CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.5 / No.3 / 2023 / pp.153-159
https://doi.org/10.51537/chaos.1246581

Chaos-based Image Encryption in Embedded Systems using Lorenz-Rossler System

Berkay Emin *,1 **and Zabit Musayev** α,2

*Department of Electronics and Automation, Osmancık Omer Derindere Vocational School, Hitit University, Corum, 19500, Turkiye, αDepartment of Electrical and Electronics Engineering,Faculty of Engineering and Architecture, Yozgat Bozok University, 66900 Yozgat, Turkiye.

ABSTRACT Digital data is increasing rapidly in the world day by day. Information security is important during data exchange over the Internet. The way to securely transmit images over the network is through the image encryption technique. In the proposed cryptography system, the hybridization of Lorenz-Rossler chaotic systems is used, and a random number sequence is generated. The security analyses such as histogram, correlation, differential attack, information entropy, and duration analysis of the study are performed. It is seen that the proposed system performs well, especially in terms of correlation. Additionally, the performance of the developed embedded system platforms is compared after testing on Nvidia Jetson Nano and Xilinx PYNQ Z1 boards. The Nvidia Jetson Nano board is more performant than the Xilinx PYNQ Z1 board. The safety and feasibility of the proposed system have been demonstrated.

KEYWORDS
Chaotic systems
Image encryption
Security analysis
Embedded systems

INTRODUCTION

With the development of technology and science, there has been an increase in the number of audio, video and other multimedia files in recent years. Data is mostly transferred to each other by people via the internet. This situation brings along information security (Ahmed *et al.* 2007). Especially military or health image data used in fields contain significant private information. The preservation of such images is very important in terms of information security. Therefore, the pixel values are changed to make the image incomprehensible before transferring the image. This is known as image encryption and is done with the help of a key.

Classical algorithms such as AES, RSA DES, and IDEA (Daemen and Rijmen 2020) have been recommended in the literature for image encryption. However, its use is often not considered appropriate due to its low speed. Many image encryption algorithms have been suggested as a way to solve the problem in the literature (Zhang and Karim 1999; Sinha and Singh 2003; Wang *et al.* 2020). Another method of image encryption is diffusion and confusion. During the confusion phase, the pixels are displaced.

During the diffusion process, the values of the pixels are changed. Usually, chaotic functions are used for this. Chaotic systems, on the other hand, are often used in image encryption operations due to their advantages such as unpredictability, pseudo-randomness, parameter sensitivity and initial value sensitivity (Zhang *et al.* 2016). When the literature in this field is examined, Al-Khasawneh and colleagues presented a new Chaos-based encryption technique using Henon, Logistic and Gaussian iterative maps and an external secret key. They applied this technique to images detected remotely (Al-Khasawneh *et al.* 2021). Akgül et al. designed a random number generator using a microcomputer-based, nonlinear chaotic system and implemented an image encryption application (Akgul *et al.* 2021). In the study, Wang et al. used the chaotic cat map for image encryption (Wang *et al.* 2009).

In this study, Lorenz-Rossler chaotic system and encryption-decryption algorithm are examined. The study's main purpose is to perform chaotic system-based RGB image encryption and decryption operations on embedded board platforms. Histogram, correlation, differential attack, information entropy and time analysis results and the obtained data are presented in the literature. It is expected that the encryption application applied on an embedded board basis will provide portability and usability due to its cost-effectiveness.

Manuscript received: 2 February 2023,
Revised: 5 April 2023,
Accepted: 16 June 2023.

[1]berkayemin@hitit.edu.tr (**Corresponding author**)
[2]zabit.musayev@bozok.edu.tr

MATERIAL AND METHODS

Lorenz-Rossler Chaotic System

The Lorenz-Rossler chaotic system was obtained by hybridizing two chaotic systems, Lorenz and Rossler, by Alsafasfeh and Al-Arni (Alsafasfeh and Al-Arni 2011). In this case, the control parameter has increased to six. The formula for the Lorenz-Rossler chaotic system is given in Equation 1.

$$\begin{aligned} \dot{x} &= (\delta - 1)y - \delta x - z, \\ \dot{y} &= (r + 1)x - (1 - a)y - 20xz, \\ \dot{z} &= 5xy - \beta z + b + xz - cx, \end{aligned} \tag{1}$$

Where delta,r,a,b,beta and c are the fixed control arguments and x,y,z are the system state variables. The researchers found the value delta = 20, r = 20, a = 9, beta = 8.5, b = 0 and c = 8 for the system to show chaotic properties. Differential equations are solved in the Google Colaboratory environment using the Runge-Kutta method with initial conditions x = 0.001, y = 0.001, z = 0.1 Figure 1 shows the chaotic behaviors of the Lorenz Rossler system.

