Engineering and Technology Journal
Journal homepage: engtechjournal.org

Image Encryption Algorithm Based on Substitution Principle and Shuffling Scheme

Atyaf S. Hamad [a] **, Alaa K. Farhan** [b*]

[a]Department of Computer Sciences, University of Technology, Baghdad, Iraq, 110030@uotechnology.edu.iq

[b]Department of Computer Sciences, University of Technology, Baghdad , Iraq, atyafshihab@gmail.com

*Corresponding author.

Submitted: 02/07/2019 Accepted: 20/09/2019 Published: 25/12/2020

KEYWORDS

Image Encryption, Number of changing pixel rate (NPCR), S-Substitution, Unified Averaged Changed Intensity (UACI),Permutation

ABSTRACT

This research presents a method of image encryption that has been designed based on the algorithm of complete shuffling, transformation of substitution box, and predicated image crypto-system. This proposed algorithm presents extra confusion in the first phase because of including an S-box based on using substitution by AES algorithm in encryption and its inverse in Decryption. In the second phase, shifting and rotation were used based on secrete key in each channel depending on the result from the chaotic map, 2D logistic map and the output was processed and used for the encryption algorithm. It is known from earlier studies that simple encryption of images based on the scheme of shuffling is insecure in the face of chosen cipher text attacks. Later, an extended algorithm has been projected. This algorithm performs well against chosen cipher text attacks. In addition, the proposed approach was analyzed for NPCR, UACI (Unified Average Changing Intensity), and Entropy analysis for determining its strength.

How to cite this article: A. S. Hhamad and A. K.. Farhan, "Image Encryption Algorithm based on Substitution Principle and Shuffling Scheme," Engineering and Technology Journal, Vol. 38, Part B, No. 03, pp. 98-103, 2020.
DOI: https://doi.org/10.30684/etj.v38i3B.433

1. Introduction

The dynamic progression in multimedia and communication industry attracted an increased concern in regards to digital image security which are being sent via open or stored channels [1,2]. The illegal digital image handling makes it necessary to guard images [3]. Data may be guarded using some cryptographic standards like AES (Advanced Encryption Standard) or IDEA (International Data Encryption Standard) [4]. None-the-less there is no possibility for encrypting images using those approaches, and that is attributed to massive dimensions of data as well as the increased association amongst the pixels in the image files [5,6]. This is why chaos- based approaches have proven their superiority for image encryption. Chaotic systems which meet key requirements of diffusion and confusion have been characterized based on their reactivations to the control parameters, initial conditions, periodicity, and pseudo-randomness. Therefore, chaotic systems have a very high level of importance for cryptology [7].

Some image encryption chaos-based algorithms with a layout of permutation–diffusion have been de-fragmented [8]. The key streams that have been utilized for the encryption of plain images are the same and irrespective of them [9], which is why they give mutual property amongst those algorithms. For improving security, an original image encryption approach is based on diffusion and confusion has been utilized [10, 11]. Their scheme represents permutation and substitution operations to obtain the necessary effect of diffusion and confusion [12, 13]. This approach includes a wide range of benefits, like a wide key space range, increased sensitivity of the key, decreased time of encryption, amongst other factors [14, 15]. None-the-less, the author has discovered that this specific approach has been exposed to certain plain-text attack which is why it puts forth a successful plain-text attack. On the other hand, the authors were not able to find the whole random code sequence which is used in an operation of diffusion, which is why it is not easy deciphering other cipher text images that have been encrypted using their algorithm. [16].

2. Logistic Map

The logistic map was discovered in 1976 by the biologist Robert May. It is a simple nonlinear polynomial mapping equation. The main idea and its objective was to study and describe the biological populations and its growth. Its important parameters are explained as follows: the 1D logistic map is represented as:

$$f(y_i) = ry_i(1 - y_i) \qquad (1)$$

Where the parameter represents the state variable, r Є[1,4],and it is considered to be the control parameter [17,18]. The phase plan for the logistic map is illustrated in Figure 1.

