A New Chaos-based Approach for Robust Image Encryption

Ibrahim Yasser[1], Abeer T. Khalil[1], Mohamed A. Mohamed[1], and Fahmi Khalifa[1,2]

[1]Electronics and Communications Engineering Department, Faculty of Engineering, Mansoura University
Mansoura Dakahlyis 35516, Egypt
[2] Bioengineering Department, university of Louisville, Louisville KY 40292, USA

Email address: {Ibrahim_yasser, abeer.twakol, mazim12}@mans.edu.eg; fahmi.khalifa@louisville.edu

Abstract

Chaotic encryptions offered various advantages over traditional encryption methods, like high security, speed, reasonable computational overheads. This paper introduces novel perturbation techniques for data encryption based on double chaotic systems. A new technique for image encryption utilizing mixed the proposed chaotic maps is presented. The proposed hybrid system parallels and combines two chaotic maps as part of a new chaotification method. It based on permutation, diffusion and system parameters, which are then involved in pixel shuffling and substitution operations, respectively. Many statistical test and security analysis indicate the validity of the results, e.g., the average values for NPCR and UACI are 99.67145% and 33.63288%, respectively. The proposed technique can achieve low residual intelligibility, high sensitivity and quality of recovered data, high security performance, and it show that the encrypted image has good resistance against attacks.

Keywords: chaotic map, cryptography, Image encryption, and Security analysis

1.Introduction

With the speedy growth of communication technology, it has become vital to protect private data from unauthorized access or attackers. Data exchange is closely related to everyday life, inlcuding education, commerce, economics, military, elearning, online banking as well as news telecasting. Modern telecommunication and multimedia technologies advancement enabled huge amount of sensitive data travel over the open and shared networks in a daily routine. This in turns require data protections before and/or during transmission or distribution. Thus, certain cryptograph methods/algorithms are utilized to convert the intelligible data to unintelligible form (i.e., encrypted) before transmitting. Modern cryptography algorithms are successful for text data. But due to the bulk data capacity and high redundancy, they fail to provide computational security. The techniques focused on chaos are considered effective in dealing with voluminous, redundant data. They provide fast, highly secure methods of encryption.

Some recent studies have shown that there are security vulnerabilities in some chaos based image encryption algorithm. Zahmoul et al [1] introduced a beta map to produce different chaotic sequences in permutation, diffusion, and substitution. Their algorithm effectively enhanced encryption security. A system of two self-regulating chaotic functions is introduced by Yayuz et al [2]. Their method aim is sufficiently apply confusion/ diffusion principles for images with different entropies. The resistance of the cryptosystem to differential attacks is increased by employing

DOI: 10.5281/zenodo.5207724
Received: March 10, 2021 Accepted August 08, 2021

additional exclusive-or (XOR) and circular rotation processes on the encrypted values of image pixels. However, the methods' complexity is high, despite good performance. An image encryption pipeline by Zhang [3] utilized both piecewise liner chaotic maps and S-box to generate key stream that exhbit excellent statistical characteristics. Zhang's cryptosystem showed near-identical encryption and decryption process with a large key space and fast encryption speed. However, the encrypted data still exhbit high correlation. Aqeel-ur-Rehman et al. [4] introduced a an hybrid image encryption method. In their method, the key stream is generated by hyper-chaotic system that is related to the plain image. Although the algorithm show high complexity, it easily be attacked due to its small key space. Huang et al [5] developed a symmetric plaintext-related encryption system in which permutation and diffusion operations into a single stage, temed as PDSO. An encryption algorithm by Lou et al. [6] utilized the DNA method for diffusion of the image pixels and permuted using a two dimensional Hénon-sine map (2D-HSM). Parvaz and Zarebnia [7] defined a chaotic system based on the combination of several maps. i.e., logistic, sine, and tent maps. Simulation results proved security and practicability of the scheme, while the encryption algorithm is not satisfactory. Wu et al. [8] proposed a 2D-HSM that demonstrated better chaotic characteristics than many existing chaos-based systems. The evaluation of the litreature work revealed the following security problems in the existing aencryption algorithms; (1) most of them can't resist chosen-plaintext attacks; (2) the encryption algorithm is also insensitive to various (if not all) chaotic secret keys; (3) the first pixel in the cipherd image cannot be decrypted in the decryption stage; (4) there are additional restrictions on parameters selection of the inverse rectangular transform system.

To partially fix the security defects, we devloped an improved image encryption algorithm. The main objective of this work is to develop a data encryption pipeline with low residual clarity, key sensitivity, and maintaining higher quality of data reconstructed by chaotic maps. Particularly, in this work we devleloped 2D alteration models for a secure image encryption algorithm. Based on the dynamical analysis and various analysis metrics, the developed map demonstrated overall hyper chaotic behviour with the high complexity and sensitivity. Furthermore, those maps are utilized in a new image encryption algorithm that is tested and evaluated on various benchemric images. Simulation results and security analysis documented the high security for proposed image encryption and the system generally possess strong capability to withstand various attacks

The reminder of this paper is sectioned as follows: In the next section, a general introduction on chaotic systems is discussed as an example of existing cryptosystems. In Section 3, the proposed cryptosystems and the proposed image encryption system are presented. Section 4 introduces the quantitative performance metrics. Section 5 presents the test results for the proposed cryptosystem. Finally, the concluding remarks and suggested future works are given is Section 6.

2. Chaotic System

In recent year, chaotic-based encryption have been shown as is one of the emerging security technologies in the modern encryption zone. Chaos theory has been established by both physicists and mathematicians and has possess important attributes, such as deterministically, nonlinearity, irregularity, and sensitivity to initial settings [9]. Thee latter attributes encourage security research community to utilize chaos theory in contemporary cryptography. A function that has some kind of disordered behavior can be defined as a chaotic map. As Table 1 shows, chaotic maps can be integrated in cipher system in two different ways. The first is by generating pseudorandom key stream using chaotic systems. While the second is by using the plain text or secret key(s) as system initial settings and/or control parameters [10]. The first way matches stream cipher while the second corresponds to block ciphers. In either way, iterations are applied on chaotic systems to obtain cipherd data. The employment of chaotic maps in cryptography systems lies in the fact that chaotic maps are characterized by sevral attractable attributes, including

DOI: 10.5281/zenodo.5207724
Received: March 10, 2021 Accepted August 08, 2021

(1) the high sensitivity to initial conditions and control parameters, (2) the unpredictability of the orbital evolution, and (3) the simplicity of both hard- and soft-ware implementations leading to high encryption rates [11].