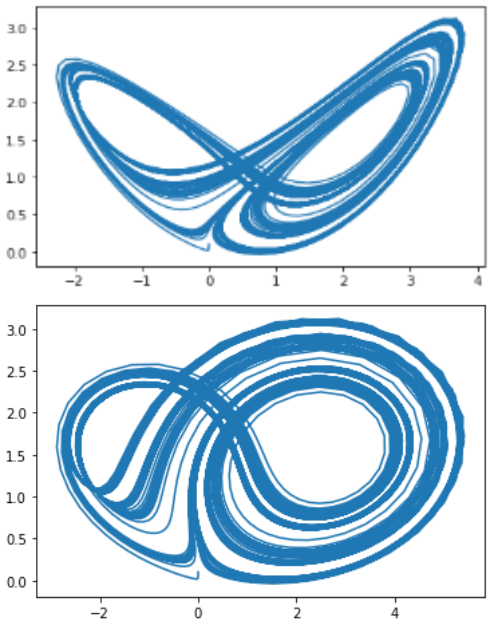


Figure 1 Attractors of Lorenz-Rossler System

Encryption and Decryption Algorithm

In the encryption process, the pixel positions of the image will be changed first. This process is called confusion. During the confusion phase, the positions of the pixels in the original image are mixed with controlled randomness. For this, a chaotic sequence is created using Equation 1. These arrays are used to encrypt the red, green and blue channels of the original view. The generated chaotic sequences are ordered from small to large and the sequences are obtained.

At the same time, the index of the values in the chaotic array is assigned to the array by sorting. Then, using these indexes, the picture is mixed. the confusion matrix is obtained separately for the three channels. The correlation coefficient between the blending process and adjacent pixels Decays, but the blended image continues to contain the statistical values of the original image. This indicates that the encryption process is not secure. In this case, the diffusion process is performed to increase encryption security.

At the propagation stage, the values of pixels are changed, the positions of which change in the process of confusion. Thus, the statistical values of the original image do not remain in the encrypted image. In the encrypted image, both pixel positions and pixel values are given in a different format from the original image. The pseudo-code for image encryption is given in Algorithm 1. The decryption algorithm, on the other hand, is the opposite of the image encryption algorithm.

Algorithm 1 Pseudo code of Image Encryption Algorithm

Input : Chaotic sequence and Image
Output : Encrypted Image
1: START
2: x,y,z chaotic sequence and image data
3: Split the image into R,G,B channels (imageR,imageG,imageB)
4: Get the dimensions of the image (m,n)
5: Normalize x,y,z chaotic arrays (x',y',z')
6: Sort the sequences x', y' and z' and mix the image R,G,B channels using the obtained index values. (shfR,shfG,shfB)
7:

for $i = 0; m \times n$ **do**
$encimgR[i] = x'[i]$ **XOR** $shfR[i]$
$encimgG[i] = y'[i]$ **XOR** $shfG[i]$
$encimgB[i] = z'[i]$ **XOR**$shfB[i]$

8: Merge encrypted R,G,B channels
9: EXIT

Image Encryption on NVIDIA Jetson Nano and Xilinx Pynq Z1 Embedded Boards

The proposed encryption and decryption algorithm was implemented on Nvidia Jetson Nano and Xilinx PYNQ Z1 platforms. General specifications of embedded boards are given in Table 1. Linux is installed as the operating system on both embedded system boards and the code written in Python on the Linux operating system is run on the system.The structure of the application of the proposed method to embedded boards is given in Figure 2. 256×256×3 peppers and 512×512×3 baboon images were used for encryption in both embedded boards.

