IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Design and Analysis of a Permutation Strategy using 3D Chaotic Map

K. Panwar[1*], R.K. Purwar[2]

[1,2]USICT, GGSIP University, New Delhi, India

[*]*Corresponding Author: kirtee.usict.900090@ipu.ac.in.*

DOI: https://doi.org/10.26438/ijcse/v7i6.295299 | Available online at: www.ijcseonline.org

Accepted: 12/Jun/2019, Published: 30/Jun/2019

Abstract— In Image encryption scheme, the permutation operation plays an important role in confusing the pixels of image and is used in combination with diffusion operation. This paper proposes an efficient 3D permutation strategy for color image that is free from sorting operation and is based on Lorenz map. It has good confusion properties than permutation algorithms that do not involve sorting operation and in comparison to permutation algorithms with similar security that involves use of sorting operation, the proposed method has lower complexity. Performance and Security of proposed permutation algorithm are analysed and results further justify that the permutation scheme is secure is computationally efficient for application in image encryption scheme.

Keywords—Image Scrambling, 3D Lorenz system, Random number generator, Encryption, Complexity.

I. Introduction

Advancement of technology has led to security threats concerning multimedia data and image encryption is one way of securing image data [1], [2]. The various challenges faced for development of secure image encryption schemes are reduction in correlation among pixels, proper diffusion operations to obtain uniform histograms, security against various plaintext attacks, etc. Secondly, image encryption process must be sensitive to secret keys as well as plain image. Another issue is that the steps involved in encryption scheme must be highly related with one another. Since image data is huge, the encryption scheme must be secure and computationally efficient.

Image encryption schemes are made sensitive to secret keys with the help of chaotic maps [3], [4], [5] as chaotic sequences are sensitive to initial conditions and good diffusion and confusion strength is achieved with mixing property of chaotic maps [6]. However, in most of the cryptanalytic works [7], [8] the encryption scheme is broken by disintegrating the confusion and diffusion steps involved [9], [10].

These chaotic sequences provide pseudo-random integer sequences or real number sequences [11], [12] for diffusion and confusion operations. While choosing a chaotic map for image encryption, the properties of chaotic maps also needs to be considered, based on which the structure of encryption scheme may become vulnerable [13], [14].

In image encryption schemes permutation process is an integral part of encryption and also one of the most time consuming process due to the sorting operation which is performed on chaotic sequences to obtain permutation position [15], [16]. A new approach for permutation is suggested in this paper which is more secure and efficient. The permutation is performed using chaotic sequences generated from 3D Lorenz system in an efficient way by swapping the pixels for better confusion properties of permutation mechanism.

Following content of this paper is organised as follows. Section II discusses chaotic properties of Lorenz map using this map random number generation procedure is given in section III. The proposed permutation strategy using pseudo-random number generator is discussed in section IV followed by analysis of its security and performance section VI. This paper is finally concluded in section VII.

II. Lorenz System

The chaotic system used for generating random numbers is obtained by solving Lorenz system [17], which is defined as

$$f\colon \begin{cases} \dot{x} = a(y-x) \\ \dot{y} = bx - y - xz \\ \dot{z} = xy - cz, \end{cases} \qquad (1)$$

by fourth order Runga-Kutta method. The states of the system used for generating chaotic sequences lie in the interval $0 \le x \le 20$, $0 \le y \le 50$, $-50 \le z \le 50$ as the system is symmetric along z axis [18]. The chaotic parameters for Lorenz system are $a = 10$, $b = 28$ and $c = \frac{8}{3}$. Using these parameters, 3 chaotic sequences are obtained. There may exist short period cycles in these chaotic sequences due to finite computer precision [19] but these sequences can be effectively used for the proposed permutation strategy given in the following section.

