Düzce University
Journal of Science & Technology

Research Article

Implementation of Real-Time Image Encryption Using Chaotic Maps in Embedded Systems

Çağrı CANDAN[a,*], M. Emin SAHIN[a]

[a] *Department of Computer Engineering, Faculty of Architecture and Engineering, Yozgat Bozok University, Yozgat, TURKEY*
** Corresponding author's e-mail address: 16008118006@ogr.bozok.edu.tr*
DOI: 10.29130/dubited.1159078

ABSTRACT

The advancement of technology has sped up the process of data transfer in the expansion of multimedia and communication tools. Digital images are one of the most frequently used data types in data transfers. These images may contain personal and confidential information. When images are sent over a public network, it is crucial for information security to transmit them to the receiving party in encrypted format. Chaos-based methods are the most commonly used image encryption techniques. In this study, a confusion and diffusion-based image encryption method is designed and implemented in real time on Jetson TX2 and Jetson Nano embedded systems using Henon and Tent chaotic maps. In order to evaluate the performance of the designed image encryption system, the encrypted images are subjected to security tests such as histogram analysis, correlation analysis, and key sensitivity analysis, which are the most frequently used tests in the literature. Moreover, the proposed system is evaluated by comparing the encryption and decryption times of two different embedded systems. The results clearly demonstrate that proposed image encryption system has a highly secure.

Keywords: *Chaos, Image encryption, Jetson Nano, Jetson TX2, Security tests*

Gömülü Sistemlerde Kaotik Haritalar Kullanılarak Gerçek Zamanlı Görüntü Şifreleme Uygulaması

ÖZET

Teknolojinin ilerlemesi, multimedya ve iletişim araçlarının yaygınlaşmasında veri aktarım sürecini hızlandırmıştır. Dijital görüntüler, veri aktarımlarında en sık kullanılan veri türlerinden biridir. Bu görüntüler kişisel ve gizli bilgiler içerebilir. Görüntülerin genel bir ağ üzerinden gönderildiğinde, alıcı tarafa şifreli olarak iletilmesi bilgi güvenliği açısından çok önemlidir. Kaos tabanlı yöntemler en yaygın olarak kullanılan görüntü şifreleme tekniklerdir. Bu çalışmada, Henon ve Tent kaotik haritaları kullanılarak Jetson TX2 ve Jetson Nano gömülü sistemler üzerinde gerçek zamanlı olarak karıştırma ve yayılma tabanlı bir görüntü şifreleme yöntemi tasarlanmış ve uygulanmıştır. Tasarlanan görüntü şifreleme sisteminin performansını değerlendirmek için şifrelenen görüntüler literatürde en sık kullanılan testlerden histogram analizi, korelasyon analizi ve anahtar duyarlılık analizi gibi güvenlik testlerine tabi tutulmaktadır. Ayrıca önerilen sistem, iki farklı gömülü sistemin şifreleme ve şifre çözme süreleri karşılaştırılarak değerlendirilmiştir. Sonuçlar, önerilen görüntü şifreleme sisteminin oldukça güvenli olduğunu açıkça göstermektedir.

Anahtar Kelimeler: *Kaos, Görüntü şifreleme, Jetson Nano, Jetson TX2, Güvenlik testleri*

Received: 08/08/2022, Revised: 29/08/2022, Accepted: 15/11/2022

I. INTRODUCTION

Due to the rapid development of technology and its integration into our daily lives, it has become easier to access devices with internet access, resulting in an increase in internet usage. After all, the recent Covid-19 has led people to spend a lot of time on the internet. Companies has started to conduct meetings and individuals has started to meet on the internet and they has also shared personal and important information over the internet. Due to the transmission of digital images over the internet (public networks), the amount of data transmitted in an unsecure internet environment is growing day by day [1]. Therefore, the increase in internet usage made information and data security important. Particularly, many applications, such as the storage and transmission of vital military image data, confidential video conferencing, medical imaging systems, and cable television, require a quick and robust security system for in the processing of information. Fast and reliable methods should be preferred for real-time image encryption [2].