Table 1 –The detailed setting

Chaotic systems	**Cryptography algorithm**
Phase space : set of real numbers	Phase space: finite set of integer numbers
Iterations	Rounds
Parameters	Key
Sensitivity to initial conditions and control parameters	Diffusion

3. The Proposed Cryptosystems

In this section, the proposed chaotic systems will be described. It is 2-D, nonlinear and discrete time that provide dynamical chaotic behavior. In stochastic searching optimization algorithms, the methods utilizing chaotic variables as a substitute of random variables are referred to as chaotic optimization algorithm. Because of the nonreapeatability and erogdicity of chaos, the latter algorithms can achieve overall searches at higher speeds than stochastic counterparts [12]. The developed chaotic maps are employed to produce the chaotic sequence and are used to control the encryption process. Among the various developed maps, two maps are investigated and their characteristics are analyzed [10].

3.1 The proposed chaotic maps

The first map can be considered as a two-dimensional extension of the logistic map and have the nearly shape of Henon map, it can represented by the following equation:

$$\begin{cases} y_{n+1} = \; tan\, y_n - k\; sin\, x_n \\ x_{n+1} = \sin x_n + \; tany_{n+1} \end{cases} \qquad (1)$$

where the state variables *x* and *y* are the simulated time series, *k* represents the external control parameter, and *n* is the number of the simulated points. The second proposed chaotic map can be called 'Eye map', it is a 2D chaos map and could be expressed as in the following model:

$$\begin{cases} y_{n+1} = \; siny_n - k\; tan\, x_n \\ x_{n+1} = \tan x_n + \; siny_{n+1} \end{cases} \qquad (2)$$

The deterministic chaotic time series are produced in the interval $x_{n\,,}y_n \in [0,1]$. Figures (1-2) illustrate the two-dimensional phase plots of the proposed finance chaotic maps. The proposed characteristic exponents of the new finance models are obtained in MATLAB for the financial parameters, e.g. k=0.9, initial state values as $x_{(0)}$ = 0.1 and $y_{(0)}$ = 0.1. The dynamics of chaotic map are denoted by orbit. The chaotic map orbit characterized by a non-smooth, discontinuous motion. From the figures, it can be observed that, each chaotic system has its special signature, which is a unique attractor characteristic. The equilibrium points of the other proposed finance chaotic system are obtained by solving the above system of equations.

3.2 The Proposed Encryption System

The overall structure of encryption and decryption stages of our method are schemtized in Fig. 3. Before the first round, a plain image is transformed into a one dimensional (1-D) array by reading all pixel values in a column-wise way. The reslting array is then divided into two halves of length [MN/2] for processing through our pipeline. Here, M and N are the number of rows and column of the input image. After finishing the first round, an intermediate cipher image is constructed, which is then transformed into a 1D array for the second encryption round. This is

DOI: 10.5281/zenodo.5207724
Received: March 10, 2021 Accepted August 08, 2021

achieved by reading all pixel values in a row-wise way. Once thse second round is doen, the final encrypted image is attained. The chaotic behavior of the developed maps directly influence both the diffusion and confusion properties of the proposed algorithm. Therefore, our system secret keys have been planned to be based only on the developed maps in order to maximize its effect on their chaotic dynamics, and thus provide higher security.

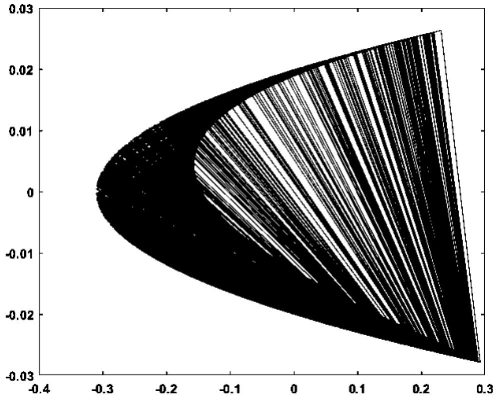


Figure 1– Numerical simulations of the 2-D phase plot in (x,y) – plane of the new finance model in Eq. (1).

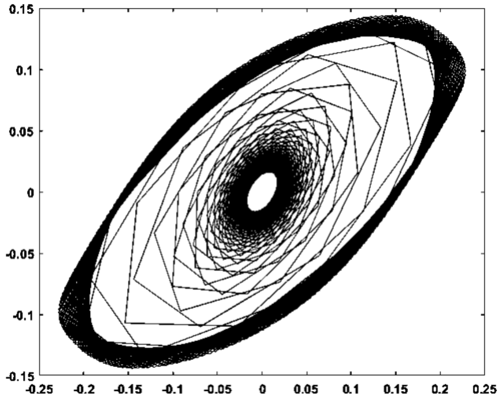


Figure 2– Numerical simulations of the 2-D phase plot in (x,y) – plane of the new finance model in Eq. (2).

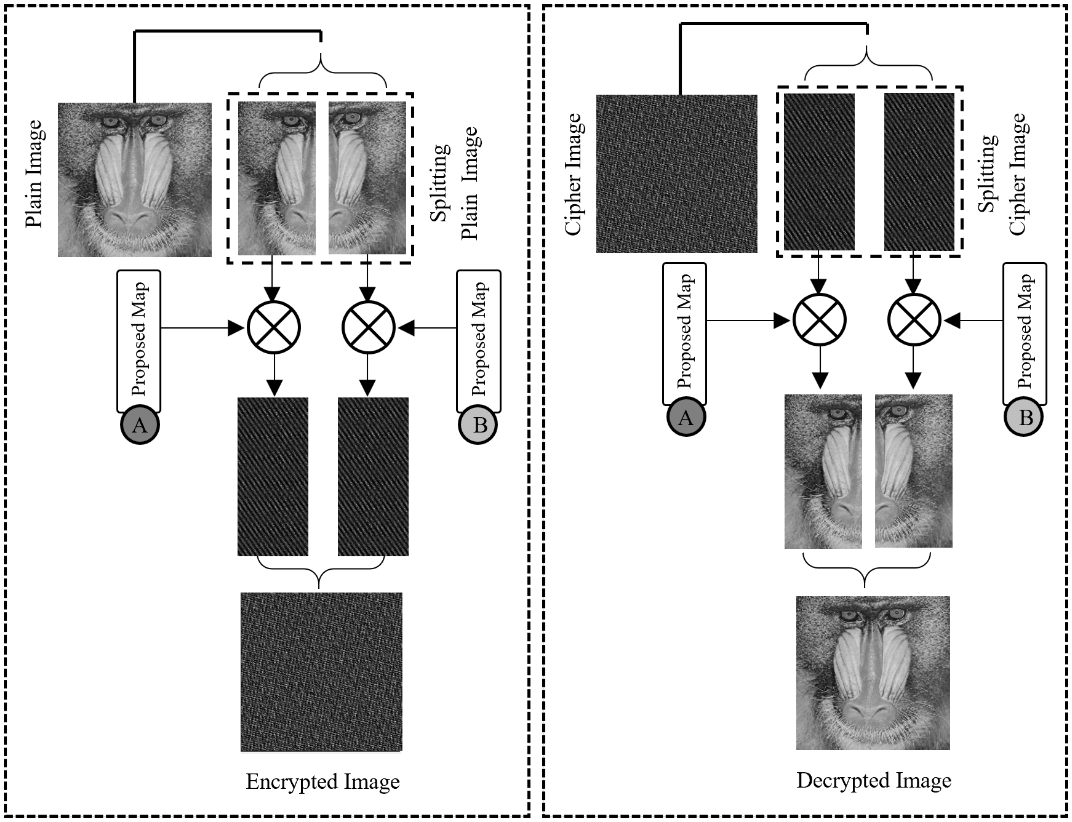


Figure 3– Basic structure of the (a) encryption and (b) decryption process of the proposed system.

