This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Chaotic map optimization for image encryption using triple objective differential evolution algorithm

Abdurrahim Toktas[1], Member, IEEE, Ugur Erkan[2], Feyza Toktas[3], Zeki Yetgin[3]
[1]Electrical and Electronics Engineering, Karamanoglu Mehmetbey University, 70200 Karaman TURKEY
[2]Computer Engineering Department, Karamanoglu Mehmetbey University, 70200 Karaman TURKEY
[3]Computer Engineering Department, Mersin University, 33343 Yenisehir, Mersin TURKEY

Corresponding author: Feyza Toktas (e-mail: feyzatoktas@ kmu.edu.tr).

ABSTRACT Chaotic maps used to shuffle and manipulate the image pixels are important for image encryption (IE). In this study, a novel 2D optimized chaotic map (OPMAP) using a triple-objective differential evolution (TODE) algorithm is presented for IE. A model for OPMAP with eight decision variables is empirically designed, and then its variables are determined utilizing TODE through minimizing a triple-objective function that involving Lyapunov exponent (LE), entropy and 0-1 test. OPMAP is assessed with respect to credible measurements like bifurcation, 3D phase space, LE, 0-1 test, permutation entropy (PE) and sample entropy (SE). The capability of OPMAP is then verified through an IE scheme including permutation and diffusion through various cryptanalyses: key space 2^{298}, mean entropy 7.9995, mean correlation 13.61E-5, number of pixels changing rate (NPCR) 99.6093, unified average changing intensity (UACI) 33.4630 and encryption processing time (EPT) 0.2919 (s). A detailed review of IE schemes reported elsewhere is presented and IE performance of OPMAP is also validated by comparison with those IE schemes with and without optimization used. The 2D-OPMAP-based IE is faster and has low computational complexity. Moreover, the proposed it shows better cryptanalysis results for the most of the comparisons.

INDEX TERMS Chaotic map, cryptography, differential evolution, image encryption

I. INTRODUCTION

Data storing, transferring and multimedia messaging have increased for last decades [1]–[3]. While the data is being transferred over the internet, it is encountered different cyberthreats such as network attacks, denial-of-service, phishing and man in the middle [4]. For that reason, data must be encrypted through reliable and secure data encryption schemes for assuring the information security during the transferring [5], [6]. Generally speaking, image encryption (IE) depends on the spatial or frequency domains. IEs operating in the frequency domains are wavelet and Fourier transforms, while chaotic maps, DNA encoding, cellular automata and compressed sensing are IEs working in the spatial domains. [7], [8]. Chaos-based IE is mostly applied schemes because of having high dynamization, complexity and sensitivity to control parameters of the maps. IE schemes based on chaotic maps are frequently operated through two processes: permutation and diffusion. Positions of image's pixels are shuffled in the permutation, and the pixel's values are manipulated in the diffusion. The diffusion and permutation are handled by generated sequences using chaotic maps. The chaotic maps are managed by control parameters called initial value and growing rate obtained from a key. Hence, the chaotic maps have a key role in IE.

Metaheuristic optimizations particularly the nature-inspired algorithms have been widely implemented to IE with single or multi-objective algorithms [9] in order to increase the efficiency of the cryptography. Metaheuristic algorithms such as genetic algorithm (GA) [10], particle swarm optimization (PSO) [11], [12], ant colony algorithm (ACO) [13], artificial bee colony (ABC) [14], whale optimization algorithm (WOA) [15], steepest descent optimization (SDO) [16], golden sine algorithm (GSA) [17] and differential evolution (DE) [18] that implemented to IE have many species. Various IE schemes based on different kind of chaotic maps and optimization algorithms have been suggested in the literature. Accomplishing an IE scheme is usually examined through various quantitative cryptanalyses such as noise attack, key sensitivity, differential attack, cropping attack, information entropy, histogram, correlation, key-space. The related studies with optimization [10], [11], [21], [22], [12]–[16], [18]–[20] and without optimization [10], [11], [22]–[31], [12], [32]–

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

[36], [13], [15], [16], [18]–[21] are elaborately surveyed and compared with our IE scheme with respect to the cryptanalyses in the following section. The developed IE schemes appear to have certain strengths and weaknesses in the encryption processes and are particularly better in cryptanalysis [37]. The main deficiency of those is that optimization was directly implemented to IE. In other words, the objective functions are calculated over the encrypted images that should be subjected to the encryption process. Hence, they likely have complexity and long encryption processing time, giving rise to IE scheme to be inapplicable to the real applications. A versatile multi-dimensional chaotic map, which is optimized via a proper multi-objective optimization, would be more effective and useful for a successful IE scheme regarding overall cryptanalyses.

In this work, a new 2D optimized chaotic map (OPMAP) designed with the use of a triple-objective DE (TODE) algorithm is proposed for IE. The decision variables of 2D-OPMAP are optimally determined for improving a comprehensive multi-objective function involving Lyapunov exponent (LE), entropy and 0-1 test. The capability of OPMAP is even assessed in terms of reliable measurements which are bifurcation, 3D phase space, LE, 0-1 test, permutation entropy (PE) and sample entropy (SE). The generic description of OPMAP-based IE scheme is drawn in Figure 1. It is conducted on 8-bit grayscale image for the sake of clarity. Its pixel value varies between 0 and 255. Yet, it can be easily implemented to colorful image such as Red-Green-Blue (RGB) using different image matrix for each color channel. To manifest the superiority of the designed OPMAP, the images are encrypted through two processes, e.g., permutation and diffusion. Notably, we use a straightforward IE scheme so as to show solely the encryption performance of OPMAP. The control parameters of OPMAP are produced in order to generate the chaotic sequences for the IE processes. The main key is obtained by XOR operation between the secret key and public key acquired from the plaintext image at the transmitter side. In this way, the decipher image can be authenticated at the receiver by reproducing the public key. While public key is being transferred, it can be also encrypted as fulfilled in [38], [39]. Since TODE is only applied to the design of OPMAP not to the IE, OPMAP freely conducts the IE processes. Hence the speed of OPMAP-based IE is competitive. The cryptanalyses demonstrate that the proposed OPMAP outperforms the reported results thanks to the optimized dynamic performance of OPMAP. The contributions of the study can be briefly expressed below:

- A 2D-OPMAP for IE is optimally designed using a triple-objective metaheuristic algorithm.
- The IE performance of OPMAP is corroborated with respect to the various cryptanalyses.
- The state-of-the-art IEs with/without optimization algorithm are elaborately reviewed and compared with the performance of OPMAP.

The 2D-OPMAP-based IE comes to fore in the comparison thanks to the outstanding cryptanalysis results: key space is 2^{298}, mean entropy is 7.9995, mean correlation is 13.61E-5, number of pixels changing rate (NPCR) is 99.6093, unified average changing intensity (UACI) is 33.4630, peak signal to noise ratio (PSNR) for 1/4 cropped decipher image is 15.25, PSNR and structural similarity index (SSIM) for 0.01 density salt and pepper noise (SPN) decipher image are 29.06 and 0.0973, encryption processing time (EPT) is 0.2919 (s), encryption throughput (ET) is 0.85646 and number of cycles per byte (NCPB) is 3897.

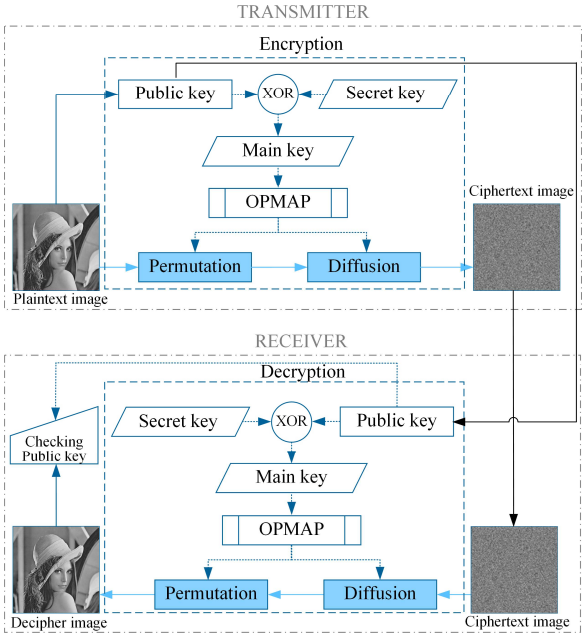


FIGURE 1. The flowchart of OPMAP-based IE.

II. RELATED STUDIES AND COMPARISION

Recently reported IE schemes are elaborately surveyed in Table I together with our study with regard to employed chaotic map and cryptanalysis results. The available data in the reported studies are listed in the table, the others are necessarily remarked as "—". Those are also reviewed pertaining the employed metaheuristic algorithms in Table II.

Suggested IEs have their own advantages and disadvantages considering the cryptanalyses. In general, they are based on logistic [11], [12], [15], [17], [18], [21], [25], sine/cosine [23], [25], [29], memristive [24], henon [29], Chebyshev [32], coupled lattice [10] and cellular automata [31], [40]. As the cryptanalyses are compared among each other, the key-spaces in [10], [19], [22]–[24], [28], [32] can be regarded the shorter, those in [14], [18], [26], [36] are medium and those in [11], [16], [20], [21], [25], [29], [34], [35], [40], [41] are considered the longer. The mean entropy can be quantized better [20], moderate [14], [24]–[31], [41] and worse [10], [11], [15], [18], [19], [21], [32]–[34], [40]. As the mean correlation coefficients for diagonal, horizontal and vertical directions in [11], [12], [14], [24] seem lower, those in [15], [16], [31]–[36], [40], [41], [19]–[21], [23], [26]–[29] appears moderate and those in [10], [13], [18], [25], [30] look higher. Differential attack can be analyzed in terms of NPCR

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

TABLE I
A DETAILED REVIEW WITH REGARD TO THE EMPLOYED CHAOTIC MAP AND CRYPTANALYSIS

Ref.	Year	Dim.	Chaotic map	Key-space	Entropy (mean)	Corr. (mean)	Differential attack (%) NPCR	Differential attack (%) UACI	Crop. attack	Noise Attack
[23]	2018	1D	Sine-sine	2^{128}	—	0.006300	99.6330	33.4716	◔	◔
[24]	2021	4D	Memristive	2^{146}	7.9993	0.000511	99.6078	33.4268	◕	—
[25]	2019	2D	Logistic-adjusted-sine	2^{338}	7.9993	0.013197	99.6042	33.4328	—	—
[26]	2019	1D	A modified chaotic	2^{212}	7.9993	0.001710	99.6040	33.4340	—	—
[27]	2019	1D	Polynomial combination	—	7.9993	0.002003	99.6191	33.6751	◔	◕
[28]	2018	1D	Three integrated cascades	2^{186}	7.9993	0.003217	99.6040	33.4740	◕	◕
[29]	2018	2D	Hénon-sine	2^{371}	7.9993	0.002417	99.6080	33.5470	◔	◕
[30]	2020	—	Fractional Fourier transform and Lorenz	—	7.9991	0.051500	99.5676	33.4352	—	—
[31]	2019	—	Cellular automata	—	7.9992	0.002033	99.5180	33.2630	—	—
[32]	2020	2D	Sine and Chebyshev	2^{158}	7.9972	0.001719	99.6090	33.4523	◔	◕
[33]	2021	1D	Sine and logistic maps and Yolo	—	7.9981	0.001523	99.7061	33.5190	◔	◕
[34]	2019	4D	Four-wing hyperchaotic	2^{700}	7.9971	0.008957	99.6000	33.4800	◕	◕
[35]	2020	1D	Sine	2^{412}	—	0.001827	99.6127	33.4691	◔	◕
[36]	2019	1D	Logistic, Sine, and Tent map's combination	2^{256}	—	0.001410	99.6244	33.4548	◔	◕
[41]	2021	4D	Lorenz system and skew tent map	2^{455}	7.9993	0.001366	99.6111	33.4682	—	—
[10]*	2020	2D	Coupled lattice	2^{128}	7.9519	0.046700	99.4547	31.3549	—	—
[19]*	2020	4D	Lorenz system	2^{111}	7.9976	0.003720	99.6340	33.4330	—	—
[20]*	2021	5D	A chaotic	2^{338}	7.9996	0.005973	99.6475	33.4700	—	—
[21]*	2019	3D	Intertwining logistic	2^{338}	7.9987	0.003250	99.6535	33.5497	—	—
[18]*	2020	3D	Intertwining logistic	2^{256}	7.9985	0.016467	99.6400	32.9500	—	—
[15]*	2021	2D	Piecewise linear chaotic and 2D logistic	—	7.9723	0.001790	99.6746	33.4753	—	—
[11]*	2021	1D	Logistic	2^{385}	7.9974	0.000113	99.6169	33.4658	◔	◕
[12]*	2018	1D	Logistic	—	—	0.000100	99.4547	31.3549	—	—
[16]*	2017	2D	Henon	2^{381}	—	0.006133	—	—	—	—
[13]*	2012	—	—	—	—	0.084940	—	—	—	—
[22]*	2015	—	Coupled nonlinear	2^{168}	—	—	—	—	—	—
[40]*	2021	4D	A chaotic system and cellular automata	2^{512}	7.9987	0.008933	99.6352	33.5614	—	—
[17]*	2021	1D	Logistic map	—	—	—	99.5937	33.4612	—	—
[14]*	2021	1D	1D chaotic map	2^{199}	7.9940	0.0001115	99.6090	33.4641	◕	◕
This study		2D	OPMAP	2^{298}	7.9995	0.0001361	99.6093	33.4630	◕	◕

