Available online at sjuoz.uoz.edu.krd

Science Journal of University of Zakho

*Vol. 9, No. 3, pp. 158– 162, September-2021*

p-ISSN: 2663-628X
e-ISSN: 2663-6298

# Color Image Encryption with a Novel Technique and Chaotic Singer Map

Araz B. Karim [a,*], Peshraw S. Abdalqader [b], Ziyad T. Najim[c], Abbas M. Salhd [d], Omar Y. Abdulhammed [e]

[a,b,c,d,e] Dept. of computer, College of Science, University of Garmian, Kurdistan Region, Iraq
(Araz.kareem@garmian.edu.krd), (Peshraw@garmian.edu.krd), (ziyad.tariq@garmian.edu.krd), (Abbas.mc@garmian.edu.krd), (Omar.y@garmain.edu.krd)

***Received: May., 2021 / Accepted: Jul., 2021 / Published: Sept., 2021*** ***https://doi.org/10.25271/sjuoz.2021.9.3.316***

**ABSTRACT:**
One of the extreme efficient, important, and necessary means used to preserve the information and contents of the image through sending it over the Internet or network communication is image encryption. In this paper, a novel technology for images encryption has been proposed by using different methods. The proposed method consists of five stages. In the first stage, the original color image is divided into eight parts and shuffles it. The second stage separates the R, G, B matrix of the original image and then converts them into a binary code. Third stage generates secret keys by using singer map, where it can generate high pseudorandom sequences with high-speed performance. In the fourth stage, the logical XOR operator is applied to encrypt the image based on the three matrix and secret keys. Fifth stage is the process of decrypting which is the opposite of the encryption process. The suggested approach efficiency is validated via entropy, correlation, UACI and NPCR tests. Likewise, empirical outcomes and security test displayed that the proposed technology achieved secrecy and was capable of facing attacks and challenges.

**KEYWORDS:** Image, encryption, shuffling, chaotic, singer map.

## 1. INTRODUCTION

Year after year, a great and rapid development is observed in information technologies, communications and networks, as well as at the same time the increase in challenges and security problems for information, images and videos that are transmitted through transmission media. Therefore, it became necessary to find feasible solutions to these problems [1]. This reality forces one to stratify new and updated methodologies and strategies on the image security in numerous domains starting from corporations to crowd services [2, 3]. At the present time, secure communication has become an important and fundamental issue at all levels, industrial, commercial, military etc... [4, 5]. Mostly, the concept of coding the important image has become a pivotal mission to deny steal and alteration of image from unauthorized users.

Encryption techniques have played and are playing an important role in solving confidential communication problems. Nevertheless, traditional approaches such as AES and DES have some security flaws; this is due to the presence of many tools and programs that are used to decode the image that has been encrypted by traditional methods [5–7]. To solve the problems and the disadvantages of traditional encryption methods, researchers and scientists have designed new encryption systems based on chaos systems [8]. In fact, the random numbers generated from the chaos system have unique and important features for the coding system. The major characteristics for a chaos-founded system is that the product data ever iterate, herewith any outer provenance cannot have the information to decipher the giddy data [9]. There are two kinds of image cipher methods, location alteration and value conversion [10]. Location alteration is a technique of permuting pixels locations wanting changing the value of each pixel. In chasm, the value conversion kind changes the value of the pixel wanting permuting pixel location [11]. However, the enforcement of only one of these types at a bit or pixel level will not supply demanded security. Consequently, the cipher methods should be enhanced further than any decipher methods to avert from the insecure image connection [12].

Digital images in many applications are confidential data and their encryption is being applied in internet communication, multimedia systems, tele-medicine and military communication to mention a few. Most government parastatals, military intelligence, forensic departments, financial institutions, hospitals and private business all deal with confidential messages. For example, hospitals deal with information about their patients, geographical areas in forensic departments, enemy positions in military intelligence, and product financial status in case of financial institutions. During their transmission especially over the internet, the content can be accessed illegally and misused by unauthorized parties. The information needs to be protected from an unauthorized person when being transferred over wireless communication networks. There are three different ways to protect digital image from unauthorized use or access. These are cryptography, steganography and watermarking. Cryptography schemes are widely used among these techniques and have been applied for protection of digital data in the past few years. Cryptography is an algorithmic process of converting a plain data to a cipher text, a form that is unreadable by an unauthorized person (eavesdropper).