3.2 Encryption / Deception Algorithm

DOI: 10.5281/zenodo.5207724

Received: March 10, 2021 Accepted August 08, 2021

In the presented cryptosystem, two separate proposed maps are utilized for both encoding and decipherment processes. The proposed maps are mathematically described by Eqs. (1) and (2) where x_{i+1} and y_{i+1} are state values with i =0,1,2,…; n and k are the parameters determining chaotic behavior of the maps and are used as a part of the secret keys in the proposed cryptosystem. According to Fig.3, the encoding steps and details are described in Algorithm 1.

Algorithm 2 Proposed encryption process

```
Input: Plain image P of size 512 × 512.
Output: Cipher image C
Begin
Step 1: Read the plain image P of size M×N (gray-scale or RGB image).
Step 2: Transform the input image into a sequence of pixels of length (MN for gray image and 3*MN for color image), change the values to the range of (0, 1) by mathematical operation, which are added into the sequence as the state values of the proposed mapping.
Step 3: Split the plan image P into two matrices have lengths of [MN/2].
Step 4: Generate the chaotic sequence with selecting two of the proposed maps by using Eqs. In which financial parameters, e.g. k=0.9, take proper input values for initial conditions initial state values as $x_{(0)}$=0.1 and $y_{(0)}$=0.1.
Step 5: Execute Eqs. (1) and (2) to change the chaotic sequence. Using different proposed chaotic maps as (A) and (B) shown in Fig. 3 for each half of a plain image and each map can has own its special parameters.
Step 6: With the same method, change the chaotic sequence into a uniformly distributed sequence by change the initial values and parameters.
Step 7: Execute the OXR to generate substituted matrix e.g. the first half [MN/2] with the first proposed chaotic map created from step 4, and the second half [MN/2] with the second chaotic sequence.
Step 8: Combination the two encrypted half image where each half has own and different encryption parameters, and mix the pixels of the combined image.
Step 9: Derive the encryption image matrix and save as cipher image C.
End
```

4. Performance Analysis

Encryption anslysis ncessiate the use of various quantitative metyric to assesss the performance of both traditional as well as proposed techniques. According to litreature, several types of methods could be used for such purpose. Those metric or parametes can be drived from the statistical, differential, and efficiency analysis [13], which are described next.

4.1. Statistical Parameters

Good encryption should have strong resistance against any statistical analysis. The security of any encryption method can be verified using several statistical examinations [14]. The first is the ***image histogram***, P_n, which describes the distribution of the image pixels by showing the frequency at each grayscale level. Generally, the of plaintext redundancy should be hidden in the distribution of cipher text, thus P_n should be uniformly distributed [14,15]. Cross ***correlation coefficient*** (R) is another analysis metrics that computes the relationship between two variables [16]. Ideally the R value should be 1.0. Finally, ***Information Entropy*** is often employed for encryption evaluation as it is a perfect index to measure the randomness degree in a given image [17].

4.2. Differential Parameters

In addition to statistical analysis, encrypted data should be sensitive to an small changes in plain-image. Attackers can change some features of the plain image to obtain changes in its encrypted form. If a little disturbance in the original image yields significant changes in the encrypted version, then attackers lose their efficiency and becomes useless [18]. Firstly, the ***mean square error*** (MSE), or the ***normalized MSE*** (NMSE), between the original and

DOI: 10.5281/zenodo.5207724
Received: March 10, 2021 Accepted August 08, 2021

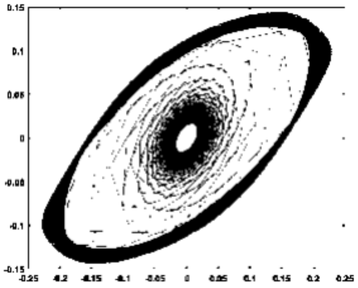
decrypted images could be used to assess sensitivity in palin image [19]. NMSE is mathematically equal to MSE divided by the its maximum [20]. Secondly, the ***peak signal to noise ratio*** (PSNR) is usually employed to evaluate the degradation between the original and recovered images [21]. Also, the ***number of pixels change rate*** (NPCR) is used to quantify the percentage of different pixel between the original and recovered images [21,22]. Particularly, NPCR measures the rate of pixels change in the chipered image after one-pixel modification in the original one. The higher NPCR value is, the more effective is the performance [22]. Practical NPCR value is ~0.99 [23]. Finally, the ***unified average changing intensity*** (UACI) is used as another metric to measure the average intensity of difference between plain and decrypted images. The practical value for UACI should be ~0.33 [23].

4.3. Efficiency parameters

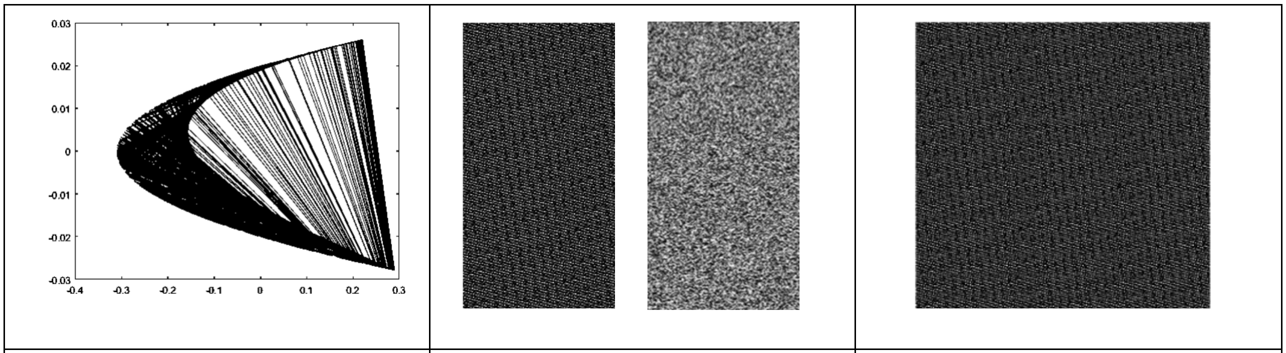
Not only staitical and differential parameters are important to assess encryption, but aslo cryptosystem efficiency and its speed are of utmost importance. This is especially needed for real-time applications. As a rule of thumb, a given encryption speed is highly dependent on the multile factors, including the underlying hardware (i.e., CPU/MPU) structure, operating system, RAM size, the programming language and machine compiler options. Therefore, it is hard to compare speed of the two encryption algorithms that use two different machines [24]. The most commonly used parameter related to efficiency analysis is the elapsed time (in seconds) that represent the total computation time for both encryption and decryption processes for each trial of experiments.