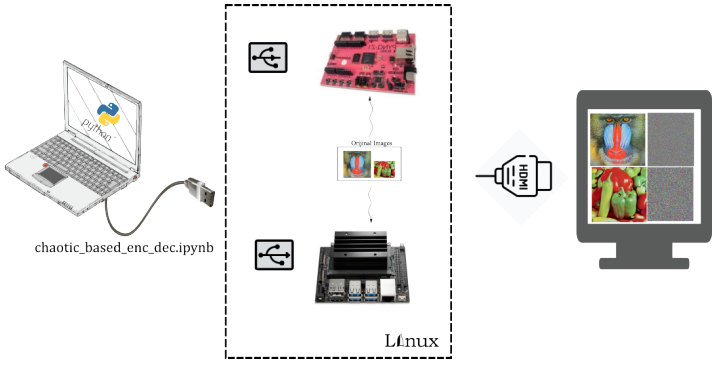
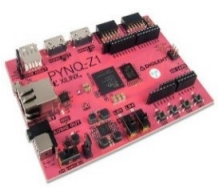


Figure 2 Application of the Proposed Method in Hardware

Table 1 The General Features of Embedded Boards




	Xilinx Pynq Z1	Nvidia Jetson Nano
GPU	ZYNQ XC7Z020-1CLG400C	NVIDIA Maxwell, 128 CUDA cores
CPU	650MHz dual-core Cortex-A9	Quad-core ARM Cortex-A57 MP-Core
Memory	512MB DDR3	4 GB 64-bit LPDDR4
Data storage	MicroSD card	MicroSD card
Power	7W-15W	5W-10W
Network	Gigabit Ethernet	Gigabit Ethernet
Other	16-pin GPIO	40-pin GPIO
Programmable logic	Artix-7 FPGA 13,300 logic segments, each with four 6-input LUTs and 8 flip-flops	-

RESULTS AND DISCUSSION

Histogram Analysis

The dispersion of pixel values in an image is revealed by histogram analysis. Color distribution in the original image According to the colors contained in the image, the histogram graph concentrates on a particular region and shows an uneven distribution. In the encryption process, the color distributions of the channels are equalized. Therefore, the histogram distributions of the original and encoded images must be different. All pixels of the encrypted image must be equally distributed in space. Therefore, the histogram distribution of the encrypted image should be uniform. In this direction, histogram analysis of the encrypted treat was performed.

Histogram graphics of the RGB channels of the original baboon image in Figure 3 (a-d) and the original peppers image in Figure 3 (i-l) are shown. When Figure 3 (a-d) and Figure 3 (i-j) are examined, it is seen that the color distributions in the original painting are uneven. The histogram graph of the RGB channels of the encrypted baboon image in Figure 3 (e-h) and the encrypted peppers image in Figure 3 (m-p) are shown. When Figure 3 (e-h) and Figure 3 (m-p) are examined, it is seen that the color distributions of the RGB channels are evenly distributed. This shows that the histogram of the encrypted image cannot be inferred and that the proposed encryption is secure.

Correlation Analysis

Correlation analysis (Cohen 1988) Decodes the linear relationship between two random variables. As a result of this analysis, the correlation coefficient was determined. Equation 2 using it, the correlation coefficient of a sequence with "n" elements is calculated, where x and y are two random variables.

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \tag{2}$$

Hence;

$$\mathrm{cov}(x,y) = \frac{1}{n}\sum_{i=1}^{n}[x_i - \mathrm{E}(x)][y_i - \mathrm{E}(y)]$$

$$\mathrm{D}(x) = \frac{1}{n}\sum_{i=1}^{n}[x_i - \mathrm{E}(x)]^2$$

$$\mathrm{E}(x) = \frac{1}{n}\sum_{i=1}^{n} x_i$$

The x and y values in the equation symbolize the two contiguous pixels in the image, and N indicates the number of pairs of pixels chosen. In our study, horizontal, vertical and diagonal pixel values were taken into account to calculate the pixel correlation in the original and encrypted images. Correlation analysis was performed for each R, G and B channel of peppers and baboon images. The horizontal correlation maps of the R, G, B channels of the peppers and baboon images are respectively shown