Image encryption is one of the most effective means to ensure the security of image information in network communications and protecting images is an ethical and legal requirement, also chaos based image encryption is widely used to fulfil the security requirements of digital images. The chaotic systems are very sensitive to initial conditions and system parameters. In this paper a novel color image encryption algorithm with a novel technique and chaotic singer map is proposed to improve encryption and decryption method to obtain the best protection. The color image is separated into eight parts and shuffled according to a novel technique to increase the security, separate the three color (red, green, blue) from original image as planes and convert it to the binary form. The XOR operation takes place between the numbers that is generated by singer map method and planes depending on a novel technique. The results show that the

* Corresponding author

proposed system provides effective and safe way for image encryption also has desirable properties of high security, robustness to cryptographic attacks. The rest of this paper is organized as follows: the related work, chaotic system and proposed system is described in Section 2, 3 and 4 respectively. The results are reported in Section 5, followed by the conclusion of the work drawn in Section 5.

## 2. RELATED WORK

In any chaotic image encryption system, there are two main issues: first is the chaotic system, which is used as a random number generator. Second is an encryption algorithm, which has an importance in terms of efficiency and speed.

In the paper [13] a new unified image encryption system with identical encryption and decryption algorithms was proposed. In this system, an external key and the Hénon map are used to generate the equivalent secret keys. Then, a kind of lifting-like transformation is employed to diffuse the image information to fulfil the image encryption. The proposed cryptosystem possesses strong sensitivities of secret key, plain image and ciphered image for the maximum relative error of their test indexes is only 0.55%. Thus the proposed can be used as a candidate scheme of network image information security.

The paper [14] suggests a novel chaos based color multiple image encryption technique. A 3D histogram equalization method has been applied to equalize the chaotic sequences histograms of Lorenz system. Confusion/diffusion of image data has been implemented by using sequences generated by histogram equalized Lorenz and Rossler system. In confusion stage, the input image colored pixels has been scrambled. Then in diffusion stage, pixel replacement is done by scrambled images and sequences of Rossler system. The proposed scheme efficiency is validated via key sensitivity, key space, entropy, horizontal, vertical, diagonal correlation, UACI and NPCR tests. The experimental results show that the proposed encryption technique has achieved confidentiality and have resistance against classical attacks. The paper [15] outlines a design for a lightweight image encryption algorithm based on a message-passing algorithm with a chaotic external message. Message-passing (MP) algorithm allows simple messages to be passed locally for the solution to a global problem, which causes the interaction among adjacent pixels without additional space cost. A two-dimensional logistic map is utilized as a pseudorandom sequence generator to yield the external message sets of edge pixels. +e external message can affect edge pixels, and then adjacent pixels interact with each other to produce an encrypted image. Experimental results prove the proposed algorithm's persistence to various existing attacks with low cost. The paper [16] proposes a new image encryption scheme based on a generalized Arnold map and Rivest–Shamir–Adleman (RSA) algorithm. First, the parameters of the generalized Arnold map are generated by an asymmetric encryption-system RSA algorithm, and the key stream is produced iteratively. Second, both rows and columns of the image are cyclically confused to hide the image data again. The additive mode diffusion operation is performed to realize third-layer hiding for image content. Overall diffusion and confusion operations are conducted twice to obtain the final cipher image. Test results prove that the encryption scheme proposed is effective and has strong anti-attack capabilities and key sensitivity. The paper [17] proposes a novel perturbation algorithm for data encryption based on double chaotic systems. The proposed chaotification method is a hybrid technique that parallels and combines the chaotic maps. It is based on combination between Discrete Wavelet Transform (DWT) to decompose the original image into sub-bands and both permutation and diffusion properties are attained using the chaotic states and parameters of the proposed maps, which are then concerned in shuffling of pixel and operations of substitution, respectively. Statistical test analyses, and comparison with other techniques indicate that the proposed algorithm has promising effect and it can resist several common attacks. Paper [18] introduces a new algorithm based on CS for image encryption. Plain image is sparse in the DCT domain, and the combination of pixels is used to reduce the dimension of the image DCT. The measurement matrix is generated using a three-dimensional chaotic system, and for further encryption, pixel scrambling is applied using a one-dimensional chaotic system to generate the scrambling vector. Experimental and analysis results show that the proposed algorithm has good performance in terms of security and image compression, as well as low time complexity. The paper [19] proposes a new light weight secure cryptographic scheme for secure image communication. In this scheme the plain image is permuted first using a sequence of pseudo random number (PRN) and encrypted by DNA computation. Two PRN sequences are generated by a Pseudo Random Number Generator (PRNG) based on cross coupled chaotic logistic map using two sets of keys. The first PRN sequence is used for permuting the plain image whereas the second PRN sequence is used for generating random DNA sequence. The number of rounds of permutation and encryption may be variable to increase security. The scheme is proposed for grey label images but the scheme may be extended for color images and text data. Simulation results exhibit that the proposed scheme can challenge any kind of attack.

