Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Supplementary materials for

Jia DUAN, Luanyun HU, Qiumei XIAO, Meiting LIU, Wenxin YU, 2025. A geographic information encryption system based on Chaos-LSTM and chaos sequence proliferation. *Front Inform Technol Electron Eng*, 26(3):427-440. https://doi.org/10.1631/FITEE.2300755

1 NIST tests and TestU01 tests

To verify the randomness of chaos proliferation sequences, the chaos proliferation sequences with length 10^6 are selected for NIST tests and TestU01 tests. The experimental results are shown in Table S1, which lists the results of 15 tests for chaotic proliferation sequences in the NIST tests and 3 tests in the TestU01 tests. Test1-Test15 belong to the NIST tests, and Test16-Test18 belongs to the TestU01 tests. Rabbit and Alphabit contain 38 and 17 different statistical tests, respectively. BlockAlpbit reorders the sequence using blocks of 1, 2, 4, 8, 16, and 32 bits, and then repeats the Alphabit tests (De la Fraga et al., 2021). In the NIST tests, the P-values of all 15 tests are greater than 0.01, and the TestU01 tests also passed, indicating that the chaotic proliferation sequences have passed all NIST tests and TestU01 tests, and have good randomness and belong to the random sequence.

Table S1 NIST and TestU01 tests of chaos proliferation sequences

Test name	Result	
	P-value	
Frequency	0.6542	Pass
Block frequency	0.3416	Pass
Runs	0.8664	Pass
Long runs of ones	0.8629	Pass
Rank	0.3055	Pass
FFT	0.9561	Pass
Nonoverlapping templates	0.4976	Pass
Overlapping templates	0.0106	Pass
Universal	0.6122	Pass
Linear complexity	0.4781	Pass
Serial	0.3375	Pass
Approximate entropy	0.7724	Pass
Cumulative Sums	0.8163	Pass
Random excursion	0.3740	Pass
Random excursion variant	0.4229	Pass
Rabbit	All 38 tests were passed	
Alphabit	All 17 tests passed	
BlockAlphabit	All 6 repetitions of alphabit tests passed	

2 Comparison of encryption performance

In order to compare and analyze its security with that of other image encryption algorithms, the color Lena image, commonly used in image encryption processing, has been added. The colored Lena plain image P and the corresponding encrypted image E processed by the encryption system are shown in Fig. S1.

a b

Fig. S1 The plain and encrypted image of colored Lena. The colored Lena plain image P (a) and encrypted i mage E (b)

The number of pixels change rate (NPCR) refers to the proportion of different pixels between two images relative to the total number of pixels. The unified average changing intensity (UACI) refers to the average ratio of the difference between all corresponding pixel positions in two images to the maximum possible difference. Their corresponding ideal values are NPCR=99.6094% and UACI=33.4635%, respectively. The closer NPCR and UACI are to the ideal value, the better the encryption effect (Rehman et al., 2018).

We have encrypted the Lena image using the proposed algorithm and the algorithms proposed in references RF1 (Hosseinzadeh et al., 2019), RF2 (Wu et al., 2015), and RF3 (Wu et al., 2016). Table S2 shows the numerical results of the encrypted images in terms of NPCR, UACI, and information entropy.

Table S2 Comparison of NPCR, UACI, and information entropy

Measure	Lena	Proposed algorithm	RF1	RF2	RF3
NPCR	R	99.6201%	99.5804%	99.6097%	99.6126%
	G	99.6506%	99.6628%		
	B	99.6185%	99.5865%		
UACI	R	33.4347%	33.4456%	33.4819%	33.4668%
	G	33.4693%	33.6561%		
	B	33.4104%	33.5512%		
Information entropy	R	7.9971	7.9977	7.9893	7.9914
	G	7.9976	7.9968	7.9896	7.9907
	B	7.9975	7.9969	7.9903	7.9907

As shown in Table S2, the NPCRs of the proposed algorithm in the RGB layer are 99.6201%, 99.6506%, and 99.6185%, which are similar to but slightly larger than those in references RF1, RF2, and RF3. The UACI of the encrypted image using the proposed algorithm is close to the expected value of 33.4635%, and its information entropy is closer to 8. It is easy to conclude that our proposed method has a good confidentiality performance.

3 Encryption quality analysis

The encryption quality analysis is conducted on the encryption algorithm proposed in this paper, including the mean squared error (MSE), the peak signal-to-noise ratio (PSNR), the structural similarity index (SSIM), and the floating frequency. MSE is a parameter that measures the difference between two images, and the higher the MSE value, the better the encryption quality. PSNR is defined based on MSE, and its PSNR is generally lower than 10 dB for high-quality encrypted images. SSIM can determine the similarity between two images. For the same image, SSIM is 1, while for completely different images, SSIM should be close to 0. The chi-square test can calculate the degree of deviation between two images, and the degree of deviation between images determines the size of the chi-square value. The larger the chi-square value, the greater the deviation between the two images. Floating frequency analysis can determine the uniformity of encryption algorithms in encrypting all rows and columns of the image (Murillo-Escobar et al., 2019).

Table S3 shows the encryption quality results of four color ciphertexts from different plaintext images. From Table S3, it can be seen that the MSE values of all color images are relatively high under different color components, the PSNR values are all below 10dB, and the SSIM values are close to zero. The chi-square values between the original and encrypted images are very large, indicating a significant deviation between them. This demonstrates that the proposed encryption system has a good encryption performance.

