458	0.1757	0.2370	0.1674

According to the CCAP test results, ACM method shows better performance than GRP method. If all numerical and visual analyses are considered for both methods, ACM is a better choice against GRP in order to break correlation of adjacent pixels in an image.

IV. CONCLUSIONS

In this paper, performance evaluation of two important permutation methods used in image processing are concerned in order to compare their performances through visual and numerical analyses. In both visual and numerical analyses, ACM method shows better performance than the GRP method. AMDS and NEPR test results are critical points under the numerical analyses for the performance evaluation of the both methods. These results demonstrate that ACM changes pixel positions more effective as well as bigger in size with respect to the GRP method for all iterations. Although the total displacement of pixels is smaller in the GRP method, the average pixel distance between the previous and next iteration of the permutation are bigger than the ACM method.

REFERENCES

[1] Patidar, V., Pareek, N. K., Purohit, G., & Sud, K. K. (2011). A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. *Optics communications*, *284*(19), 4331-4339.

[2] Enayatifar, R., Abdullah, A. H., Isnin, I. F., Altameem, A., & Lee, M. (2017). Image encryption using a synchronous permutation-diffusion technique. *Optics and Lasers in Engineering*, *90*, 146-154.

[3] Huang, L., Cai, S., Xiong, X., & Xiao, M. (2019). On symmetric color image encryption system with permutation-diffusion simultaneous operation. *Optics and Lasers in Engineering*, *115*, 7-20.

[4] Belazi, A., El-Latif, A. A. A., & Belghith, S. (2016). A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing*, *128*, 155-170.

[5] Patro, K. A. K., & Acharya, B. (2019). An efficient colour image encryption scheme based on 1-D chaotic maps. *Journal of Information Security and Applications*, *46*, 23-41.

[6] Huang, H., He, X., Xiang, Y., Wen, W., & Zhang, Y. (2018). A compression-diffusion-permutation strategy for securing image. *Signal Processing*, *150*, 183-190.

[7] Oğraş, H., & Türk, M. (2017). A Robust Chaos-Based Image Cryptosystem with an Improved Key Generator and Plain Image Sensitivity Mechanism. *J. Inf. Secur*, *8*, 23-41.

[8] Patro, K. A. K., & Acharya, B. (2018). Secure multi–level permutation operation based multiple colour image encryption. *Journal of information security and applications*, *40*, 111-133.

[9] Ping, P., Xu, F., Mao, Y., & Wang, Z. (2018). Designing permutation–substitution image encryption networks with Henon map. *Neurocomputing*, *283*, 53-63.

[10] Oğraş, H., & Türk, M. (2016). A Secure Chaos-based Image Cryptosystem with an Improved Sine Key Generator. *American Journal of Signal Processing*, *6*(3), 67-76.

[11] Chen, F., Wong, K. W., Liao, X., & Xiang, T. (2014). Period distribution of generalized discrete Arnold cat map. *Theoretical Computer Science*, *552*, 13-25.

[12] Abbas, N. A. (2016). Image encryption based on independent component analysis and arnold's cat map. *Egyptian informatics journal*, *17*(1), 139-146.

[13] Chai, X., Fu, X., Gan, Z., Lu, Y., & Chen, Y. (2019). A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Processing*, *155*, 44-62.

[14] Dhall, S., Pal, S. K., & Sharma, K. (2018). A chaos-based probabilistic block cipher for image encryption. *Journal of King Saud University-Computer and Information Sciences*.

[15] Nazari, S., Moin, M. S., & Kanan, H. R. (2016). A face template protection approach using chaos and GRP permutation. *Security and Communication Networks*, *9*(18), 4957-4972.

[16] Hua, Z., & Zhou, Y. (2016). Image encryption using 2D Logistic-adjusted-Sine map. *Information Sciences*, *339*, 237-253.

[17] Xiangdong, L. I. U., Junxing, Z., Jinhai, Z., & Xiqin, H. (2008). Image scrambling algorithm based on chaos theory and sorting transformation. *IJCSNS International Journal of Computer Science and Network Security*, *8*(1), 64-68.

BIOGRAPHIES

HIDAYET OGRAS received his Ph.D degree in Electrical and Electronics Engineering from the University of Firat, Elazig, Turkey, in 2017. He is currently an Assistant Professor at department of Electronics Communication in Batman University and his research interests cover chaos-based Cryptography and Steganography. He is also interested in Secure Communication Systems and Signal Processing.

FIDAN ŞEHMUS is an assistant professor at department of electronic technology in Batman University. He received his bachelor’s degree in Electric Education from University of Gazi, Ankara, Turkey. In 2010 he completed his graduate education at Afyon Kocatepe University, Turkey. He received Ph.D. degree in Electrical and Electronics Engineering from the University of Firat, Elazig, Turkey, in 2018. His works focuses control systems and power electronics of Wind Turbine. He is also interested in machine learning and its real application.