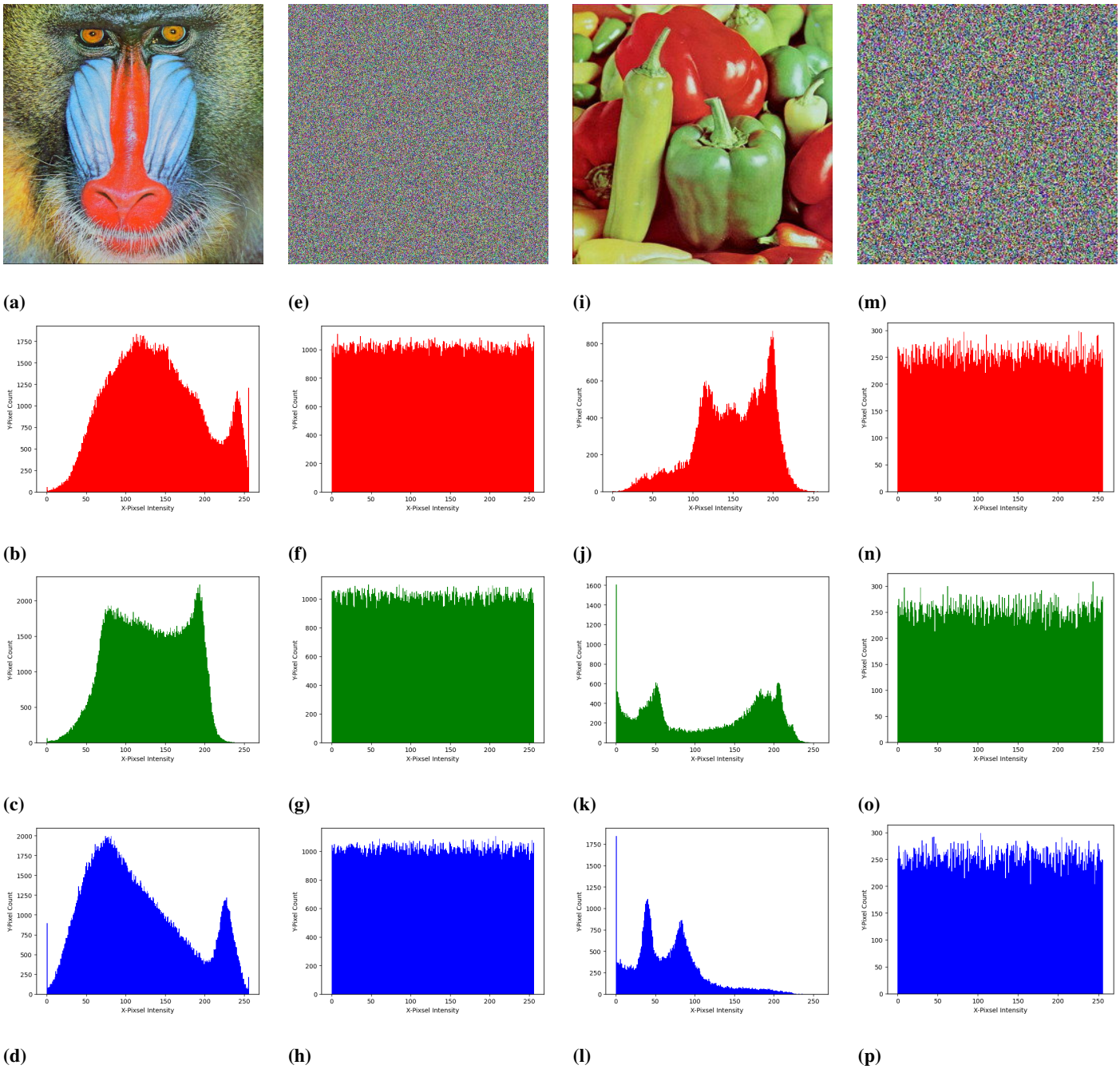


Figure 3 Histogram Graph of the Original and Encrypted Baboon-Peppers Image

in Figure 4 and Figure 5. The obtained correlation coefficient values and their comparison with the literature are given in Table 2.

The correlation cannot be less than -1 and greater than +1. The fact that the correlation coefficient is very close to -1 and +1 means that the relationship between pixel values is strong and that it is close to zero means the relationship between pixel values is weak. When Table 2 is examined, it is seen that the correlation coefficients to the original image are close to one. On the other hand, it is observed that the correlation coefficients of encrypted images for RGB channels are approximately zero. The results obtained are in harmony with recent studies in the literature. According to the results of correlation analysis, it can be said that the image encryption method performed successfully performs the encryption process.

