Color Image Encryption Scheme Based on Key Dependent S-box and Arnold's Cat Map

Supriyo D E
Dept. of ECE, Techno Engineering College
Banipur, West Bengal-743233, India

Nilankar Bhanja
Dept. of ECE, Techno Engineering College
Banipur, West Bengal-743233, India

Sanjib Kumar Dhara
Dept. of ECE, Techno Engineering College
Banipur, West Bengal-743233, India

Sourav Paul
Dept. of ECE, Techno Engineering College
Banipur, West Bengal-743233, India

Sanchita Das
Dept. of ECE, Techno Engineering College
Banipur, West Bengal-743233, India

***Abstract*— Chaos-based image encryption technique has explored a new era of multimedia data security over the last decade. In this paper, logistic map based key dependent a new substitution box (S-box) has been introduced. Further, the designed S-box is employed for key expansion. On the other hand, Arnold's Cat map is used for performing the image permutation process. Next, the key diffusion technique has been carried out by executing the exclusive-OR operation in between permuted image and expanded key. Several relevant cryptanalyses such as key space, differential attack, key sensitivity, histogram, correlation, entropy have been tested for the validation of the proposed scheme. Further, the performance of the proposed scheme is compared with the different related existing schemes for established the effectiveness of the proposed algorithm.**

Keywords*— *Image Encryption; Arnold's Cat map; Logistic Map; S-box; Cryptanalysis

I. INTRODUCTION

Nowadays, multimedia data plays a vital role in the modern communication system. Digital image security is one of the major issues while it is stored in the cloud or transmitted through an insecure network. Image encryption is an efficient process for the confidentiality of visual information. However, highly correlated data make the process challenging for real-time implementation. There exist several well-established data encryption techniques such as DES, IDEA, 3DES, AES, etc. But, these are not suitable for image encryption. The prime constraints of image encryption are its large volume and high correlation.

In the recent trends of image encryption, researchers are developed different image encryption schemes using cellular automata [1][2], genetic algorithm, chaos [3]-[6], etc. The non-linear and dynamic nature of different chaotic maps explores a new scope of research for image encryption.

In [3], Pareek et al. have proposed an image encryption scheme using the logistic map. The said scheme used an external 80-bit key which was further derived to set the initial condition of the logistic map. The scheme did not have enough key space to prevent the brute force attack. On the other hand, multidimensional chaotic maps have been incorporated to design an image encryption scheme in [4]. The scheme has employed Arnold's Cat map for getting the scrambled image. Thereafter, image encryption has been performed by Rossler Chaotic Map. In Zhang et. al's scheme [5], the authors are reported a chaotic image encryption algorithm based on circular substitution box and key stream buffer. The scheme has employed the logistic map and piecewise linear chaotic map to produce random numbers. Image encryption based on a modified Henon map using hybrid chaotic shift transform has been found in [6]. In spite of having good performance in different analyses the encryption/ decryption speed of the said scheme is slower than the other related existing schemes.

In this paper, we have implemented image permutation and substitution technique for image encryption. The image permutation technique has been designed using Arnold's Cat map. Next, we have employed the logistic map to generate a key dependent S-box for key expansion. Finally, the encrypted image has been obtained by performing the exclusive-OR operation in between the expanded key and the permuted image. Moreover, the proposed algorithm is assessed through various security analyses.

Rest of the paper is organized as follows: Section 2 elaborates the proposed image encryption scheme. Experimental results and different security analyses along with comparative studies have been presented in Section 3. Finally, the paper is concluded in Section 4.

II. PROPOSED SCHEME

The proposed image encryption scheme has associated with two phases: Key expansion and image encryption. The key expansion technique newly introduces key dependent dynamic substitution box (S-box). On the other hand, in the image encryption phase, Arnold's cat map and exclusive-OR operation have been incorporated for permutation and substitution operation respectively. Overall block diagram for the proposed scheme has been presented in Fig. 1.