* represent the optimization algorithms used. ◔: poorer ◑: moderate, ◕: better

TABLE II
A SURVEY ON THE METAHEURISTIC OPTIMIZATION-BASED IE SCHEMES

Ref.	Year	Dim.	Type of chaotic map	Optimization algorithm	Obj.#	Objective function	Decision variable
[10]	2020	2D	Coupled lattice	GA	Two	Entropy and correlation coefficient	Key
[19]	2020	4D	Chaotic map based on Lorenz system	Pareto evolutionary algorithm-II	Four	Weighting objective function including correlation coefficient, entropy, NPCR, UACI	Initial parameter of the map
[20]	2021	5D	Chaotic	Dual local search	Three	UACI, entropy, NPCR	Initial parameter of the map
[21]	2019	3D	Intertwining logistic	Memetic DE	Two	Entropy and correlation coefficient	Key
[18]	2020	3D	Intertwining logistic	DE	Single	Entropy	A sequence for DNA process
[15]	2021	2D	Piecewise linear chaotic and 2D logistic	WOA	Single	Entropy	Initial parameter of the map
[11]	2021	1D	Logistic	PSO	Two	Weighting objective function including entropy and correlation coefficient	Key
[12]	2018	1D	Logistic	PSO	Single	Correlation coefficient	Key
[16]	2017	2D	Henon	SDO	Single	A complex object function based on CCD plane	Image
[13]	2012	—	—	ACO	Single	Energy	Key
[22]	2015	—	Coupled nonlinear	Hybrid of PSO and GA	Single	PSNR	Key
[40]	2021	4D	A chaotic system and cellular automata	PSO	Single	Correlation coefficient	Initial parameter of the map
[17]	2021	1D	Logistic map	GSA II	Single	NIST	Initial parameter of the map
[14]	2021	1D	1D chaotic map	ABC	Two	Weighting objective function including LE and entropy	Map's variables
This study		2D	OPMAP	DE	Three	Weighting objective function including entropy, LE and 0-1 test	Map's variables

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

and UACI which are the randomness test. The proof of IE schemes with regard to NPCR can be in order from strongest [11], [14], [34]–[36], [41], [17], [24]–[29], [32], moderate [15], [18]–[21], [23], [30], [31], [33], [40] to weakest [10], [12]. On the other hand, those can be sorted from the robust [11], [14], [17], [20], [23], [35], [36], [41], moderate [24]–[26], [28]–[30], [32]–[34], [40] to the weakest [10], [12], [18], [27], [31] pertaining the UACI. The IE schemes and respectively seem better [14], [24], moderate [11], [23], [28], [32], [34] and weaker [27], [29], [33], [35], [36] counter the cropping attack. Eventually, those in [11], [14], [28], [36] and [27], [29], [32]–[35], and [23] seem well, fair and worse with regard to the noise attacks, respectively. Therefore, the proposed IE with OPMAP stands out due to eminent results of key-space, information entropy, correlation, NPCR, UACI, as well as cropping and noise attacks among the others reported elsewhere.

From Table II, the metaheuristic optimization algorithms GA, PSO, ACO, ABC, PSO, GA, SDO, WOA, GSA and DE were generally applied to IE schemes. Decision variables that searched by the optimization algorithms are the most critical targets. The optimization algorithms were often used to optimally find out the keys for IE [10]–[13], [21], initial parameters of the chaotic maps [15], [19], [20] or chaotic sequence [18] or ciphertext image for minimizing or maximizing different objective functions. NPCR [19], [20], correlation coefficient [10]–[12], [19], [21], UACI [19], [20], PSNR and entropy [10], [11], [15], [18]–[21] that depend on the ciphertext images were the most used objective functions. Notice that those objectives are evaluated on the decipher image that should be incurred the whole processes of IE scheme. In other words, the image should be undergone the processes of IE scheme to encrypt so as to evaluate the objective functions in each generation of the optimization process. This may lead to low encryption speed; thus, IEs might not be applicable to the realistic systems. In [14], primitive study based on 1D chaotic map was performed through dual-objective function including LE and entropy using ABC algorithm. 0-1 test which is an effective metric was not considered in both objectives and the assessment of the optimized chaotic map. Since the chaotic map was 1D and has four decision variables, its nonlinear and diversity performance were limited. As for the proposed 2D-OPMAP, it is derived by finding out optimally eight decision variables using TODE including the entropy, LE and 0-1 test. The triple-objective function is implemented to the output of OPMAP. The plaintext image is thus encrypted through the encryption processes managed by OPMAP.

III. DESING OF 2D-OPMAP USING TODE

First, working principle of DE algorithm, and then the three objective functions for 2D-OPMAP are clarified here. Afterward, OPMAP with eight decision variables and implementation of TODE to optimize OPMAP are addressed. Eventually, the optimized OPMAP is introduced.

A. DE ALGORITHM AND ITS IMPLEMENTATION

DE algorithm was developed inspiring by the natural evolution of living organism species [42]. A flowchart pertaining DE and its implementation to the optimization of OPMAP are illustrated in Figure 2. DE mimics the evolution phenomena of the living organism mainly in three phases: mutation, crossover and selection. Assume that the evolution progresses from generation to generation. It is known that chromosomes which contain genes are the structures within a cell of a living organism. The population in DE accordingly comprises chromosomes each consists of genes. The chromosomes and the genes respectively correspond to the decision variables and its dimension.

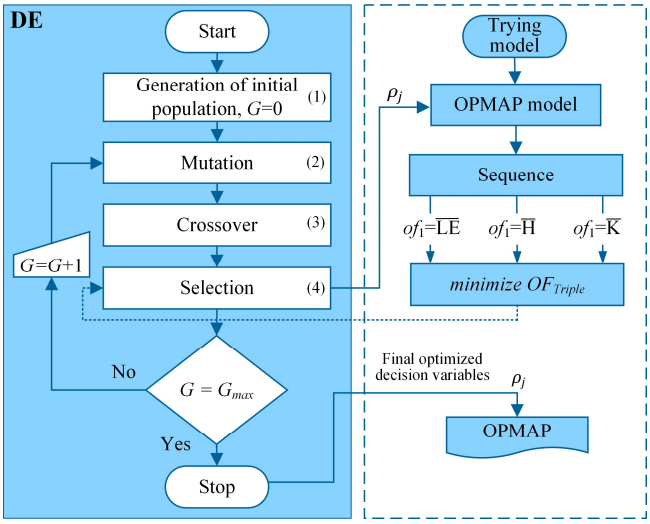


FIGURE 2. Flowchart of DE and its implementation to the optimization of OPMAP

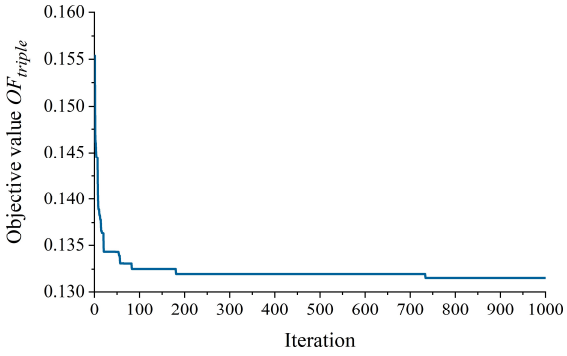


FIGURE 3. Convergence tendency of TODE in the optimization of OPMAP.

In the initial phase, random values related to the decision variables for candidate solutions are generated Eq. (1) between two specified lower bound (L_b) $\rho_j^{(l)}$ and upper bound (U_b) $\rho_j^{(u)}$ to constitute the initial generation (G) as follows:

$$\rho_{j,i,G=0} = \rho_j^{(l)} + rand_j[0,1].\left(\rho_j^{(u)} - \rho_j^{(l)}\right) \quad (1)$$

where, NP is the number of populations (chromosome number i = 1, 2, …, NP) and D is the number of variables (gene number j = 1, 2, …, D). The objective value of each generated variable

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

is then calculated to assess the efficacy and the robustness of each chromosome. In the mutation phase, new variables are regenerated Eq. (2) by mutating the randomly selected three individuals in the range of mutation factor (F). The following operator is used to regenerate the new variables.

$$n_{j,i,G+1} = \rho_{j,r_3,G} + F.(\rho_{j,r_1,G} - \rho_{j,r_2,G}) \tag{2}$$

here, r_1, r_2 and r_3 are randomly selected chromosomes for mutated individuals $n_{j,i,G+1}$. All individuals are thus mutated by involving the other two variables into the other. In the crossover phase, the mutated variables pertaining new generation are randomly exchanged Eq. (3) with respect to the previous generation deciding by the following operator including a crossover rate (CR).

$$\rho_{j,u,G+1} = \begin{cases} \rho_{j,n,G+1} & if\ rand[0,1] \le CR\ \vee\ j = j_{rand} \\ \rho_{j,i,G} & otherwise \end{cases} \tag{3}$$

Meanwhile a model for OPMAP embedded with decision variables is tried to optimize. In the selection phase, the objective value of each variable is computed based on the sequence of the tried OPMAP, which is the triple objective function involving LE, information entropy and 0-1 test. The decision variables which make the objective value lower are selected; in other words, the best variables are transferred to the subsequent generation, the others are discarded by the following operator.

$$\rho_{i,G+1} = \begin{cases} \rho_{u,G+1} & if\ OF(\rho_{u,G+1}) \le OF(\rho_{i,G}) \\ \rho_{i,G} & otherwise \end{cases} \tag{4}$$

These three phases sequentially continue up to a predefined maximum number of generation (MNG).

B. THE DESIGN OF OPMAP

A model for 2D-OPMAP in which unknown variables are sprinkled is empirically designed with the best in essay as follows:

$$\begin{aligned} v_{i+1} &= mod\big((\rho_1 w_i + \rho_2 r v_i)(e^{\rho_3} + \rho_4 w_i), 1\big) \\ w_{i+1} &= mod\big((\rho_5 v_{i+1} + \rho_6 r w_i)(e^{\rho_7} + \rho_8 v_{i+1}), 1\big) \end{aligned} \tag{5}$$

where, u is the growing rate, and v_i and w_i are the initial values. $mod(\cdot\ ,1)$ is used to wrap the sequence around 1. The model involving eight unknown coefficients ρ_j, $j \in [1,8]$ is regarded as the decision variables in the optimization. Now, appropriate objectives are needed for evaluating chaotic performance of the map in the optimization process. There are several precision metrics such as LE, 0-1 test, SE, PE, bifurcation and trajectory analyses for measuring the chaotic performance of a map. In investigation of the multiple objective functions, we aimed to comb out the most impactful three objective functions in the optimization and to use the others in the assessment of the map independently. Thence we essayed LE, entropy, 0-1 test, SE and PE separately, and we have chosen LE, entropy and 0-1 test due the their most effectiveness in the optimization. The decision variables are then optimally determined for improving the following three objectives.

1) OBJECTIVE FUNCTION 1: LE

The LE of which equation is given below is a logarithmic measure for the mean expansion rate per iteration of the distance between two infinitesimal close trajectories [43].

$$LE = \lim_{n\to\infty} \sum_{i=1}^{n-1} ln|f'(v_i)| \tag{6}$$

here $f(v_i) = v_{i+1}$ is the chaotic map and the iteration number is n. The LE can be employed to evaluate predictability and sensibility of the chaotic system to the control parameters which are growing rate and initial value. For better chaotic behavior, the LE should be as high as possible in a large range of the growing rate. Therefore, the permutation and diffusion performance of the ciphertext image can be improved by maximizing the LE of a map.

2) OBJECTIVE FUNCTION 2: ENTROPY

The information entropy is well-known and effective metric that is able to evaluate the disorderliness of an image. It is considered for optimizing of the chaotic map. It can be implemented as follows:

$$Y = floor(256x_i) \tag{7}$$

$$H(Y) = \sum_{i=0}^{255} p(y_i) log_2 \frac{1}{p(y_i)} \tag{8}$$

where, x_i is a single sequence produced from the two maps v_{i+1} and w_{i+1} that is explained in Section IV, B (Algorithm 2). Since x_i is $[0,1]$, Y is adapted to be $[0,255]$ corresponding to 8-bit pixels value by multiplying 256 and taking $floor(\cdot)$.