Henri Poincare proposed the name "chaos" which is an ordered state of disorder that is particularly sensitive to initial conditions and includes a noise-like power spectrum [3]. In recent years, chaotic systems have been the topic of various scientific and technical such as different chaotic systems have been introduced to the literature, and their application fields have expanded significantly [3-5]. With the advancement of technology, it has begun to be utilized in a variety of sectors, including chaotic systems, communication, image processing, fuzzy logic, control, optimization, and mechatronics, particularly in the study of encryption. Chaotic signals include some undesirable characteristics such as wide-band, noise-like, difficult-to-predict, and non-periodic characteristics, which dramatically increase mixing and propagation of encrypted data [4]. The most important considerations in encryption include the complexity and sensitivity of the encrypted data and the nature of the encryption algorithms.

Because of several characteristics of chaotic systems, numerous researchers use chaotic systems [5]–[8]. Kocarev and Jakimoski focused on chaos-based designs in their study. In their paper, the relationship between chaos and cryptology was discussed, and it was explained that in cryptology research, chaos-based systems satisfy encryption criteria due to their characteristics [9]. Tong et al. proposed and published a combined chaos-based encryption technique for wireless sensor networks employing cubic and logistic chaotic maps [10]. Assad et al. evaluated chaos-based block cipher algorithms generally [11]. Chen et al. submitted a symmetric encryption technique for image encryption utilizing a 3D chaotic map [12]. Hraoui et al. devised a chaos-based encryption method utilizing the logistic chaotic map to use in image encryption and analysed the AES algorithm's performance and security for comparison [13].

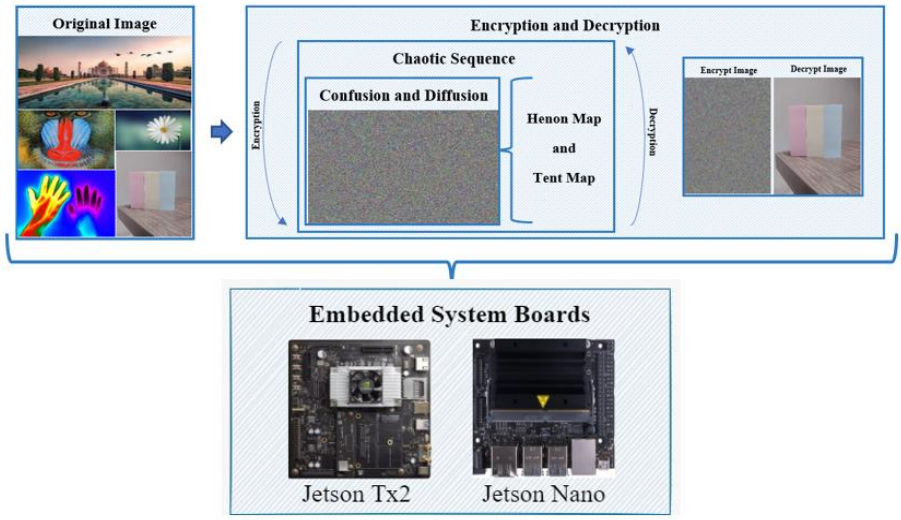


Figure 1. *An overview of the study*

In this study, image encryption is performed on two different embedded systems, which are Jetson TX2 and Jetson Nano, using Henon and Tent chaotic maps, and the results are obtained by comparing the two systems. The rest of the study is structured as follows. The chaos-based cryptosystems used are discussed in Section 2 and used chaotic systems are given. The encryption and decryption process with confusion and diffusion are detailed in same section in addition to embedded systems. The performance of our proposed cryptosystem in terms of security analyses and experimental results are submitted in Section 3. Conclusions are given in Section 4. An overview of the study is given in Figure 1.

II. MATERIAL AND METHODS

Image encryption has different requirements than text encryption. Alternatively, chaos theory and chaotic maps are well suited for chaos-based encryption. With simple equations, pixel confusion and diffusion operations, which are the requirements of image encryption, can be easily performed. In this paper, an image encryption application is carried out on embedded system platforms with the help of confusion and diffusion processes by using Tent and Henon chaotic maps in the literature.

A. CHAOTIC SYSTEMS

In this study, Henon and Tent maps, which are chaotic maps used for image encryption, are introduced and used within the scope of the study.

