İSTANBUL UNIVERSITY
CERRAHPAŞA

RESEARCH ARTICLE
Electrica 2021; 21(2): 209-215

Comparative Analysis of the Effects of Chaotic Systems on the Robustness of Image Encryption

Melih Yıldırım

The Scientific and Technological Research Council of Turkey (TUBITAK), Ankara, Turkey

Cite this article as: M. Yıldırım, "Comparative Analysis of the Effects of Chaotic Systems on the Robustness of Image Encryption", Electrica, vol. 21, no. 2, pp. 209-215, May, 2021.

ABSTRACT

In this study, we carried out a comparative analysis to examine the effects of various chaotic systems on the robustness of image encryption. To do that, a chaotic-system-based encryption scheme was used. Different kinds of chaotic systems such as sine map, logistic map, and tent map have been used to understand the effects of chaotic systems on encryption. In the encryption scheme, confusion and diffusion processes have been performed. Row- and column-based scrambling algorithms have been used for confusion, whereas simplified modulo-operation-based algorithm has been used for diffusion. In the analysis part, the correlation of two neighboring pixels and entropy are calculated to understand the effects of three different chaotic maps. Furthermore, numerous tests such as parameter value sensitivity, initial condition sensitivity, robustness against noise, robustness against data loss, and chi-squared test have been done to evaluate the performances of chaotic systems. All analyses in this study have been carried out in MATLAB environment.

Keywords: Chaotic system, image encryption, robustness

Corresponding Author:
Melih Yıldırım

E-mail:
melih.yildirim@tubitak.gov.tr

Received: March 18, 2021

Accepted: April 5, 2021

Available Online Date:
May 20, 2021

DOI: 10.5152/electrica.2021.21027

Introduction

With rapid improvements in information technology, ensuring secure transmission of digital data has become an important issue [1-3]. The image or video data should be encrypted for maintaining the security in data transfer [4]. Numerous image encryption schemes have been proposed in literature to achieve that [1, 5-20], among which are chaotic-system-based image encryption schemes [1, 5-16, 20].

Typically, an image encryption algorithm includes two stages that are confusion and diffusion [1]. Confusion phase can be performed by pixel position permutation, whereas diffusion phase can be carried out by pixel value transformation [15].

In this study, the effects of various chaotic systems on the robustness of image encryption have been examined. For this purpose, three chaotic systems that are sine map, logistic map, and tent map have been used. Analyses, including adjacent pixel correlation, information entropy, initial condition value sensitivity, parameter value sensitivity, robustness against noise, robustness against data loss, and chi-squared test have been carried out to determine the performance of the chaotic systems.

Chaotic-map-based image encryption scheme

A chaotic-system-based encryption algorithm to cipher the image has been used in this study. Three chaotic maps that are sine map, logistic map, and tent map have been employed in the encryption algorithm.

Sine map can be described by equation (1) [8].

$$X_{n+1} = b\sin(\pi X_n)/4 \tag{1}$$

where b $\in$ (0, 4], $X_n \in$ (0, 1), and the initial value $X_0 \in$ (0, 1).

Logistic map can be defined by equation (2) [8].

$$X_{n+1} = rX_n(1 - X_n) \quad (2)$$

where r $\in$ (0, 4], $X_n \in$ (0, 1), and the initial value $X_0 \in$ (0, 1).

Tent map can be described by equation (3) [2].

$$X_{n+1} = \begin{cases} \mu X_n, & \text{if } X_n < 0.5 \\ \mu(1 - X_n), & \text{if } X_n \geq 0.5 \end{cases} \quad (3)$$

where $\mu \in$ (0, 2], $X_n \in$ (0, 1), and the initial value $X_0 \in$ (0, 1).

In the encryption scheme, there are two stages such as confusion and diffusion. Row- and column-based scrambling algorithms have been used to perform permutation operation with regard to pixel positions in the plain image as confusion, and a modulo-based diffusion algorithm has been simplified in this study [21].

Row-scrambling-based confusion

Parameter value and initial value belonging to the corresponding chaotic map are chosen. For the plain image of size $M \times N$, the iteration of chaotic maps were done as given in equations (1-3). *C* was calculateshown in equation (4) and different *M* different values were generated.

$$c = \text{mod}\,(\text{round}(X_n \times 10^{14}), 256) \quad (4)$$

where mod denotes modulo operation and round operation rounds a numeric number to its closest integer. The sequence *c* is sorted and then the new sequence *d* depending on the indices of elements of sequence *c* is generated. $d = \{d_1, d_2, \ldots, d_M\}$. The rows of plain image depending on *d* are rearranged. Carry the d_1 row to the first row, d_2 row to the second row, and so on. *M* rows according to *d* are carried [21].