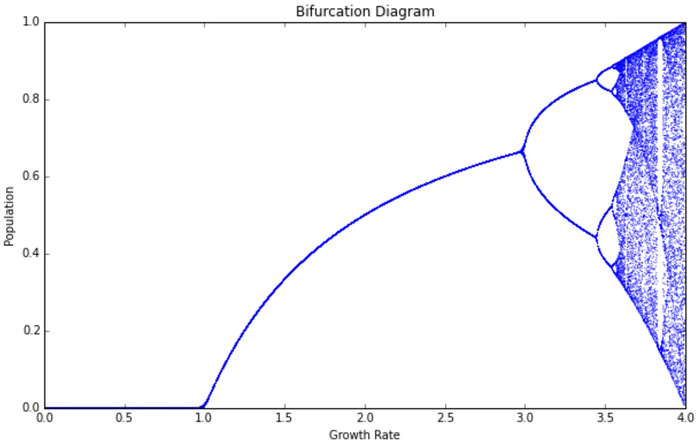

Figure 1: The Logistic map phase plane. [18]

The 2D-Logistic map has been introduced by Liu , as described in Eq.(2).

$$f(X_i) = R_1 X \left(1 - X_i\right) + Q_1 z_i^2 \qquad (2)$$

$$f(Y_i) = R_2 y_i (1 - z_i) + Q_2 (y_i^2 + y_i z_i)$$

This map depends on two main parameters, (Y) and (Z) that controls the behavior of this map. The experiments show a considerable improvement in terms of the complexity and the security where their values belong to [0,1].The chaotic behavior appears when the values of the control parameters are; [0.15 < Q1 < 0.21, 0.13 < Q2 < 0.15,2.75 < R1< 3.4, and 2.7 < R2< 3.45] [18].Where the initial values of Xn,Yn∈[0,1].After some iterations the resulting values of X and Y also belong to[0,1].

3. The Proposed Cryptosystem

Data in an image are strongly correlated amongst neighboring pixels. For disturbing this high correlation, in the proposed method of encryption the image is processed in two stages; confusion and diffusion. Encryption in the beginning of the original image pixels are replaced by other pixels, depending on the values in the S-Box (AES), when each pixel is converted to a binary block as 8-bits, each block of 8 bits is split in half and converted to decimal, the first one represents the number of the row and the second one is the column, the row and column are used as indexing S-Box (AES) to get a new value, this is repeated to each pixel in the image.

We have adopted shuffling (shift and rotate) pixel locations of the plain image in the algorithm. In order to lose no generality, in the second process, the image is split to channels (R, G, B), each byte in R is shifted and rotated to the left by using K1, which is sequence of bytes from a 2D chaotic output and K1 corresponds to shifting of the R channel and so on, as K2 and K3correspond to the shifting for each of G and B respectively. In Decryption, the same process is repeated but in the reverse order (shifted to right). Figure 2 and algorithms1, 2, and 3 explain this process:

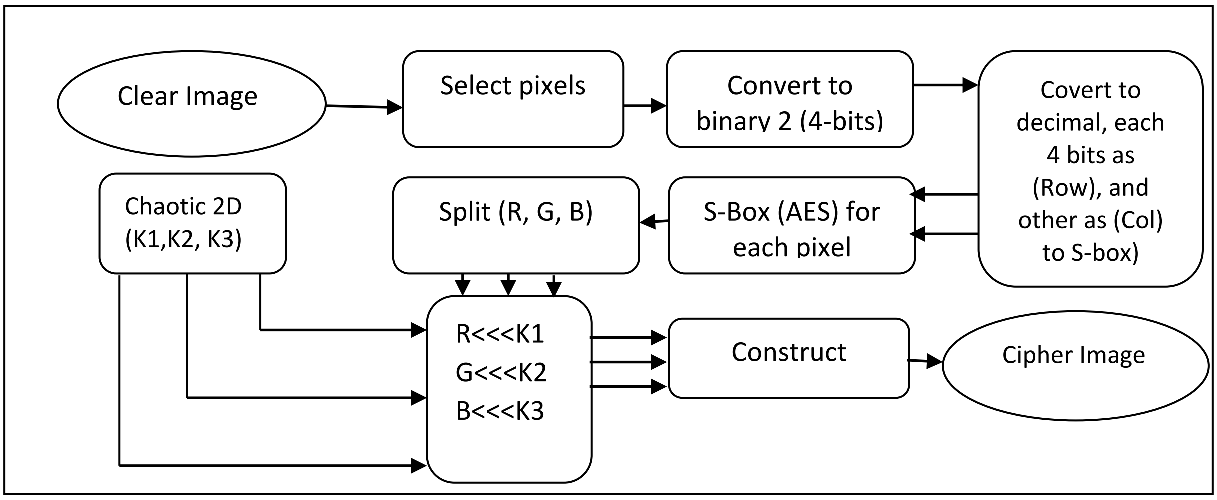
Clear Image
Select pixels
Convert to binary 2 (4-bits)
Covert to decimal, each 4 bits as (Row), and other as (Col) to S-box)
Chaotic 2D (K1,K2, K3)
Split (R, G, B)
S-Box (AES) for each pixel
R<<<K1
G<<<K2
B<<<K3
Construct
Cipher Image

