Applications and Applied Mathematics: An International Journal (AAM)

Volume 16 | Issue 1 Article 33

6-2021

A Novel Color Image Encryption Scheme Based on Arnold's Cat Map and 16-Byte S-box

Tariq Shah
Quaid-i-Azam University

Ayesha Qureshi
Quaid-i-Azam University

Muhammad Usman
University of Education, Vehari Campus

Recommended Citation

Shah, Tariq; Qureshi, Ayesha; and Usman, Muhammad (2021). A Novel Color Image Encryption Scheme Based on Arnold's Cat Map and 16-Byte S-box, Applications and Applied Mathematics: An International Journal (AAM), Vol. 16, Iss. 1, Article 33.
Available at: https://digitalcommons.pvamu.edu/aam/vol16/iss1/33

Available at
http://pvamu.edu/aam
Appl. Appl. Math.
ISSN: 1932-9466

Applications and Applied
Mathematics:
An International Journal
(AAM)

Vol. 16, Issue 1 (June 2021), pp. 591 – 603

A Novel Color Image Encryption Scheme Based on Arnold’s Cat Map and 16-Byte S-box

[1]Tariq Shah, [2*]Ayesha Qureshi, and [3]Muhammad Usman

[1]Department of Mathematics
Quaid-i-Azam University
Islamabad 44000, Pakistan
stariqshah@gmail.com
[2]Department of Mathematics
Quaid-i-Azam University
Islamabad 44000, Pakistan
ayesha.qureshi6@gmail.com
[3]Department of Mathematics
University of Education, Vehari Campus
Vehari 61100, Pakistan
dr.usman@ue.edu.pk

[*]Corresponding author

Received: February 25, 2020; Accepted: November 1, 2020

Abstract

The presented work sets out to subsidize to the general body of knowledge in the field of cryptography application by evolving color image encryption and decryption scheme based on the amalgamation of pixel shuffling and efficient substitution. Arnold’s cat map is applied to snap off the correlation in pixels of image and the shuffled image is encrypted by 16-byte S-box substitution. Computer simulations with a standard test image and the outcome is presented to scrutinize the competence of the projected system. Several image-quality measures and security analyses have been made out for the encrypted image to estimate the statistical and differential strength of the scheme. A comparison is presented by following out the scheme with 256-byte S-box and 16-nibble S-box to support for sturdiness of the idea. It is concluded from the results of analyses that the proposed scheme with 16-byte S-box can resist exhaustive attacks and is apt for practical applications.

Keywords: Cryptography; color image; Arnold’s cat map; 16-byte S-box, encryption /decryption; statistical and differential attacks

MSC 2010 No.: 68U10, 94A60, 68P25

1. Introduction

The conceptions of many modern cryptographic algorithms usually make use of dynamical chaotic maps which own random-like attributes and chaotic behavior, for example, Khan et al. (2019) implemented the concept of Brownian motion along with orientation utilizing unique ternary relations which rely on random motion depending upon spatial and time coordinates. Furthermore, to increase a security level of encryption algorithm a dynamical map having chaotic behavior is used. Shah et al. (2019) suggested an encryption algorithm, for audio processing, based on permutation and substitution network. For substitution purpose S-boxes are generated with the help of Mobius transformation while Henon chaotic map is utilized (for permutation network) to perform pixel-wise permutation. Ye et al. (2018) presented a strong mechanism for chaotic encryption scheme by employing secure hash algorithm-3 (SHA-3) along with three-dimensional logistic map and electrocardiograph (ECG) signal. Mixed chaotic map together with Josephus traversing was utilized (for chaotic image encryption algorithm) by Wang et al. (2018). Naseer et al. (2018) employed three-dimensional mixed chaotic map for image encryption.

Shannon (1948) highlights the excellent role of chaotic dynamic map towards communication networks. According to him, there are two basic properties for an encryption system to resist statistical attacks: namely, confusion and diffusion. Confusion is responsible for hiding the association between actual and encrypted data sets while diffusion process generates a random variation in entire encrypted data. Substitution method in which an object is replaced by any other object can serve as a confusion and permutation (i.e., rearrangement of objects) serve as a most elementary diffusion method. Therefore, the frequent usage of substitution and permutation procedures in chaotic dynamical system almost become the basic requirement of cryptography.

The current research work aims to execute the two interesting and commonly used ideas: permutation-substitution networks and chaos theory, for color image encryption scheme. Because of randomness and strong safety of chaotic maps, these are frequently used in the encryption algorithms. Moreover, most often one has a option for non-linear module and it is S-box for a block cipher. In order to attain dominant significance of encryption there is need to substitute every image's pixel by other gray value.