5. Experimental Simulations and Results

Most of the encryption methods are cracked using statistical analyses, which are to find relations between the encrypted and plain images. In this work, all simulation experiments have been done using the same machine and the same MATLAB programming version. Our machine was connected to internet most of time. All of the simulation experiments have been applied more than one time and hence the elapsed time has represented the average simulation time for all trials for each experiment. The performance of the developed algorithm is tested using MATLAB R2017a where it is examined through a series of tests. Table 2 summarized the simulation settings.

		
(a)	(b)	(c)

DOI: 10.5281/zenodo.5207724
Received: March 10, 2021 Accepted August 08, 2021



(d) (e) (f)

Figure 4 – Simulation steps for (encryption [a-f], decryption [f-a]): (a) original image; (b) Splitting image [MN/2] (c) the chaotic map that is used to encrypt the first half of splitting image; (d) The second chaotic map used to encrypt the other half of splitting image; (e) encrypted image using proposed maps, and (f) final encrypted image.

The proposed algorithm is instigated using our chaotic maps for both encoding and decipherment of digital input image. We used the standard images (Lena, Cameraman, Baboon, etc.) having a size of 512 × 512 pixels, which are consider as plain (original) images and the two proposed maps are performed with multi map orbit key. The foremost straight investigation to judge the chaotic degree of the encrypted data is by the sense of sight. Alternatively, the correlation coefficient can calculate the randomness of scrambled images quantitatively. In order to apply our chaotic maps, both k and n parameters must be determined according to Step 1 in Algorithm 1. Based on our experimental experience, general combinations of k and n can always give very unsystematic results. In our simulation, $k = 0.9$ and $n = 512$ were adopted in Step 1. The initial conditions of our chaotic maps used are chosen as, $x_{(0)} = 0.1$ and $y_{(0)} = 0.1$ for the first random key.

Figure 4 shows the details of the encoding steps. The encrypted data can be referred in Fig. 4(a) the decrypted steps are carried out to attain the encrypted image, as can be observed in Fig. 4 (f). The visual investigation of Fig. 4 not only shows the successful possibility of applying our technique in both encryption and decryption stages, but aslo reveals the effectiveness of information hiding capability of our algorithm.

Table 2– The simulation settings

Name	Detailed Settings
HARDWARE	
CPU	Core™ i5-2400
Frequency	3.10GHz
RAM	4G
Hard drive	160G
SOFTWARE	
Operating system	Windows7
Language	MATLAB R2017a(7.14)

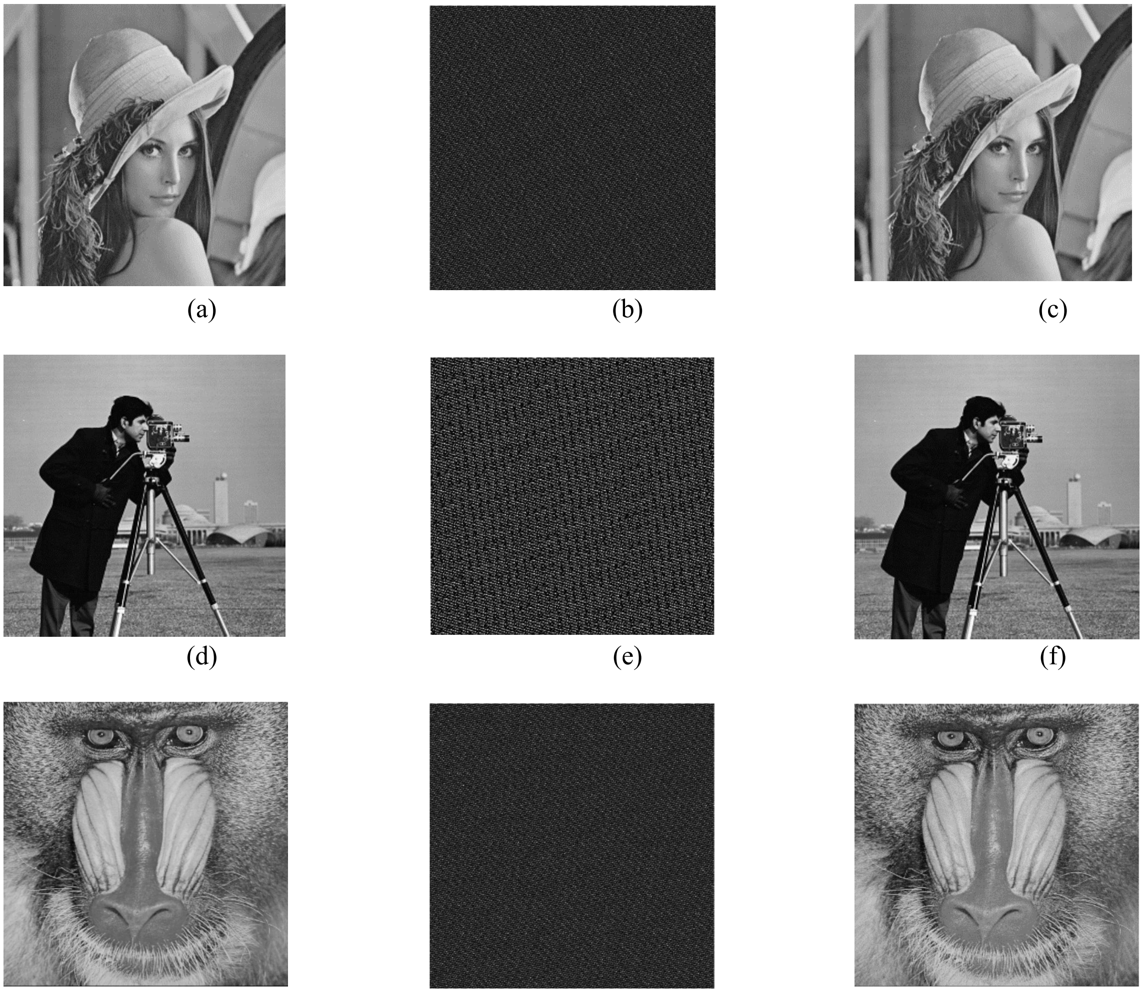
The encoding and decipherment results are demostrated in Fig. 5. As mentioned above, four benchmark digital images are utilized to test the proposed encryption algorithm. As demonstrated in Figure 5, the cipherd images appear to be so noisy in a way that none of the original image information can be retrieved. Using the correct secret keys in the decoding process, the deciphered images are the same as original images. In addition to visual illustration, other quantitative metrics are used to assess the quality of encryption, such as the distributions of image greylevels or the image histogram. Histogram analysis examines pixels' distribution and if that distribution is