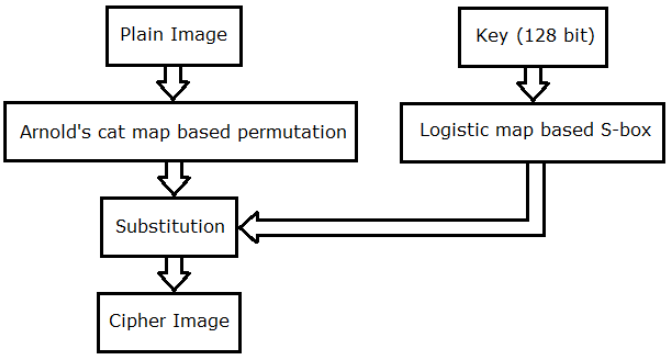


Figure 1 Block diagram for the image encryption scheme

A. Key expansion

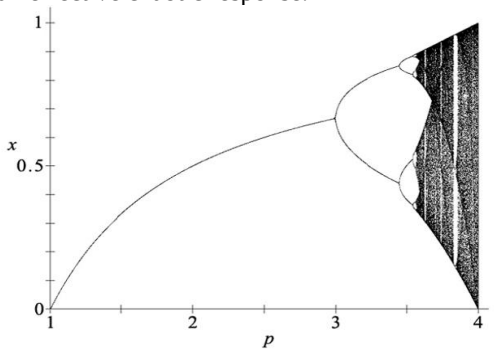
The key expansion technique consists of logistic map based dynamic S-box. Here, a brief on the logistic map has been presented.

1) Logistic map: The logistic map is one of the most well-known chaotic models in the field of nonlinear dynamics. Mathematically it can be written as follows

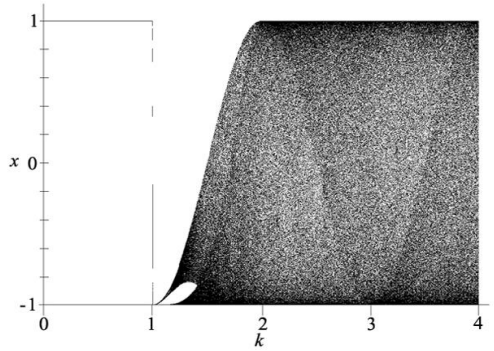
$$x_{n+1} = rx_n(1 - x_n) \quad (1)$$

where the *r* is controlling parameter

The bifurcation diagram and Lyapunov Exponent (LE) of the logistic map have been depicted in Fig. 2(a) and (b) respectively. From the above observation, it can be concluded that the logistic map shows sensitive chaotic nature for r ≈ 4. In this paper, we have considered the value of r = 3.999 for getting an effective chaotic response.



(a)



(b)

Figure 2 (a) Bifurcation diagram and (b) Lyapunov Exponent (LE) of the logistic map

2) S-box: The scheme accepts the 128-bit key i.e. (4 × 4) bytes key for the encryption process as shown in Fig. 3.

00H	01H	02H	03H
04H	05H	06H	07H
08H	09H	0AH	0BH
0CH	0DH	0EH	0FH

Figure 3 128-bit sample key (*key*)

Here, the initial value (x_1) of the logistic map is set by the following operation

$$x_1 = \left(\sum_{i=1}^{4} \sum_{j=1}^{4} key_{i,j} \ mod\ 256 \right) \Big/ 255 \quad (2)$$

Next, the obtained x_1 is used in eq. (1) for generating the chaotic sequence. In this context, we have discarded few initial values for further consideration to avoid the inertia of the chaotic map. Furthermore, the scheme has dynamically chosen the starting position (pos) of the generated sequence (x).

$$pos = \left(\sum_{i=1}^{4} \sum_{j=1}^{4} key^2{}_{i,j} \ mod\ l \right) \quad (3)$$

where l is the length of x

Thereafter, 256 consecutive sequences have been selected for generating the S-box as follows

```
if(pos>255)
    y=x(pos-255:pos);
else
    y=x(pos:pos+255);
end if
```

(4)

Next, the obtained data has been mapped to its equivalent 8-bit unsigned integer by using the eq. (5).

$$\boldsymbol{Y} = \boldsymbol{y} \times 256 \quad (5)$$

Finally, ***Y*** vector is rearranged in (16×16) matrix as S-box.