Figure 2: Proposal Encryption Algorithm

```
Algorithm (1): Encryption Algorithm
Input: Clear Image, Secrete Keys
Output: Encrypted Image
Begin
Step 1: Pick each pixels and covert it to binary
Step 2:Convert each 8 binary bits(of the pixel) to 2 decimal numbers as a Row and a Column
Step 3:Substitution process in S-Box of AES (as Row, Column) for each pixel to get a new pixel value
Step 4:Split the image to (R,G,B)
Step 5:Shifted and Rotate each value in Rchannel by using K1,and so on to G and Bas (R<<<K1,G<<<K2 and B<<<K3)
Step 5:Construct (R,G,B) into the Cipher Image
End
```

```
Algorithm (2):Decryption Algorithm
Input: Encrypted Image, Secrete Keys
Output: Clear Image
Begin
Step 1:Split the image to (R,G,B)
Step 2:Shift and Rotate each value in Rchannel by using K1,and so on to G and Bas (R>>>K1,G>>>K2 and B>>>K3)
Step 3:Construct (R,G,B) to Image
Step 4: Select each pixel and convert it to binary
Step 2: Convert each binary 8 bits (of the pixel) to 2 decimal numbers as a Row and a Column.
Step 3:Substitute using S-Box$^{-1}$of AES (As Row, Column) for each pixel to get the new pixel
End
```

Algorithm (3): Secret Keys Generation Algorithm

Input: Parameter and Condition of 2D Chaotic Map

Output: K1,K2 and K3 Sequences

```
Begin
Step 1:Apply the equation of 2D chaotic map to get a huge sequence of Xi ,Yi  and store it in the buffer
Step 2: Convert Xi and Yi from floating to integer numbers based on deleting the real part.
Step 3:ConcatX and Y to obtain one sequence
Step 4:Split the sequence in step 3 to three keys as (K1,K2, and K3)
End
```

4. Analysis of the Proposed Algorithm

This part presents the implementation of the proposed encryption and decryption algorithms for an example image using the secret keys from 2D chaotic map and the proposed algorithm has been analyzed with some common analyses such as Correlation, NPCR, UACI, and entropy analysis.

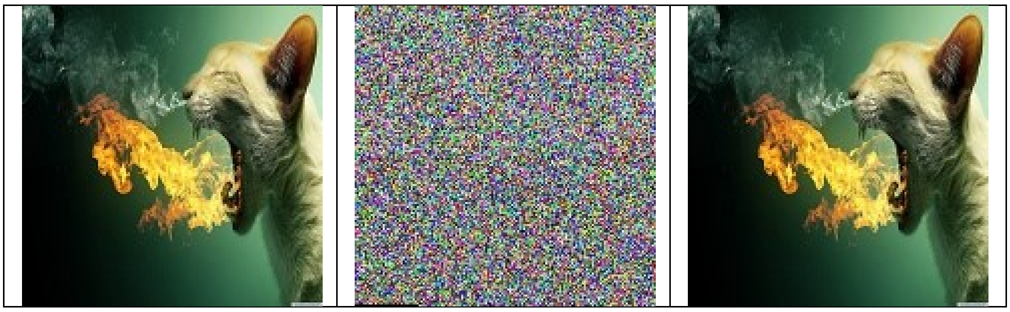

Figure 3: Encrypted and Decrypted Images

I. Correlation between two adjacent pixels

This correlation may be computed based on the following equation:

$$r_{xy}=\frac{cov\ (x,y)}{(\sqrt{(D(x))}\sqrt{(D(y))}} \qquad (3)$$

Where:

$$cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))((y_i-E(y))$$

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i$$

$$E(y)=\frac{1}{N}\sum_{i=1}^{N}y_i$$

Where: $N=height\times width$

Initially, the association amongst different colors of the image and its encrypted version have been tested, and both results have been subjected to comparison. It has been concluded from Table 1 that the presented approach shows considerably more efficient statistical characteristics [3].