The report introduces an image encryption technique based on Arnold's cat map and 16-byte S-box substitution. The main focus of this research work is to evaluate the complexity of encryption based on the amalgamation of chaos and 16-byte S-box substitution in comparison with the 64-byte and 16-nibble S-box substitutions. The current research article is devised as follows: the description and attributes of Arnold's cat map has been done in Section 2. In Section 3, the algebraic structure of 16-bye S-box is discussed. Section 4 covers the encryption and decryption scheme while the Section 5 presents pseudo code for the encryption system. Section 6 deals with the experimental work, whereas the security analyses have been performed in Section 7. Lastly, in Section 8 conclusion of the whole study has been made.

2. Arnold’s cat map

In order to shuffle the positions of pixels of a plain image one requires a 2-D invertible chaotic map which is known as Arnold’s cat map. If $X = \begin{bmatrix} x \\ y \end{bmatrix}$ is an $N \times N$ matrix of some image, then Arnold’s cat map is the transformation:

$$\Gamma \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x + py \\ qx + (pq+1)y \end{bmatrix} modN, \tag{1}$$

where p and q are positive integers, Chen et al. (2004), and Scharinger (1998). Due to this transformation, given in Equation (1), the actual position of pixels of image has been shuffled randomly. From Equation (1) it is clear that the transformation is linear and with the help of mod function the shuffling of pixels can easily and efficiently be done. The correlation among the neighboring pixels can be fully interrupted after performing various iterations. Nevertheless, if iterated enough times, the original image reappears. Hence it cannot be used alone and for the security of the algorithm further processing is needed.

3. Sixteen-byte S-box

In Qureshi and Shah (2017), a methodology for the expression of 16-byte S-box is exhibited. The S-box is constructed by members of a subgroup, of the multiplicative group $GF(2^8)^*$, having order equal to fifteen (say H_{15}) along with zero. Moreover, the group $GF(2^8)^*$ comprises of irreducible polynomial for multiplication $f(x) = x^8 + x^4 + x^3 + x^2 + 1$. The S-box contains a permutation of all 16 8-bit values of $H_{15} \cup \{0\}$ and is constructed by employing a fractional linear fractional transformation, which is constrained, on members of subgroup. The elements of the S-box are given in Table 1.

Table 1. Small 8 × 8 S-box

	0	1	2	3
0	152	79	147	220
1	69	0	10	146
2	214	221	78	68
3	11	1	153	215

4. Encryption scheme

The proposed image encryption technique begins with the shuffling of the pixel positions of the plain image using Arnold’s cat map. After that, it makes substitution of the pixel values of the shuffled image utilizing the S-box table. The matrix of substituted pixels is then XORed with a random matrix generated by using the logistic map. These steps are completed for all the three channels of the RGB image. The encrypted channels are combined to get the RGB encrypted image. Arnold’s cat map may be executed for k number of iterations.

The algorithm of decryption is like the algorithm of encryption apart from the fact that the Arnold's cat map is replaced by its inverse and utilizing the inverse S-box substitution at the start of round. The algorithm of decryption restores the actual image of the same quality.

The process of substitution for the 16-byte S-box is completed as follows: The two leftmost least significant bits (LSBs) of the input pixel of the shuffled image are employed as row index whereas the two rightmost LSBs are employed as column index to select an eight-bit S-box value. LSBs of the S-box values become the most significant bits (MSBs) and MSBs of the plain image pixels become the LSBs of the substituted pixels. In this way, pixels of the whole image are substituted. Figure 1 elaborates the step-by-step encryption scheme.

5. Pseudo code for the proposed image encryption scheme

Input: Plain mage I of size $m \times n \times 3$.

Output: Encrypted image C of size $m \times n \times 3$.

```
1. $I \rightarrow R, G, B$ (Split the image $I$ into red, green, and blue channels each of size $m \times n$).
2. $\mathrm{R, G, B} \rightarrow [R; A]_{m\times m}, [G; A]_{m\times m}, [B; A]_{m\times m}; A$ is a random matrix of order $n - m \times n \; (m > n)$.
3. $R(i,j) \rightarrow R\big((i + pj) mod\, m\big), (qi + (pq+1)j) mod\, m) = R(i', j');\; i, j = 1,2, \dots, m, \;\& \, p, q \in Z^{+}$.
4. $R(i', j') \rightarrow R\big(S(i'), S(j')\big)$.
5. $x_{k+1} = r x_k (1 - x_k);\, x_0 = 0.1 \;\&\; r = 3.9$.
6. Reshape the sequence as $\{x_k\} \rightarrow \begin{bmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_n & x_{n+1} & \cdots & x_{2n-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_{(m-1)n} & x_{(m-1)n+1} & \cdots & x_{mn-1} \end{bmatrix}_{m\times n} = M$.
7. $R\big(S(i'), S(j')\big) \oplus M \rightarrow EncR$.
8. Repeat steps 3 to 7 for $G$ and $B$ to get $EncG$ and $EncB$.
9. $cat(3; EncR; EncG; EncB) \rightarrow \; C$.
```