Differential Attack Analysis (NPCR-UACI)

NPCR ("Number of Pixels Change Rate") and UACI ("Unified Average Changing Intensity") analyzes Differential cryptanalysis developed by Biham and Shamir (Biham and Shamir 1990) to examine how minor changes in the original image affect the encrypted images. NPCR is a metric that measures the rate of pixel change in an image. The NPCR value is calculated as given in Equation 3. The matrix D(i,j) in Equation 3 is calculated from Equation 4. Here, A and B represent the pixel value of the original and encrypted images, respectively. M × N represents the size of the encrypted image.

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100 \tag{3}$$

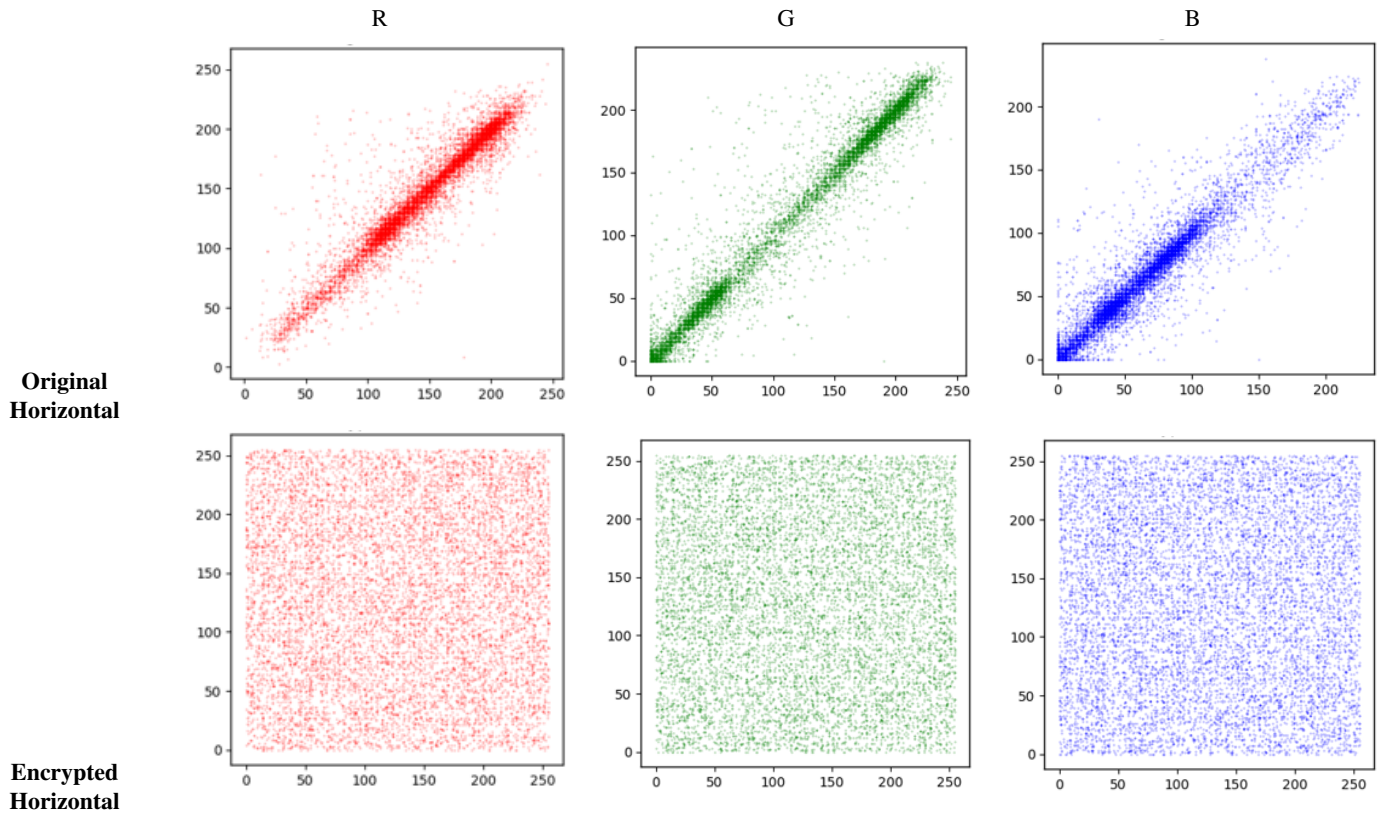


Figure 4 The horizontal correlation coefficient maps of the R, G, B channels of peppers