III. RANDOM NUMBER GENERATION FOR PERMUTATION OF PIXELS

With Lorenz system given in section II, three chaotic sequences of real numbers $X = \{x_i\}_{i=1}^{L+k}$, $Y = \{y_i\}_{i=1}^{L+k}$ and $Z = \{z_i\}_{i=1}^{L+k}$ are generated where L represents size of plain image. First k elements in each sequence is discarded to avoid recovering of control parameters of chaotic map [20]. From three sequences of real numbers three integer sequences are obtained as

$$\begin{cases} \overline{X(\imath)} = \text{mod}(\text{floor}((|x(i)|*10^{14} - \text{Fix}(|x(i)|)*10^{14})),256) \\ \overline{Y(\imath)} = \text{mod}(\text{floor}((|y(i)|*10^{14} - \text{Fix}(|y(i)|)*10^{14})),256) \\ \overline{Z(\imath)} = \text{mod}(\text{floor}((|z(i)|*10^{14} - \text{Fix}(|z(i)|))*10^{14})),256) \end{cases}$$
(2)

The structure of real number sequences generated by (2) can be observed with State Map Network (SMN) [21]. For chaotic map $f: [0,1] \to [0,1]$ iterated using computing precision domain of 2 bits, a relation exist from node $(\mathrm{i}, \mathrm{j}, \mathrm{k})$ to node $(\mathrm{i}', \mathrm{j}', \mathrm{k}')$ if $f\left(\frac{i}{2^2}, \frac{j}{2^2}, \frac{k}{2^2}\right) = (\frac{i\prime}{2^2}, \frac{j\prime}{2^2}, \frac{k\prime}{2^2})$. Some of the periodic series nodes $(x_0, x_1, \ldots, x_{repeated})$ of Lorenz system observed in 2 bit precision domain are listed in Table 1. x_0 denotes seed node and $x_{repeated}$ denotes the repeated node.

Table 1. Lorenz Map series for 2-bit computing precision domain

Seed Node (x_0)	**Sequence Nodes ($x_0, x_1, \ldots, x_{repeated}$)**
(1,1,1)	(1,1,1), (0,2,0), (3,1,2), (3,0,2), (2,2,3), (4,3,2), (3,3,3), (0,4,2), (2,1,3), (3,1,2)
(0,0,1)	(0,0,1), (0,0,4)
(0,0,2)	(0,0,2), (0,0,4)
(1,1,2)	(1,1,2), (4,3,2), (3,3,3), (0,4,2), (2,1,3), (3,1,2), (3,0,2), (2,2,3), (4,3,2)

A similar structure will exist for Lorenz map at higher precision domain. Through this structure, the periodic nature of chaotic sequence is analysed based on which random number generation of integer sequences is improved. If two or three consecutive positions occur in the permutation sequence then the integer sequences will also repeat, due to which a series of pixels will be shifted from one position to some other position but in same order. Therefore, in order to enhance security, the integer sequences from the point of repetition are updated again by iterating chaotic sequences. The initial conditions for re-iterating the chaotic sequences are defined by adding secret keys of Lorenz map with last output from real number sequences. The obtained integer sequence is appended to the previously obtained sequence.

IV. PERMUTATION STRATEGY USING LORENZ SYSTEM

A strategy for scrambling pixels of plain image is proposed in this section, which can be used in image encryption schemes along with diffusion operation to provide fast and secure image encryption schemes. In generating permutation sequence the integer sequences are used to obtain three matrices to specify location of each pixel with which current pixel can be swapped. Also, for secure image scrambling scheme, the secret keys can be updated using SHA-2 hash function before encryption as in [22]. By making encryption scheme sensitive towards changes in plaintext the image scrambling scheme is secure from known/chosen plaintext attacks.

1) Generate random integer sequence $\bar{X} = \{\bar{x}_i\}_{i=1}^{L}$, $\bar{Y} = \{\bar{y}_i\}_{i=1}^{L}$ and $\bar{Z} = \{\bar{z}_i\}_{i=1}^{L}$ as in (2). Sequence $\bar{X}$ and $\bar{Y}$ specifies position of pixel to be swapped and sequence $\bar{Z}$ specifies one of the three RGB components.