3) OBJECTIVE FUNCTION 3: THE 0-1 TEST

The 0-1 test was developed for measuring the growth rates of trajectory of a chaotic system [44]. It simply detects the occurrence of non-regular stationary responses of any sequence of a dynamical system with respect to the 2D Euclidean group. Assume that the test input is a 1D time series $\phi(n)$ used to drive the 2D system [35].

$$p(n+1) = p(n) + \phi(n) cos(cn) \tag{9}$$

$$q(n+1) = q(n) + \phi(n) sin(cn) \tag{10}$$

where, $c \in (0,2\pi)$ is fixed. The time-averaged mean square displacement can be defined as

$$\begin{aligned} M(n) = \lim_{N=\infty} \frac{1}{N} \sum_{j=1}^{N} ([p(j+n) - p(j)]^2 \\ + [q(j+n) - q(j)]^2),\ n = 1, 2, \ldots \end{aligned} \tag{11}$$

and its growth rate can be defined as

$$K = \lim_{n=\infty} \frac{\log M(n)}{\log n} \tag{12}$$

It takes either the value $K \approx 1$ consulting fully chaotic system or $K \approx 0$ pointing out non-chaotic system.

4) TRIPLE OBJECTIVE FUNCTION

OPMAP is optimized to determine the decision variables for improving the following three objectives:

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

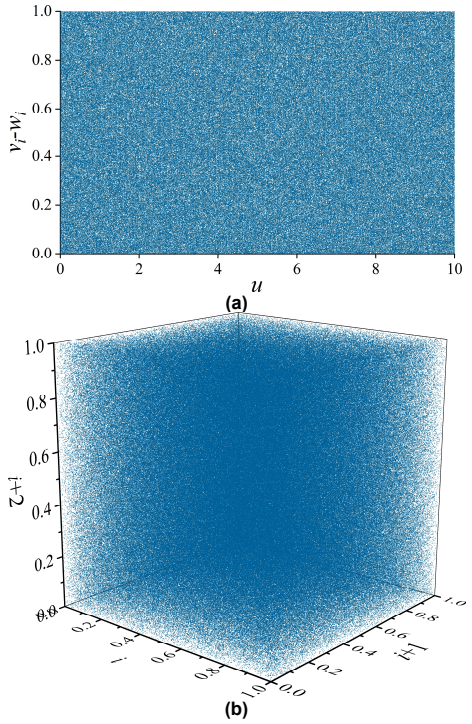


FIGURE 4. a) Bifurcation diagram of OPMAP for 10^3 iterations, b) 3D chaotic trajectory for 10^6 iterations.

$$of_i = \{of_1 = \overline{LE}, of_2 = \overline{H}, of_3 = \overline{K}\} \tag{13}$$

Here, $\overline{LE}$, $\overline{H}$ and $\overline{K}$ are respectively the average of LE, H and K. A minimizing single triple objective function is composed of the three objective functions as follows:

$$OF_{triple} = w_1 \frac{1}{of_1} + w_2(8 - of_2) + w_3(1 - of_3) \tag{14}$$

where, w_1, w_2 and w_3 the weighting factors that are set as 0.2, 0.6 and 0.2, respectively. The three objective functions are implemented to minimize using $1/of_1$, $8 - of_2$ and $1 - of_3$ in which 8 is the maximum entropy value and 1 is the maximum value of 0-1 test.

OPMAP is optimized to determine the decision variables through TODE for minimizing the triple-objective function OF_{triple} in Eq. (14). TODE, the NP, G_{max}, F and CR are set 30, 1000, 0.6 and 0.8; and L_b and U_b are taken as -10 and 10, respectively. The convergence path of the optimization is curved in Figure 3. Once approximately 800 iterations, TODE reaches to the last objective value 0.13147. During the optimization process, decision variables sprinkled in OPMAP are rounded to the nearest hundredth. Eventually, the found-out variables $\rho_j, j = \{1,2, \dots, 8\}$ of OPMAP are -6.72, 10, 10, 9.48, 2.62, 10, 9.44 and -7.16, respectively. The final OPMAP in which the optimized variables substituted is given below:

$$\begin{aligned} v_{i+1} &= mod\big((-6.72w_i + 10uv_i)(e^{10} + 9.48w_i), 1\big) \\ w_{i+1} &= mod\big((2.62v_{i+1} + 10uw_i)(e^{9.44} - 7.16v_{i+1}), 1\big) \end{aligned} \tag{15}$$

here, u is the growing rate, and v_i and w_i are the initial values of OPMAP.

IV. THE ASSESSMENT OF 2D-OPMAP

The spatial dynamic distribution of 2D-OPMAP is examined from the perspective of bifurcation and chaotic trajectory in Figure 4. The bifurcation diagram showing the diversity and ergodicity of the OPMAP is scattered in Figure 4(a). 3D phase space chaotic trajectory that shows the dynamic characteristic of OPMAP in 3D phase space is revealed in Figure 4(b). Assume that $X = [x_1, x_2, x_3, x_4, x_5, x_6, \dots, x_N]$ is the sequence of 2D OPMAP. (i)-axis is $X_i = [x_1, x_4, x_7, \dots, x_{N-2}]$, ($i$+1)-axis is $X_i = [x_2, x_5, x_8, \dots, x_{N-1}]$ and (i+2)-axis is $X_{i+2} = [x_3, x_6, x_9, \dots, x_N]$. A fully dynamic system is hoped to occupy whole phase spaces without any clustering and repetitive paths.

Moreover, the chaotic performance of OPMAP is measured with respect to the LE and 0-1 test in Figure 5(a)-(b), respectively. It is compared with those reported to validate the outstanding chaotic performance. Given that the higher and more stable LE in positive region, the better the chaotic capability. It is evident that the best result among the reviewed LEs is approximately 5 [21], [30], the LE of OPMAP outperforms the others due to the fact that it is about 13. On the other hand, the 0-1 test of OPMAP seems the best with almost 1 among the reported ones (See Figure 5b). In order to further examine the complexity performance of OPMAP, independent measurements such as SE and PE, which are not used as the objective functions, are utilized [39], [40]. SE assesses the complexity of a dynamic system. It measures the similarity of the sequence produced by a chaotic map. Suppose that $\{v_1, v_2, \dots, v_N\}$ is a sequence, $v_m(i) = \{v_i, v_{i+1}, \dots, v_{i+m+1}\}$ is a template vector, m is the dimension and the acceptance tolerance is r. Therefore, the SE can be defined as:

$$SE(m, r, N) = -log\frac{A}{B} \tag{16}$$

where, A and B respectively represent the number of vectors for $d[X_{m+1}(i), X_{m+1}(j)] < r$ and $d[X_m(i), X_m(j)] < r$, and $d[X_m(i), X_m(j)]$ is the Chebyshev distance between $X_m(i)$ and $X_m(j)$. The higher the SE, the better the complexity of a sequence is considered. The SE variation of OPMAP is illustrated in Figure 5(c) including comparison with the state of the arts. OPMAP demonstrates higher complexity as it is about 2.2 better in the comparison. PE is even a reliable measurement of the complexity of a dynamic system [45]. The higher the PE, the more complex the sequence of a chaotic map. The PE of OPMAP that is calculated for embedding dimension 2 and time delay 1 is comparatively plotted in Figure 5(d). Given that the PE can get maximum value of 1 at these parameters. The PE of OPMAP is the highest with a value of 1 within the others. With these results, OPMAP has the best complexity and randomness thanks to the optimized chaotic characteristic.

V. THE PROPOSED 2D-OPMAP-BASED IE SCHEME

In this section, obtaining the control parameters of 2D-OPMAP is outlined in Algorithm 1. Then the generation of sequence via OPMAP is expressed in Algorithm 2 and the IE scheme is processed through permutation and diffusion in Algorithm 3.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

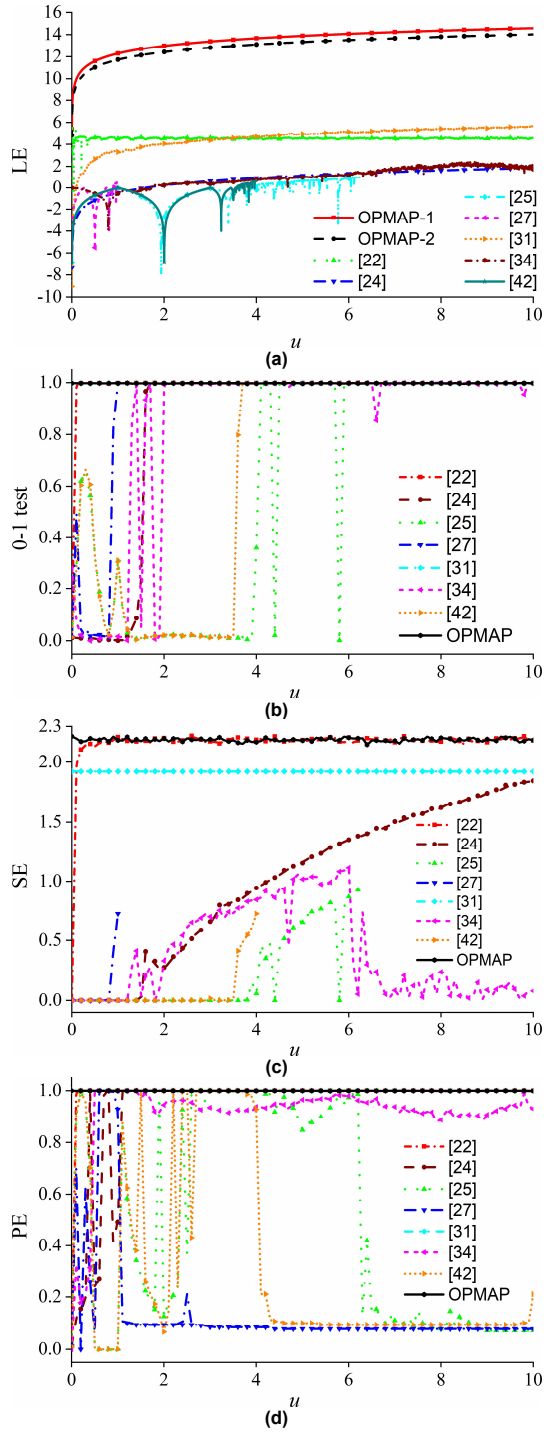


FIGURE 5. The assessment of OPMAP and comparison with the state of the arts: a) LE, b) 0-1 test, c) SE, d) PE.

A. THE CONTROL PARAMETERS OBTAINED FROM THE KEYS

In IE scheme, the main key is firstly computed via XOR operation with a public key produced by the plaintext image and a secret key. The initial values v and w, and the growing rate u are obtained from the main key. These parameters are utilized in OPMAP to generate chaotic sequences. The chaotic sequences are deployed in the permutation and diffusion processes of IE. Acquiring the control parameters are clarified in Algorithm 1. In Line 1, a matrix A sized $m \times n$ is formed by importing the plaintext image in the algorithm. In Line 2, three vectors A_1, A_2 and A_3 that acquired from the plaintext image is computed to form the public key. A_1, A_2, A_3 sized m, n, $m+n-1$ are obtained by summing row, column and diagonal pixels of A, respectively. Thereafter, the public key B is formed by combining SHA-512 and MD5 hash values using the three vectors A_1, A_2 and A_3. In Line 3, a secret key C is constituted using hash function in [46]–[48]. In Line 4, the main key D is acquired via XOR operation between the public and secret key. In Line 5, the main key D is separated into eight sub-matrices, then the columns of them are incurred an operation $mod(sum(E,2),2)$. E matrix sized 8×8 is obtained by combining each sub-matrix sized 8×1. In Line 6, a decimal matrix F is formed by combining the binary matrix F. In lines 7 and 8, the initial values $W := [w_1 \;\; w_2]$ and $V := [v_1 \;\; v_2]$ are achieved. Eventually, in Lines 9 and 10, the growing rate $U := [u_1 \;\; u_2]$ is accomplished.

B. THE IE PROCESSES

The generation of chaotic sequences via 2D OPMAP using the control parameters that are growing rates and initial values is explained in Algorithm 2. IE which is processed by permutation and diffusion is elucidated step-by-step in Algorithm 3 and it is illustrated in Figure 6 for the Lena image of 5x5 pixel. The pixels are shuffled in position and handled in pixel's values through the two processes managed by OPMAP. In Line 1, a vector A sized $m \times n$ is formed by importing the plaintext image in the algorithm. In Lines 2 and 5, the chaotic sequences X_1 and X_2 are generated by OPMAP using the initial value V and W, and growing rate U which are achieved by Algorithm 2. In Line 3, vector Y_1 is formed by sorting the chaotic sequence X_1 in ascending order. In Line 4, the permutated matrix A_1 is obtained by positionally confusing the pixels of A according to the sorted sequence Y_1. In Line 6, a vector Y_2 is formed with $Y_2 := \mathrm{floor}(256X_2)$ to use in diffusion processes. In Line 7, the diffusion matrix A_2 is achieved as the ciphertext image by XOR operation between the permutated matrix A_1 and vector Y_2.