A. 1. Henon Map

Henon suggested in 1976 a 2-D chaotic system that was presented as a simplified solution of the Poincare map for the Lorenz model, which includes a chaotic attractor and is represented by equations of state. [14]. The mathematical expression for the Henon map is given in Eqs. (1) and (2):

$$x_{i+1} = y_{i+1} + 1 - \alpha x_i^2 \quad (1)$$

$$y_{i+1} = \beta x_i \quad (2)$$

The parameters required for the initial values x_0 and y_0 to be chaotic are α=1.4 and β=0.3. Each point is mapped to the x_i ve y_i point. A chaotic sequence x_i is obtained to maintain encryption process.

A. 2. Tent Map

Yoshida et al. published in 1983 an analytical investigation on the chaotic behaviours of the Tent map encompassing the entire chaotic region with regard to invariant density and power spectrum [15].

$$x_{n+1} = f_r(x_n) = \begin{cases} rx_n & , \ x_n < \frac{1}{2} \\ r(1 - x_n), & \frac{1}{2} \geq x_n \end{cases} \quad (3)$$

In Eq. (3), r is a positive real number. An x_n array is generated in the defined range [0, 1]. This generated sequence is a chaotic sequence which is used for encryption.

B. SCHEME OF ENCRYPTED SYSTEM

In this part, the image to be encrypted is selected as a 525x700 coloured paper photograph and implemented encryption processes. First, chaotic sequences are produced and the parameters used to produce these chaotic sequences are given in Table 1 for both Tent and Henon maps. Cloude Shannon emphasized in his article "Communication of hidden systems" that robust encryption methods should be built on confusion and diffusion techniques [16].

Table 1. *Parameters used in chaotic maps*

	Henon Map	**Tent Map**
r	-	1.9
α	1.4	-
β	0.3	-
x_0	0.9	0.52
y_0	0.5	-

Confusion is the technique of concealing the connection between the key and the plain text or image. It is typically accomplished through substitution approaches. The goal of confusion is to eliminate the statistical association between blocks of plaintext and ciphertext. Diffusion is the action of a single symbol of plaintext on many symbols of ciphertext. The purpose of using this technique is to conceal the statistical features of plain text. Thus, although the cryptanalyst can analyse similar plaintext and ciphertext pairs, no guesswork can be made about the plaintext corresponding to the ciphertext. The generated chaotic sequences are used first to confusion the image and then to provide the diffusion stage. The encryption diagram is shown in Figure 2.

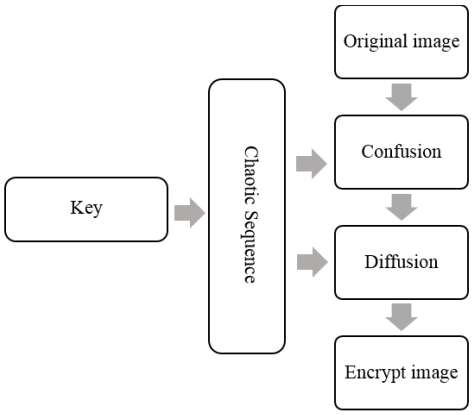


Figure 2. *Architecture of an image cryptosystem based on chaos*

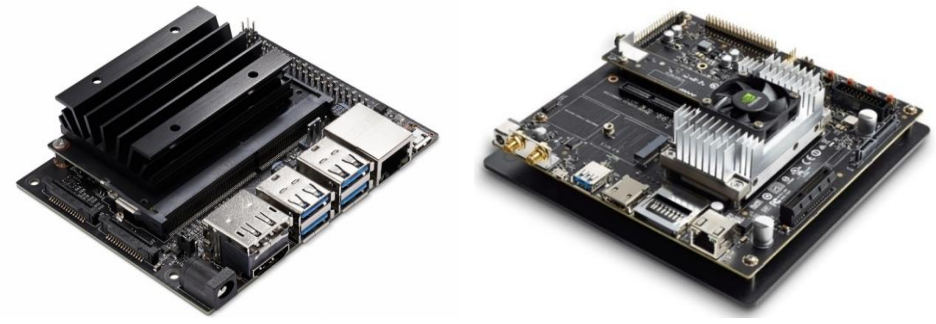
Decryption relies on chaotic maps, and the XOR operation can be reversed. Applying confusion and diffusion processes to the same keys performs decryption. In other words, the decryption procedure involves applying encryption steps in reverse order, beginning with the final one. The reverse diffusion process is used to return the coded image produced by the confusion step to its state prior to diffusion. Assuming that the size of our chaotic arrays image used in the mixed part in the study is *N*M*, *N*M* chaotic values are obtained. The image is mixed by using the indices obtained while ranking these values, then the diffusion stage is provided by the XOR process. On the other hand, on the reverse side, the confusing image is found by performing XOR operation on the opposite side, the solving function is performed with the indices produced from the same chaotic map, and the decrypted image is obtained.