2) Obtain matrix Mr, Mg and Mb of size $W \times H$ each. Starting from first position the process continues, pixel from current position is moved to another location determined by Lorenz system as

$$Mr(i,j)_k = \begin{cases} R(\overline{x_\imath}, \overline{y_\imath}) \ \ if\ \overline{z_k} = 1, \\ G(\overline{x_\imath}, \overline{y_\jmath}) \ \ if\ \overline{z_k} = 2, \\ B(\overline{x_\imath}, \overline{y_\jmath)} \ \ if\ \overline{z_k} = 3. \end{cases} \quad (3)$$

and the pixel at position determined by Lorenz system is moved to current position as

$$⍰ \quad \begin{cases} Mr(\overline{x_\imath}, \overline{y_\imath})_k = R(i,j) \ \text{ if}\ \overline{z_k} = 1, \\ Mg(\overline{x_\imath}, \overline{y_\jmath})_k = G(i,j) \ \text{ if}\ \overline{z_k} = 2, \\ Mb(\overline{x_\imath}, \overline{y_\jmath)}_k = B(i,j) \ \text{ if}\ \overline{z_k} = 3, \end{cases} \quad (4)$$

where $k = 1,2, \ldots, (W \times H)$, value of $\bar{x}_i$ is used to identify particular row in plain image I, $\overline{y_\jmath}$ is used to identify particular column in plain image and $\overline{z_k}$ identifies RGB components of color image. The pixel at position (i, j, k) is swapped with pixel at position $(\bar{x}_i, \bar{y}_j, \bar{z}_k)$. The first pixel in plain image is swapped with a specific pixel defined by integer sequences, and next pixel is swapped with next pixel specified by the same and so on as shown in Fig. 1.

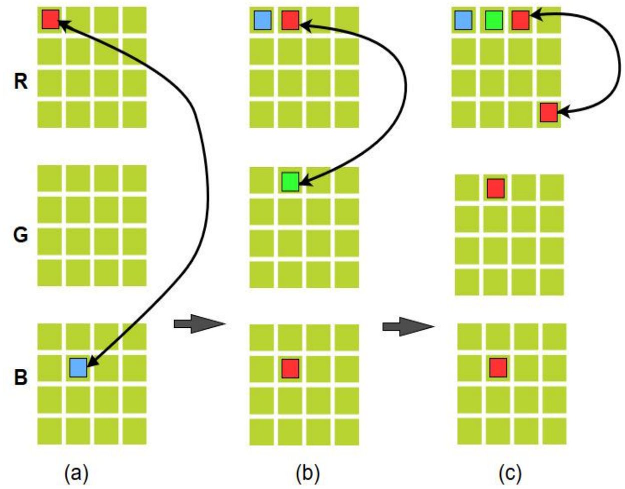

Figure 1. Permutation strategy: (a) First pixel is swapped with a specific pixel of blue component which is defined by integer sequences; (b) Second pixel is swapped with another pixel whose position is given by next value in each of the three integer sequences; (c) Third pixel is swapped with pixel whose position in given by next value in the integer sequences.

V. Analysis of Performance and Security Features

In this section, effectiveness of proposed permutation strategy is analysed. The proposed permutation strategy must be used along with secure diffusion operation for image encryption scheme. The test image has been taken from USC-SIPI "miscellaneous" dataset. The initial parameters of Lorenz chaotic map used for encryption are ($x_0 = 1.2, y_0 = 0.99749, z_0 = 1$). The experiments are performed using Matlab 2019a on PC with 3.2 GHz CPU and 8G RAM.