VI. THE CRYPTANALYSES

An IE scheme is required to enhance the resistant against to potential cyber threats through network attacks. Hence the security of an IE scheme should be evaluated by simulating some cyber threats [37]. The most credible cryptanalyses are histogram, correlation, key sensitivity, key-space, differential attack, information entropy, cropping attack and noise attack. The cryptanalyses that are tested on the test images sized 512×512 are performed with the agency of MATLAB R2020b operating over a computer having I(R) Xeon(R) CPU E5-1620 v4 @ 3.5 GHz and 64 GB RAM. The results of the proposed OPMAP-based IE are also compared with available the state of the arts [11], [24], [51]–[53], [25]–[27], [29], [32], [33], [49], [50].

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

Algorithm 1: The control parameters obtained from the main key

1. Import the image matrix A
2. Produce a public key $B \coloneqq [b_{1p}]_{1\times512}$ by SHA-512/MD5
3. Produce a secret key $C \coloneqq [d_{1p}]_{1\times512}$ being a binary row matrix
4. Obtain the main key $D \coloneqq B$ XOR C and reform D to 8×8×8
5. Calculate $E \coloneqq \mathrm{mod}(\mathrm{sum}(D,2),2)$, reform E to be in size of 8×8
6. Obtain $F \coloneqq [128\ 64\ 32\ 16\ 8\ 4\ 2\ 1]E$
7. Figure out the initial values $v_i \leftarrow \frac{\mathrm{mod}(f_{1i}*\mathrm{sum}(F),256)}{256}$, $i \in \{1,3\}$
8. Figure out the initial values $w_i \leftarrow \frac{\mathrm{mod}(f_{1i}*\mathrm{sum}(F),256)}{256}$, $i \in \{2,4\}$
9. Compute $G \coloneqq \mathrm{mod}\left(\left(sum(F(5:6))\ sum(F(7:8))\right)*\ sum(F)\right),256)$
10. Obtain the growing rate $u_i \leftarrow \frac{g_{1,i}}{256} + \mathrm{mod}(g_{1,i},10)$, $i \in \{1,2\}$

Algorithm 2: The generation of chaotic sequence via 2D-OPMAP

1. Set the initial values y_1 and z_1 and the growing rate u
2. $j = 1$
3. For i from 1 to $\frac{mn}{2}+1$
4. $y_{i+1} = mod\left((-6.72z_i + 10uy_i)(e^{10} + 9.48z_i),1\right)$
5. $z_{i+1} = mod\left((2.62y_{i+1} - 10uz_i)(e^{9.44} - 7.16y_{i+1}),1\right)$
6. $x_j = y_{i+1}$
7. $x_{j+1} = z_{i+1}$
8. $j = j + 2$
9. End For
10. $X \coloneqq [x_{ij}]_{1\times mn}$

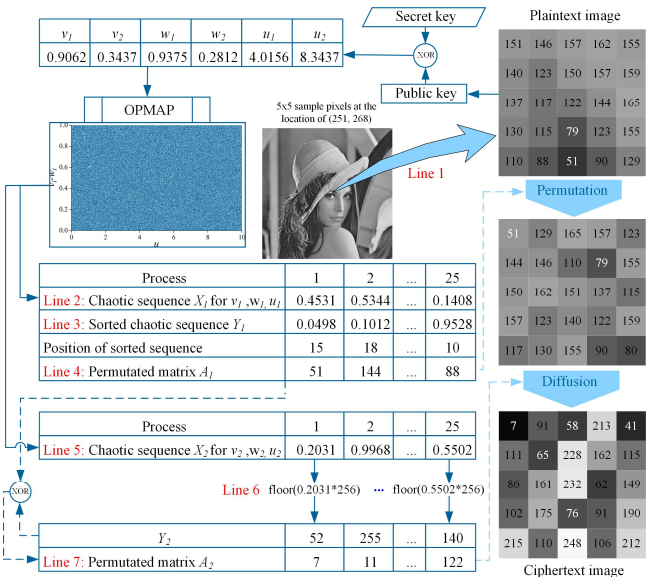
Algorithm 3: Encryption processes of IE with 2D-OPMAP

//Permutation

1. Import the image matrix A
2. Produce the chaotic sequence $X_1 \coloneqq [x_{1r}^1]_{1\times mn}$ using control parameters
3. Form $Y_1 \coloneqq [y_{1r}^1]_{1\times mn}$ by sorting ascending order X_1
4. Calculate a permutated matrix $A_1 \coloneqq [a_{kl}^1]_{m\times n}$ by $a_{kl}^1 \coloneqq a_{ij}$ so that $x_{1,n(i-1)+j}^1 = y_{1,n(k-1)+l}^1$

//Diffusion

5. Produce the chaotic sequence $X_2 \coloneqq [x_{1r}^2]_{1\times mn}$ using the control parameters
6. Constitute vector $Y_2 \coloneqq [y_{1r}^2]_{1\times mn}$ defined by $Y_2 \coloneqq \mathrm{floor}(256X_2)$ and reform Y_2 to be $m\times n$
7. Accomplish the diffused matrix $A_2 \coloneqq [a_{kl}^2]_{m\times n}$ by $A_2 \coloneqq A_1 \oplus Y_2$



v_1	v_2	w_1	w_2	u_1	u_2
0.9062	0.3437	0.9375	0.2812	4.0156	8.3437

Process	1	2	...	25
Line 2: Chaotic sequence X_1 for v_1 ,w_1, u_1	0.4531	0.5344	...	0.1408
Line 3: Sorted chaotic sequence Y_1	0.0498	0.1012	...	0.9528
Position of sorted sequence	15	18	...	10
Line 4: Permutated matrix A_1	51	144	...	88

Process	1	2	...	25
Line 5: Chaotic sequence X_2 for v_2 ,w_2, u_2	0.2031	0.9968	...	0.5502
Y_2	52	255	...	140
Line 7: Permutated matrix A_2	7	11	...	122

FIGURE 6. An illustrative example for OPMAP-based IE.

A. KEY SPACE

Brute-force is the well-known cyberattack depending on prediction of the key by trying various keys. A ciphertext image encrypted via a short key may be vulnerable to such attacks. Long keys lead to withstand in longer time and it might be unfeasible to forecast the key in case it has the sufficient length. This analysis is able to prove capability of an IE to the brute-force attacks. An IE is considered secure if the key has the minimum length 2^{100} [54]. In OPMAP-based IE scheme, a SHA 512-bit-length key is employed, and is six floating numbers with 10^{15} precision. The key space is hence $10^{15\times6} = 10^{90} \cong 2^{298}$ that is much higher than 2^{100}.

B. KEY SENSITIVITY

Key sensitivity analyses an IE scheme whether it is sensitive to slight change in the key. It is expected that one-bit alteration leads to a big change in the encryption or decryption. In analysis, five secret keys including the original one and its four one-bit altered versions are listed in Table III. The ciphertext images encrypted with these keys are shown in Figure 7. Their pixel to pixel difference images are also illustrated in Figure 7 to investigate the same pixel value that seems black color. It is evident that any black region is not seen in Figure 7(g), (h), (i), and (j).

The other analysis in the context of key sensitivity is to examine whether the decipher images with one-bit altered keys contains any remnant data related to the plaintext image. To this end, the ciphertext images encrypted with the original key are decrypted using the four one-bit altered keys in Figure 8. The decipher image with original key (Key 1) is accurately decrypted as it is expected (See Figure 8(b)), the other decipher images is very different from the plaintext image.

Table IV contains numerical results pertaining to the discriminating result of the difference images to define the key sensitivity in terms of percentage, mean square error (MSE) and number of bit change rate (NBCR) [55]. The discriminating levels are achieved as 99.6098% for Key 2, 99.6056% for Key 3, 99.6208% for Key 4, and 99.6182% for Key 5, and the average of these levels is 99.6136%. The NBCR can calculated as given below:

$$Ham(I_1,I_2) = \frac{1}{MxN}\sum_{i=1}^{MxNxT_c}(I_1(i)\ \mathrm{XOR}\ I_2(i))\mathrm{x}100\% \tag{17}$$

$$NBCR(I_1,I_2) = \frac{Ham(I_1,I_2)}{T_c} \tag{18}$$

where, I_1 and I_2 are the two images with mxn size. $Ham(I_1,I_2)$ is the Hamming distance that defines the different bits between two images. T_c is the key length. The more NBCR is close to 50%, the more I_1 and I_2 are different from each other. NBCR results of a whole secret key for the Lena image are plotted in Figure 9. This plot is obtained by altered all bits of a secret key. First the number of 512 one-bit altered secret keys are obtained from 1st to 512th bits. Then the image is separately encrypted with the original key and one-bit altered key, they are denoted as C_1 and C_2 their score is calculated as $NBCR(C_1,C_2)$. Afterwards the ciphertext

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

image C_1 is decrypted with the original key and one-bit altered key, and their score is computed as $NBCR(D_1, D_2)$. The both NBCR varies between 49.9% and 50.1%. The last numerical analysis is the MSE that can be computed as follows

$$MSE := \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(e_{ij} - f_{ij})^2 \quad (19)$$

here $E := [e_{ij}]$ and $F := [f_{ij}]$ are the two images under consideration. It is obvious that the recommended IE is highly susceptible to the keys due to the variety ability of OPMAP.

C. HISTOGRAM

Histogram is able to show a graphical representation of the pixel's values versus that of sorting values. Hence, the monotony of image pixels and the diffusion capacity of OPMAP can be investigated. The more uniform the histogram, the better the diffusion performance. The histograms of the test images and the pertaining ciphertext images are shown in Figure 10. The OPMAP-based IE uniformly modifies the pixel's value. Therefore, the IE scheme is resistant to the statistical attacks and no information can be extracted from the ciphertext images. For further examining the histogram, χ^2 tests and variance of the histogram can be checked out. Variance and χ^2 tests for a gray scale image are figured out as given below:

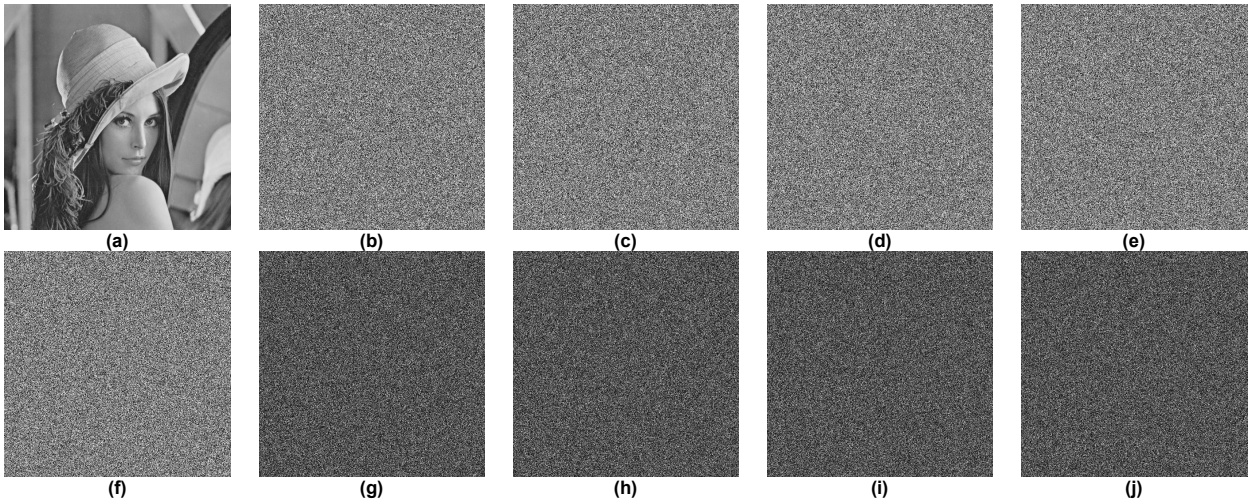


FIGURE 7. Key sensitivity cryptanalysis: a) plaintext image; ciphered images with b) Key 1; c) Key 2; d) Key 3; e) Key 4; f) Key 5; difference image between g) (b) and (c), h) (b) and (d), i) (b) and (e), j) (b) and (f).