Column-scrambling-based confusion

After row scrambling is completed, a similar operation is performed for the columns of the image. We erase the sequence *c* to generate a new sequence and continue to do the iteration of chaotic maps given in equations (1-3), *c* was calculated as shown in equation (4), and different values of $M \times N$ obtained. The sequence *c* is sorted, and then the new sequence *e* depending on the indices of elements of sequence *c* is generated. $e_{ixj} = \{e_{1\times1}, e_{1\times2}, \ldots, e_{M\times N}\}$, (i = 1,2,…,M), (j=1,2,…,N). The columns of each row of the image depending on e_{ixj} are rearranged. Carry the e_{ix1} column of the i^{th} row to the first column, e_{ix2} column of the i^{th} row to the second column, and so on. *N* columns of each row of the image depending on to e_{ixj} are carried [21].

Modulo-operation-based diffusion

After confusion stage is completed, diffusion stage is carried out. In this study, we simplified the modulo-operation-based diffusion operation given in [21]. The modulo operation used as diffusion operation had only two terms in the suggested study, whereas the modulo-based diffusion algorithm given in [21] included four terms. The diffusion equation used in this study is presented in equation (5).

$$C_{i\times j} = \text{mod}((C_{i\times j} + e_{i\times j}), 256) \quad (5)$$

where C_{ixj} is the current ciphered value of the pixel. By using equation (5), pixel value transformation throughout the image was performed.

Analysis results

The results of the study were presented after performing numerous analyses, such as adjacent pixel correlation, information entropy, initial condition sensitivity, parameter sensitivity, robustness against noise, robustness against data loss, and chi-squared test. For each analysis, the impact of the chaotic system on the robustness of encryption is given.

Adjacent pixel correlation

A good encryption scheme should reduce the correlation coefficient between neighboring pixels, as the correlation coefficient between neighboring pixels of a plain image in vertical, horizontal, and diagonal directions is high [22]. To perform the analysis of correlation coefficient p_{xy}, the following equation is calculated [10, 23].

$$\rho_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}} \quad (6)$$

where cov(*x,y*)=[*x*-*E*(*x*)][*y*-*E*(*y*)] and $p_{xy} \in$ [0,1]. *E*(*x*) and *E*(*y*) are the average values of *x* and *y*, respectively, and *D*(*x*) and *D*(*y*) denote the standard deviations belonging to *x* and *y*, respectively. The lower the value of p_{xy}, the lower the correlation between neighboring pixels. Thus, the correlation for the encrypted image is supposed to be approximately zero. Table 1 gives the correlation coefficient values belonging to the plain images and the encrypted images for three chaotic maps. When we examine the effects of chaotic maps on the value of correlation, Table 1 reveals that tent map provides better performance with regard to vertical and horizontal coefficients, whereas the diagonal coefficient of sine-map-based encryption is lower compared with that of other chaotic maps.

Information entropy

The distribution of gray-scale values (0–255) for an image can be given by information entropy. High information entropy leads to a uniform distribution. The entropy of a source is calculated using equation (7) [22].

$$H(s) = -\sum_{i=0}^{N} p(s_i) \log_2 p(s_i) \quad (7)$$

Table 1. Correlation coefficients belonging to the plain image and the encrypted images for three chaotic maps

	Diagonal	Vertical	Horizontal
Plain image	0.9213	0.9727	0.9456
Logistic map	0.0054	0.0081	-0.0045
Sine map	0.0023	0.0072	0.0056
Tent map	0.0062	0.0001	-0.0012

Table 2 shows the entropy values belonging to the plain image and the encrypted images for three chaotic maps. The information value is calculated as 7.4318 for the plain image. For encrypted images, the information entropy values obtained are 7.9974, 7.9973, and 7.9971 using sine map, logistic map, and tent map, respectively. Therefore, sine-map-based encryption scheme leads to a more uniform distribution for the encrypted image.