A. Encryption Results

For initial conditions that may lead to short period cycles [23], the proposed permutation strategy would cause swapping of pixels at different locations with different values which gives good confusion strength to encryption scheme. The proposed permutation can be compared to permutation using 3D Cat Map. The permuted image obtained using Lorenz system in one round of iteration is more confused than permuted image obtained using 3D chaotic cat map in one round of iteration which is performed according to (5) in [6] as

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = A \begin{pmatrix} x \\ y \\ z \end{pmatrix} \qquad (5)$$

where,

$$A = \begin{matrix} 1 + a_x b_z b_y & a_z & a_z + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x \\ a_x b_x b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{matrix}$$

and (x, y, z) are current pixel position in plain image and $(x^{'}, y^{'}, z')$ is the new calculated position to which the pixel is placed. The results of permutation using proposed strategy and traditional cat map are shown in Fig. 2. The visual information in Fig. 2(f) indicates that more rounds of permutation are needed with 3D cat map whereas no such information is revealed in Fig. 2(b).Therefore, it can be justified that the proposed permutation strategy is more secure.

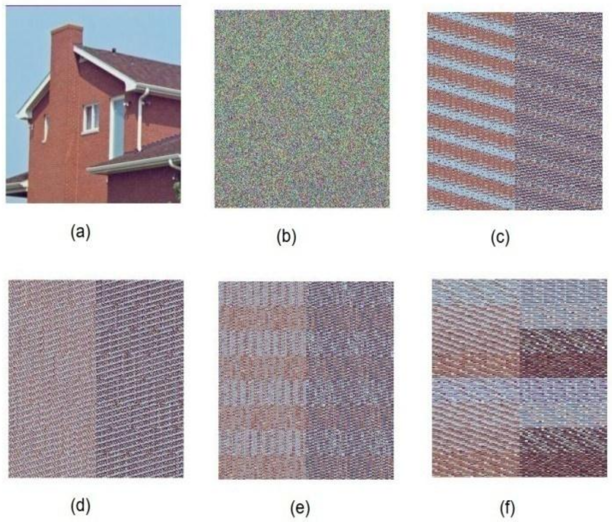

Figure 2. Permutation results: (a) Plain Image; (b) Image Permuted using proposed strategy; (c) Image permuted using 3D cat map after

one permutation round; (d) Image permuted using 3D cat map after 2 rounds of permutation; (e) Image permuted using 3D cat map after 3 rounds of permutation; (f) Image permuted using 3D cat map after 6 rounds of permutation.

B. Correlation Distribution of Adjacent Pixels

To justify the effect of proposed permutation strategy, adjacent pixel distribution is plotted and compared with plain image as well as 3D cat map based permutation. Adjacent pixel correlation of image is calculated as in [24] as

$$r_{a,b} = \frac{cov(a,b)}{\sqrt{D(a)D(b)}},$$

Where, $cov(a,b) = \frac{1}{n}\sum_{i=1}^{N}(a_i - E(a_i))\big(b_i - E(b_i)\big)$, $E(a) = \frac{1}{n}\sum_{i=1}^{N} a_i$, $D(a) = \frac{1}{n}\sum_{i=1}^{N}(a_i - E(a_i))^2$, a & b are gray scale values of two adjacent pixels in image, $E(a)$ denotes expectation of a, $D(a)$ denotes variance and n represents the total number of samples.

Scrambling image pixels with 3D cat map is compared with the proposed strategy for one round of encryption. Correlation distribution of plain image and encrypted image is shown in Fig. 3.