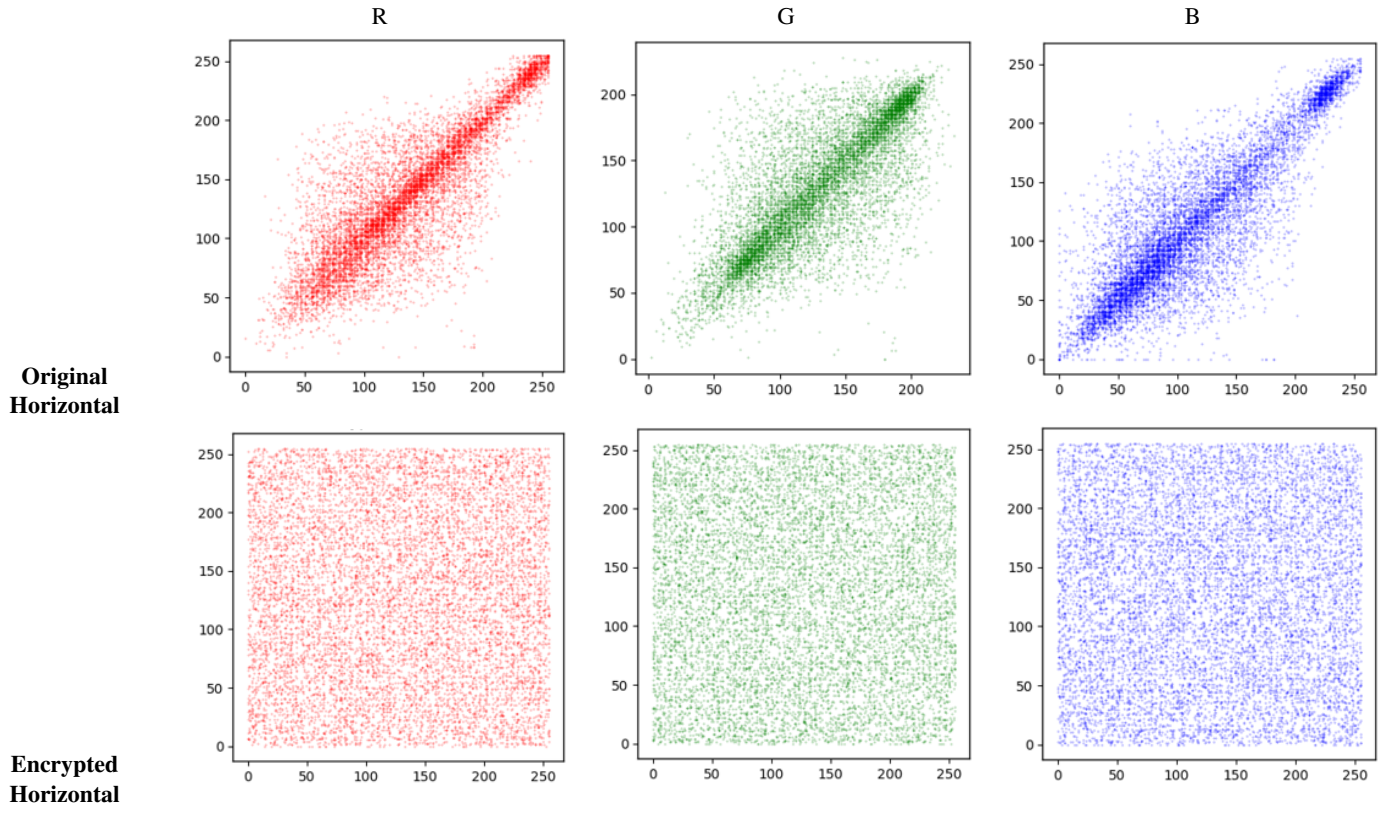


Figure 5 The horizontal correlation coefficient maps of the R, G, B channels of baboon