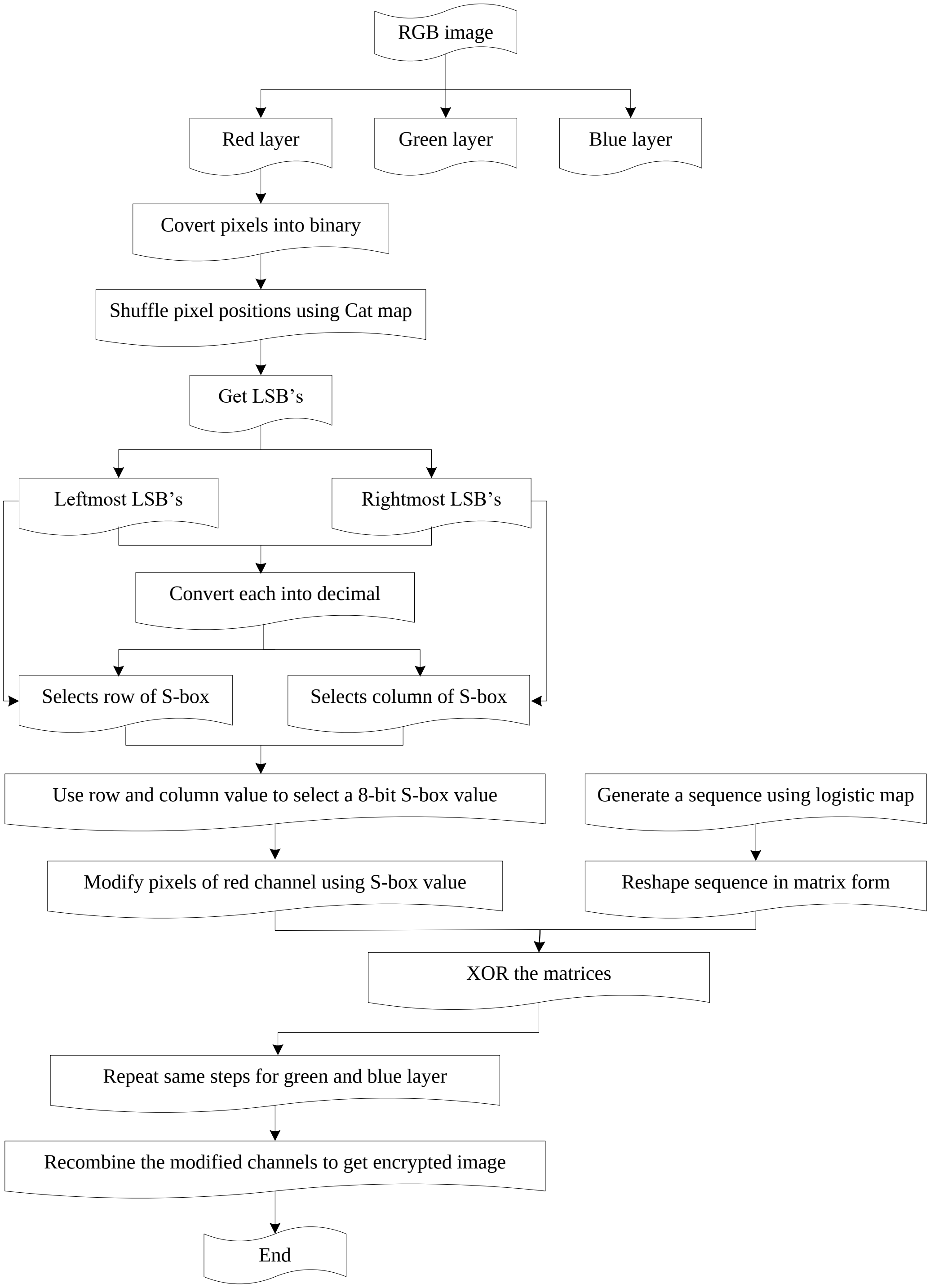

RGB image
Red layer
Green layer
Blue layer
Covert pixels into binary
Shuffle pixel positions using Cat map
Get LSB’s
Leftmost LSB’s
Rightmost LSB’s
Convert each into decimal
Selects row of S-box
Selects column of S-box
Use row and column value to select a 8-bit S-box value
Generate a sequence using logistic map
Modify pixels of red channel using S-box value
Reshape sequence in matrix form
XOR the matrices
Repeat same steps for green and blue layer
Recombine the modified channels to get encrypted image
End