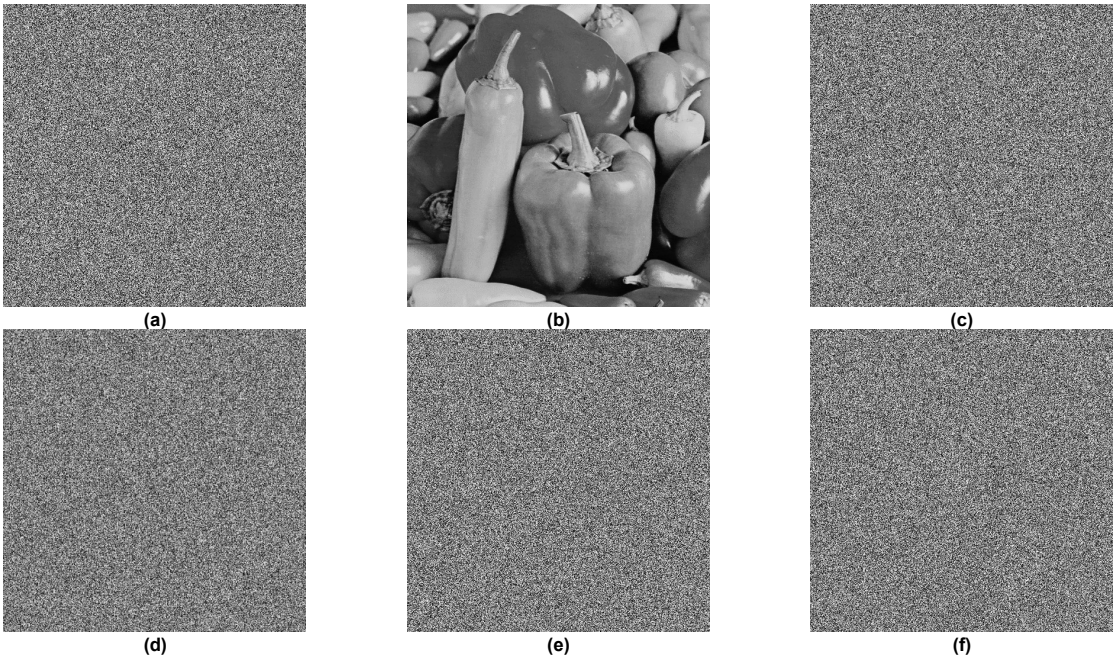


FIGURE 8. Key sensitivity cryptanalysis: ciphered image with a) Key 1 (original); deciphered images with b) Key 1, c) Key 2, d) Key 3, e) Key 4, f) Key 5.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

TABLE III
THE SECRET KEY AND ITS ONE-BIT ALTERED VERSIONS

Key	512-bit key
Key 1 (original)	0010111000101110101000010100100011111…110
Key 2 (altered)	1010111000101110101000010100100011111…110
Key 3 (altered)	0110111000101110101000010100100011111…110
Key 4 (altered)	0000111000101110101000010100100011111…110
Key 5 (altered)	0011111000101110101000010100100011111…110

TABLE IV
THE NUMERICAL DIFFERENCE OF IMAGES WITH ONE-BIT ALTERED SECRET KEYS 7(B)

Figure	Keys	Percentage (%)	NBCR (%)	MSE
7(c)	Key 2	99.6098	50.03%	10918.62
7(d)	Key 3	99.6056	49.96%	10918.70
7(e)	Key 4	99.6208	50.04%	10942.40
7(f)	Key 5	99.6182	49.98%	10945.30
Mean		99.6136	50.00%	10931.26

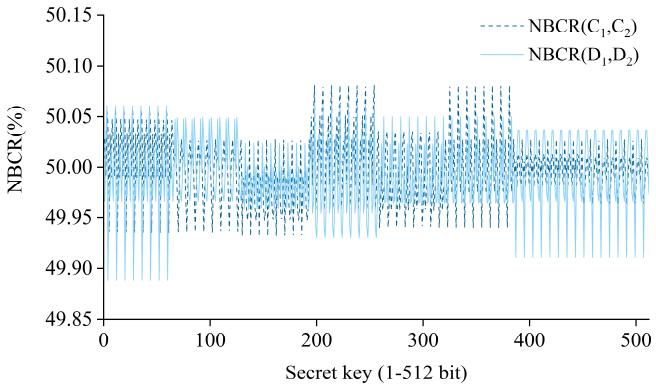


FIGURE 9. **The NBCR results for the Lena image.**

$$var(\boldsymbol{X}) = \frac{1}{n^2}\sum_{i=0}^{n}\sum_{j=1}^{n}\frac{1}{2}(x_i - x_j)^2 \tag{20}$$

$$\chi^2 = \sum_{i=0}^{255}\frac{\left(n_i - \frac{n}{256}\right)^2}{\frac{n}{256}} \tag{21}$$

here the repetition frequency of the pixel's value i is n_i and the total number of pixels is n. The supposed repetition frequency of every pixel's value is computed using $\frac{n}{256}$. X=$\{x_1, x_2, \dots, x_{256}\}$ including the histogram pixel values is a vector. x_i is the pixels number whose gray value is equal to i and x_j is the numbers of pixels whose gray value is equal to j. The variance is expected to be lower ever to get high uniformity. Nevertheless, $\chi^2(0.05; 255)$ should be lower than 293.25 to verify the significant level of 0.05 of χ^2 test [56]. The result which is regarding to the χ^2 test and variance is given in Table V for the test images in Figure 10.

Given that the pixel's values of a ciphertext image are varied when the image is encrypted. The more the complexity of variation, the more the encryption quality. The quality of IE can be measured by the average variation per pixel level. The frequency of pixel variation implies that the quality and efficacy of IE are proper. Encryption quality (EQ) given in Eq. (22) that measures the gray level variation rate was suggested for evaluation of this variation [57]. The more the EQ, the more the variation. In other words, the high EQ means that the IE highly manipulates the ciphertext image. It can be computed as given below:

$$EQ = \sum_{L=0}^{255}|H_L(C) - H_L(P)|/256 \tag{22}$$

Where, $L = \{1,2, \dots 255\}$ gray level pixel's value. Plaintext image, C is ciphertext image. $H_L(C)$ and $H_L(P)$ are the number of pixels respective to each pixel value for ciphertext and plaintext images, respectively. The proposed OPMAP-based IE is hence verified with respect to the results.

D. INFORMATION ENTROPY

Information entropy is a well-known metric that measures the disorderliness of an image [4]. Remember that information entropy in Eq. (8) is also utilized in the triple objective function in the optimization of OPMAP. The more the entropy close to 8, the more diffused the ciphertext image. The entropy of the test images encrypted via the proposed OPMAP-based IE is shown in Table VI and the results are verified in Table VII by comparison with the available ones in the literature [24]–[27], [29], [32], [33]. All entropies shown in the Table VI are so close to 8. Moreover, the images encrypted using the proposed OPMAP-based IE have the best entropy with 7.9995 among the reported IE schemes [24]–[27], [29], [32], [33]. Therefore, the proposed IE scheme with OPMAP provides the safest images against cyberattacks.

E. CORRELATION COEFFICIENT

Correlation analysis depends on the evaluation of the correlation coefficients of the adjacent pixels in three directions: Vertical, Diagonal and Horizontal. It is desired that an IE scheme minimizes the correlation coefficient of a ciphertext image. The correlation coefficient of an image that can be computed in three directions is:

$$r_{xy} = \frac{E[x - E(x)][y - E(y)]}{\sqrt{D(x)\sqrt{D(y)}}} \tag{23}$$

where, $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $D(x) = \frac{1}{N}\sum_{i=1}^{N}[(x_i - E(x)]^2$ are the two auxiliary equations. x_i and y_i are pixel values of i-th pair of the selected adjacent pixels, and N represents the number of the pixel samples, which are randomly selected as $N = 3000$ pixel samples. The three directions are diagonal, horizontal and vertical.

The correlation coefficients of the ciphertext test images using the OPMAP-based IE scheme are shown in Table VIII, and also they are checked with the available ones in the literature in Table IX [24]–[27], [29], [32], [33]. The proposed IE reduces the correlation coefficients very close to zero that can be seen in Table VIII. Moreover, it surpasses IE schemes in view of the correlation coefficients given in Table IX in the literature.

The 3D correlation distributions of the plaintext and the related ciphertext test images in the three directions are disclosed in Figure 11. The test images are indexed as Lena:1,

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

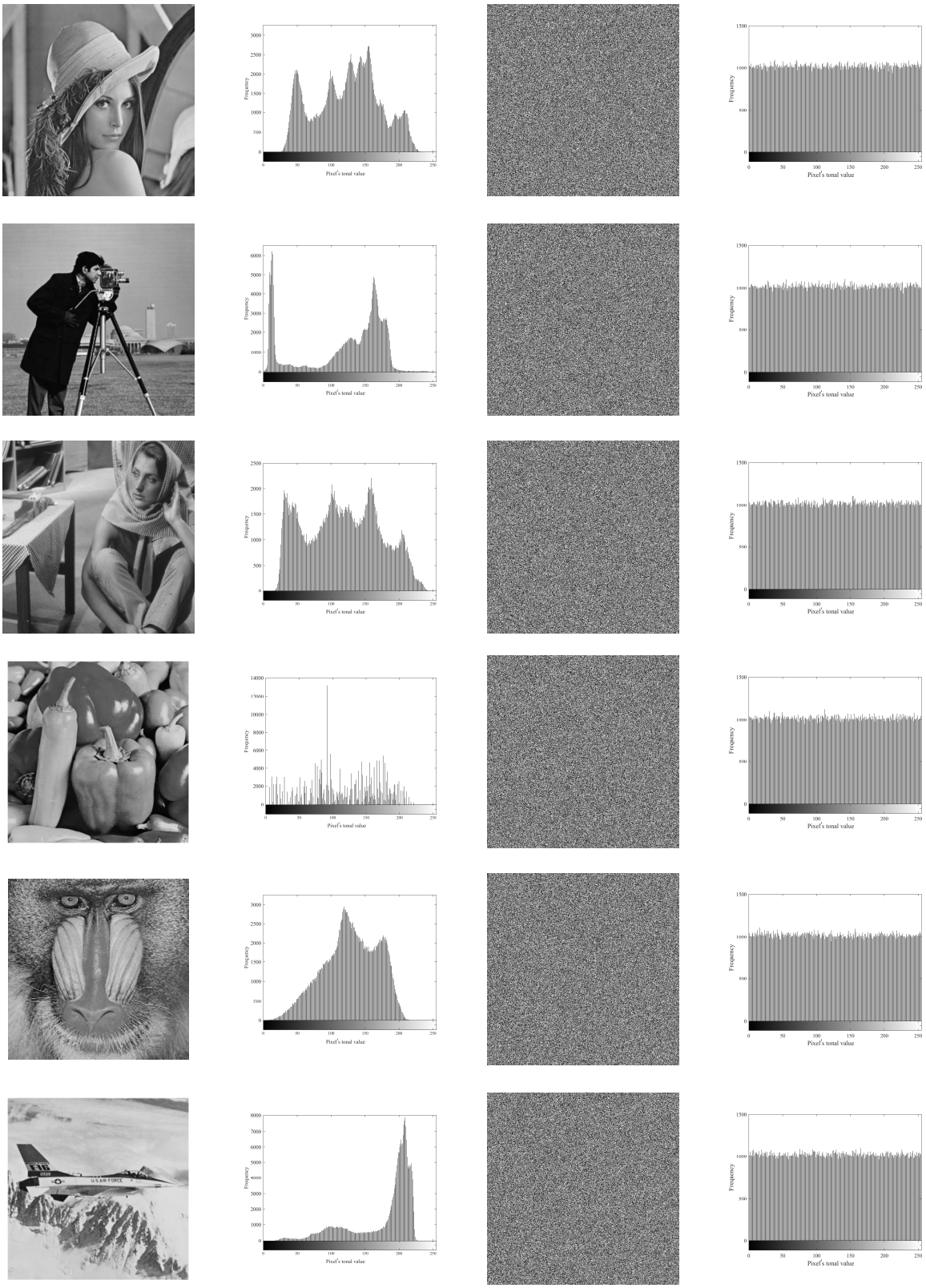


FIGURE 10. **Histograms: (a) the plaintext images, (b) histograms of the plaintext images, (c) the ciphered images, (d) the histograms of ciphered images.**

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

TABLE V
HISTOGRAM RESULTS IN TERMS OF VARIANCE AND χ^2 OF THE TEST IMAGES

Test	Image	Lena	Cameraman	Peppers	Baboon	Barbara	Airplane
var	Plaintext	6333788.75	1674120.58	2196605.10	845463.33	3821955.00	2832714.39
	Ciphertext	1021.28	992.89	1028.93	1012.23	985.09	1017.13
χ^2	Plaintext	158344.71	418530.14	549151.27	211365.83	95548.87	708178.59
	Ciphertext	256.83	252.21	259.30	256.04	243.27	253.29
	EQ	667.15	1003.57	516.78	1060.28	831.34	1078.74

TABLE VI
ENTROPIES OF THE CIPHERTEXT AND PLAINTEXT IMAGES VIA THE IE WITH OPMAP

Image	Lena	Cameraman	Barbara	Peppers	Baboon	Airplane
Plaintext image	7.4455	7.0479	7.6321	6.7624	7.2925	6.7135
Ciphertext image	7.9994	7.9995	7.9995	7.9995	7.9994	7.9995

TABLE VII
THE ENTROPIES OF THE CIPHERTEXT IMAGES AND THE COMPARISON WITH THE STATE OF THE ARTS

Ciphertext image	[24]	[25]	[26]	[27]	[29]	[32]	[33]	OPMAP
Lena	7.9994	7.9993	7.9993	7.9975	7.9994	7.9970	7.9982	7.9994
Cameraman	7.9970	-	-	-	7.9993	7.9973	-	7.9995
Barbara	-	7.9992	-	7.9985	-	-	7.9981	7.9995
Peppers	-	-	7.9994	-	7.9993	7.9969	-	7.9995