C. EMBEDDED SYSTEM

Today, the use of embedded systems is increasing widely. In this part, the encryption application is carried out on the Jetson TX2 and Jetson Nano embedded board by taking advantage of the various features offered by the embedded systems. This study proposes an enhanced cryptographic method with a high level of security and high speed thanks to Jetson Nano and Jetson TX2. Figure 3 shows the Jetson Nano and Jetson TX2 embedded system that is used. Development kits features are given Table 2.

Table 2. *Jetson Development Kits Features*

	Jetson TX2	**Jetson Nano**
GPU	GPU NVIDIA Pascal,256 CUDA cores	NVIDIA Maxwell, 128 CUDA cores
CPU	Dual-core Denver 2 64-bit + Quad-core ARM Cortex-A57 MPCore	Quad-core ARM Cortex-A57 MPCore
Memory	Memory 8 GB 128-bit LPDDR4	4 GB 64-bit LPDDR4
Display	2x DSI, 2x DP 1.2. HDMI 2.0, eDP 1.4	HDMI 2.0, DP 1.2, eDP 1.4, 2x DSI
USB	USB 3, USB 2	USB 3, USB 2
Connectivity	1 Gigabit Ethernet, 802.11ac WLAN, Bluetooth	Gigabit Ethernet
Mechanical	50mm x 87mm	45mm x 70mm