Figure 1. Encryption Scheme

6. Experimental analyses

An experimental analysis of above encryption scheme has been performed in this section. The plain image of size 768×512 bytes is depicted in Figure 2(A) and the histograms of the red, green, and blue channels of original image are presented in Figure 2(B, C, and D). The hidden keys in cat map are opted as $p = q = 1, k = 5$. Encrypted image using 16-byte S-box with the histograms depicting all three channels (i.e., red, green, and blue) are presented in Figure 3(A, B, C, and D). Figure 4 (A, B, C, and D) highlights the encrypted image using AES S-box with the histograms of R, G, and B channels while encrypted image using 16-nibble S-box with the histograms of R, G, and B channels are depicted in Figure 5(A, B, C, and D). Decrypted image using 16-byte S-box with the histograms of R, G, and B channels are presented in Figure 6(A, B, C, and D). The histograms in Figure 3 and 4 show the uniform distribution of pixel values in the cipher image. This indicates that the proposed encryption scheme is capable of hiding image data while using 16-byte and 256-byte S-box. But the histograms in Figure 5 shows the weakness of 16-nibble S-box. Same results can be seen in the case of 3D histograms in Figure 7.

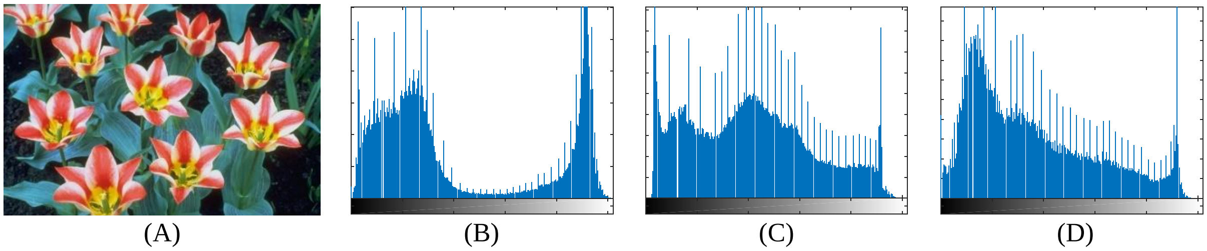


Figure 2. (A) Plain image, (B) Histogram of red channel, (C) Histogram of green channel, (D) Histogram of blue channel

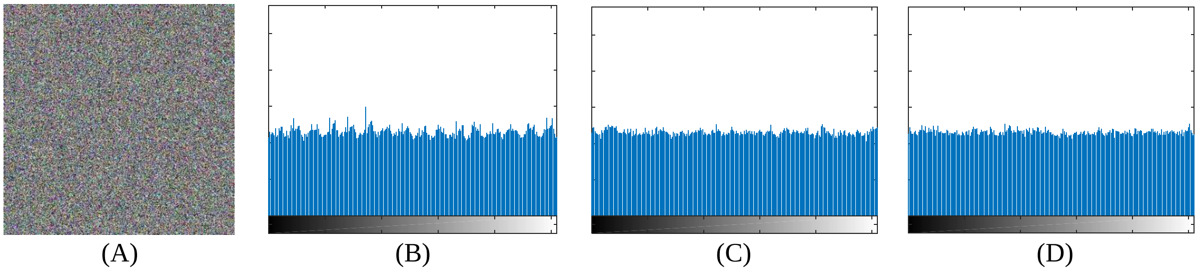


Figure 3. (A) Encrypted image using 16-byte S-box, (B) Histogram of red channel, (C) Histogram of green channel, (D) Histogram of blue channel, (E) Decrypted image

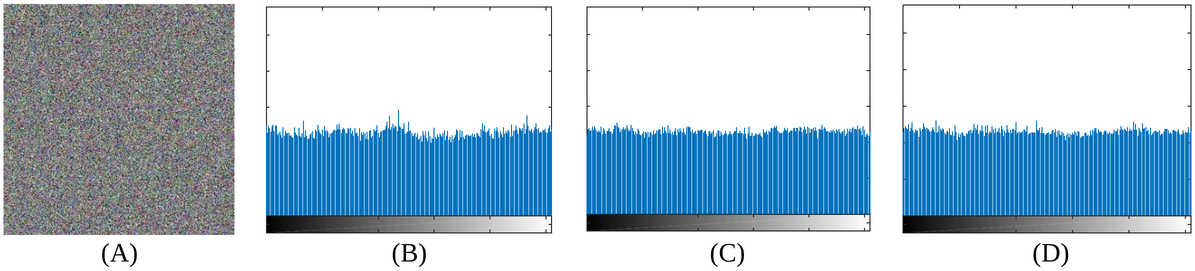


Figure 4. (A) Encrypted image using 256-byte S-box, (B) Histogram of red channel, (C) Histogram of green channel, (D) Histogram of blue channel

