International Journal of Pure and Applied Mathematics
Volume 119 No. 16 2018, 455-460
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue
http://www.acadpubl.eu/hub/

HENON AND LFSR ASSISTED KEY BASED ENCRYPTION

Santhiya Devi. R, Rajarajeswari.V, Thenmozhi. K, RengarajanAmirtharajan and PadmapriyaPraveenkumar*

Department of ECE, School of EEE, SASTRA Deemed University, Thanjavur, India

*Corresponding author: padmapriya@ece.sastra.edu

Abstract: In present times, the role of multimedia data protection is becoming vital as they are transmitted over a public channel. Data encryption schemes ensure the protection of confidential data from unauthorised access. Recently, many image encryption algorithms have been proposed. In this paper, a new medical image encryption algorithm is proposed which uses Henon map for confusing the image and Linear Feedback Shift Register (LFSR) for diffusion. NPCR, UACI, Correlation are the metrics used for calculating the efficiency of the algorithm.The analysed metric values show that the proposed algorithm can withstand differential attacks. The results demonstrate that the proposed work can provide security for the DICOM images.

Keywords:LFSR, Henon map, NPCR, UACI, Image encryption.

1. Introduction

In today's world information should be secured, as it is subjected to the different type of attacks. In this proposed system the chaotic sequences created by Henon map is used. It depends on only two parameters alpha and beta since it is discrete[1–3]. LFSR will generate random sequence based on the value of the input seed [4–7] though it appears random, it will generate deterministic sequences, the randomness is introduced by the seed [8,9]. The confused image obtained by applying Space filling curve [10]is taken as input for LFSR; then the modified pixel values are further encrypted by XORing with the key generated by Henon map [12]. The method is analysed by calculating metrics values like NPCR, UACI, correlation [11,13].

2.Proposed Methodology

In the proposed methodology Medical image of size 256×256 is considered, and the encryption scheme encrypts it. It includes two phase, (a) Encryption phase and (b) Decryption phase as in Figure 1 (a) and (b).

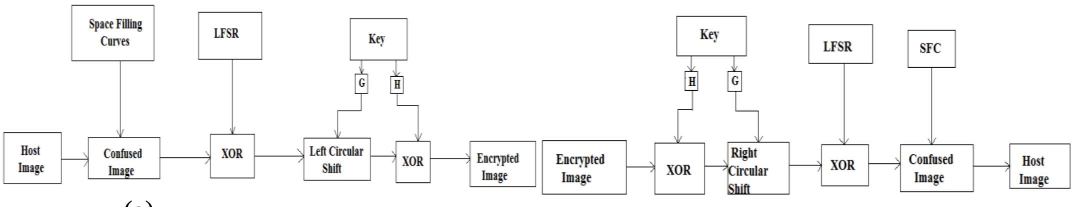
2.1. Encryption Phase

The Encryption phase requires two keys. LFSR is used to generate the first key sequence. The first pixel of the host image is given as input to the LFSR, and the equation x^4+1 gives the tap positions. After each shift, the register content of the LFSR is converted to a decimalvalue, and it is given as key 1. The second key sequence is generated by using the Henon map (1). To be chaotic, this map uses the values x=1.4 and y=0.3,

$$G_{n+1} = 1-xG_n^2+H_n$$

$$H_{n+1}= yG_n \qquad (1)$$

The generated G value is then sorted in ascending order, and the new index value of this is G’ and H’=floor(mod(H×10^{17}),256).



(a)

(b)

Figure 1.Block Diagram of the proposed algorithm: (a) Encryption phase; b) Decryption phase.

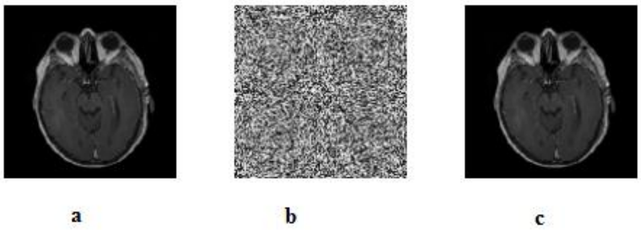


Figure 2. Output of the proposed algorithm:a) Host Image; b) Encrypted Image; c) Decrypted Image.

Step 1: Host image is first confused by using the Space-filling curves.