TABLE I: The association between the original and the encrypted images

		G	B
Diagonal	0.7186	0.7083	0.6702
Horizontal	0.769	0.764	0.674

	1	9	9
Vertical	0.670 2	0.690 2	0.600 2

II. NPCR and UACI

NPCR, which is a Number of Pixels Change Rate, indicates the number of pixels change rate while on pixel of plain image changed. NPCR converges to 100%, the more sensitive the cryptosystem to the changing of the plain image, and the more effective for the crypto-system to resist plain-text attacks. UACI indicates the mean value of the intensity of the differences between plain and cipher images, it converges to 33.333%, the more the cryptosystem is effective in resisting differential attacks. Those two metrics are calculated from the following equations [10]:

$$UACI = \frac{1}{Width \times Height}\sum_{i,j}\left(\frac{c_1(i,j)-c_2(i,j)}{255}\right) \times 100\% \qquad (4)$$

$$NPCR = \frac{\sum_{i,j} D\,(i,j)}{Width \times Height} \times 100\%$$

c1(i, j) and c2(i, j) are the encrypted-image prior to changing one pixel of the plain image and after it, respectively. And in the case wherec1(i,j) ≠c2(i,j), then D(i, j) = 1otherwise,D(i, j) = 0.The results after changing a pixel's R value are shown in Table 2:

TABLE II: NPCR and UACI Results

Position	**R**	**G**	**B**
UACI	33.4745%	33.4714%	33
NPCR	99.6010%	99.6120%	99.6120%

III. Information Entropy

Image information entropy may be represented by the following equation [5]:

$$H(m) = \sum_{i=0}^{2N-1} p(m_i) log_2 \frac{1}{p\,(m_i)} \qquad (5)$$

Where p(mi) is mi probability, and log2 is base 2 logarithms which expresses the entropy, N is the number of bits that are utilized for representing a pixel, and fora pixel's one color channel, it is evident that N = 8. In case where the image is ideally random, that will mean that for every i, p(mi) = 1/256, and it is easily found that H(m) = 8. And the cipher image results have been listed in Table 3.

TABLE III: Information Entropy

Position	**R**	**G**	**B**
Information Entropy	7.203404	7. 201111	7.88800

5. Conclusions

The results of the evaluation of the algorithm have proven its efficiency, as depicted in Figure 3. The values of each of the Correlation, NPCR, UACI, and entropy as the analysis of this algorithm are considerably close to the optimum values. In addition, this algorithm has provided an additional level confusion because of the S-box transformation. Mainly, this algorithm hits the S-P (P via shift and rotate) network idea of Shanon directly as a result of the operations of permutation and substitution.

References

[1] Y. Song, Z. Zhu, W. Zhang, H. Yu and Y. Zhao, “Efficient and Secure Image Encryption Algorithm Using a Novel Key-Substitution Architecture,” in IEEE Access, vol. 7, pp. 84386-84400, 2019, doi: 10.1109/ACCESS.2019.2923018.

[2] A Kadhim , “Mouse Movement with 3D Chaotic Logistic Maps to Generate Random Numbers”, - Diyala Journal For Pure Science, vol. 13, no. 3-part 2, pp. 24-39, 2017.

[3] H. Natiq, “A new hyper chaotic map and its application for image encryption”, *Eur. Phys. J. Plus* **133,** 6, 2018. https://doi.org/10.1140/epjp/i2018-11834-2.

[4] F. Alaa Kadhim, G. H. Abdul-Majeed and R. S. Ali, "Enhancement CAST block algorithm to encrypt big data," 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), Baghdad, 2017, pp. 80-85, doi: 10.1109/NTICT.2017.7976119.