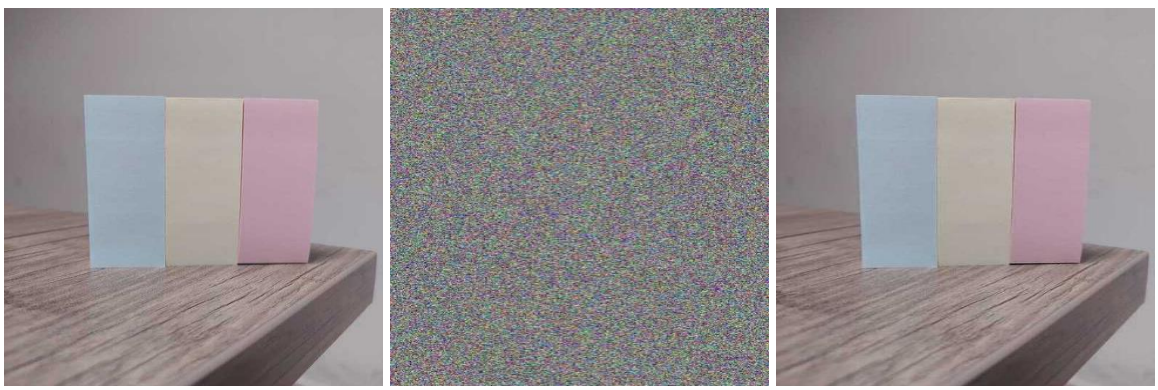


(a) ***(b)***

Figure 3. (a) *Jetson Nano* ***(b)*** *Jetson TX2*

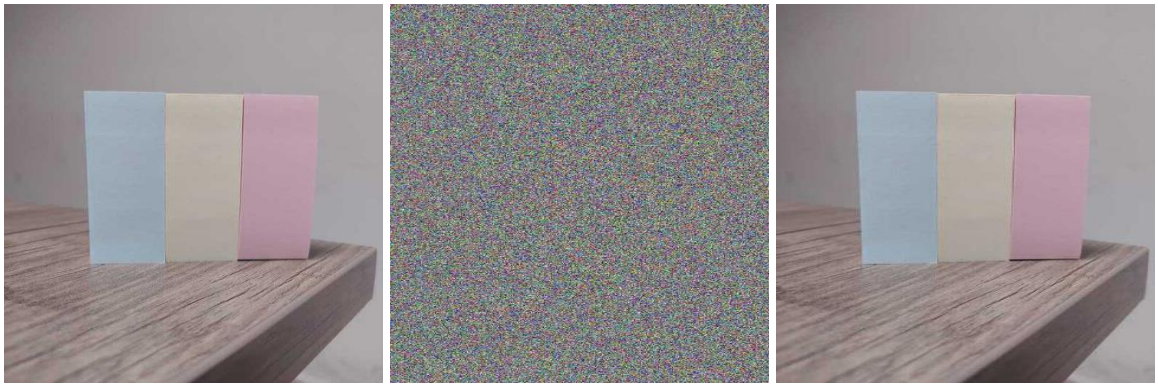
III. EXPERIMENTAL RESULTS

In this part, a confusion and diffusion-based image encryption method is designed and implemented in real-time on Jetson TX2 and Jetson Nano embedded systems using Henon and Tent chaotic maps. As it is known from the results obtained from the studies in the literature that a good encyryption process should be strong against all cryptanalytic, statistical, and brute force attacks. Performance and security analyses are presented by comparing the results of the encryption process with the information of the original image. The image used in the experiment is original and the encrypted and decoded versions of the image for Tent map are given in Figure 4a, 4b and 4c, respectively and their images for Henon map are given in Figure 5a, 5b and 5c, respectively.



(a) ***(b)*** ***(c)***

Figure 4. (a) *Original Image* ***(b)*** *Encrypted image* ***(c)*** *Decrypted image for Tent map*



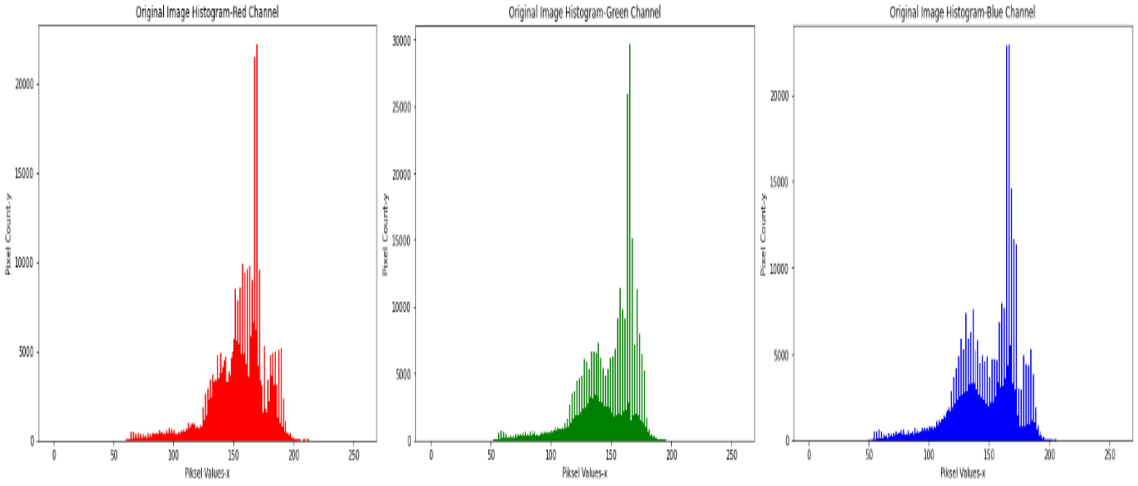
(a) ***(b)*** ***(c)***

Figure 5. (a) *Original Image* ***(a)*** *Encrypted image* ***(a)*** *Decrypted image for Henon map*

The quality of an encryption system is directly proportional to the ability of encryption and decryption with appropriate performance and the inability of the unauthorized system to obtain information about the plain image. Encryption is performed for an image using the embedded system platform, as a result of the experiment, the results are obtained by looking at the security tests separately such as histogram correlation analysis and key sensitivity analysis. These test analyses are given below under separate headings.