3) Key generation: In this section, using the input key (key) and S-box a complete key (completekey) set for image encryption has been generated as per the dimension of the plain image. The Key generation has been performed as follows

```
for k = 1:plane
 for j = 1:N/4
  for i = 1:M/4
   key1 = subByte(key);
   completekey((i-1)×4+1:i×4,(j-1)×4+1:j×4,k)=key1^6 mod 256;
   key = key⊕key1;
  end
 end
end
```

(6)

where (M × N × plane) is the dimension of plain image and subByte() is used to substitute the each byte from S-box

B. Image encryption

In this phase, initially, confusion operation has been performed by implementing the permutation operation. The positional displacement of consecutive pixels has been carried out using the Arnold's Cat map.

1) Arnold's Cat map: It is a linear transformation to shift the position of the matrix elements. It is computed as follows

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\ N = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\ N \quad (7)$$

where $(N \times N)$ is the size of the image, p and q are positive integer and $det(A) = 1$, (x_n, y_n) is the position of samples in the $(N \times N)$ data such as image, so that $(x_n, y_n) \in \{0,1,2 \dots\dots, N-1\}$

In the context of image permutation, Arnold's Cat map has been applied to the plain image (P) for several number of iteration (<Arnold's period). Finally, exclusive-OR operation has been performed in between the permuted image (PI) and

the expanded key (completekey) for obtaining the cipher image (CI) as shown below.

$$CI = PI \oplus completekey \quad (8)$$

III. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

The simulation results of the proposed scheme are demonstrated here. Different sample images from the database of images namely, STARE Image Database [7], UCID Image Database [8], and The USC-SIPI Image Database [9] are used to verify the performance of the proposed scheme. All the work being done by software Matlab 7.1. The computational platform is Windows 7 with CPU INTEL CORE I3 at 1.7 GHz and RAM 4.00 GB.

A. Encryption and decryption tests

The performance of the proposed scheme has been tested by several images. The encryption-decryption outcomes of selected well-known images are shown in Fig. 4. Here, Fig. 4 (d)-(f), Fig. 4 (g)-(i), and Fig. 4 (j)-(l) present the permuted images, cipher images, and deciphered images respectively for the plain images shown in Fig. (a)-(c). From the visual analysis, it is observed that the obtained cipher images appear as noisy images.

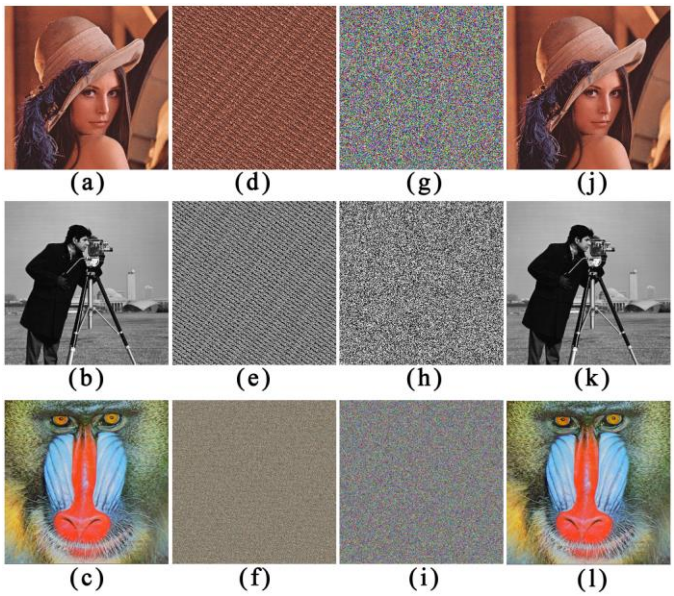


Figure 4 Plain image (a) Lena (b) Cameraman (c) Mandrill; Permuted image of (d) Lena (e) Cameraman (f) Mandrill; Cipher image of (g) Lena (h) Cameraman (i) Mandrill; Decipher image of (j) Lena (k) Cameraman (l) Mandrill;

B. Key space analysis

A good encryption scheme should have a large key space to protect the brute force attack. The proposed scheme has employed 128-bit key. It contains 2^{128} different key combinations. So, the proposed scheme ensures a sufficiently large key space ($> 2^{104}$) to prevent the brute force attack [10] [11].