## 3. CHAOTIC SYSTEMS

The idea of chaos is one of the novel and basic motifs in new science that extremely widens the area of our grasping of the universe; also, its denomination refers to the random and erratic conduct that takes place in our real modern world [20]. It is also one of the behaviors associated with the non-linear physical system. The major chaotic systems are parts into three classes: one-dimensional chaotic systems such as Chebyshev and Singer map, two-dimensional chaotic systems such as 2D logistic map, three dimensional chaotic systems such as Lorenz system [18].

### 3.1 Chaotic Singer Map

The chaotic approaches have substantial features that can be utilized to enhance the concourse optimization approaches. These features include, (a) the randomly (b) susceptibility to the premier situations and (c) gravity [21], and they are transformed into chaotic maps. The Singer map is one of the extreme folk chaotic maps, described as:

$ch_{i+1} = \mu\left(7.86ch_i - 23.3ch_i^2 + 28.75ch_i^3 - 13.30187ch_i^4\right)$, $\mu = 1.07$

## 4. PROPSED METHOD

Image ciphering is partition into three main sets: (i) Location substitution depend algorithm, (ii) value based conversion algorithm, (iii) visual conversion depend algorithm. In this work, it has been suggested 2 stage ciphering and deciphering algorithms. The proposed system composed of four main steps. First is split the original color image into eight parts (P1, ……. , P8), then shuffling it. Second is use chaotic singer map to generate chaotic sequence random numbers to use in ciphering image. Third is applying logical XOR operations to encrypt the color image. Finally is decryption step that is an reverse of the ciphering method. Figure (1) shows the block diagram of the proposed approach and in the next sub-segment, every phase will debate in detach.

### 4.1 Image shuffling

Image ciphering deficiency is safe by low correlation between adjacent pixel (reduce inter-pixel correlation), combating

statistical offensives and other kinds of offensive, since the image is characterized with high correlation among pixels, high redundancy, bulk capacity of data, the shuffling is done in this approach as shown in algorithm (1)

Algorithm (1) Image shuffling

**Input**: color image with size 128*128 pixels
**Output**: color image shuffling

**Begin**
**Step1**: read color image as a 2-D array
**Step2**: divide the color image into two row and four column to get eight parts ($P_1$, ……., $P_8$).
**Step3**: convert 2-D array into 1-D array
**Step4**: int a[i]=8, b[i]=8, j
For i= 0 to 8 do
**Begin**
b[i]=swap (a[8-i],a[1+i])
**End**
**Step5:** convert 1-D array into 2-D array as a b[2][4]
**Step6**: for i= 0 to 1
**Begin**
For j= 0 to 3 do
Int c[i][j]= swap (int b[i][j+1], b[i+1][j])
**End**
**End**

### 4.2 Generation random numbers by chaotic singer map

The singer method works to excess key area and a lot of complexity and completes randomization of pseudo sequences. The main goal of using singer map is generating a sequence of random keys which are used later in the process of encryption. The singer map is done as shown in algorithm (2).