DOI: 10.5281/zenodo.5207724
Received: March 10, 2021 Accepted August 08, 2021

uniform, i.e., greylevel occurrences are close, the encoding process is performing well. In otherwords, the closer the encoded data distributions are, the higher the encryption level is. Figure 6 shows the histograms for the selected sample images and their respective scrambled images.

5.1. Key Sensitivity Analysis

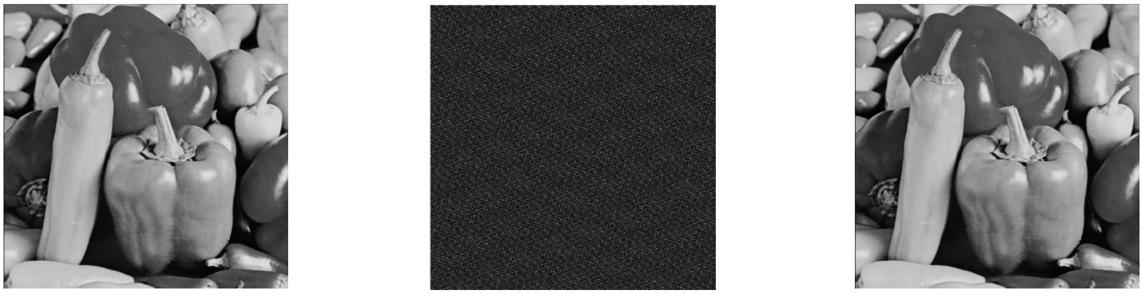
Key sensitivity analysis is considered as one of the most important metric of encryption evaluation. Typically, small changes in the employed secret key lead to compeletely different results during the decipherment. That means that the coded information cannot be deciphered even if a single parameter has been altered. Not only changes to key parameters affetct the decoding, but aslo the order of the keys is necessary to be known. Alternatively, the data cannot be decoding by knowing all the keys parts as the decoding is not performed in the correct order. Figure 7 demonstrate the scrambled image form of the proposed approach when using the specific keys, where Fig.7 (a) shows the original cameraman image and Fig. 7. (b-c) show the encrypted images using different encrypted keys. Additional example in Fig. 8 showing the key sensitivity results. Figure 8 (a) shows the deciphered image using same encoding keys, while Fig. 8 (b,c) show illegal decoded images using the wrong keys. Figure 9 explain the


(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

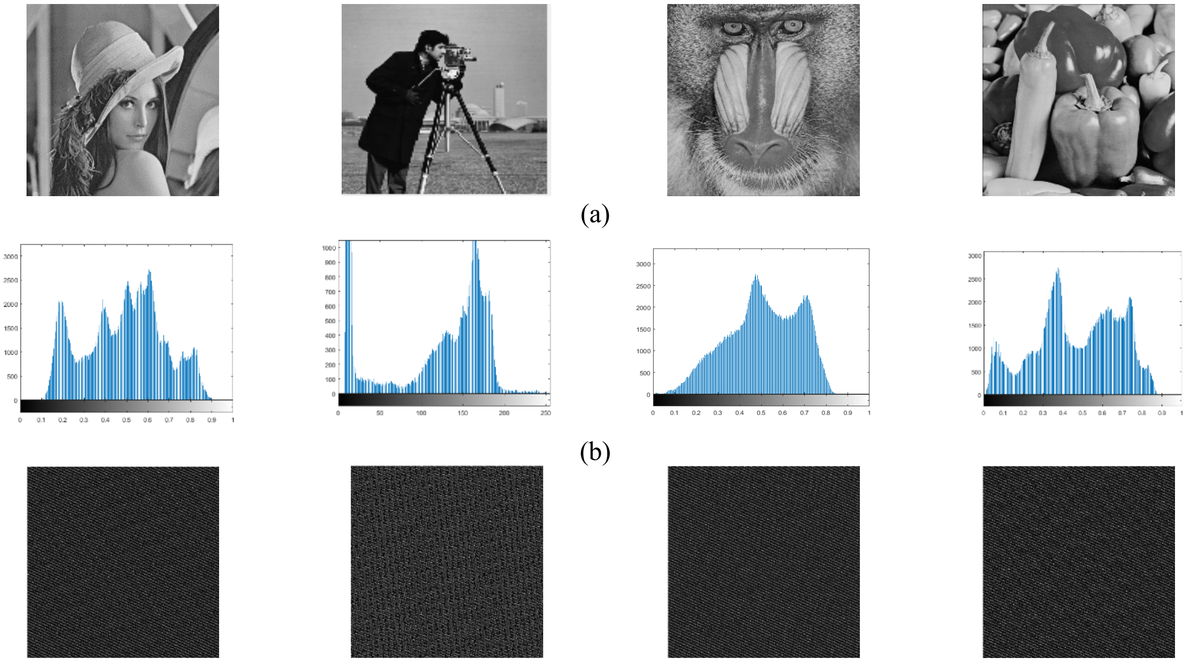
DOI: 10.5281/zenodo.5207724
Received: March 10, 2021 Accepted August 08, 2021



(k) (l) (m)

Figure 5 – Encryption (second column) and decryption (third column) results using right keys for (a) Lena (d) Cameraman, (g) Baboon , and (k) Peppers plain images.

effect of small changes in parameter during the encoding process. Figure 9 (i) shows this effect, according to the change in the proposed maps *k* parameter form 0.5 to 0.91. Figure 9 (ii) shows this effect, according to the change in the proposed maps iteration from 100 to 1000. The demonstrated results assure that the deciphered data are all concealed, which means that (1) unless the correct key is employed during decryption, the original images cannot be recovered, and (2) small changes will not produce correct decipherment results. Therefore, those results document that the proposed encryption algorithm has high key sensitivity.