Step 2: The confused image is then XORed with the key 1 that is generated by the LFSR.

Step 3: Then the image is subjected to left circular shift with the help of sorted G’ value of key 2.

Step 4: The encrypted image is obtained by XOR of the circularly shifted image with H’ of key 2.

2.2. Decryption Phase

Step 1: The Encrypted image is XORed with the H’ Value of the key 2.

Step 2: It is then right shifted circularly with the G’ Value of key 2.

Step 3: The circularly shifted image is XORed with the key 1.

Step 4: To obtain the original image, space-filling curves are applied.

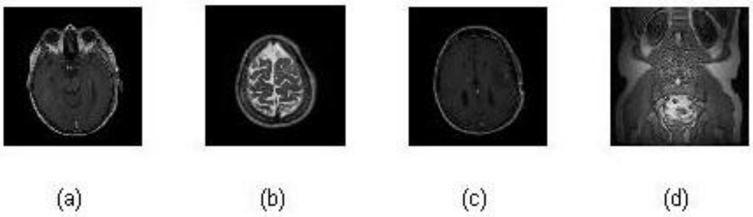
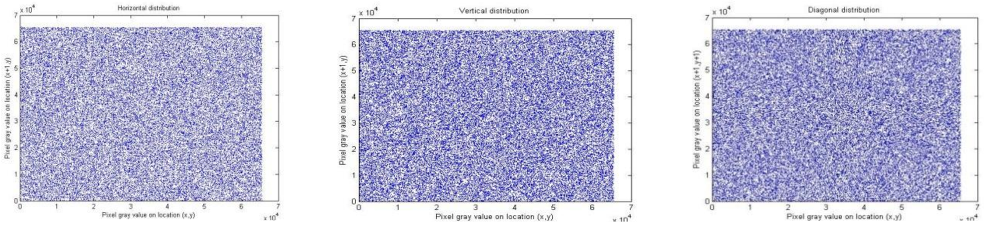


Figure 3. Different test images: (a) test_image 1; (b) test_image 2; (c) test_image 3; (d) test_image 4.

Table 1. Analysed Metrics for different images.

Image	Horizontal Correlation	Vertical Correlation	Diagonal Correlation	NPCR	UACI
Test_image 1	0.0015	-0.0014	0.0245	99.732	32.417
Test_image2	0.0076	-0.006871	0.0049	99.788	32.243
Test_image3	0.0067	-0.0018	0.00117	99.789	32.371
Test_image4	-0.00055	0.0072	0.00146	99.732	32.417
Ref. [12]	**0.0060**	**-0.0072**	**0.0245**	**99.757**	**33.342**



(a) Horizontal correlation (b) Vertical correlation (c) Diagonal correlation

Figure 4. Correlation Analysis of Encrypted Image.

3. METRICS

3.1. Number of Pixel Change Rate (NPCR) and Unified Average Change in Intensity (UACI)

The Number of Pixel Change Rate (NPCR) and Unified Average Change in Intensity (UACI) provide the data about how far the proposed methodology hold good. They both test the cipher image resistance to differential attacks by manipulating the number of pixel change and their average intensity.

$$\mathrm{NPCR} = \frac{\sum_{\mathrm{mn}} \mathrm{I(m,n)}}{\mathrm{W\,X\,H}} X\ 100\%$$

$$UACI = \frac{1}{W\ X\ H}\left[\frac{\sum_{m,n} |J1(m,n) - J2(m,n)|}{255}\right] X\ 100\%$$

$$\text{where } I(m,n) = \begin{cases} 0 \; if \; J1(m,n) = J2(m,n) \\ 1 \; if \; J(m,n) \neq J2(m,n) \end{cases}$$

From table (1) the values are close to the optimum value. So, the algorithm can withstand differential attacks.

3.2 Correlation

The good encryption algorithm should break the relationship between adjacent pixels, the relation between an adjacent pixel in cipher image is tested with correlation metrics. The relation between the adjacent pixels is verified horizontally, vertically and also diagonally.

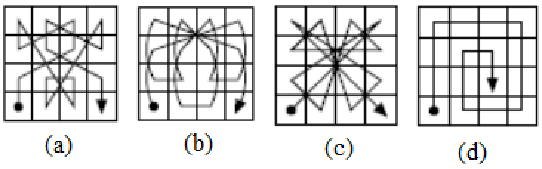


Figure 5. Different Space Filling Curves:(a) The Bat SFC; (b) The Spider SFC; (c) The Samurai SFC; (d) The Spiral SFC.