Table 2 Correlation Coefficients Values Comparison

		Original			Encrypted		
	Channel	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
proposed method (peppers)	R	0.9515	0.9463	0.9153	0.0181	-0.0007	-0.0011
	G	0.9759	0.9680	0.9487	0.0012	0.0157	-0.0079
	B	0.9472	0.9365	0.9050	-0.0019	0.0073	-0.0035
proposed method (baboon)	R	0.8512	0.9198	0.8449	0.0102	-0.0099	-0.0029
	G	0.7844	0.7599	0.9304	0.0025	0.0011	0.0026
	B	0.8736	0.9228	0.8529	0.0026	0.0024	-0.0153
(Xin *et al.* 2023) *(512×512×3)*	R	0.9621	0.9646	0.9513	-0.0005	0.0004	0.0007
	G	0.9789	0.9774	0.9599	-0.0004	0.0002	0.0004
	B	0.9616	0.9628	0.9401	-0.0006	0.0003	0.0006
(Yan *et al.* 2023) *(256×256×3)*	R	0.9904	0.9796	0.9701	0.0080	-0.0060	0.0026
	G	0.9820	0.9659	0.9547	-0.0092	-0.0090	0.00009
	B	0.9555	0.9324	0.9144	0.0060	-0.0069	0.0036
Demirtaş (2022) *(512×512×3)*	R	0.9643	0.9635	0.9598	-0.0051	-0.0092	0.0012
	G	0.9808	0.9821	0.9695	0.0007	0.0068	-0.0034
	B	0.9645	0.9659	0.9455	0.0080	0.0014	-0.0052

$$D(i,j) = \begin{cases} 1 & \text{if } A(i,j) \neq B(i,j) \\ 0 & \text{if } A(i,j) = B(i,j) \end{cases} \tag{4}$$

UACI is a metric that measures the average intensity of change in an image, calculated as given in Equation 5. The L value is the number of bits that express the pixel of the image.

$$\text{UACI} = \frac{1}{M \times N} \left[\sum_{i,j} \frac{|A(i,j) - B(i,j)|}{2^L - 1} \right] \times 100 \tag{5}$$

In the literature, the most appropriate NPCR and UACI values are stated as NPCRopt = 99.61% and UACIopt =33.46% (Girdhar and Kumar 2018). In addition, NPCR, UACI values greater than 99.6% and close to or greater than 30%, respectively, is accepted as an indication of successful encryption (Praveenkumar *et al.* 2015).NPCR and UACI results are shown in Table 3. It is seen that the NPCR value is greater than 99.6% and the UACI value is close to 30% for both images used in the study. In addition, it was observed that the results were compatible with similar studies in the literature. Based on these results, it is clear that the developed encryption algorithm is strong against differential attacks.

Information Entropy Analysis

The encrypted data must be in such a way that no guesses can be made about the original data. Information entropy analysis measures the randomness in the encrypted image and demonstrates the average amount of information that the image carries. The entropy coefficient Equation 6 calculated by the given formula. Here, H (s) is the entropy value of the source, while N represents the bit value. In the literature, the ideal entropy value of the encrypted image is expected to be eight. The entropy test is applied to each of the RGB channels separately.

$$H(s) = \sum_{i=0}^{2^N-1} P(S_i) log_2 \frac{1}{P(S_i)} \tag{6}$$

The entropy values of the information obtained in the study and its comparison with the literature are given in Table **??**. It is seen that the entropy values of the RGB channels of the encrypted images are close to 8. Therefore, it can be said that the proposed method is quite resistant to attacks.

Table 3 NPCR and UACI Results and Comparison

	NPCR	UACI
Proposed method (peppers)	99.6154	28.8371
Proposed method (baboon)	99.6067	29.9783
(Ali and Ali 2020)	99.6094	33.4635
(Yu *et al.* 2022)	99.6069	33.4422
(Sheela *et al.* 2018)	99.5865	28.6372

Table 4 Time Analysis of Embedded System (Unit: s)

	Embedded Board	Encryption Time	Decryption Time
proposed method (peppers)	Google Colaboratory Environment	0.6133	0.3978
	Xilinx PYNQ Z1	2.8670	6.6832
	Nvidia Jetson Nano	1.480	1.719
proposed method (baboon)	Google Colaboratory Environment	0.8842	1.3358
	Xilinx PYNQ Z1	11.4452	25.9610
	Nvidia Jetson Nano	5.8907	6.8535

Time Analysis

Operations performed on Google Colaboratory Environment were also performed on Xilinx PYNQ Z1 and Nvidia Jetson Nano embedded boards. Thus, the performances of different embedded boards in encryption and decryption processes were compared. In the table 4, the times obtained during the test phase are given in seconds. According to the results obtained, it is seen that the time in the software environment is more advantageous. In embedded platforms, it has been observed that the Nvidia Jetson Nano board is faster in encryption and decryption processes than the other boards.