Algorithm (2) Generation random numbers by chaotic singer map

**Input**: value of Q, R
**Output**: sequence of random numbers
**Begin**
**Step1**: Q=1.07, R=1.03, float Z[i]
**Step2**: for i=1 to size of original color image
Z[i]= Q(7.86$R_i$ −23.31$R_i$2 + 28.75$R_i$3−13.302875$R_i$4)
**Step3**: Generate sequence of random number
**End**

### 4.3 XOR operations

Because the image has some characteristics, such as a great data capability, rise redundancy, and powerful engagement amidst neighboring pixels, ciphering it using traditional methods like a AES, DES is inappropriate and useless.
In this work, 128*128*3 color image are used, separate R, G, B of color image into three matrices (MR, MG, MB), for encryption, firstly all values are convert to binary code. Secondly, each matrix is XOR with the random number that generated by chaotic singer method (CS) to get a new three matrices (SMR, SMG, SMB) as shown in the following equations:

SMR= MR ⊕ CS ……...1
SMG= MG ⊕ CS……...2
SMB= MB ⊕ CS ……. .3
Fourthly, the result of eq. (1) is XOR with the result of eq.(2) and their results are XOR with eq.(3) as shown in the following equations:

EX= SMR ⊕ SMG ……...4
EXE= EX ⊕ SMB…….....5

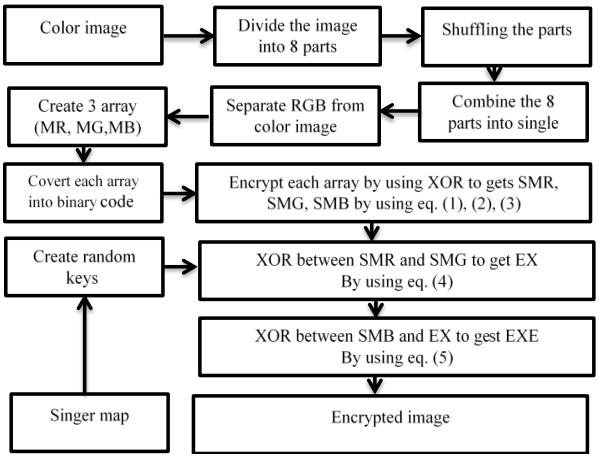
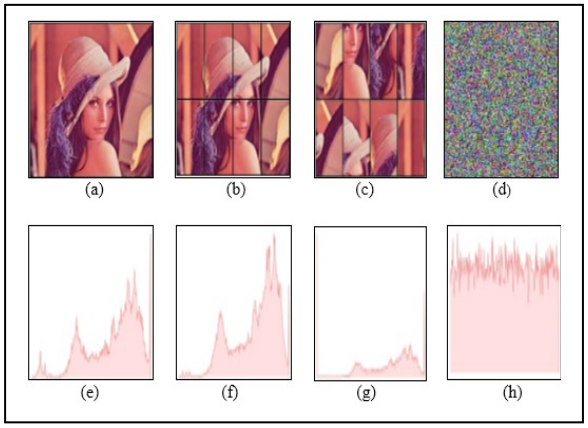



Figure (1) Block diagram of the proposed approach

## 5. RESULTS

In this part, experimental analysis of the proposed method has been done. The same standard Lena and peppers color image of size 256x256×3 is opted to make performance comparisons with existing color image ciphering algorithms. In this part, we analyze the experimental results depending on some factors. Figure (2) and Figure (3) demonstrate the original Lena image and Pepper image with their histograms before and after dividing, shuffling and applying XOR operation.

Figure.2. Lena image. (a) Original image. (b) Divided image. (c) Shuffling image (d) Encrypted image. (e) Histogram of image a. (f) Histogram of image b. (g) Histogram of image c. (h) Histogram of image d.