Sensitivity to parameter and initial condition values

A efficient encryption algorithm should be highly sensitive to the initial condition and parameter values [24]. A slight alteration in secret parameter and initial condition values leads to a huge change in the decrypted image. It means that when the secret parameter value and initial condition value used in encryption and decryption phases are not equal, an identical decrypted image as the plain image cannot be obtained. Table 3 shows sensitivity to the initial condition and parameter values for different chaotic maps, namely sine, logistic, and tent maps. As can be seen from Table 3, all the chaotic maps have the same sensitivity, which is 10^{-15} to the parameter value of chaotic maps. However, sine- and tent-map-based encryption has more sensitivity to the initial condition value compared with logistic-map-based encryption. For example, in the logistic-map-based encryption, when we decrypt the encrypted image using the parameter value with only 10^{-15} difference compared with the value used in the encryption phase, the plain image cannot be obtained correctly. Similarly, in the logistic-map-based encryption, when we decrypt the encrypted image using the initial condition value X_0 with only 10^{-19} difference compared with the value used in the encryption phase, the plain image is not acquired appropriately.

Robustness to noise and data loss

In the transmission and processing stages of the encrypted image, data loss can occur in the encrypted image or noise can be added to it [10, 25]. To determine the behavior of the robustness of chaotic-map-based encryption scheme, we enabled data loss to the image and also corrupted it by noise. In the data loss analysis, we cropped the encrypted images at half and quarter degrees, given in Figures 1 and 2, respectively. In noise analysis, we added salt and pepper noise, including in-

Table 2. Information entropy values belonging to the plain image and the encrypted images for three chaotic maps

	Encrypted image		
Plain image	**Logistic map**	**Sine map**	**Tent map**
7.4318	7.9973	7.9974	7.9971

Table 3. Sensitivity to parameter and initial condition values for different chaotic maps

	Logistic map	Sine map	Tent map
Parameter value	10^{-15}	10^{-15}	10^{-15}
Initial condition value	10^{-19}	10^{-21}	10^{-21}

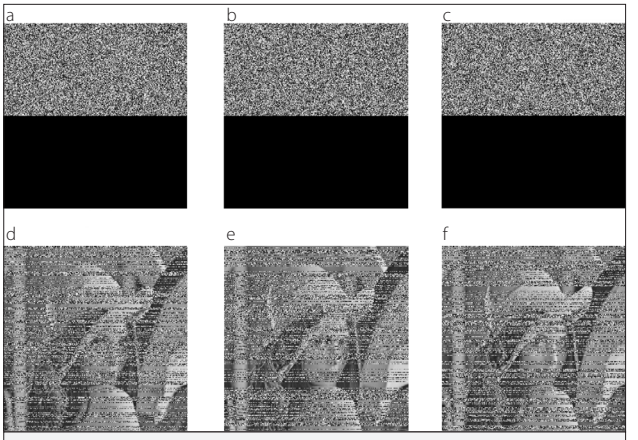

Figure 1. a-f. Encrypted images with 1/2-degree cropping (a) logistic map, (b) sine map, (c) tent map (d) decrypted image of (a), (e) decrypted image of (b), (f) decrypted image of (c)

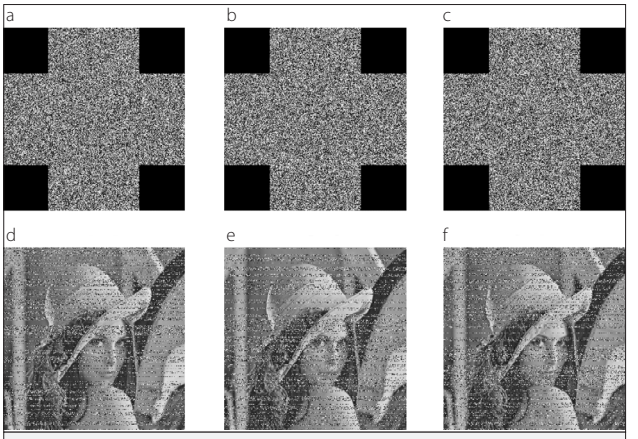

Figure 2. a-f. Encrypted images with 1/4 degree cropping (a) logistic map, (b) sine map, (c) tent map (d) decrypted image of (a), (e) decrypted image of (b), (f) decrypted image of (c)