C. Resistance against differential attack

Differential attack is one of the essential properties of a cryptosystem. In this context, we have examined the proposed scheme in terms of plain text sensitivity. Here, the performance of the scheme has been measured by computing the number of pixel change rate (NPCR) and the unified average changing intensity (UACI) [12]. The average of the obtained NPCR and UACI values are compared with the Kulkarni et al's scheme [4]. The comparative outcomes are presented in Table 1.

TABLE I. PLAINTEXT SENSITIVITY ANALYSIS

Test item	NPCR(%)		UACI(%)	
	Ref. [4]	*Proposed scheme*	*Ref. [4]*	*Proposed scheme*
Average Score	0.7782%	99.356%	0.1375%	32.9451%

D. Key sensitivity

The key sensitivity of a cryptosystem can be measured in between two cipher images obtained from the minimum change (1-bit) in key. This investigation has been carried out by measuring the NPCR and UACI from the relative two cipher images. The proposed scheme has ensured a good key sensitivity and the obtained results are shown in Table 2. In addition, Sheela et al. [6] have shown the average NPCR and UACI values 99.533% and 32.784% respectively for key sensitivity. Moreover, the proposed scheme is unable to extract any visual information from the cipher images if slight alteration (1-bit) has appeared in the key for decryption process. It implies that the proposed scheme has a good key dependency in terms of data confidentiality.

TABLE II. KEY SENSITIVITY ANALYSIS

Test item	NPCR(%)	UACI(%)
Lena	99.6225%	33.4044%
Cameraman	99.6116%	33.3598%
Mandrill	99.6023%	33.5411%

E. Histogram analysis

A good image encryption scheme should always provide a cipher image with a uniform histogram distribution for any plain images. We have analyzed the histograms of several encrypted images for the proposed algorithm. The obtained outcomes are depicted in Fig. 5.

F. Correlation analysis

Digital image is highly correlated with its adjacent pixels. A good cryptosystem should break this strong correlation by implying the encryption technique. In this context, the proposed scheme has ensured a good performance and the obtained results are furnished and compared with the related existing schemes in Table 3. Further, Fig. 6 presents the correlation distributions of the plain image and cipher image of Lena.

TABLE III. CORRELATION ANALYSIS

Test item	Correlation	Lena	Cameraman	Mandrill
Ref. [5]	HC	0.0017	0.0029	-
	VC	-0.0022	-0.0012	-
	DC	0.0009	0.0005	-
Ref. [4]	HC	-0.0374	-0.007	-
	VC	-0.0152	-0.0082	-
	DC	-0.0042	0.0174	-
Proposed	HC	0.0026	0.0027	0.0018

scheme	VC	0.0022	0.0009	0.0001
	DC	-0.0008	-0.0007	0.0003

Where HC: Horizontal Correlation, VC: Vertical Correlation, DC: Diagonal Correlation

G. *Entropy test*

It is a measuring tool to determine the degree of randomness of a data sequence. An ideal 8-bit random data sequence should achieve the entropy value 8. The performance of the proposed scheme has been evaluated by measuring the entropy of several cipher images. The obtained outcomes are furnished in Table 4. Further, the secured results are compared with Zhang et al.'s scheme [5] and Sheela et al.'s scheme [6].