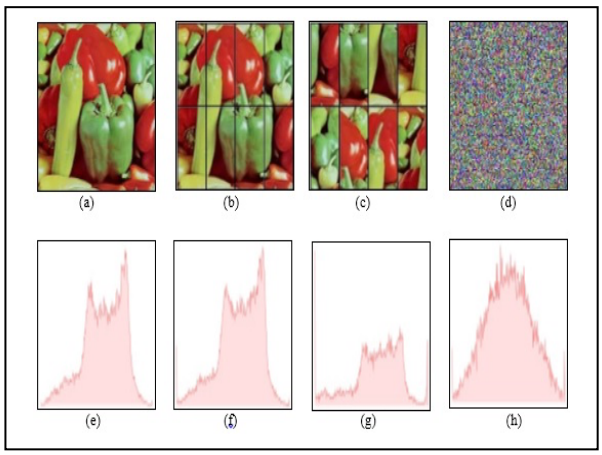




Fig.3. Pepper image. (a) Original image. (b) Divided image. (c) Shuffling image (d) Encrypted image. (e) Histogram of image a. (f) Histogram of image b.(g) Histogram of image c.(h) Histogram of image d

We have some important measures to experiment the force of image ciphering algorithm that is durable versus diverse offensives which are:
-Entropy
-PSNR (Peak Signal to Noise Ratio)
-NPCR (Number of Pixel Change Rate)
-UACI (Unified Average Changing Intensity).
Entropy is one of the statistical scalar parameters used for the image encryption evaluation. It shows the most frequency occurring patterns. It depends on the probability of the pixels values and measures the degree of randomness, In general, the greater the entropy, the harder it becomes to break the cryptosystem.
Peak Signal to Noise Ratio is used to assess the performance of an image encryption algorithm. PSNR reflects the encryption quality and measures the distortion in the decrypted image compared with the original image. Higher PSNR value means the loss data in the decrypted image is zero or negligible, and this indicates that the decrypted image is identical to the original image, which leads to the higher efficiency of the encryption technique
NPCR and UACI have become two of the most widely used methods of security analysis in encrypting images for differential attacks. The NPCR is centered on an exact number or an absolute number that indicates the value of how much the pixel's value changes, whereas, UACI focuses on the difference between the original image and the encrypted one. NPCR has a distance between 0-1. If the NPCR shows the number 0 then all the pixels in picture A are the same as in picture B. Moreover, if the NPCR shows number 1, then all the pixels in picture B change totally compared to picture A. The value in UACI also has a distance between 0-1, the highest UACI means that the proposed technique is resistant against differential attacks. Where in the case of image encryption, image A is the original image and image B is the encrypted image.
Table (1) and figure (4) displays the values of some important measures and Table (2) displays the correlation coefficients of the plain and encrypts images of the Lena and Peppers. The outcomes showed the correlation coefficients value of the encoded image is near to 0. This indicates that the suggested approach is efficient and impedance versus statistical attacks. Table (3) and figure (5) displays the comparison between the proposed method (as Lena image) and the other algorithms relative to the aspect of NPCR and UACI, entropy. We deduce that suggested algorithm done preferable outcomes than the remainder.

Table (1) Values of measures

| Parameters | Image (Lena) | Image (Peppers) |
|---|---|---|
| NPCR% | 99.6701 | 99.6630 |
| UACI% | 33.6872 | 33.6690 |
| PSNR | 27.998 | 27.789 |
| Entropy | 7.99993 | 7.99991 |

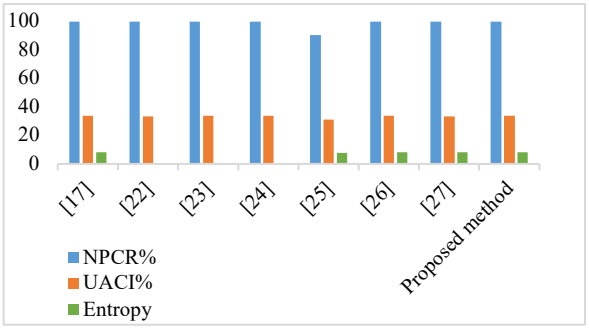



Figure.4. Values of measures

Table (2) correlation coefficients for original and ciphered images

| Direction | Image (Lena) | | Image (Peppers) | |
|---|---|---|---|---|
| | Original | Encrypted | Original | Encrypted |
| Horizontal | 0.9700 | − 0.0131 | 0.9316 | − 0.0035 |
| Vertical | 0.9374 | − 0.0258 | 0.9772 | 0.8249 |