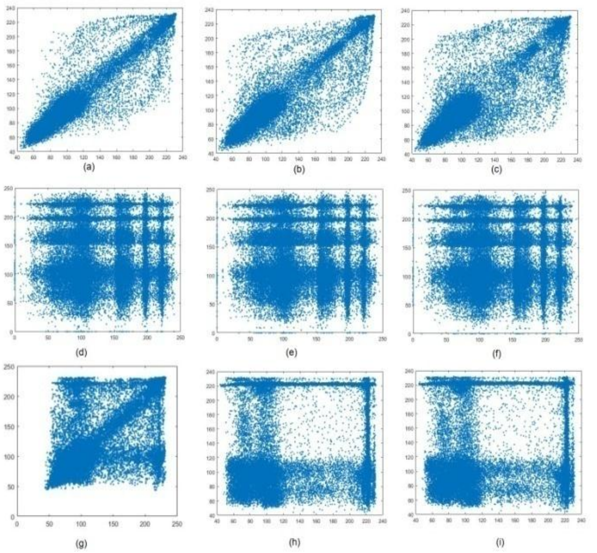

Figure 3. Adjacent pixel correlation distribution of plain and permuted images: (a) Plain Image- horizontal correlation; (b) Plain Image- vertical correlation; (c) Plain Image - diagonal correlation; (d) Horizontal correlation of permuted image (using proposed strategy); (e) Vertical correlation of permuted image (using proposed strategy); (f) Diagonal correlation of permuted image (using proposed strategy); (g) Horizontal correlation of permuted image (using 3D cat map); (h) Vertical correlation of permuted image (using 3D cat map); (i) Diagonal correlation of permuted image (using 3D cat map)

Fig. 3(d)-(f) indicates that adjacent pixel correlation among pixels have been reduced with proposed scheme as compared to distribution shown in Fig. 3(g)-(i). The distribution in Fig. 3 justifies the effectiveness of proposed scheme as compared to original image as well as permuted image obtained using 3D cat map.

C. Complexity

The proposed permutation sequence is generated by transforming the sequence of real numbers to sequence of integer numbers which makes it faster than traditional permutation sequences [3], [6], [13], [19] which are generated by sorting the sequence of real numbers and complexity of sorting a sequence of numbers is $\mathrm{O}(n\log n)$. The complexity of generating proposed permutation sequence is $\mathrm{O}(n)$. Also, if image scrambling is performed using 3D cat map, number of iterations round is more and for proposed scheme required results can be obtained in simply one round of encryption. Therefore, for fast encryption the proposed permutation strategy must be used.

VI. CONCLUSION

A new image scrambling scheme for color image is proposed in this paper. The image scrambling scheme is capable of providing enhanced security for image encryption when used in combination with appropriate diffusion operation. The proposed scheme effectively reduces adjacent pixel correlation in plain image in one round of permutation. Secondly, the complexity of permutation operation is reduced as the operation is free from sorting operation. The experimental results further justify the effectiveness of the permutation scheme.

ACKNOWLEDGEMENT

This research work is sponsored by Ministry of Electronics and Information Technology (MeitY), Government of India, under Visvesvaraya PhD Scheme.

REFERENCES

[1] Y. Patil and P. Deshmukh, “A review: Mobile cloud computing: Its challenges and security,” *International Journal of Scientific Research in Network Security and communication*, vol. 6, no. 1, pp. 11–13, 2018.

[2] P. Devi, “Attacks on cloud data: A big security issue,” *International Journal of Scientific Research in Network Security and communication*, vol. 6, no. 2, pp. 15–18, 2018.

[3] L. Chen, S. Tang, Q. Li, and S. Zhong, “A new 4D hyperchaotic system with high complexity,” *Mathematics and Computers in Simulation*, vol. 146, pp. 44–56, 2018.

[4] N. Yujun, W. Xingyuan, W. Mingjun, and Z. Huaguang, “A new hyperchaotic system and its circuit implementation,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 11, pp.3518–3524, 2010.

[5] A. Jain and N. Rajpal, “A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps,” *Multimedia Tools and Applications*, vol. 75, no. 10, pp. 5455–5472, May 2016.

[6] G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[7] K. Wang, L. Zou, A. Song, Z. He et al., “On the security of 3D cat map based symmetric image encryption scheme,” *Physics Letters A*, vol. 343, no. 6, pp. 432–439, 2005.

[8] F.-G. Jeng, W.-L. Huang, and T.-H. Chen, “Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes,” *Signal Processing: Image Communication*, vol. 34, pp. 45–51, 2015.

[9] K. Panwar, R. Purwar, and A. Jain, “Cryptanalysis and improvement of a color image encryption scheme based on DNA sequences and multiple 1D chaotic maps,” *International Journal of Bifurcation and Chaos*, 2019 (in press).