TABLE VIII
CORRELATION COEFFICIENTS OF THE CIPHERTEXT IMAGES

Direction	Lena	Cameraman	Barbara	Peppers	Baboon	Airplane
Horizontal	10×10^{-6}	-89×10^{-7}	-64×10^{-6}	79×10^{-6}	-38×10^{-6}	-63×10^{-6}
Vertical	-35×10^{-5}	12×10^{-6}	-43×10^{-5}	-36×10^{-5}	-25×10^{-6}	68×10^{-6}
Diagonal	-11×10^{-5}	-80×10^{-6}	-37×10^{-6}	-62×10^{-5}	-56×10^{-7}	91×10^{-6}

TABLE IX
THE COMPARATIVE CORRELATION COEFFICIENTS OF THE CIPHERTEXT IMAGES

Ciphertext image	Direction	[24]	[25]	[26]	[27]	[29]	[32]	[33]	OPMAP
Lena	Horizontal	73×10^{-5}	13×10^{-3}	10×10^{-4}	27×10^{-4}	32×10^{-4}	22×10^{-4}	14×10^{-4}	10×10^{-6}
	Vertical	44×10^{-5}	17×10^{-3}	-15×10^{-4}	13×10^{-4}	16×10^{-4}	13×10^{-4}	14×10^{-4}	-35×10^{-5}
	Diagonal	36×10^{-5}	67×10^{-5}	26×10^{-4}	11×10^{-4}	23×10^{-4}	8×10^{-4}	12×10^{-4}	-11×10^{-5}
Cameraman	Horizontal	93×10^{-4}	-	-	-	14×10^{-4}	39×10^{-4}	-	-89×10^{-7}
	Vertical	10×10^{-5}	-	-	-	2×10^{-4}	7×10^{-4}	-	12×10^{-6}
	Diagonal	31×10^{-4}	-	-	-	35×10^{-4}	86×10^{-4}	-	-80×10^{-6}
Barbara	Horizontal	-	-70×10^{-4}	-	-13×10^{-4}	-	-	12×10^{-4}	-64×10^{-6}
	Vertical	-	-79×10^{-4}	-	43×10^{-4}	-	-	27×10^{-4}	-43×10^{-5}
	Diagonal	-	-22×10^{-3}	-	10×10^{-4}	-	-	-10×10^{-4}	-37×10^{-6}
Peppers	Horizontal	-	-	7×10^{-5}	-	6×10^{-4}	1×10^{-4}	-	79×10^{-6}
	Vertical	-	-	43×10^{-4}	-	38×10^{-4}	-26×10^{-4}	-	-36×10^{-5}
	Diagonal	-	-	-18×10^{-4}	-	10×10^{-4}	-23×10^{-4}	-	-62×10^{-5}

TABLE X
DIFFERENTIAL ATTACK ANALYSIS FOR THE CIPHERTEXT IMAGES VIA THE PROPOSED OPMAP

Test	Lena	Cameraman	Barbara	Peppers	Baboon	Airplane
NPCR	99.6103	99.6094	99.6101	99.6082	99.6087	99.6090
UACI	33.4633	33.4654	33.4583	33.4616	33.4671	33.4623
NBCR	50.01	50.02	49.99	50.01	50.00%	50.01
MSE	10938.38	10939.74	10934.05	10934.44	10932.98	10930.42

TABLE XI
DIFFERENTIAL ATTACK ANALYSIS AND THE COMPARISON WITH THE STATE OF THE ARTS

Image	Test	[24]	[25]	[26]	[27]	[29]	[32]	[33]	OPMAP
Lena	NPCR	99.6078	99.5800	99.6000	99.6912	99.6000	99.6093	99.6621	99.6103
	UACI	33.4268	33.4300	33.4700	33.5098	33.5000	33.45969	33.5278	33.4633
Cameraman	NPCR	99.6323	-	-	-	99.6000	99.6068	-	99.6094
	UACI	33.4096	-	-	-	33.5500	33.4461	-	33.4654
Barbara	NPCR	-	99.6100	-	99.6912	-	-	99.7501	99.6101
	UACI	-	33.4300	-	33.5098	-	-	33.5102	33.4583
Peppers	NPCR	-	-	0.9960	-	99.6100	99.6057	-	99.6082
	UACI	-	-	33.4600	-	33.5200	33.50204	-	33.4616

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

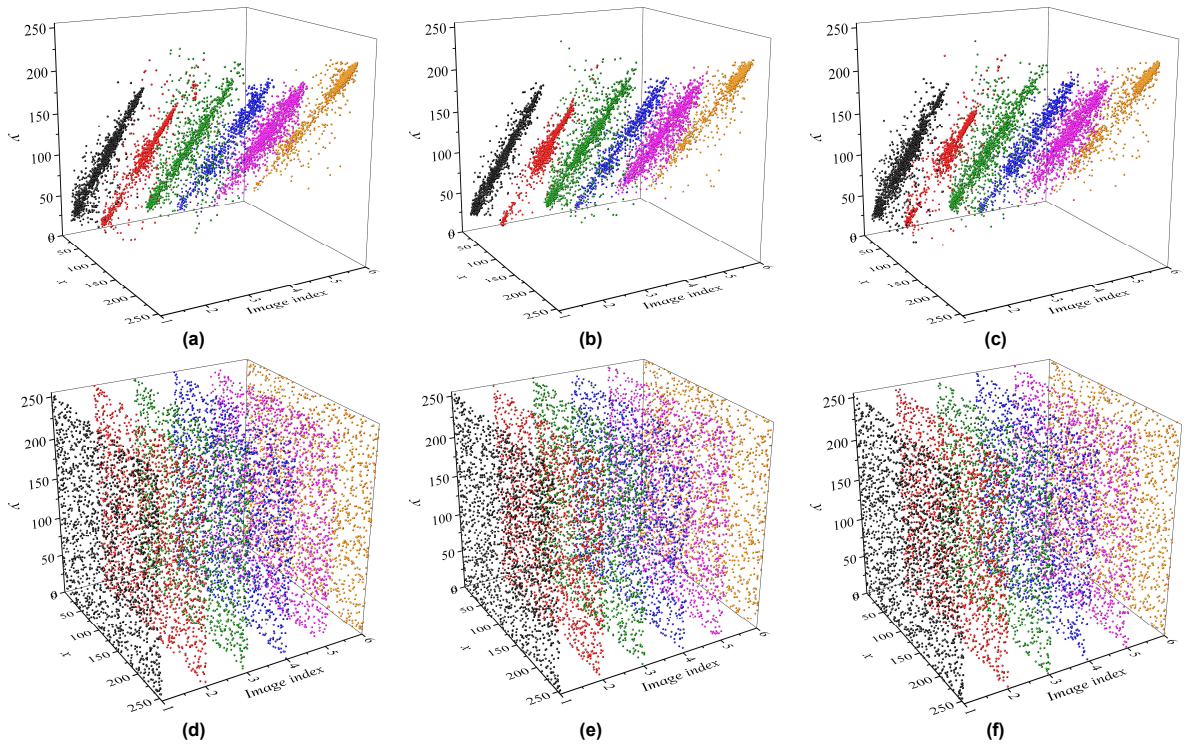


FIGURE 11. **The correlation distribution of the test images for the three directions: a) Plaintext Image-Horizontal, b) Plaintext image-Vertical, c) Plaintext image-Diagonal, d) Ciphertext image-Horizontal, e) Ciphertext image-Vertical, f) Ciphertext image-Diagonal *(Image index of Lena:1, Cameraman: 2, Barbara: 3, Peppers: 4, Baboon: 5, Airplane: 6)*.**

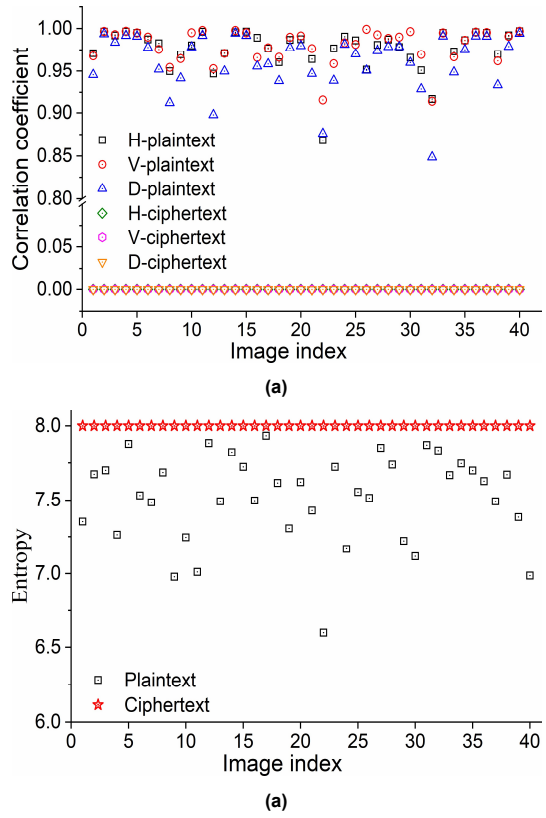


FIGURE 12. **Cryptanalyses for the plaintext and ciphertext 40#text-images** [58] **a) Correlation coefficients, b) Entropy.**

Cameraman: 2, Barbara: 3, Peppers: 4, Baboon: 5, Airplane: 6. The correlation distributions of the plaintext images mainly concentrate on $y = x$ line in Figure 11(a)-(c), while those of respective ciphertext images uniformly distribute and occupy all over the phase.

In order to further examine the proof of IE with OPMAP, an image database including 600x600 pixels 40#text-images with various features are employed for computation of correlation coefficient and entropy [58]. The computed results for the 40#text-images are scattered in Figure 12. As the mean of correlation coefficients of plaintext 40#text-images is 0.9729, that of ciphertext 40#text-images is diminished to $1.11x10^{-6}$. On the other hand, while the average entropy of the plaintext 40#text-images is 7.5154, that of ciphertext 40#text-images is 7.9996. Therefore, the proposed OPMAP-based IE shows stable encryption performance not for a limited number of images but also a large number of images.

F. DIFFERENTIAL ATTACK

This cryptanalysis attack aims to unravel the key and descry IE. It proves an IE counters the cyberthreats by examining the difference between two ciphertext images one of which one-pixel altered in the plaintext image. Therefore, encryption capacity of an IE can be appraised if it is sensitive to the minor change in the pixels of plaintext image. Differential attack analysis can be evaluated as follows:

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

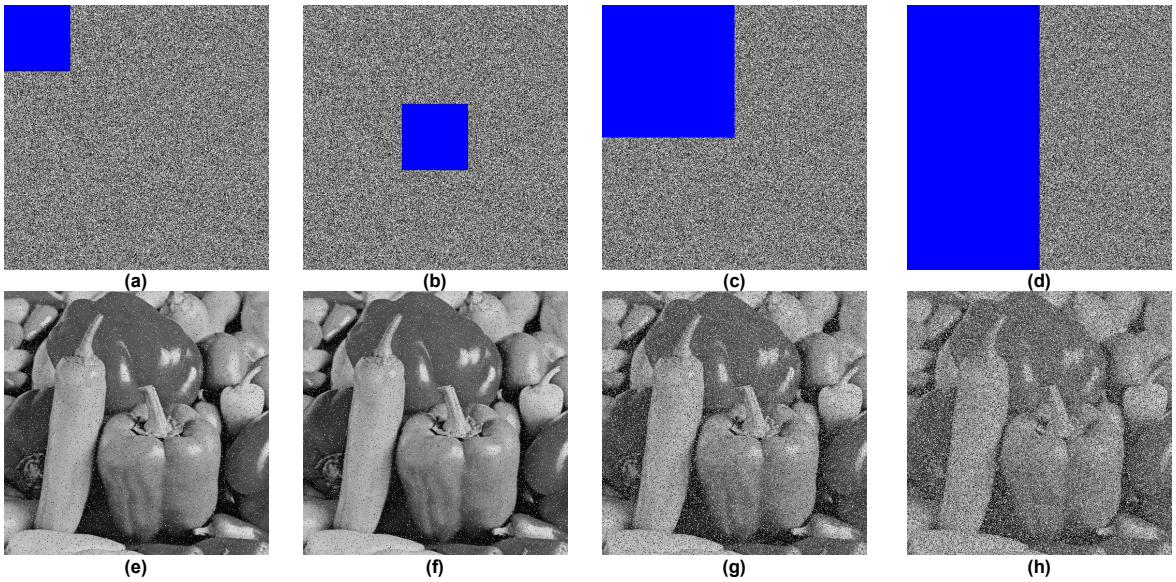


FIGURE 13. **Cropping attack analysis for the proposed OPMAP-based IE with for the Peppers image, ciphered images cropped with ratios a) 1/16, b) 1/16 (middle), c) 1/4, d) 1/2, and deciphered images with ratios e) 1/16, f) 1/16 (middle), g) 1/4, h) 1/2.**