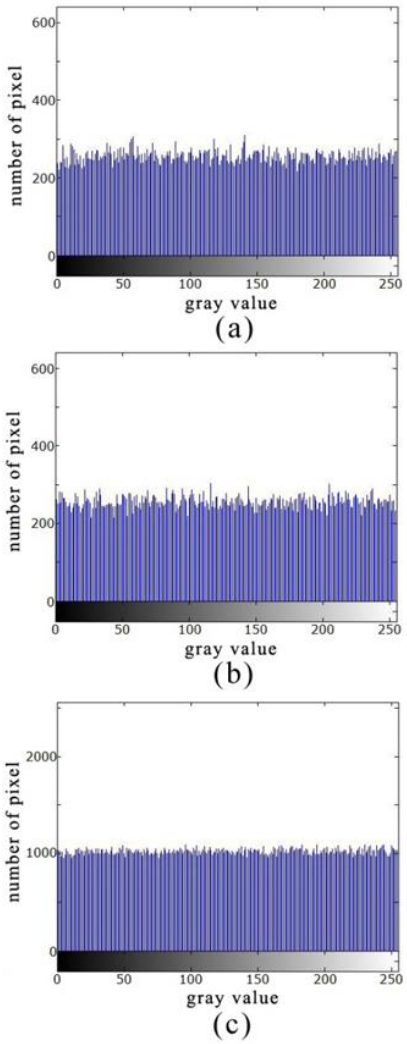


Figure 5 Histogram of cipher image (a) Lena (b) Cameraman (c) Mandrill

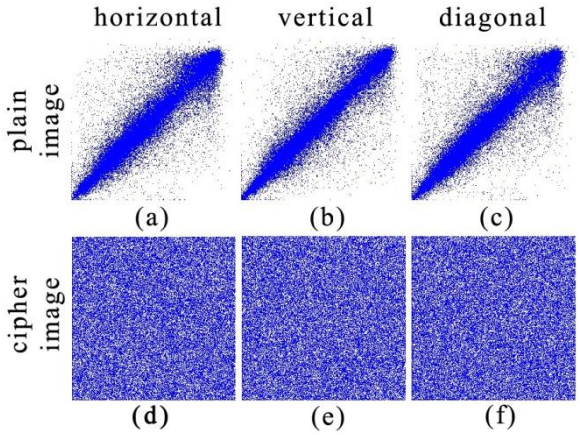


Figure 6 Correlation distribution of Lena plain image for (a) horizontal direction (b) vertical direction (c) diagonal direction; Correlation distribution of Lena cipher image for (d) horizontal direction (e) vertical direction (f) diagonal direction

TABLE IV. ENTROPY ANALYSIS

Test item	**Entropy**		
	Ref. [5]	***Ref. [6]***	***Proposed scheme***
Lena	7.9137	7.9990	7.9990
Cameraman	7.9103	7.9990	7.9989
Mandrill	-	7.9990	7.9997

H. *PSNR analysis*

Peak Signal to Noise Ratio (PSNR) has been determined for the cipher image with respect to plain image for ensuring the data loss at the cipher end of the proposed scheme. A good cryptosystem should have a low PSNR value (<10dB) for its cipher images. In this context, the obtained results presented in Table 5 show the effectiveness of the proposed scheme.

TABLE V. PSNR ANALYSIS

Test item	**PSNR (dB)**	
	Ref. [6]	***Proposed scheme***
Lena	9.2335	8.3948
Cameraman	8.3497	8.3551
Mandrill	9.7271	8.8060

I. *Timing analysis*

The processing speed of the proposed image encryption scheme has been tested under the previously mentioned hardware and software interface. The average encryption and decryption time taken by the proposed cryptosystem for the plain image of size (256 × 256) is 19.30441 s and 8.450054 s respectively.

IV. CONCLUSION

In this paper, a chaos based image encryption scheme has been proposed. Here, the newly introduced key expansion technique enhances the performance of the overall encryption process. As a result, the scheme achieves a good score in the key sensitivity analysis. The proposed algorithm also provides good responses against different security analyses. In comparative studies, the scheme shows good performance with respect to Kulkarni et al.'s scheme [4], Zhang et al.'s

scheme [5], and Sheela et al.'s scheme [6]. In future, we may also improve the performance of this work more on plaintext sensitivity by incorporating new techniques in the image permutation process. The efficiency in encryption/ decryption time can be improved further by implementing the algorithm optimization technique.