[10] K. Panwar, R. K. Purwar, and A. Jain, “Cryptanalysis of an image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion,” in the proceedings of 2018 *5th International Conference on Signal Processing and Integrated Networks (SPIN), IEEE,* Feb 2018, pp. 236–239.

[11] A. Gerosa, R. Bernardini, and S. Pietri, “A fully integrated chaotic system for the generation of truly random numbers,” *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 49, no. 7, pp. 993–1000, 2002.

[12] L. Kocarev and G. Jakimoski, “Pseudorandom bits generated by chaotic maps*,” IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 50, no. 1, pp. 123–126, 2003.

[13] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, “On the security defects of an image encryption scheme,” *Image and Vision Computing*, vol. 27, no. 9, pp. 1371–1381, 2009.

[14] C. Li, D. Lin, and J. L¨u, “Cryptanalyzing an image-scrambling encryption algorithm of pixel bits,” *IEEE MultiMedia*, vol. 24, no. 3, pp. 64–71, 2017.

[15] Q. Yin and C. Wang, “A new chaotic image encryption scheme using breadth-first search and dynamic diffusion,” *International Journal of Bifurcation and Chaos*, vol. 28, no. 04, p. 1850047, 2018.

[16] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, “An image encryption algorithm based on compound homogeneous hyper-chaotic system,” *Nonlinear Dynamics*, vol. 89, no. 1, pp. 61–79, 2017.

[17] F. O¨ zkaynak and A. B. O¨ zer, “A method for designing strong s-boxes based on chaotic Lorenz system,” *Physics Letters A*, vol. 374, no. 36, pp. 3733–3738, 2010.

[18] M. Moghtadaei and M. H. Golpayegani, “Complex dynamic behaviours of the complex lorenz system*,” Scientia Iranica*, vol. 19, no. 3, pp. 733– 738, 2012.

[19] C. Li, M. Z. Chen, and K.-T. Lo, “Breaking an image encryption algorithm based on chaos,” *International Journal of Bifurcation and Chaos*, vol. 21, no. 07, pp. 2067–2076, 2011.

[20] C. Li, D. Lin, B. Feng, J. L¨u, and F. Hao, “Cryptanalysis of a chaotic image encryption algorithm based on information entropy,” *IEEE Access*, vol. 6, pp. 75 834–75 842, 2018.

[21] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen, “Dynamic analysis of digital chaotic maps via state-mapping networks,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2019.

[22] Z. Li, C. Peng, L. Li, and X. Zhu, “A novel plaintext-related image encryption scheme using hyper-chaotic system,” *Nonlinear Dynamics*, vol. 94, no. 2, pp. 1319–1333, 2018.

[23] Z. Galias and W. Tucker, “Short periodic orbits for the lorenz system,” in the proceedings of 2008 *International Conference on Signals and Electronic Systems*. IEEE, pp. 285–288, 2008.

[24] K. Panwar, R. Purwar, and A. Jain, “Cryptanalysis and improvement of an image encryption scheme using combination of one-dimensional chaotic maps,” *Journal of Electronic Imaging*, vol. 27, no. 5, pp. 1 –18, 2018.

Authors Profile

Kirtee Panwar is a research scholar at USICT, GGSIP University, Delhi, India. She received her M.Tech degree in Applied Computational Mathematics from Jaypee Institute of Information Technology Noida, India. She has pursued B.Tech in Computer Science and Engineering from U.P. Technical University Lucknow, India. Her area of interest is multimedia security, watermarking techniques, cryptography techniques, etc.

R. Purwar has obtained his ME (computer science & engineering) degree from MNREC Allahabad (currently known as MNNIT Allahabad). He has pursued his doctorate from university school of information and communication technology (USICT), GGSIP University, Delhi. He is a life member of Computer Society of India (CSI) and Indian Society of Technical Education (ISTE). He has various publications in peer reviewed quality international journals and conferences. His research interests include image/video processing, pattern recognition, video security and database management.