[5] M. Benssalah, Y. Rhaskali and M. S. Azzaz, "Medical Images Encryption Based on Elliptic Curve Cryptography and Chaos Theory," 2018 International Conference on Smart Communications in Network Technologies (SaCoNeT), El Oued, 2018, pp. 222-226, doi10.1109/SaCoNeT.2018.8585512.

[6] A. K. Farhan and M. A. A. Ali, "Database protection system depend on modified hash function", Proc. Conf. Cihan Univ.-Erbil Commun. Eng. Compute. Sci., pp. 1-101, Mar. 2017.

[7] X. Liu, D. Xiao, W. Huang and C. Liu, "Quantum Block Image Encryption Based on Arnold Transform and Sine Chaotification Model," in IEEE Access, vol. 7, pp. 57188-57199, 2019. doi: 10.1109/ACCESS.2019.2914184.

[8] A. Kadhim, S. Khalaf, ”New Approach for Security Chatting in Real Time”, International Journal of Emerging Trends and Technology in Computer Science (IJETTCS),vol. 4, no.3, 2015.

[9] T. K. Hazra and S. Bhattacharyya, "Image encryption by blockwise pixel shuffling using Modified Fisher Yates shuffle and pseudorandom permutations," 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, 2016, pp. 1-6, doi: 10.1109/IEMCON.2016.7746312

[10] X. Wang, S. Gao, L. Yu, Y. Sun and H. Sun, "Chaotic Image Encryption Algorithm Based on Bit-Combination Scrambling in Decimal System and Dynamic Diffusion," in IEEE Access, vol. 7, pp. 103662-103677, 2019, doi: 10.1109/ACCESS.2019.2931052.

[11] Z. Wu, X. Zhang and X. Zhong, "Generalized Chaos Synchronization Circuit Simulation and Asymmetric Image Encryption," in IEEE Access, vol. 7, pp. 37989-38008, 2019, doi: 10.1109/ACCESS.2019.2906770.

[12] M. I. Wade, M. Chouikha, T. Gill, W. Patterson, T. M. Washington and J. Zeng, "Distributed Image Encryption Based On a Homomorphic Cryptographic Approach," 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York City, NY, USA, 2019, pp. 0686-0696, doi: 10.1109/UEMCON47517.2019.8993025.

[13] A. U. Rehman, H. Wang, M. M. Ali Shahid, S. Iqbal, Z. Abbas and A. Firdous, "A Selective Cross-Substitution Technique for Encrypting Color Images Using Chaos, DNA Rules and SHA-512," in IEEE Access, vol. 7, pp. 162786-162802, 2019, doi: 10.1109/ACCESS.2019.2951749

[14] R. Das, S. Manna and S. Dutta, "Cumulative image encryption approach based on user defined operation, character repositioning, text key and image key encryption technique and secret sharing scheme," *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, Chennai, 2017, pp. 748-753, doi: 10.1109/ICPCSI.2017.8391813.

[15] M. K. Abdmouleh, A. Khalfallah and M. S. Bouhlel, "A Novel Selective Encryption DWT-Based Algorithm for Medical Images," *2017 14th International Conference on Computer Graphics, Imaging and Visualization*, Marrakesh, 2017, pp. 79-84, doi: 10.1109/CGiV.2017.10.

[16] X. Geng and Q. Ding, "Similar-short Periodicity Analysis and Application in Image Compression Encryption of Digital Chaos," *2012 Fifth International Workshop on Chaos-fractals Theories and Applications*, Dalian, 2012, pp. 167-171, doi: 10.1109/IWCFTA.2012.44.

[17] Wenting Yuan, Xuelin Yang, Wei Guo and Weisheng Hu, "A double-domain image encryption using hyper chaos," *2017 19th International Conference on Transparent Optical Networks (ICTON)*, Girona, 2017, pp. 1-4, doi: 10.1109/ICTON.2017.8025092.

[18] Y. Luo, M. Du and D. Liu, "JPEG Image Encryption Algorithm Based on Spatiotemporal Chaos," 2012 Fifth International Workshop on Chaos-fractals Theories and Applications, Dalian, 2012, pp. 191-195, doi: 10.1109/IWCFTA.2012.49.