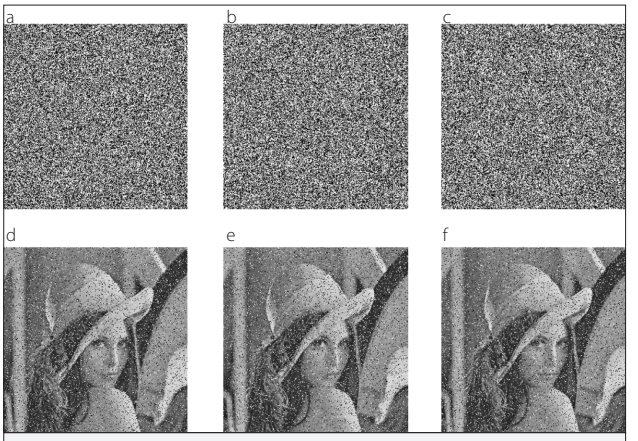

Figure 3. a-f. Encrypted images with noise strength of 0.2 (a) logistic map, (b) sine map, (c) tent map (d) decrypted image of (a), (e) decrypted image of (b), (f) decrypted image of (c)

tensity of 0.2 and 0.05 to the encrypted images using various chaotic maps given in Figures 3 and 4, respectively.

The effects of various chaotic maps on the robustness to data loss and noise are verified using parameters such as structural similarity index metric (SSIM), mean absolute error (MAE), mean squared error (MSE), and peak signal to noise ratio (PSNR). We compared the plain images with the decrypted images using these metrics. The formulas of parameters are given in equations (8-11) [25-27]. The equation for SSIM is presented in equation (8).

$$\text{SSIM} = \frac{(2\bar{x}\bar{y} + C_1)(2\sigma_{xy} + C_2)}{(\sigma_x^2 + \sigma_y^2 + C_2)((\bar{x})^2(\bar{y})^2 + C_1)} \quad (8)$$

where $\bar{x}$, $\bar{y}$, σ_x^2, σ_y^2, and σ_{xy} represent the average of the image for theoretical result, the average of the image for analysis result, the variance of the image for theoretical result, the variance of the image for analysis result, and the covariance of the images for theoretical result and analysis results, respectively. C_1 and C_2 are constant. The equation of MSE is presented as follows:

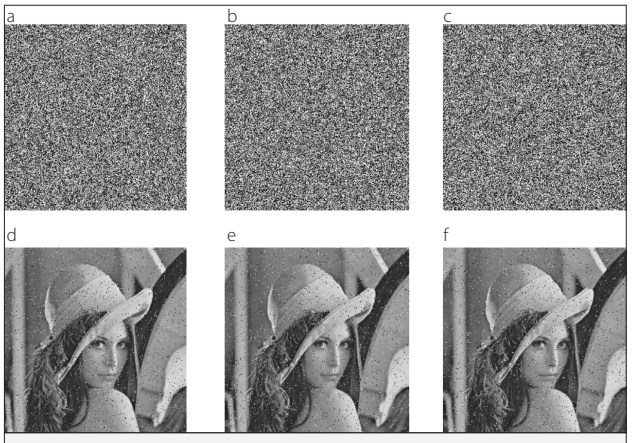

Figure 4. a-f. Encrypted images with noise strength of 0.05 (a) logistic map, (b) sine map, (c) tent map (d) decrypted image of (a), (e) decrypted image of (b), (f) decrypted image of (c)

$$\text{MSE} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j) - y(i,j))^2 \quad (9)$$

where M and N denote the width and height in the image. $x(i,j)$ and $y(i,j)$ indicate the theoretical result and analysis result, respectively. MAE can be calculated as follows:

$$\text{MAE} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}|x(i,j) - y(i,j)| \quad (10)$$

PSNR can be defined as given in equation (11).

$$\text{PSNR} = 10\log_{10}\frac{(2^8 - 1)^2}{\sqrt{\text{MSE}}} \quad (11)$$

where $x(i,j)$ is equal to $y(i,j)$, PSNR, MAE, MSE, and SSIM are calculated as ∞, 0, 0, and 1, respectively.

Table 4 demonstrates the quality measurement parameters to determine the robustness against data loss and noise in terms of chaotic maps used in the encryption. When we compare chaotic maps in terms of SSIM belonging to data loss analysis, it can be seen that the tent map for half degree cropping and logistic map for one-fourth degree cropping enable higher robustness. Similarly, when we compare chaotic maps in terms of SSIM belonging to noise analysis, it can be seen that tent map for the noise strength of 0.2 and logistic map for the noise strength of 0.05 provide higher robustness.

Chi-squared test

In this part of the study, chi-squared test was carried out to justify the uniformity of the histogram of the encrypted image [5, 20].