Table (3) Comparison between proposed method and some other methods

| Reference | NPCR% | UACI% | Entropy |
|---|---|---|---|
| [17] | 99.6641 | 33.6124 | 7.99930 |
| [22] | 99.6137 | 33.4594 | - |
| [23] | 99.6452 | 33.6152 | - |
| [24] | 99.620 | 33.505 | - |
| [25] | 90.21 | 31.00 | 7.52200 |
| [26] | 99.6048 | 33.5044 | 7.98900 |
| [27] | 99.6286 | 33.4533 | 7.99990 |
| Proposed method | 99.6665 | 33.6781 | 7.99992 |

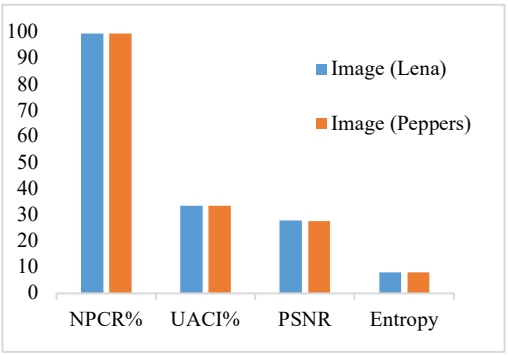



Figure.5. Comparison among suggested method and other methods

## 6. CONCLUSION

In this approach, a color image encryption algorithm depending on the new techniques and chaotic singer maps is suggested, where the color images are divided into eight parts and are shuffled according to a specific technique mentioned in algorithm (1). The three planes color (R, G, B) are separated from the shuffled image and converted into the binary form. The XOR operation is achieved between singer map's numbers and the planes depending on the new technique. The proposed method utilizes the randomness of the chaos singer maps in order to fetch a highly secured encrypted of the three matrix color with low computational complexity. The results of the proposed approach were compared with the other algorithms and showed their superiority in the terms of Entropy, UACI and NPCR. Happily, the enforcement procedure of this algorithm is modest and effective, in extension the empirical outcomes as it appears in table (1, 2 and 3) which display that the suggested asymmetric image ciphering approach is secure and efficient and has risen key sensibility and good anti-attack abilities.

## REFERENCES

[1] Han C., (2019), "An image encryption algorithm based on modified logistic chaotic map", Optik - International Journal for Light an Electron Optics 181, 779–785, https://doi.org/10.1016/j.ijleo.2018.12.178.
[2] Gan Z, Chai X, Zhang M, Lu Y (2018), "A double color image encryption scheme based on three-dimensional brownian motion". Multimed Tools Appl, 77(21):27919–27953.
[3] Sahari ML, Boukemara I (2018), " A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption". Nonlinear Dyn 94(1):723–744.
[4] Alvarez G, Li S (2006), "Some basic cryptographic requirements for chaos-based cryptosystems". Int J Bifurc Chaos 16(08):2129–2151.

[5] Liu H, Kadir A, Niu Y (2014), "Chaos-based color image block encryption scheme using S-box". AEU Int J Electron Commun 68(7):676–686.

[6] Fridrich J (1998), "Symmetric ciphers based on two-dimensional chaotic maps". Int J Bifurc Chaos 8(06):1259–1284

[7] Kiraz MS, Uzunkol O (2016), "Efficient and verifiable algorithms for secure outsourcing of cryptographic computations". Int J Inf Secur 15(5):519–537.

[8] Arpac B, Kurt E., Celik K., Ciylan B., (2020) "Colored Image Encryption and Decryption with a New Algorithm and a Hyperchaotic Electrical Circuit", Journal of Electrical Engineering & Technology, https ://doi.org/10.1007/ s42835-020-00393-x.

[9] Lian S, Sun J, Wang Z (2005), "Security analysis of a chaos-based image encryption algorithm". Phys A 351(2–4):645–661.