Table S3 Quality metrics analysis

Cryptogram	MSE			PSNR (dB)			SSIM			Chi-square value
	R	G	B	R	G	B	R	G	B	
Image A (256×256×3)	8455	7251	8111	8.86	9.53	9.04	0.0094	0.0110	0.0107	88773
Image B (512×512×3)	7991	7524	7665	9.10	9.37	9.29	0.0091	0.0096	0.0097	441450
Image C (1024×1024×3)	9493	8308	9847	8.36	8.94	8.20	0.0086	0.0092	0.0084	1975387
Lena (256×256×3)	8550	9487	10442	8.81	8.36	7.94	0.0112	0.0061	0.0069	63970

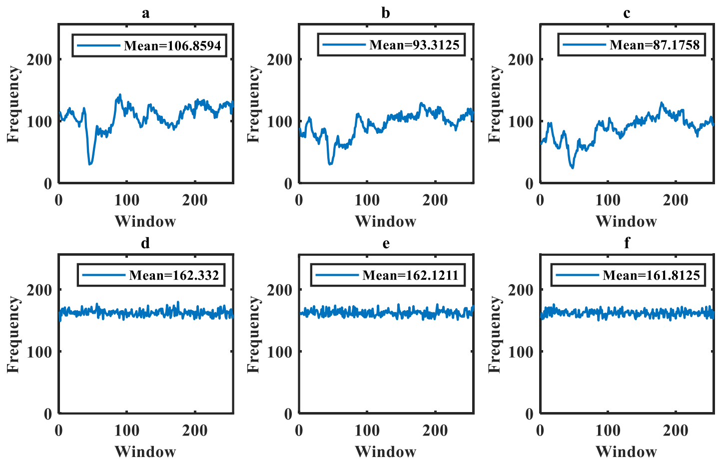

Fig. S2 Column floating frequency (CFF) and its mean: (a) R-component of P; (b) G-component of P; (c) B-component P; (d) R-component of E; (e) G-component of E; (f) B-component of E

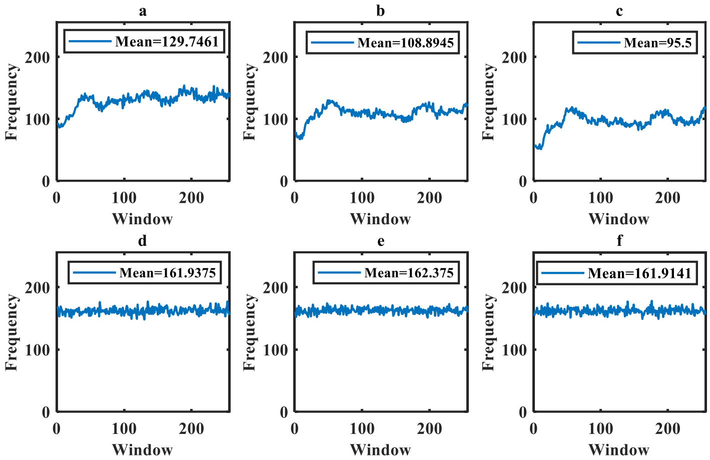

Fig. S3 Row floating frequency (RFF) and its mean: (a) R-component of P; (b) G-component of P; (c) B-component P; (d) R-component of E; (e) G-component of E; (f) B-component of E

Floating frequency analysis was performed on the plain image P and encrypted image E of the colored Lena image with size 256×256×3. Figs. S2 and S3, respectively, show the column floating frequency (CFF) and row floating frequency (RFF) of plain image P and its corresponding encrypted image E. It can be seen that, whether it is CFF or RFF, the mean of the plain image P is relatively low compared to the mean of the encrypted image E, and the fluctuation of the plain image is significant. The mean CFF and RFF of the encrypted image E are both around 162, indicating that the encryption system has high encryption efficiency in the corresponding direction.

References

De la Fraga LG, Mancillas-López C, Tlelo-Cuautle E, 2021. Tlelo-Cuautle E. Designing an authenticated Hash function with a 2D chaotic map. *Nonlinear Dyn*, 104(4):4569-4580. https://doi.org/10.1007/s11071-021-06491-3

Hosseinzadeh R, Zarebnia M, Parvaz R, 2019. Hybrid image encryption algorithm based on 3D chaotic system and choquet fuzzy integral. *Opt Laser Technol*, 120:105698. https://doi.org/10.1016/j.optlastec.2019.105698

Murillo-Escobar MA, Meranza-Castillón MO, López-Gutiérrez RM, et al., 2019. Suggested integral analysis for chaos-based image cryptosystems. *Entropy*, 21(8):815. https://doi.org/10.3390/e21080815

Rehman AU, Liao XF, Ashraf R, et al., 2018. A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2. *Optik*, 159:348-367. https://doi.org/10.1016/j.ijleo.2018.01.064

Wu XJ, Kan HB, Kurths J, 2015. A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. *Appl Soft Comput*, 37:24-39. https://doi.org/10.1016/j.asoc.2015.08.008

Wu XJ, Wang DW, Kurths J, et al., 2016. A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. *Inf Sci*, 349-350:137-153. https://doi.org/10.1016/j.ins.2016.02.041