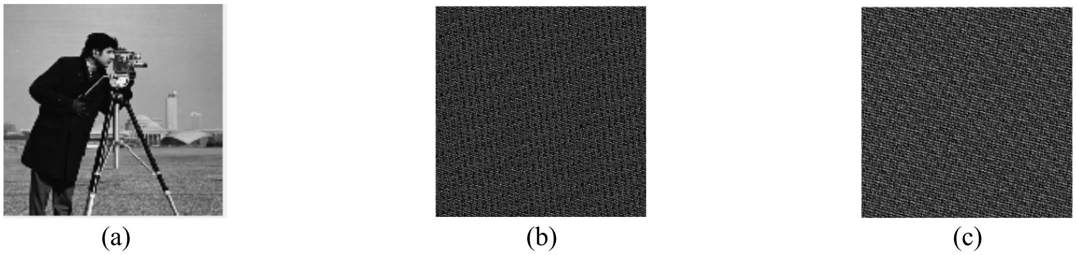
(a)

(b)

(c)

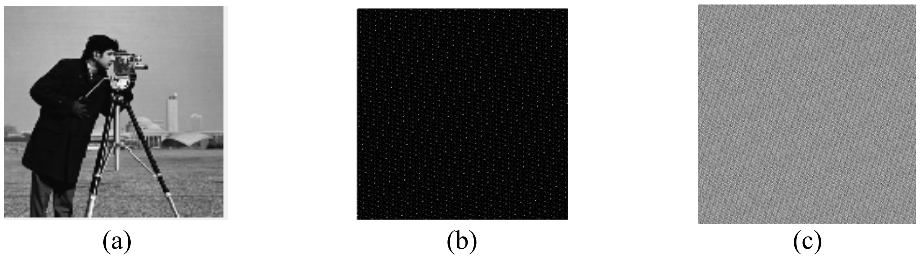
Figure 6 – Histogram analysis: (a) Plain images (b) histogram of original images; and (c) Cipherd images.

DOI: 10.5281/zenodo.5207724
Received: March 10, 2021 Accepted August 08, 2021



(a) (b) (c)

Figure 7 – An example of key sensitivity of encryption process using Cameraman: (a) plain image; (b) encrypted image (n=1000,k=0.9,$x_{(0)}$=0.1,$y_{(0)}$=0.1); (c) encrypted image (n=500,k=0.7,$x_{(0)}$=0.2,$y_{(0)}$=0.2)

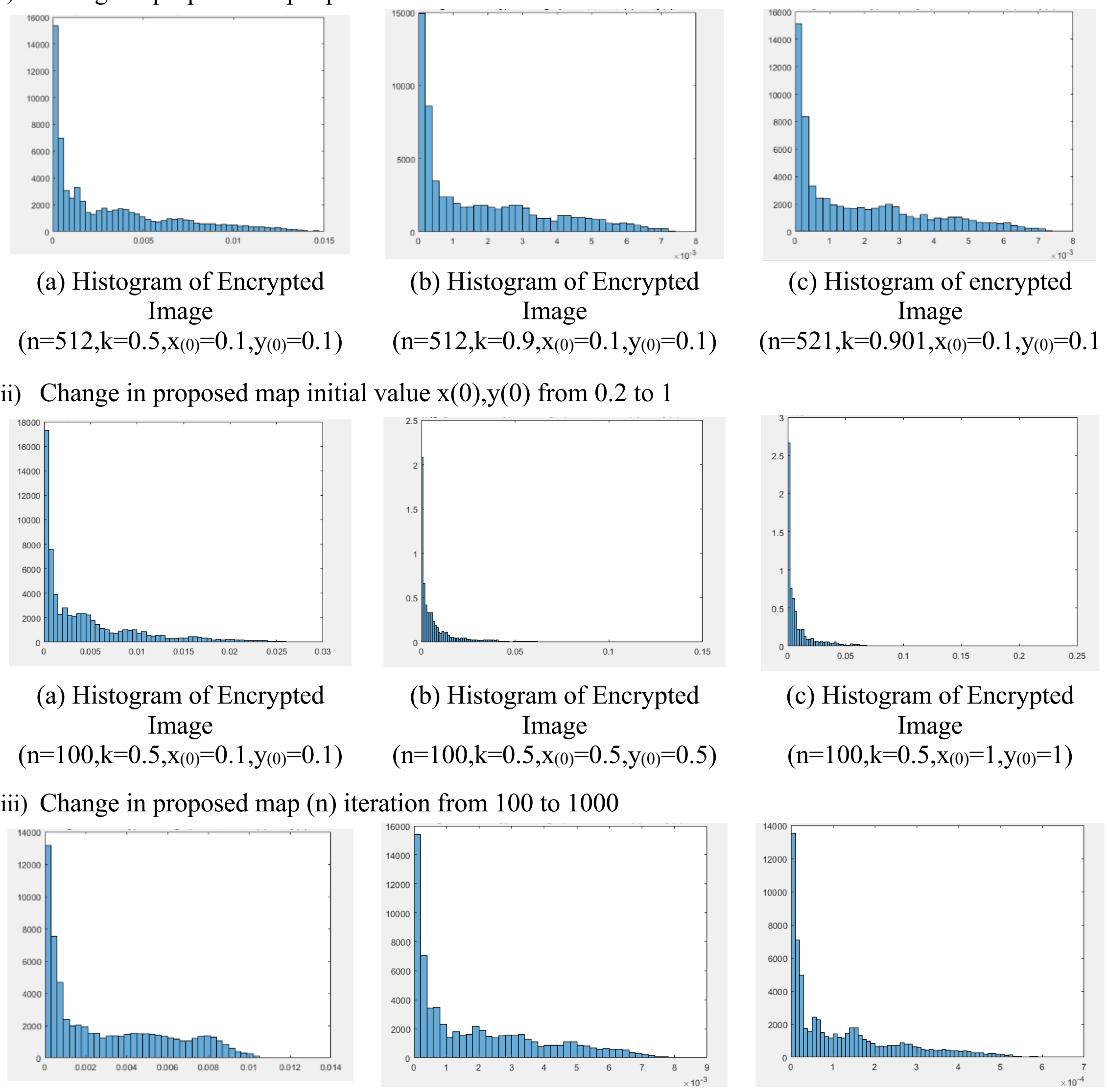


(a) (b) (c)

Figure 8– An example of key sensitivity of decrypted process using Cameraman..