Table 4. Quality measurement parameters for the robustness analysis of data loss and noise

Analysis	Chaotic maps	SSIM	MSE	MAE	PSNR
1/2 degree cropping	Logistic map	0.0827	3.8354e+03	36.2755	12.2927
	Sine map	0.0872	3.8960e+03	36.5927	12.2246
	Tent map	0.0898	3.8695e+03	36.4659	12.2543
1/4 degree cropping	Logistic map	0.1791	1.9314e+03	18.2106	15.2720
	Sine map	0.1716	1.9397e+03	18.2283	15.2534
	Tent map	0.1777	1.9344e+03	18.1894	15.2653
Noise strength of 0.2	Logistic map	0.1853	1.5625e+03	14.7350	16.1926
	Sine map	0.1879	1.5544e+03	14.5854	16.2152
	Tent map	0.1915	1.5315e+03	14.4630	16.2797
Noise strength of 0.05	Logistic map	0.4609	378.2404	3.5670	22.3531
	Sine map	0.4565	404.7725	3.7351	22.0587
	Tent map	0.4466	404.4683	3.7911	22.0620

Table 5. Chi-squared test of the plain image and the encrypted images based on three chaotic maps

Plain image	Logistic map	Sine map	Tent map
4.1155e+04	247.5703	239.4922	262.6563

The chi-squared test can be defined as follows:

$$\chi^2 = \sum_{i=0}^{255} \frac{(q_i - q)^2}{q} \quad (12)$$

where q_i shows the occurrence frequency of the pixel value i in the image and q is expressed as follows:

$$q = \frac{M \times N}{256} \quad (13)$$

when the value of chi-squared is lower, the distribution of the encrypted image becomes more uniform. As can be clearly seen from Table 5, the encrypted image using sine map is more uniform compared with the encrypted images with other chaotic maps.

Conclusion

In this study, we compared the encryption schemes with various chaotic maps such as sine, logistic, and tent maps to evaluate the effects of chaotic systems on the robustness of image encryption. In the encryption scheme, row- and column-based scrambling algorithms for confusion and simplified modulo-operation-based algorithm for diffusion were used. We carried out numerous analyses, including adjacent pixel correlation, information entropy, initial condition value sensitivity, parameter value sensitivity, robustness against noise, robustness against data loss, and chi-squared test. In the adjacent pixel correlation analysis, sine and tent maps enabled better performance than that of logistic map. When we compared information entropy for the three chaotic maps, it was clear that sine map enabled higher robustness. All chaotic maps had same sensitivity in terms of secret parameter value; however, sine and tent maps provided more robustness in terms of initial condition sensitivity. Tent map offered more robustness for half degree data loss and noise strength of 0.2, whereas logistic map enabled more robustness for one-fourth degree data loss and noise strength of 0.05. Chi-squared test reveals that sine map enabled more uniformity in the encrypted image than other chaotic maps.

Peer-review: Externally peer-reviewed.

Conflict of Interest: The author have no conflicts of interest to declare.

Financial Disclosure: The author declared that this study has received no financial support.