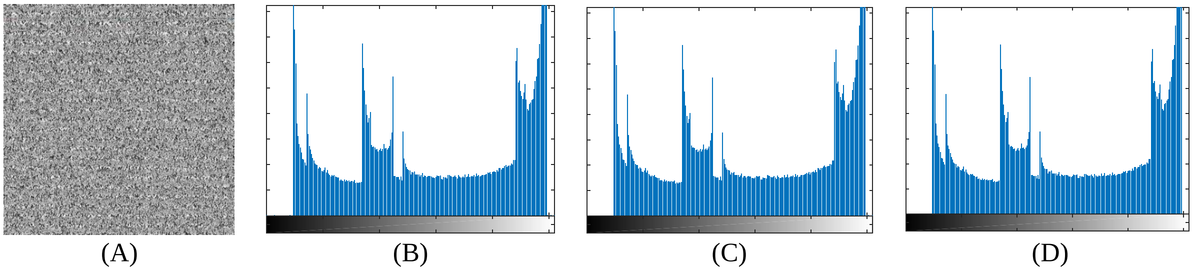


Figure 5. (A) Encrypted image using 16-nibble S-box, (B) Histogram of red channel, (C) histogram of green channel, (D) Histogram of blue channel

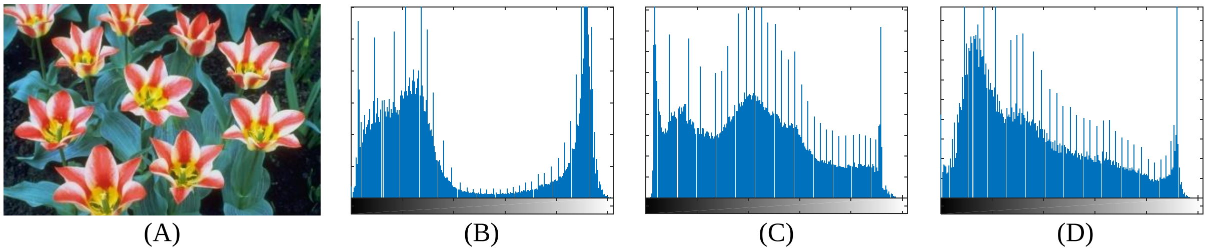
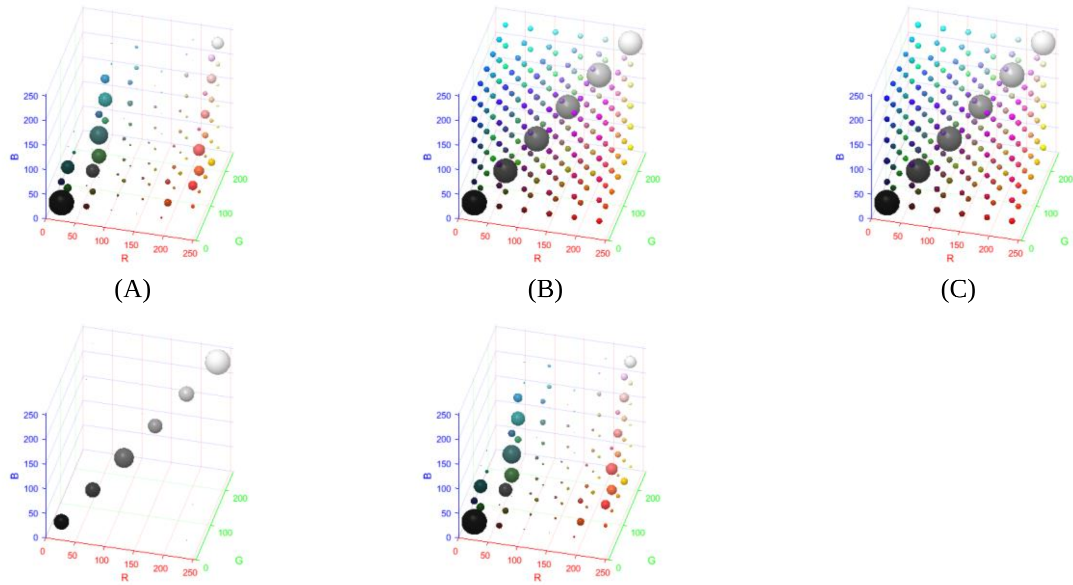