DOI: 10.5281/zenodo.5207724

Received: March 10, 2021 Accepted August 08, 2021



(i) Change in proposed map k parameter form 0.5 to 0.901

(a) Histogram of Encrypted Image (n=512,k=0.5,x(0)=0.1,y(0)=0.1)

(b) Histogram of Encrypted Image (n=512,k=0.9,x(0)=0.1,y(0)=0.1)

(c) Histogram of encrypted Image (n=521,k=0.901,x(0)=0.1,y(0)=0.1

(ii) Change in proposed map initial value x(0),y(0) from 0.2 to 1

(a) Histogram of Encrypted Image (n=100,k=0.5,x(0)=0.1,y(0)=0.1)

(b) Histogram of Encrypted Image (n=100,k=0.5,x(0)=0.5,y(0)=0.5)

(c) Histogram of Encrypted Image (n=100,k=0.5,x(0)=1,y(0)=1)

(iii) Change in proposed map (n) iteration from 100 to 1000

(a) Histogram of Encrypted Image (n=100,k=0.5,x(0)=0,y(0)=0.1)

(b) Histogram of Encrypted Image (n=500,k=0.5,x(0)=0,y(0)=0.1)

(c) Histogram of Encrypted Image (n=1000,k=0.5,x(0)=0,y(0)=0.1)

Figure 9– The explain the effect of small change in parameter during the encryption process

Statistical Analyses

To statistically analyze our experimental results, different metrics are used, including MSE, PSNR, excusion time (ET), and Shanon entropy. Table 3 shows the average values of those metrics using the samples images, analyzed using the proposed algorithm. It is worth mentioning that the proposed encryption uses different averages when encrypting different input data. This successively can considerably rise the resistance of our cryptography system against both unknown/chosen attacks and differential attacks. As shown in the table, the decryption quality of our method can satisfy security and performance requirements, evidenced by the PSNR<8.4642, and entropy>7.9974. It is shown that this algorithm yields better security performance in comparison to the results are mentioned in [25].

Table 3– Evaluation Parameters of the encryption quality of the proposed approach.

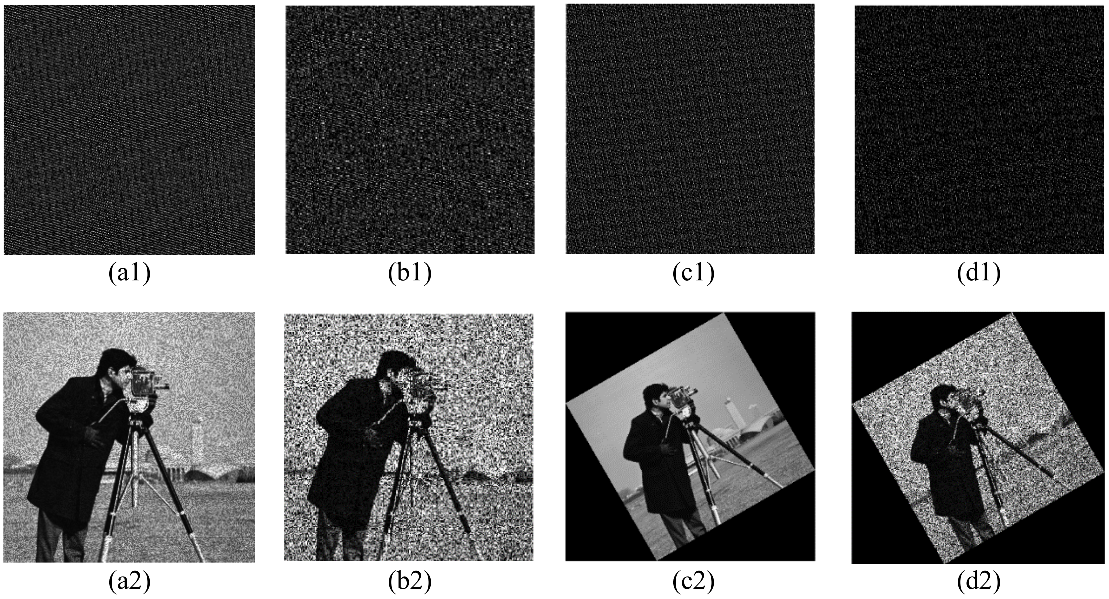
Image Name	MSE	PSNR	ET (Sec)	Entropy

DOI: 10.5281/zenodo.5207724
Received: March 10, 2021 Accepted August 08, 2021

Lena	9694.30	8.4740	1.071362	7.9999
Cameraman	9788.81	8.4731	0.994226	7.9991
Baboon	8354.21	8.4798	1.082035	7.9994
Peppers	8897.10	8.4761	1.071352	7.9992
Average	9183.61	8.4758	1.054744	7.9994

5.2. Resistance to Different Attacks Analysis

This part of the analysis tests the algorithm's ability to resist attacks. Noise attacks are typical image attack methods, which often occur during the process of the transmission of cipher images. In our analysis, two known metrics were analyzed, namely; the NPCR and UACI metrics. In general, the algorithm should demonstrate good sensitivity to plain image, which means a small change in the original image can cause great difference in ciphered version. The effect of speckle noise attack, and rotation attacks are illustrated in Fig. 10.


(a1) (b1) (c1) (d1)

(a2) (b2) (c2) (d2)

Figure 13– Noise attacks: (a1) cipher and decrypted (a2) images with 5% speckle noise; (b1) Cipher and decrypted (b2) images with 50% speckle noise; (c1) cipher and decrypted (c2) images with rotation of 30 degrees; (d1) cipher and decrypted (d2) images with 50% speckle noise and rotation of 30 degrees.

It is a general form of cryptanalysis and a secure encryption scheme should have strong ability of resisting this attacks. For an image encryption scheme, its ability of resisting differential attack can be measured by the number of pixel changing rate and unified average changed intensity. The outcomes can be observed in Table 4, and Table 5. As can be observed, NPCR is above 99% while UACI is above 33%. These outcomes imply the high sensitivity of the proposed algorithm towards the minute modification made to the plain image; the decrypted images will be totally different even if there is only one bit of alteration between the two plain images. In our test, the results of four encrypted images and the average value NPCR and UACI is 99.67145% and 33.63288%, respectively. By contrast, the values of NPCR and UACI in our scheme are closer to the ideal value, which proves that the proposed encryption scheme is highly sensitive to resisting differential attack.

Table 4– The NPCR(%) of encrypted images for our approach and other litreature algorithms.

DOI: 10.5281/zenodo.5207724
Received: March 10, 2021 Accepted August 08, 2021

Image Name	Proposed method	Wang et al. [26]	Luo et al. [6]	Amina et al. [27]	Alawida et al. [28]	Wu et al. [8]
Lena	99.6653	99.59	99.6137	99.6452	99.620	99.6002
Cameraman	99.6924	99.59	99.6131	N/A	N/A	99.6082
Baboon	99.6711	99.56	99.6111	99.6154	99.601	99.5903
Peppers	99.6570	99.61	99.6137	99.6315	99.617	99.6112

Table 5– The UACI(%) of encrypted images for our approach other litreature algorithms.