References

1. X. Wang, L. Feng, H. Zhao, "Fast image encryption algorithm based on parallel computing system", Information Sciences, vol. 486 pp. 340-358, 2019 [Crossref]
2. C. Zhu, K. Sun, "Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps", IEEE Access vol. 6, pp. 18759-18770, 2018. [Crossref]
3. Y. Li, C. Wang, H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation", Optics and Lasers in Engineering, vol. 90, pp. 238-246, 2017. [Crossref]
4. Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-Box", Chaos, Solitons and Fractals, vol. 95, pp. 92-101, 2017. [Crossref]
5. Y. Xian, X. Wang, X. Yan, Q. Li, X. Wang, "Image Encryption Based on Chaotic Sub-Block Scrambling and Chaotic Digit Selection Diffusion", Optics and Lasers in Engineering, vol. 134, 2020. [Crossref]
6. M. Alawida, A. Samsudin, J. Sen Teh, R.S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption", Signal Processing, vol. 160, pp. 45-58, 2019. [Crossref]
7. Z. J. Huang, S. Cheng, L. H. Gong, N. R. Zhou, "Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform", Optics and Lasers in Engineering, vol. 124, pp. 105821, 2020. [Crossref]
8. Y. Zhou, L. Bao, C.L.P. Chen, "A new 1D chaotic system for image encryption", Signal Processing, vol. 97, pp. 172-182, 2014. [Crossref]
9. Z. H. Guan, F. Huang, W. Guan, "Chaos-based image encryption algorithm", Physics Letters A, vol. 346, pp. 153-157, 2005. [Crossref]
10. Q. Xu, K. Sun, C. Cao, C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map", Optics and Lasers in Engineering, vol. 121, pp. 203-214, 2019. [Crossref]
11. H. Liu, B. Zhao, L. Huang, "Quantum image encryption scheme using Arnold transform and S-box scrambling", Entropy, vol. 21, pp. 1-14, 2019. [Crossref]
12. M. Yildirim, "DNA Encoding for RGB Image Encryption with Memristor Based Neuron Model and Chaos Phenomenon", Microelectronics Journal, vol. 104, pp. 104878, Oct 2020. [Crossref]
13. L.G. Nardo, E.G. Nepomuceno, J. Arias-Garcia, D.N. Butusov, "Image encryption using finite-precision error", Chaos, Solitons & Fractals, vol. 123, pp. 69-78, 2019. [Crossref]
14. T. Abdeljawad, S. Banerjee, G. Wu, "Discrete tempered fractional calculus for new chaotic systems with short memory and image encryption", Optik, vol. 218, pp. 163698, 2020. [Crossref]
15. M. Yildirim, F. Kacar, "Chaotic Circuit with OTA based Memristor on Image Cryptology", AEÜ - International Journal of Electronics and Communications, 153490, 2020. [Crossref]
16. Z. Hua, S. Yi, Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion", Signal Processing, vol. 144, pp. 134-144, 2018. [Crossref]
17. T. Chuman, W. Sirichotedumrong, H. Kiya, "Encryption-then-compression systems using grayscale-based image encryption for JPEG images", IEEE Transactions on Information Forensics and Security, vol. 14, pp. 1515-1525, 2018. [Crossref]
18. Z. Hua, B. Xu, F. Jin, H. Huang, "Image encryption using josephus problem and filtering diffusion", IEEE Access, vol. 7, pp. 8660-8674, 2019. [Crossref]
19. H. Karmouni, M. Sayyouri, H. Qjidaa, "A novel image encryption method based on fractional discrete Meixner moments", Optics and Lasers in Engineering, vol. 137, pp. 106346, 2021. [Crossref]
20. M. Yildirim, "A color image encryption scheme reducing the correlations between R, G, B components", Optik, pp. 166728, 2021. [Crossref]
21. X. Wang, L. Teng, X. Qin, "A novel colour image encryption algorithm based on chaos", Signal Processing vol. 92, pp. 1101-1108, 2012. [Crossref]

22. C.K. Volos, I.M. Kyprianidis, I.N. Stouboulos, "Image encryption process based on chaotic synchronization phenomena", Signal Processing, vol. 93, pp. 1328-1340, 2013. [Crossref]
23. S. Kandar, D. Chaudhuri, A. Bhattacharjee, B.C. Dhara, "Image encryption using sequence generated by cyclic group", Journal of Information Security and Applications, vol. 44, pp. 117-129, 2019. [Crossref]
24. W. Liu, K. Sun, C. Zhu, "A fast image encryption algorithm based on chaotic map", Optics and Lasers in Engineering, vol. 84, pp. 26-36, 2016. [Crossref]
25. M. Yildirim, "Analog circuit implementation based on median filter for salt and pepper noise reduction in image", Analog Integrated Circuits and Signal Processing, pp. 1-8, 2021. [Crossref]
26. M. Yildirim, F. Kacar, "Adapting Laplacian based filtering in digital image processing to a retina-inspired analog image processing circuit", Analog Integrated Circuits and Signal Processing, vol. 100, pp. 537-545, 2019. [Crossref]
27. S. Karakus, E. Avci, "A new image steganography method with optimum pixel similarity for data hiding in medical images", Medical Hypotheses, vol. 139, pp. 109691, 2020. [Crossref]

Melih Yildirim received his B.Sc. in Electronics and Communication Engineering from Kocaeli University, Turkey; M.Sc. in Electromagnetics Design in Electrical and Electronics Engineering from the University of Nottingham, UK; and PhD in Electrical and Electronics Engineering from Istanbul University, Turkey, in 2010, 2013, and 2018, respectively. He was a recipient of the full scholarship granted by the Republic of Turkey, Ministry of National Education, during his postgraduate education. Currently, he is a scientific programs expert at The Scientific and Technological Research Council of Turkey (TUBITAK), Ankara, Turkey. His main research interests include analog circuits, memristive structures for bio-inspired circuit design, and neuromorphic architectures.