Figure 6. (A) Cipher image, (B) Histogram of red channel, (C) Histogram of green channel, (D) Histogram of blue channel



(A) (B) (C)

(D) (E)

Figure 7. 3D histograms (A) Plain image, (B) Encrypted image using 16-byte S-box, (C) Encrypted image using 256-byte S-box, (D) Encrypted image using 16-nibble S-box, (E) Decrypted image using proposed scheme

7. Security analyses

This section presents the security analyses by calculating different image quality measures for encrypted image with reference to the plain image of “Peppers” of size 512×512. Table 2 displays the results of these measures of the three above mentioned cases. One can conclude from these results that the application of 16-byte S-box improves the image quality measures and brings them very close to the 256-byte case, instead of very small size than AES S-box. Further, it enhances the resistance of the encrypted image against differential attacks. Thus, the 16-byte S-boxes may play role in the improvement of lightweight ciphers that utilize 16-nibble S-boxes. Table 3 gives a comparison between the proposed scheme and some existing robust schemes to estimate the security of the algorithm against differential attacks.

7.1. Mean square error (MSE)

The quality of an encrypted image has been assessed by mean square error in image processing. It is actually, cumulative squared difference between encrypted and original image. The mathematical formula for MSE is:

$$MSE = \frac{1}{M \times N} \sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y) - C(x,y)]^2, \tag{2}$$

where $I(x,y)$ is an actual image, $C(x,y)$ is the encrypted one and M, N are the image’s dimensions, Ahmet and Paul (1995). The larger values of MSE are realized as the well ace.

7.2. Peak signal-to-noise ratio (PSNR)

The fidelity of a signal representation can be affected by corrupting noise. The ratio between two powers (i.e., signal power and corrupting noise power) is determined by a tool known as PSNR (Peak signal-to-noise ratio), Huynh-Thu and Ghanbari (2008). Since signals own a very wide dynamic range that's why PSNR is mathematically expressed as logarithmic decibel scale. It has been employed in the current work to access quality of encrypted image. The plain image is served as signal while noise correspond to the distortion which is generated during encryption process. A larger value of PSNR generally correspond to the higher quality of reconstruction. Mathematically, it is written as (for an image I (in dB)):

$$PSNR = 10.\log_{10} \frac{{MAX_I}^2}{\sqrt{MSE}}. \tag{3}$$

7.3. Normalized cross correlation (NK)

The correlation function is utilized to quantify the closeness of original and encrypted images. The similarity of original and encrypted images is measured by Normalized Cross-Correlation (NK) which is given as

$$NK = \frac{\sum_{y=1}^{M} \sum_{x=1}^{N} (I(x,y) \times C(x,y))}{\sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y)]^2}, \tag{4}$$

where $I(x,y)$ is an actual image, $C(x,y)$ is an encrypted one and M, N are the image's dimensions, Ahmet and Paul (1995).

7.4. Average difference (AD)

It is mean value of difference between test image and reference signal. Mathematically it can be expressed as

$$AD = \frac{1}{M \times N} \sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y) - C(x,y)], \tag{5}$$

where $I(x,y)$ is an actual image, $C(x,y)$ is an encrypted one and M, N are the image's dimensions, Ahmet and Paul (1995).

7.5. Structural content (SC)

Structural content (SC) is also utilized to measure the similarity between actual and encrypted images. It is defined as:

$$SC = \frac{\sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y))]^2}{\sum_{y=1}^{M} \sum_{x=1}^{N} [C(x,y))]^2}, \tag{6}$$

where $I(x,y)$ is an actual image, $C(x,y)$ is an encrypted one version and M,N are the image's dimensions, Ahmet and Paul (1995).

7.6. Maximum difference (MD)

Maximum difference measures the maximum of error signal (i.e., difference between test image and reference signal).

$$MD = max|I(x,y) - I'(x,y)|, \tag{7}$$

where $I(x,y)$ is an actual image, $C(x,y)$ is an encrypted one and M,N are the image's dimensions, Ahmet and Paul (1995).

7.7. Normalized absolute error (NAE)

Normalized absolute error between the encrypted and plain image is defined as:

$$NAE = \frac{\sum_{y=1}^{M}\sum_{x=1}^{N}|I(x,y) - C(x,y)|}{\sum_{y=1}^{M}\sum_{x=1}^{N}|I(x,y))|}, \tag{8}$$

where $I(x,y)$ is an actual image, $C(x,y)$ is an encrypted one and M,N are the image's dimensions, Ahmet and Paul (1995).