CONCLUSION

In this study, an encryption algorithm is developed using Lorenz-Rossler chaotic systems. To measure the reliability of the designed system, histogram, correlation, differential attack, and information entropy analysis are performed. According to the results of the analysis, it has been determined that the developed encryption algorithm is resistant to attacks. Considering the experimental results, it has been observed that the proposed method allows the original image to be obtained again without any data loss. The application results obtained on embedded system boards are presented according to encryption and decryption duration comparatively. When the results are inspected, it is seen that the Nvidia Jetson Nano board is faster in encryption and decryption than the Xilinx PYNQ Z1. The authors are hopeful that a better, the mutually beneficial dialogue will gradually be established between the chaos and cryptography communities.

Availability of data and material

Not applicable.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Ahmed, H. E. D. H., H. M. Kalash, and O. S. Farag Allah, 2007 An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for image encryption and decryption. Informatica (Ljubljana) .

Akgul, A., B. Gurevin, I. Pehlivan, M. Yildiz, M. C. Kutlu, *et al.*, 2021 Development of micro computer based mobile random number generator with an encryption application. Integration **81**: 1–16.

Al-Khasawneh, M. A., I. Uddin, S. A. A. Shah, A. M. Khasawneh, L. M. Abualigah, *et al.*, 2021 An improved chaotic image encryption algorithm using Hadoop-based MapReduce framework for massive remote sensed images in parallel IoT applications. Cluster Computing **25**: 999–1013.

Ali, T. S. and R. Ali, 2020 A new chaos based color image encryption algorithm using permutation substitution and Boolean operation. Multimedia Tools and Applications **79**: 19853–19873.

Alsafasfeh, Q. H. and M. S. Al-Arni, 2011 A New Chaotic Behavior from Lorenz and Rossler Systems and Its Electronic Circuit Implementation. Circuits and Systems **02**: 101–105.

Biham, E. and A. Shamir, 1990 Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology **4**: 3–72.

Cohen, J., 1988 *Statistical Power Analysis for the Behavioral Sciences*.

Daemen, J. and V. Rijmen, 2020 The Design of Rijndael: The Advanced Encryption Standard (AES). The Design of Rijndael .

Demirtaş, M., 2022 A new RGB color image encryption scheme based on cross-channel pixel and bit scrambling using chaos. Optik **265**: 0–2.

Girdhar, A. and V. Kumar, 2018 A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences. Multimedia Tools and Applications .

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, 2015 Pixel scattering matrix formalism for image encryption-A key scheduled substitution and diffusion approach. AEU - International Journal of Electronics and Communications .

Sheela, S. J., K. V. Suresh, and D. Tandur, 2018 Image encryption based on modified Henon map using hybrid chaotic shift transform. Multimedia Tools and Applications **77**: 25223–25251.

Sinha, A. and K. Singh, 2003 A technique for image encryption using digital signature. Optics Communications .

Wang, X., Y. Su, C. Luo, and C. Wang, 2020 A novel image encryption algorithm based on fractional order 5D cellular neural network and Fisher-Yates scrambling. PLoS ONE .

Wang, Y., K.-W. Wong, X. Liao, T. Xiang, and G. Chen, 2009 A chaos-based image encryption algorithm with variable control parameters. Chaos, Solitons and Fractals **41**: 1773–1783.

Xin, J., H. Hu, and J. Zheng, 2023 3D variable-structure chaotic system and its application in color image encryption with new Rubik's Cube-like permutation. Nonlinear Dynamics .

Yan, S., L. Li, and B. Gu, 2023 *Design of a new four-dimensional chaotic system and its application to color image encryption*.

Yu, J., W. Xie, Z. Zhong, and H. Wang, 2022 Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation. Chaos, Solitons and Fractals **162**: 112456.

Zhang, S. and M. A. Karim, 1999 Color image encryption using double random phase encoding. Microwave and Optical Technology Letters .

Zhang, Y. Q., X. Y. Wang, J. Liu, and Z. L. Chi, 2016 An image encryption scheme based on the MLNCML system using DNA sequences. Optics and Lasers in Engineering **82**: 95–103.

How to cite this article: Emin, B., and Musayev, Z. Chaos-based Image Encryption in Embedded Systems using Lorenz-Rossler System. *Chaos Theory and Applications*, 5(3), 153-159, 2023.