FIGURE 14. **The comparative cropping attack analysis for the decipher Lena image cropped with 1/16 ratio: (a)** [32]**, (b)** [24]**, (c)** [49]**, (d)** [50]**, (e) [11] (f)** [51]**, (g)** [52]**, (h)** [53]**, (i) OPMAP.**

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

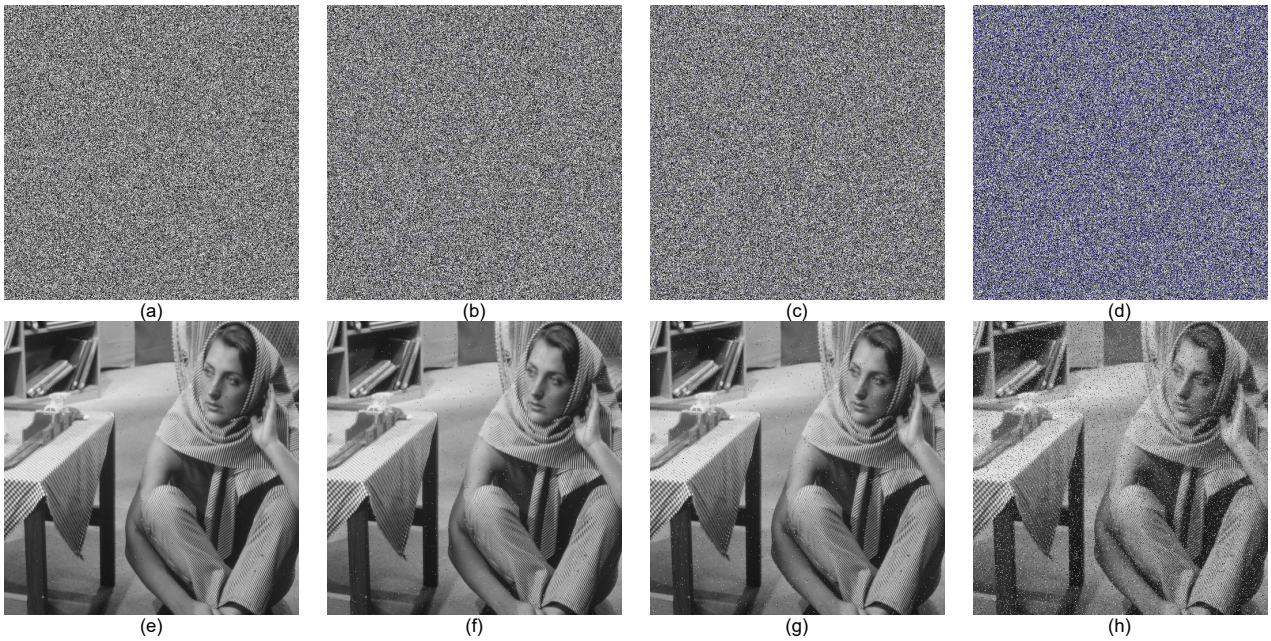


FIGURE 15. Ciphertext images with adding different SPN densities are a) 0.001, b) 0.005, c) 0.01, d) 0.1 and the related decipher images with SPN densities are e) 0.001, f) 0.005, g) 0.01, h) 0.1 (SPN is shown with blue pixels).

TABLE XII
THE PSNR AND SSIM METRICS WITH CROPPING EFFECTS WITH PLAINTEXT IMAGE REFERENCE VIA OPMAP

Image	Metric	Cropping ratio					
		1/16		1/4		1/2	
		Ciphertext	Decipher	Ciphertext	Decipher	Ciphertext	Decipher
Lena	PSNR	8.91	21.37	8.01	15.25	7.70	12.15
	SSIM	0.1056	0.8299	0.1578	0.7482	0.1912	0.4147
Camera.	PSNR	7.82	20.58	7.49	14.93	7.73	11.81
	SSIM	0.1404	0.7859	0.2385	0.5329	0.1587	0.3691
Barbara	PSNR	8.76	20.98	7.29	15.02	7.01	11.98
	SSIM	0.0957	0.8667	0.1065	0.6662	0.1484	0.4680
Pepper	PSNR	8.61	21.02	7.97	14.99	7.18	11.96
	SSIM	0.0815	0.8275	0.1204	0.6015	0.1770	0.4193
Baboon	PSNR	8.82	21.78	8.46	15.66	7.16	12.69
	SSIM	0.1668	0.7962	0.1018	0.7043	0.1417	0.4897
Airplane	PSNR	7.41	20.23	6.06	14.25	4.94	11.17
	SSIM	0.1075	0.7682	0.1807	0.5495	0.2863	0.3894

TABLE XIII
THE PSNR METRIC FOR CROPPING EFFECTS AND COMPARISON WITH THE STATE OF THE ARTS

Image	Cropping ratio	[24]	[11]	[51]	OPMAP
Lena	1/16	17.58	16.66	20.78	21.37
	1/4	15.03	10.64	14.96	15.25
	1/2	12.13	10.66	12.08	12.15

TABLE XIV
THE PSNR AND SSIM METRICS FOR NOISE EFFECTS WITH PLAINTEXT IMAGE REFERENCE VIA OPMAP

Image	Metric	SPN density							
		0.001		0.005		0.01		0.1	
		Ciphertext	Decipher	Ciphertext	Decipher	Ciphertext	Decipher	Ciphertext	Decipher
Barbara	PSNR	8.81	40.23	8.78	32.40	8.76	29.06	8.29	18.91
	SSIM	0.065	0.998	0.064	0.996	0.061	0.0973	0.051	0.0817

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

$$D(i,j) = \begin{cases} 0, if\ C^1(i,j) = C^2(i,j) \\ 1, if\ C^1(i,j) \neq C^2\ (i,j) \end{cases} \quad (24)$$

$$NPCR = \frac{\sum_{i,j} D(i,j)}{mxn} x100\% \quad (25)$$

$$UACI = \frac{1}{mxn}\left[\sum_{i,j} \frac{|C^1(i,j) - C^2(i,j)|}{255}\right] x100\% \quad (26)$$

here m stands for the height, n refers to width of a test image. C^1 and C^2 are ciphertext images before and after one-pixel altered in a plaintext image. For a one-pixel altered 8-bit grayscale images image, the ideal scores of NPCR is 99.6094% and UACI is 33.4635% [59]. The NPCR and UACI values for the test images encrypted via the IE with OPMAP are given in Table X. Moreover, NBCR and MSE for the same images are inserted in Table X. The NPCR and UACI values for Cameraman, Lena, Barbara and Peppers are compared with the state of the arts in Table XI. Therefore, the outcomes of the proposed OPMAP-based IE are the closest to the ideal scores.

G. CROPPING ATTACK

This analysis puts to proof an IE scheme for losing some region of the ciphertext images. It hereby assesses the recovering performance of an IE scheme. Therefore, a resistant IE could decrypt a cropped ciphertext image with a least degradation. The ciphertext Peppers image cropped with the ratios of 1/16, 1/16 (middle), 1/4, 1/2 and decipher images are illustrated in Figure 13. Furthermore, the decipher Lena images those of ciphertext image cropped with ratio 1/16 is compared with the state of the art in Figure 14. From the illustrated results, the proposed IE decrypts the cropped images with the minimum degradation.

Moreover, the decipher images with cropping attack by the OPMAP-based IE are numerically assessed in terms of reliable full-reference image quality metrics such as PSNR Eq. (27) and SSIM Eq. (28).

$$PSNR := 10 \log\left(\frac{255^2}{MSE}\right) \quad (27)$$

$$\mathrm{SSIM}(X,Y) := \frac{(2\mu_X\mu_Y + C_1) + (2\sigma_{XY} + C_2)}{(\mu_X^2 + \mu_Y^2 + C_1) + (\sigma_X^2 + \sigma_Y^2 + C_2)} \quad (28)$$

where μ_X and μ_Y are the mean intensities; σ_X and σ_Y are the standard deviations and σ_{XY} is the cross-covariance of images X and Y. Besides, $C_1 := (K_1L)^2$ and $C_2 := (K_2L)^2$ are two constants with $K_1 = 0.01,\ K_2 = 0.03$ and $L = 255$ for 8-bit grayscale images [60], [61]. The higher the both metrics, the lower the degradation. The PSNR and SSIM results of the decipher images via the proposed OPMAP-based IE with are given in Table XII, and that of the Lena image are checked with the state of the arts in Table XIII [11], [24], [51]. Owing to higher metrics, the cropping attack analysis of the OPMAP-based IE is confirmed.

H. NOISE ATTACK

This analysis puts the proof an IE for adding some SPN to the ciphertext images. Noise attack analysis is hereby employed to apprise the redeeming performances of an IE scheme. The decipher images with different SPN densities 0.001, 0.005, 0.01, 0.1 are presented in Figure 15. Hence, they are verified through the PSNR and SSIM tabulated in Table XIV. Eventually, the suggested OPMAP-based IE redeems the images with the least degradation.

I. ENCRYPTION SPEED AND COMPUTATIONAL COMPLEXITY

The encryption speed is significant to evaluate an IE scheme to be eligible to the real systems. The EPT of the proposed OPMAP-based IE with is 0.2919 (s). This time includes production time of the public key 0.0145 (s). The decryption time is 0.2763 (s). Additionally, the computational complexity of an algorithm could be assessed via big O notation. The computational complexity of the proposed IE is $O(m \times n)$, here m and n stand for size of the image. In order to validate the speed of the IE scheme, a further comparison with the state of the arts are performed through independent parameters such as the ET in Eq. (29) and NCPB in Eq. (30) in addition to encryption processing time. Notice that the ET and NCPB depend on the image size and central process unit (CPU) speed, respectively. The comparative results are given in Table XV. The ET calculates processed image's byte per second and NCPB computes the operated CPU clock per byte. For a faster IE scheme, the ET should be increased and the NCPB should decreased as much as possible. Therefore, the speed of OPMAP is competitive as compared with the others, meaning that it could be applied to the real systems.

$$ET := \frac{Image\ size\ (Byte)}{Encryption\ Time\ (s)} \quad (29)$$

$$NCPB := \frac{CPU\ Speed\ (Hz)}{ET} \quad (30)$$

TABLE XV
COMPARATIVE ENCRYPTION SPEED PARAMETERS

Ref.	CPU (GHz)	EPT(s) (512x512)	ET (Mbps)	NCPB
[23]	3.2	0.5042	0.49583	6155
[26]	3.2	0.0700	3.57143	854
[27]	3.8	0.2810	0.88968	4073
[28]	3.6	0.4442	0.56281	6100
[31]	2.3	0.2240	1.11607	1965
[32]	2.6	0.0605	4.13223	600
[33]	3.5	0.2760	0.90580	3685
[34]	3.3	1.2800	0.19531	16113
[35]	2.3	0.0239	10.46025	210
[36]	3.6	0.9730	0.25694	13362
[19]*	—	14.8750	0.01681	—
[18]*	1.7	600.00	0.00042	3890991
[15]*	—	89.1550	0.00280	—
[11]*	3.0	1.1247	0.22228	12871
[14]*	3.5	0.1748	1.43021	2334
This study	3.5	0.2919	0.85646	3897

The works indicated with asterisk represent the optimization algorithms used.

VII. CONCLUSION

The proposed 2D-OPMAP is modeled with eight decision variables that are optimized using TODE algorithm. OPMAP optimization considers the three objective functions including

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

the entropy, LE and 0-1 test. OPMAP is assessed with respect to many reliable measurements pertaining bifurcation, 3D phase space, LE, 0-1 test, PE and SE. OPMAP-based IE is incurred numerous cryptanalyses, and the observable and quantitative numeric results are validated with the state of the arts with/without optimization used. The outperforming cryptanalyses like key space, mean entropy, mean correlation, NPCR, UACI, encryption processing time are 2^{298}, 7.9995, 0.0001361, 99.6093, 33.4630 and 0.2919 (s), respectively. The results of copping and noise attacks are also remarkable. They are elaborately surveyed and compared with state of the arts so as to validate superiority of the IE with OPMAP. It is clearly demonstrated that the proposed IE comes to fore within the compared ones thanks to the optimized chaotic properties of OPMAP that achieved by TODE. The proposed OPMAP-based IE scheme does not employ optimization in the IE processes although OPMAP is constituted by the triple-objective optimization. As a result, the recommended 2D-OPMAP-based IE fast and securely encrypts the images due to the optimized dynamic characteristic of the OPMAP.

REFERENCES

[1] K. Xuejing and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Process. Image Commun.*, vol. 80, pp. 1–11, Feb. 2020.

[2] M. Alawida, A. Samsudin, J. Sen Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45–58, Jul. 2019.

[3] L. Bao, S. Yi, and Y. Zhou, "Combination of Sharing Matrix and Image Encryption for Lossless (k,n)-Secret Image Sharing," *IEEE Trans. Image Process.*, vol. 26, no. 12, pp. 5618–5631, Dec. 2017.

[4] F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble, "Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data," *IEEE Trans. Ind. Informatics*, vol. 15, no. 7, pp. 4362–4369, Jul. 2019.