7.8. Root mean square error (RMSE)

It is the square root of average of the square of all the errors. It is commonly utilized for the numerical predictions of metric error. It is mathematically represented as:

$$RMSE = \sqrt{\frac{1}{M \times N}\sum_{y=1}^{M}\sum_{x=1}^{N}[I(x,y) - C(x,y)]^2}, \tag{9}$$

where $I(x,y)$ is an actual image, $C(x,y)$ is an encrypted one and M,N are the image's dimensions, Ahmet and Paul (1995).

7.9. Universal quality index (UQI)

Universal quality index is utilized to perform three comparisons between actual and distorted image, namely, luminance, contrast, and structural comparisons. It is mathematically defined as (for two images *X* and *Y*):

$$UQI(I,C) = \frac{4\mu_I\mu_C\mu_{IC}}{(\mu_I^2 + \mu_C^2)(\sigma_I^2 + \sigma_C^2)}, \tag{10}$$

where μ_I, μ_C represent the average values of actual and encrypted images while σ_I, σ_C represent the standard deviation of original and distorted images, Wang (2002).

7.10. Mutual information (MI)

It is employed to attain the information related to actual image through distorted image. The MI of two images *I* and *C* is expressed as:

$$MI(I,C) = \sum_{y \in C} \sum_{x \in I} p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)}, \tag{11}$$

where $p(x,y)$ being the probability joint function of I and C, and $p(x), p(y)$ are the marginal probability distribution functions of I and C respectively, Cover and Thomas (2006).

7.11. Structural similarity (SSIM)

It is an enhanced version of UQI which is used to measure the closeness or similarity that exist between two images. If one image has a perfect quality, then SSIM measures the quality of other image when both are being compared. One can calculate SSIM on several windows of an image. The SSIM for two windows X and Y having same dimension $N \times N$ is:

$$SSIM(X,Y) = \frac{(2\mu_X\mu_Y + c_1)(2\sigma_{XY} + c_2)}{(\mu_X^2 + \mu_Y^2 + c_1)(\sigma_X^2 + \sigma_Y^2 + c_2)}, \tag{12}$$

where μ_X and μ_Y, σ_X^2 and σ_Y^2, and σ_{XY} being mean of X, mean of Y, variance of X, variance of Y, and covariance of X and Y, respectively. Whereas $c_1 = (k_1 L)^2$ and $c_2 = (k_2 L)^2$ corresponds to the variables used to stabilize the division with weak denominator, L denotes the dynamic range of pixel values, $k_1 = 0.01$ and $k_2 = 0.03$ by default, Wang et al. (2004). The range of SSIM lies between -1 and 1 and for the identical data its value comes out to be 1.

7.12. Number of pixels change rate (NPCR)

NPCR has been used to test the influence of change made by single pixel on pixels of entire image by the suggested algorithm. This means that it corresponds to rate of change of number of encrypted image's pixels when one byte of actual image is varied. Suppose that number of encrypted images is two (i.e., C_1 and C_2) having dimension equal to $M \times N$ corresponding to two actual images differing by one byte. The value of NPCR shows the sensitivity of cryptosystem. For instance, the cryptosystem becomes more and more sensitive to variations in actual image as its (NPCR) value approaches to 100% and such cryptosystem offers great resistance against attacks of plain text. It is mathematically defined as, Wu et al. (2011):

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%, \tag{13}$$

where

$$D(i,j)=\begin{cases}0, & if\ C_1(i,j)=C_2(i,j),\\ 1, & if\ C_1(i,j)\neq C_2(i,j).\end{cases} \tag{14}$$

7.13. Unified average changing intensity (UACI)

UACI is a technique used in calculation of gauge influences of slight variations in actual image or its sensitiveness. Consider two encrypted images C_1 and C_2 of dimension $M \times N$, corresponding to two plain-text images which are differ by one byte. The higher value of UACI correspond that cryptosystem is more effective and leads to be safer against differential attack. The UACI is defined by the Wu et al. (2011).

8. Conclusion

The presented work deals with the complexity of encryption based on the amalgamation of chaos and S-box substitution. 256-byte S-box, 16-byte S-box and 16-nibble S-box has been considered for the experimental study. Results of different image quality measures show that the 16-nibble S-box improves the complexity of encryption than 16-nibble S-box and produces the very close results with 256-byte S-box. The security of the proposed scheme against differential attacks is estimated by comparison of results with some of robust existing algorithms. Hence, the cryptography applications that use 16-nibble S-boxes can be amended by replacing them with 16-byte S-boxes.