REFERENCES

[1] S. De and J. Bhaumik, "TBLT-AES: A Robust Image Encryption Scheme," Journal of Discrete Mathematical Sciences & Cryptography, vol. 17, no. 3, pp. 273-288, 2014

[2] J. Bahumik and S. De, "A Symmetric Key-Based Image Encryption Scheme," Proceedings of the International Conference on Computing and Communication Systems, Lecture Notes in Networks and Systems 24, pp. 663-672, Springer Nature Singapore Pte Ltd. 2018

[3] N. K. Pareek, Vinod Patidar and K.K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, vol. 24, no. 9, pp. 926-934, 2006

[4] N. S. Kulkarni, B. Raman and I. Gupta, "Image Encryption based on Multidimensional Chaotic Maps," International Journal of Information Processing, vol. 2, no. 4, pp. 29-40, 2008

[5] 1X. Zhang, Z. Zhao and J. Wang, "Chaotic image encryption based on circular substitution box and key stream buffer," Signal Processing: Image Communication, vol. 29, no. 8, pp. 902-913, 2014

[6] S. J. Sheela, K. V. Suresh and D. Tandur, "Image encryption based on modified Henon map using hybrid chaotic shift transform," Multimed Tools Appl., vol. 77, pp. 25223–25251, 2018

[7] University of California, San Diego, "STARE Image Database", https://cecas.clemson.edu/ ahoover/stare, Accessed 02 May 2018

[8] Nottingham Trent University, UK, "UCID Image Database", http://jasoncantarella.com/downloads/ucid.v2.tar.gz, Accessed 02 May 2018

[9] University of Southern California, "The USC-SIPI Image Database", http://sipi.usc.edu/database/database.php, Accessed 02 May 2018

[10] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129-2151, 2006

[11] D. Stinson, "Cryptography: Theory and Practice," Second ed. CRC/C&H, 2002

[12] Y. Wu, J. P. Noonan and S. Agaian, "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, 2011

AUTHORS

Supriyo De is currently working as an Assistant Professor in the Department of Electronics and Communication Engineering, Techno Engineering College Banipur, WB, India. He received his B. Tech. and M. Tech. degrees in Electronics and Communication Engineering from Maulana Abul Kalam Azad University of Technology, West Bengal (Formerly known as West Bengal University of Technology) in 2006 and 2009 respectively. His research interests include Digital Signal Processing, Cryptography, and Digital Image Processing.

Nilankar Bhanja is currently working as an Assistant Professor in the Department of Electronics and Communication Engineering, Techno Engineering College Banipur, WB, India. He received his B. Tech. degree in Electronics and Communication Engineering from Maulana Abul Kalam Azad University of Technology, West Bengal (Formerly known as West Bengal University of Technology) in 2005. He also achieved his M. Tech degree in Mechatronics from IIEST, formerly known as Bengal Engineering and Science University (BESU) in 2009. His research interests include Machine learning, Robotics, and Artificial intelligence.

Sanjib Kumar Dhara is currently working as an Assistant Professor in the Department of Electronics and Communication Engineering, Techno Engineering College Banipur, WB, India. He received his M.Sc. degree in Electronics from Vidyasagar University, West Bengal in 2003. He also achieved his M.Tech degree in Matrials Engineering from IIEST, formerly known as Bengal Engineering and Science University (BESU) in 2010. His research interests include Intelligent Systems Approach, Microcontroller based system design, and Machine learning.

Sourav Paul is currently pursuing his B.Tech degree in the Department of Electronics and Communication Engineering, Techno Engineering College Banipur, WB, India. His research interests include Machine learning, Robotics, Signal Processing, and Artificial intelligence.

Sanchita Das is currently pursuing her B.Tech degree in the Department of Electronics and Communication Engineering, Techno Engineering College Banipur, WB, India. Her research interests include Machine learning, Robotics, Signal Processing, and Artificial intelligence.