Image Name	Proposed method	Wang et al. [26]	Luo et al. [6]	Amina et al. [27]	Alawida et al. [28]	Wu et al. [8]
Lena	33.6307	33.48	33.4594	33.6152	33.505	33.5079
Cameraman	33.6551	33.53	33.4615	N/A	N/A	33.5574
Baboon	33.6529	33.58	33.4629	33.4354	33.424	33.5281
Peppers	33.5928	33.41	33.3948	33.5073	33.391	33.5265

6. Conclusions and Suggested Future Work

In an effort to improve encryption quality and performance, this work have introduced novel chaotic maps for digital image. The developed maps have simple mathematic tool which have been adopted in the permutation-substitution network structure of the proposed system to enhance the confusion and diffusion properties, and thus, withstand various existing cryptography attacks and cryptanalysis techniques. Experiemntal results documented the high security and robustness of our method, the average NPCR and UACI values were 99.67145% and 33.63288%, respectively. Additionally, the proposed system demonstrated extreme sensitive to initial conditions and unpredictability, which makes our system suitable for a wide range of applications, such as wireless communications. Several research venues are yet to be pursed, including the randomization of key selection process, increasing the the number of superimposed shares to increase the layers of security, and applying multiple types of maps to the same image to improve the encryption level. Another resercah venue is the application domain, such as apply our developed maps for other multimedia security algorithms (e.g., video, text) for fog computing.

References

1. Zahmoul, R., Ejbali, R., & Zaied, M. (2017). Image encryption based on new Beta chaotic maps. Optics and Lasers in Engineering, 96, 39-49.
2. Yavuz, E., Yazıcı, R., Kasapbaşı, M. C., & Yamaç, E. (2016). A chaos-based image encryption algorithm with simple logical functions. Computers & Electrical Engineering, 54, 471-483..
3. Zhang, Y. (2018). The unified image encryption algorithm based on chaos and cubic S-Box. Information Sciences, 450, 361-377..
4. Liao, X., Hahsmi, M. A., & Haider, R. (2018). An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. Optik-International Journal for Light and Electron Optics, 153, 117-134.
5. Huang, L., Cai, S., Xiong, X., & Xiao, M. (2019). On symmetric color image encryption system with permutation-diffusion simultaneous operation. Optics and Lasers in Engineering, 115, 7-20.
6. Luo, H., & Ge, B. (2019). Image encryption based on Henon chaotic system with nonlinear term. Multimedia Tools and Applications, 78(24), 34323-34352.
7. Parvaz, R., & Zarebnia, M. (2018). A combination chaotic system and application in color image encryption. Optics & Laser Technology, 101, 30-41.

DOI: 10.5281/zenodo.5207724
Received: March 10, 2021 Accepted August 08, 2021

8. Wu, J., Liao, X., & Yang, B. (2018). Image encryption using 2D Hénon-Sine map and DNA approach. Signal Processing, 153, 11-23.
9. Yousif, B., Khalifa, F., Makram, A., & Takieldeen, A. (2020). A novel image encryption/decryption scheme based on integrating multiple chaotic maps. AIP Advances, 10(7), 075220.
10. Yasser, I., Khalifa, F., Mohamed, M. A., & Samrah, A. S. (2020). A new image encryption scheme based on hybrid chaotic maps. Complexity, 2020.
11. Li, C., Luo, G., & Li, C. (2019). An Image Encryption Scheme Based on The Three-dimensional Chaotic Logistic Map. Int. J. Netw. Secur., 21(1), 22-29.
12. Su, S., Su, Y., & Xu, M. (2014). Comparisons of firefly algorithm with chaotic maps. Comput Model New Technol, 18(12), 326-332.
13. Sekar, J. G., & Arun, C. (2020). Comparative performance analysis of chaos based image encryption techniques. Journal of critical reviews, 7(9), 1138-1143.
14. Wang, X., Guan, N., Zhao, H., Wang, S., & Zhang, Y. (2020). A new image encryption scheme based on coupling map lattices with mixed multi-chaos. Scientific reports, 10(1), 1-15.
15. Pratt, W. K. (2013). Introduction to digital image processing. CRC press.
16. Xian, Y., & Wang, X. (2021). Fractal sorting matrix and its application on chaotic image encryption. Information Sciences, 547, 1154-1169.
17. Khan, M., Jamal, S. S., & Waqas, U. A. (2020). A novel combination of information hiding and confidentiality scheme. Multimedia Tools and Applications, 79(41), 30983-31005.
18. Waseem, H. M., Jamal, S. S., Hussain, I., & Khan, M. (2021). A novel hybrid secure confidentiality mechanism for medical environment based on Kramer's spin principle. International Journal of Theoretical Physics, 60(1), 314-330.
19. Cox, I. J., Miller, M. L., Linnartz, J. P. M., & Kalker, T. (2018). A Review of Watermarking Principles and Practices 1. Digital Signal Processing for Multimedia Systems, 461-485.
20. Yasser, I., Mohamed, M. A., Samra, A. S., & Khalifa, F. (2020). A chaotic-based encryption/decryption framework for secure multimedia communications. Entropy, 22(11), 1253.
21. Arshad, U., Khan, M., Shaukat, S., Amin, M., & Shah, T. (2020). An efficient image privacy scheme based on nonlinear chaotic system and linear canonical transformation. Physica a: statistical mechanics and its applications, 546, 123458.
22. Ali, K. M., & Khan, M. (2019). A new construction of confusion component of block ciphers. Multimedia Tools and Applications, 78(22), 32585-32604.
23. Alghafis, A., Waseem, H. M., Khan, M., Jamal, S. S., Amin, M., & Batool, S. I. (2020). A novel digital contents privacy scheme based on quantum harmonic oscillator and schrodinger paradox. Wireless Networks, 1-20.
24. Nkapkop, J. D. D., Effa, J. Y., Fouda, J. S. A. E., Alidou, M., Bitjoka, L., & Borda, M. (2014). A fast image encryption algorithm based on chaotic maps and the linear diophantine equation. Computer science and applications, 1(4), 232-243.
25. Norouzi, B., Seyedzadeh, S. M., Mirzakuchaki, S., & Mosavi, M. R. (2014). A novel image encryption based on hash function with only two-round diffusion process. Multimedia systems, 20(1), 45-64.
26. Wang, X., Wang, S., Wei, N., & Zhang, Y. (2019). A novel chaotic image encryption scheme based on hash function and cyclic shift. IETE Technical Review, 36(1), 39-48.
27. Amina, S., & Mohamed, F. K. (2018). An efficient and secure chaotic cipher algorithm for image content preservation. Communications in Nonlinear Science and Numerical Simulation, 60, 12-32.
28. Alawida, M., Samsudin, A., Teh, J. S., & Alkhawaldeh, R. S. (2019). A new hybrid digital chaotic system with applications in image encryption. Signal Processing, 160, 45-58.

DOI: 10.5281/zenodo.5207724
Received: March 10, 2021 Accepted August 08, 2021