Table 2. Image Quality Measures

No.	Quality measure	16-byte S-box			256-byte S-box			16-nibble S-box		
		Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
01	MSE	7992.13	11231.9	11112.9	7980.45	11236	11144	7871.9	12667.8	14839.8
02	PSNR	9.1041	7.6262	7.6725	9.1105	7.6246	7.6603	9.1700	7.1037	6.4165
03	NK	0.7802	0.7766	1.3316	0.7790	0.7734	1.3226	0.9204	0.9160	1.5676
04	AD	22.3317	-12.1989	-61.2117	22.5257	-11.6357	-60.5037	-0.6317	-34.8920	-83.9702
05	SC	1.1276	0.8735	0.2938	1.1312	0.8781	0.2950	0.8602	0.6670	0.2242
06	MD	225	230	223	224	232	221	204	217	199
07	NAE	0.4933	0.7496	1.2935	0.4929	0.7490	1.2972	0.4994	0.7981	1.5171
08	RMSE	89.3987	105.9810	105.4180	89.3333	106	105.5650	88.7237	112.5510	121.8190
09	UQI	0.0002	-0.0007	-0.0001	-0.00005	-0.0004	-0.0008	0.00005	-0.0001	-0.00003
10	MI	0.1396	0.1613	0.1518	0.1422	0.1623	0.1533	0.1248	0.1445	0.1347
11	SSIM	0.0105	0.0077	0.0075	0.0103	0.0079	0.0069	0.0095	0.0071	0.0064
12	NPCR	99.59			99.63			0		
13	UACI	33.40			33.45			0		

Table 3. Comparison of NPCR and UACI values

Scheme ↓/ Test →	NPCR	UACI
Khan et al. (2019)	99.64	33.49
Ye et al. (2019)	99.59	33.42
Wang et al. (2018)	99.58	33.43
Proposed	99.59	33.40

REFERENCES

Ahmet, M.E. and Paul, S.F. (1995). Image quality measures and their performance, IEEE Transactions on Communication, Vol. 43, No. 12, pp. 2959-2965.

Chen, G., Mao, Y., and Chui, C.K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons & Fractals, Vol. 21, No. 3, pp. 749-761.

Cover, T.M. and Thomas, J.A. (2006). *Elements of Information Theory*, Wiley-Interscience, New Jersey.

Huynh-Thu, Q. and Ghanbari, M. (2008). Scope of validity of PSNR in image/video quality assessment, Electronics Letters, Vol. 44, No. 13, pp. 800-801.

Khan, M., Masood, F., Alghafis, A., Amin, M., and Naqvi, S.I.B. (2019). A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion, PLoS ONE, Vol. 14, No. 12, pp. 1-23.

Naseer, Y., Shah, D., and Shah, T. (2018). A Novel Approach to improve multimedia security utilizing 3D Mixed Chaotic map, Microprocessors and Microsystems, Vol. 65, pp. 1-6.

Qureshi, A and Shah, T. (2017). S-box on subgroup of Galois field based on linear fractional transformation, Electronics Letters, Vol. 53, No. 9, pp. 604-606.

Scharinger, J. (1998). *Secure and fast encryption using chaotic kolmogorov flows*. Information Theory Workshop, Killarney, pp. 124-125.

Shah, D., Shah, T., and Jamal, S.S. (2019). Digital audio signals encryption by Mobius transformation and Hénon map, Multimedia Systems, Vol. 26, pp. 235-245.

Shannon, C.E. (1948) A Mathematical Theory of Communication, Bell System Technical Journal, Vol. 27, No. 3, pp. 379-423.

Wang, Z. (2002). A Universal Image Quality Index, IEEE Signal Processing Letters, Vol. 9, No. 3, pp. 81-84.

Wang, Z., Bovik, A.C., Sheikh, H.R., and Simoncelli, E.P. (2004). Image quality assessment: From error visibility to structural similarity, IEEE Transactions on Image Processing, Vol. 13, No. 4, pp. 600-612

Wang, X., Zhu, X., and Zhang, Y. (2018). An image encryption algorithm based on Josephus traversing and mixed chaotic map, IEEE Access, Vol. 6, pp. 23733-23746.

Wu, Y., Noonan, J.P., and Again, S. (2011). NPCR and UACI randomness tests for image encryption, Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), pp. 31-38.

Ye, G., Jiao, K., Pan, C., and Huang, X. (2018). An effective framework for chaotic image encryption based on 3D logistic map, Security and Communication Networks, DOI: 10.1155/2018/8402578, pp. 1-11.