4. Results and Discussion

In the proposed scheme, Henon in companion with LFSR is used to permute the image pixels. Figure 2 (a-c) provides the test image 1, its encrypted output and the decrypted output. Figure 3 (a-d) shows the test images considered in the proposed encryption scheme. Figure 4 (a-c) represents the correlation graphs in horizontal, vertical and diagonal directions respectively. Figure 5 (a-d)accounts for the various SFC curves used in diffusing the DICOM images. Table 1 provides the metrics of various test images considered. From the table, the measured value proves that the proposed scheme can sustain any brute force attack.

5. Conclusion

Thus, the randomness provided by Henon map is efficiently used for confusing the image, and further strengthened by diffusing by using LFSR. The analysed metric values show that the proposed algorithm can withstand differential attack. The results demonstrate that the proposed work can provide security for the DICOM images.

References

[1] A. Akhshani, A. Akhavan, S.-C. Lim, Z. Hassan, An image encryption scheme based on quantum logistic map, Commun. Nonlinear Sci. Numer. Simul. 17 (2012) 4653–4661. doi:10.1016/J.CNSNS.2012.05.033.

[2] A.M. Ayoup, A.H. Hussein, M.A.A. Attia, Efficient selective image encryption, Multimed. Tools Appl. 75 (2016) 17171–17186. doi:10.1007/s11042-015-2985-7.

[3] S.N. George, D.P. Pattathil, A Secure LFSR Based Random Measurement Matrix for Compressive Sensing, Sens. Imaging. 15 (2014) 85. doi:10.1007/s11220-014-0085-9.

[4] M. Jain, A. Kumar, R.C. Choudhary, Improved diagonal queue medical image

steganography using Chaos theory, LFSR, and Rabin cryptosystem, Brain Informatics. 4 (2017) 95–106. doi:10.1007/s40708-016-0057-z.

[5] U. Kirchgraber, D. Stoffer, Transversal homoclinic points of the Hénon map, Ann. Di Mat. Pura Ed Appl. 185 (2006) S187–S204. doi:10.1007/s10231-004-0142-4.

[6] D. Ravichandran, P. Praveenkumar, J.B. Balaguru Rayappan, R. Amirtharajan, Chaos based crossover and mutation for securing DICOM image, Comput. Biol. Med. 72 (2016) 170–184. doi:10.1016/j.compbiomed.2016.03.020.

[7] G. Schrack, L. Stocco, Generation of Spatial Orders and Space-Filling Curves, IEEE Trans. Image Process. 24 (2015) 1791–1800. doi:10.1109/TIP.2015.2409571.

[8] X.-J. Tong, M. Zhang, Z. Wang, Y. Liu, A image encryption scheme based on dynamical perturbation and linear feedback shift register, Nonlinear Dyn. 78 (2014) 2277–2291. doi:10.1007/s11071-014-1564-1.

[9] E. Vaferi, R. Sabbaghi-Nadooshan, A new encryption algorithm for color images based on total chaotic shuffling scheme, Opt. - Int. J. Light Electron Opt. 126 (2015) 2474–2480. doi:10.1016/J.IJLEO.2015.06.012.

[10] Y. Zhang, Switching-induced Wada basin boundaries in the Hénon map, Nonlinear Dyn. 73 (2013) 2221–2229. doi:10.1007/s11071-013-0936-2.

[11] Y. Zheng, J. Jin, A novel image encryption scheme based on Hénon map and compound spatiotemporal chaos, Multimed. Tools Appl. 74 (2015) 7803–7820. doi:10.1007/s11042-014-2024-0.

[12] J. Sree Subhashini,V. Bakyalakshmi “PARALLEL MINING OF FREQUENT ITEMSETS USING MAP REDUCE AND FIDOOP, International Journal of Innovations in Scientific and Engineering Research (IJISER),vol3 no11,pp94-97,2016

[13] Y.-G. Yang, Q.-X. Pan, S.-J. Sun, P. Xu, Novel Image Encryption based on Quantum Walks, Sci. Rep. 5 (2015) 7784. doi:10.1038/srep07784.