[10] Benlashram A., Al-Ghamdi M., AlTalhi R. and Laabidi K., (2020), " A novel approach of image encryption using pixel shuffling and 3D chaotic map", Journal of Physics: Conference Series, doi:10.1088/1742-6596/1447/1/012009.

[11] Pareek N. K., (2012), "Design and analysis of a novel digital image encryption scheme". International Journal of Network Security & Its Applications (IJNSA), 95-108.

[12] Kiraz MS, Uzunkol O (2016), " Efficient and verifiable algorithms for secure outsourcing of cryptographic computations". International journal of information security, 15(5):519–537.

[13] Zhang Y., (2020)," A new unified image encryption algorithm based on a lifting transformation and chaos", information science, 547, 307-327, https://doi.org/10.1016/j.ins.2020.07.058.

[14] Malik D. S. & Shah T., (2020), "Color multiple image encryption scheme based on 3D-chaotic maps", Mathematics and Computers in Simulation 178, 646-666, https://doi.org/10.1016/j.matcom.2020.07.007.

[15] Liu H., Zhao B., Huang L. & Liu Y, (2020), " A Lightweight Image Encryption Algorithm Based on Message Passing and Chaotic Map", security and communication networks, Article ID 7151836, 12 pages, https://doi.org/10.1155/2020/7151836.

[16] Jiao k., Ye G., Dong Y., Huang L., & He J., (2020), " Image Encryption Scheme Based on a Generalized Arnold Mapand RSA Algorithm", security and communication networks, Volume 2020, Article ID 9721675, 14 pages, https://doi.org/10.1155/2020/9721675.

[17] Yasser I., Khalifa F., Mohamed M. A., and Samrah A. S., (2020), "New Image Encryption Scheme Based on Hybrid Chaotic Maps", Volume 2020, Article ID 9597619, 23 pages, https://doi.org/10.1155/2020/9597619

[18] A. Hadj Brahim, A. Ali Pacha, N. Hadj Said, (2020) " Image encryption based on compressive sensing and chaos systems", Optics and Laser Technology, https://doi.org/10.1016/j.optlastec.2020.106489.

[19] Mondal B., Mandal T., (2016), "A light weight secure image encryption scheme based on chaos & DNA computing", Journal of King Saud University – Computer and Information Sciences, 29, 499–504,http://dx.doi.org/10.1016/ j.jksuci.2016.02.003

[20] Yoosefian S., Nezhad D., Safdarian N., Zadeh S., (2020), " New method for fingerprint images encryption using DNA sequence and chaotic tent map", S0030-4026(20)31492, https://doi.org/10.1016/j.ijleo.2020.165661.

[21] Chuang L.Y., Yang C.H., Li J.C., (2011), "Chaotic maps based on binary particle swarm optimization for feature selection". Applied Soft Computing. 11(1), 239–248.

[22] Luo H. and Ge B.,(2019), "Image encryption based on Henon chaotic system with nonlinear term", Multimedia Tools and Applications, vol. 78, no. 24, pp. 34323–34352.

[23] Amina S. and Mohamed F.K., (2018), "An efficient and secure chaotic cipher algorithm for image content preservation", Communications in Nonlinear Science and Numerical Simulation", vol. 60, pp. 12–32.

[24] Alawida M., Samsudin A., The J. S., and Alkhawaldeh R.S., (2019), "A new hybrid digital chaotic system with applications in image encryption" Signal Processing, vol. 160, pp. 45–58.

[25] Hasnat A., Barman D. and Mandal S. N., (2016), "A novel image encryption algorithm using pixel shuffling and pixel intensity reversal". International Conference on Emerging Technological Trends [ICETT].

[26] Hossain, M, Rahman, M, Rahman, A and Islam, S (2014), "A new approach of image encryption using 3D chaotic map to enhance security of multimedia component". 3rd International Conference on Informatics, Electronics & Vision.

[27] Jose A.P., Artiles, Chaves D. P. B., Pimentel C., (2019), "Image encryption using block cipher and chaotic sequences", Signal Processing: Image Communication, https://doi.org/10.1016/j.image.2019.08.014