[5] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of a DNA-based image encryption scheme," *Inf. Sci. (Ny).*, vol. 520, pp. 130–141, May 2020.

[6] Y. Liu, Z. Qin, X. Liao, and J. Wu, "Cryptanalysis and enhancement of an image encryption scheme based on a 1-D coupled Sine map," *Nonlinear Dyn.*, vol. 100, pp. 2917–2931, May 2020.

[7] W. Wen, K. Wei, Y. Zhang, Y. Fang, and M. Li, "Colour light field image encryption based on DNA sequences and chaotic systems," *Nonlinear Dyn.*, vol. 99, no. 2, pp. 1587–1600, Jan. 2020.

[8] P. Zheng and J. Huang, "Efficient Encrypted Images Filtering and Transform Coding with Walsh-Hadamard Transform and Parallelization," *IEEE Trans. Image Process.*, vol. 27, no. 5, pp. 2541–2556, May 2018.

[9] S. Carbas, A. Toktas, and D. Ustun, Eds., *Nature-Inspired Metaheuristic Algorithms for Engineering Optimization Applications*. Springer Singapore, 2021.

[10] S. Suri and R. Vijay, "A Pareto-optimal evolutionary approach of image encryption using coupled map lattice and DNA," *Neural Comput. Appl.*, vol. 32, no. 15, pp. 11859–11873, Aug. 2020.

[11] X. Wang and Y. Li, "Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence," *Opt. Lasers Eng.*, vol. 137, p. 106393, Feb. 2021.

[12] M. Ahmad, M. Z. Alam, Z. Umayya, S. Khan, and F. Ahmad, "An image encryption approach using particle swarm optimization and chaotic map," *Int. J. Inf. Technol.*, vol. 10, no. 3, pp. 247–255, Sep. 2018.

[13] N. K. Sreelaja and G. A. Vijayalakshmi Pai, "Stream cipher for binary image encryption using Ant Colony Optimization based key generation," *Appl. Soft Comput. J.*, vol. 12, no. 9, pp. 2879–2895, Sep. 2012.

[14] A. Toktas, U. Erkan, and D. Ustun, "An image encryption scheme based on an optimal chaotic map derived by multi-objective optimization using ABC algorithm," *Nonlinear Dyn. 2021 1052*, vol. 105, no. 2, pp. 1885–1909, Jul. 2021.

[15] S. Saravanan and M. Sivabalakrishnan, "A hybrid chaotic map with coefficient improved whale optimization-based parameter tuning for enhanced image encryption," *Soft Comput.*, vol. 48, pp. 1–24, Jan. 2021.

[16] Y. Su, C. Tang, X. Chen, B. Li, W. Xu, and Z. Lei, "Cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm and Henon map," *Opt. Lasers Eng.*, vol. 88, pp. 20–27, Jan. 2017.

[17] A. S. Muhammad and F. Özkaynak, "SIEA: Secure Image Encryption Algorithm Based on Chaotic Systems Optimization Algorithms and PUFs," *Symmetry 2021, Vol. 13, Page 824*, vol. 13, no. 5, p. 824, 2021.

[18] M. Dua, A. Wesanekar, V. Gupta, M. Bhola, and S. Dua, "Differential evolution optimization of intertwining logistic map-DNA based image encryption technique," *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 9, pp. 3771–3786, Sep. 2020.

[19] M. Kaur, D. Singh, and R. S. Uppal, "Parallel strength Pareto evolutionary algorithm-II based image encryption," *IET Image Process.*, vol. 14, no. 6, pp. 1015–1026, May 2020.

[20] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimens. Syst. Signal Process.*, vol. 32, no. 1, pp. 281–301, Jan. 2020.

[21] M. Kaur, V. Kumar, and L. Li, "Color image encryption approach based on memetic differential evolution," *Neural Comput. Appl.*, vol. 31, no. 11, pp. 7975–7987, Nov. 2019.

[22] S. Sajasi and A. M. Eftekhari Moghadam, "An adaptive image steganographic scheme based on Noise Visibility Function and an optimal chaotic based encryption method," *Appl. Soft Comput. J.*, vol. 30, pp. 375–389, May 2015.

[23] H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 144, pp. 444–452, Mar. 2018.

[24] Y. Yang, L. Wang, S. Duan, and L. Luo, "Dynamical analysis and image encryption application of a novel memristive hyperchaotic system," *Opt. Laser Technol.*, vol. 133, p. 106553, Jan. 2021.

[25] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 1, pp. 219–237, Jan. 2019.

[26] S. Hanis and R. Amutha, "A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterfly-like structure," *Nonlinear Dyn.*, vol. 95, no. 1, pp. 421–432, Jan. 2019.

[27] M. Asgari-Chenaghlu, M. A. Balafar, and M. R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," *Signal Processing*, vol. 157, pp. 1–13, Apr. 2019.

[28] R. Lan, J. He, S. Wang, T. Gu, and X. Luo, "Integrated chaotic systems for image encryption," *Signal Processing*, vol. 147, pp. 133–145, Jun. 2018.

[29] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Processing*, vol. 153, pp. 11–23, Dec. 2018.

[30] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation," *Opt. Laser Technol.*, vol. 121, p. 105777, Jan. 2020.

[31] R. Enayatifar, F. G. Guimarães, and P. Siarry, "Index-based permutation-diffusion in multiple-image encryption using DNA sequence," *Opt. Lasers Eng.*, vol. 115, pp. 131–140, Apr. 2019.

[32] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision," *Signal Processing*, vol. 168, no. 107340, pp. 1–10, Mar. 2020.

[33] M. Asgari-Chenaghlu *et al.*, "Cy: Chaotic yolo for user intended image encryption and sharing in social media," *Inf. Sci. (Ny).*, vol. 542, pp. 212–227, Jan. 2021.

[34] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3111691, IEEE Access

cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, Feb. 2019.

[35] A. Mansouri and X. Wang, "A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme," *Inf. Sci. (Ny).*, vol. 520, pp. 46–62, May 2020.

[36] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci. (Ny).*, vol. 480, pp. 403–419, Apr. 2019.

[37] X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, "Color image compression and encryption scheme based on compressive sensing and double random encryption strategy," *Signal Processing*, vol. 176, p. 107684, Nov. 2020.

[38] G. Ye *et al.*, "Asymmetric image encryption scheme based on the Quantum logistic map and cyclic modulo diffusion," *Math. Biosci. Eng. 2021 55427*, vol. 18, no. 5, pp. 5427–5448, 2021.

[39] G. Ye, K. Jiao, H. Wu, C. Pan, and X. Huang, "An Asymmetric Image Encryption Algorithm Based on a Fractional-Order Chaotic System and the RSA Public-Key Cryptosystem," *https://doi.org/10.1142/S0218127420502338*, vol. 30, no. 15, 2020.

[40] J. Zeng and C. Wang, "A Novel Hyperchaotic Image Encryption System Based on Particle Swarm Optimization Algorithm and Cellular Automata," *Secur. Commun. Networks*, vol. 2021, 2021.

[41] Z. Li, C. Peng, W. Tan, and L. Li, "An Effective Chaos-Based Image Encryption Scheme Using Imitating Jigsaw Method," *Complexity*, vol. 2021, 2021.

[42] R. Storn and K. Price, "Differential Evolution – A Simple and Efficient Heuristic for global Optimization over Continuous Spaces," *J. Glob. Optim.*, vol. 11, no. 4, pp. 341–359, 1997.

[43] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.

[44] G. A. Gottwald and I. Melbourne, "The 0-1 test for chaos: A review," in *Lecture Notes in Physics*, vol. 915, Springer Verlag, 2016, pp. 221–247.

[45] C. Bandt and B. Pompe, "Permutation Entropy: A Natural Complexity Measure for Time Series," *Phys. Rev. Lett.*, vol. 88, no. 17, p. 4, 2002.

[46] J. Wang, G. Liu, Y. Chen, and S. Wang, "Construction and Analysis of SHA-256 Compression Function Based on Chaos S-Box," *IEEE Access*, vol. 9, pp. 61768–61777, 2021.

[47] M. Alawida, J. Sen Teh, D. P. Oyinloye, W. H. Alshoura, M. Ahmad, and R. S. Alkhawaldeh, "A New Hash Function Based on Chaotic Maps and Deterministic Finite State Automata," *IEEE Access*, vol. 8, pp. 113163–113174, 2020.

[48] M. Alawida, A. Samsudin, N. Alajarmeh, J. Sen Teh, M. Ahmad, and W. H. Alshoura, "A Novel Hash Function Based on a Chaotic Sponge and DNA Sequence," *IEEE Access*, vol. 9, pp. 17882–17897, 2021.

[49] F. Yang, J. Mou, J. Liu, C. Ma, and H. Yan, "Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application," *Signal Processing*, vol. 169, pp. 1–16, Apr. 2020.

[50] Y. Wu, L. Zhang, T. Qian, X. Liu, and Q. Xie, "Content-adaptive image encryption with partial unwinding decomposition," *Signal Processing*, vol. 181, p. 107911, Apr. 2021.

[51] Y. Luo *et al.*, "A robust image encryption algorithm based on Chua's circuit and compressive sensing," *Signal Processing*, vol. 161, pp. 227–247, Aug. 2019.

[52] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Processing*, vol. 148, pp. 124–144, Jul. 2018.

[53] X. Wang and S. Gao, "Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network," *Inf. Sci. (Ny).*, vol. 539, pp. 195–214, Oct. 2020.

[54] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurc. Chaos*, vol. 16, no. 8, pp. 2129–2151, Aug. 2006.

[55] J. C. H. Castro, J. M. Sierra, A. Seznec, A. Izquierdo, and A. Ribagorda, "The strict avalanche criterion randomness test," *Math. Comput. Simul.*, vol. 68, no. 1, pp. 1–7, Feb. 2005.

[56] X. Zhang, Z. Zhao, and J. Wang, "Chaotic image encryption based on circular substitution box and key stream buffer," *Signal Process. Image Commun.*, vol. 29, no. 8, pp. 902–913, 2014.

[57] H. E. H. Ahmed, H. M. Kalash, and O. S. F. Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images," *Opt. Eng.*, vol. 45, no. 10, p. 107003, Oct. 2006.

[58] N. Asuni and A. Giachetti, "TESTIMAGES: a large-scale archive for testing visual devices and basic image processing algorithms," in *STAG: Smart Tools & Apps for Graphics (2014)*, 2014.

[59] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," *Cyber Journals Multidiscip. Journals Sci. Technol. J. Sel. Areas Telecommun.*, pp. 31–38, 2011.

[60] U. Erkan, S. Enginoglu, and D. N. H. Thanh, "A Recursive Mean Filter for Image Denoising," *2019 Int. Artif. Intell. Data Process. Symp.*, pp. 1–5, Sep. 2019.

[61] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.



ABDURRAHIM TOKTAS received BSc degree in Electrical and Electronics Engineering at Gaziantep University, Turkey, in Jul. 2002. He received MSc and PhD degrees in EEE at Mersin University, Turkey, in Jan. 2010 and Jul. 2014, respectively. Since Jan. 2015, he has been with Department of Electrical and Electronics Engineering, Karamanoglu Mehmetbey University, Turkey. His current research interests include modelling, radar absorber, antenna design, MIMO antenna, UWB antenna, surrogate model, evolutionary optimization, machine learnings and cryptology.



UGUR ERKAN received the BSc. degree in computer engineering from Selçuk University, Turkey, in 2001, the MSc. degree in mathematics and the PhD degree in mechatronics engineering from Gaziosmanpaşa University, Turkey, in 2012 and 2017, respectively. He is currently an Assistant Professor with the Department of Computer Engineering, Karamanoğlu Mehmetbey University, Karaman, Turkey. His research interests include image processing, image denoising, image restoration, image encryption, and machine learning.



FEYZA TOKTAS received the BSc degree in Electrical and Electronics Engineering from Gaziantep University, Gaziantep, Turkey, in 2002 and the MSc. degree in computer engineering from Karamanoglu Mehmetbey University, Karaman, Turkey, in 2019. She is currently pursuing PhD degree in Computer Engineering at Mersin University, Mersin, Turkey. From 2007 to 2014, she was a lecturer with the Vocational School, Mersin University, Mersin, Turkey. From 2014 up to now, she has been with the Karamanoglu Mehmetbey University, Karaman, Turkey as a project engineer. Her research interest includes image encryption, surrogate model, and optimization algorithms.



ZEKİ YETGİN is currently professor at the department of computer engineering in Mersin University. He received a BSc degree in 1999 and an MSc degree in 2002 from Eastern Mediterrenean University, Computer Engineering Department, Turkish Republic of Northern Cyprus. He has received his PhD in Department of Computer Engineering from Dokuz Eylul University, Izmir, Turkey, in 2008. He received Assoc.Prof. degree in 2014 and promoted to Prof. position in 2020. His research interests are machine learning, optimization, network and multimedia. He is particularly involved in honey formation optimization and QoE of multimedia services.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/