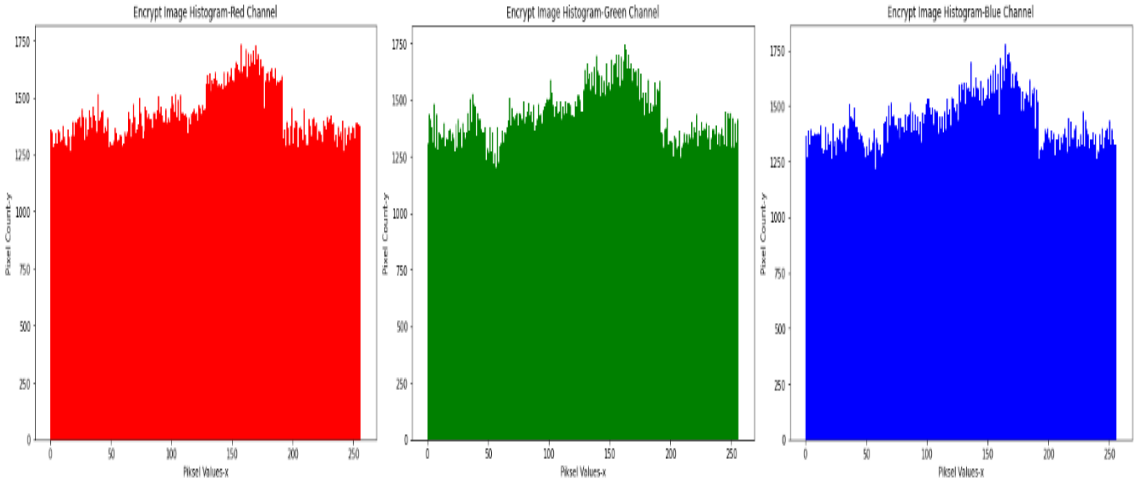
A. HISTOGRAM ANALYSES

In histogram analysis, a histogram graphically displays the number of colour values in a numerical image. As can be seen from the histogram graphs in Fig. 6, chaos-based confusing produces an encrypted image with a histogram graph that is nearly linear in character and regularity, despite the fact that the histogram information of the plain image remains unchanged. Some statistical characteristics of the original image are retained even though the pixels are mixed solely during the confusion step. Secure encryption can be accomplished with fewer cycles during the diffusion stage since the pixel values change. Figures 6, and 8 show the RGB (Red-Blue-Green) channel histogram graphs of original images for Tent and Henon map, respectively. Likewise, Figures 7, and 9 show the RGB (Red-Blue-Green) channel histogram graphs of the encrypted images for Tent and Henon map, respectively.



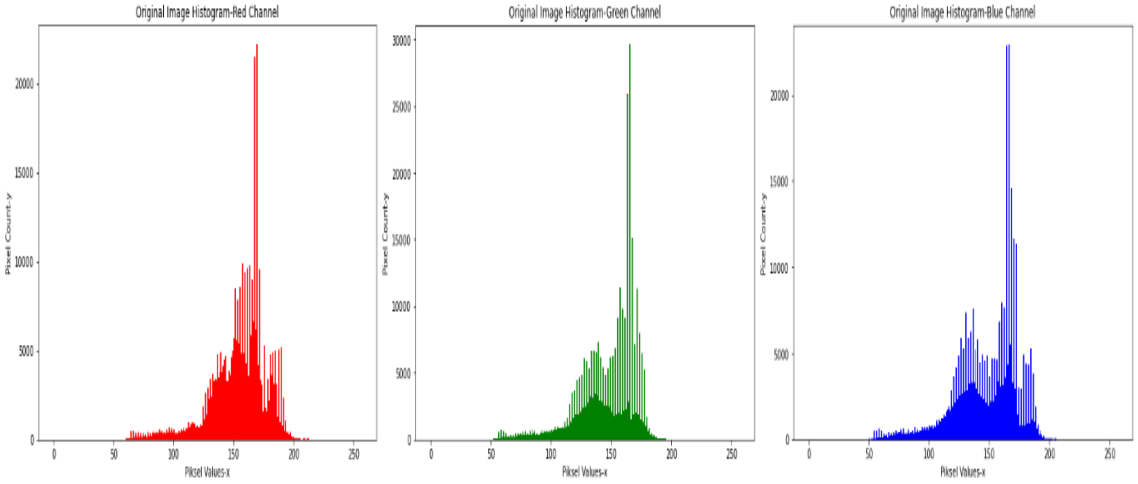
(a) ***(b)*** ***(c)***

Figure 6. (a) *Red channel,* ***(b)*** *Green channel and* ***(c)*** *Blue channel histogram plot of original image for Tent map*



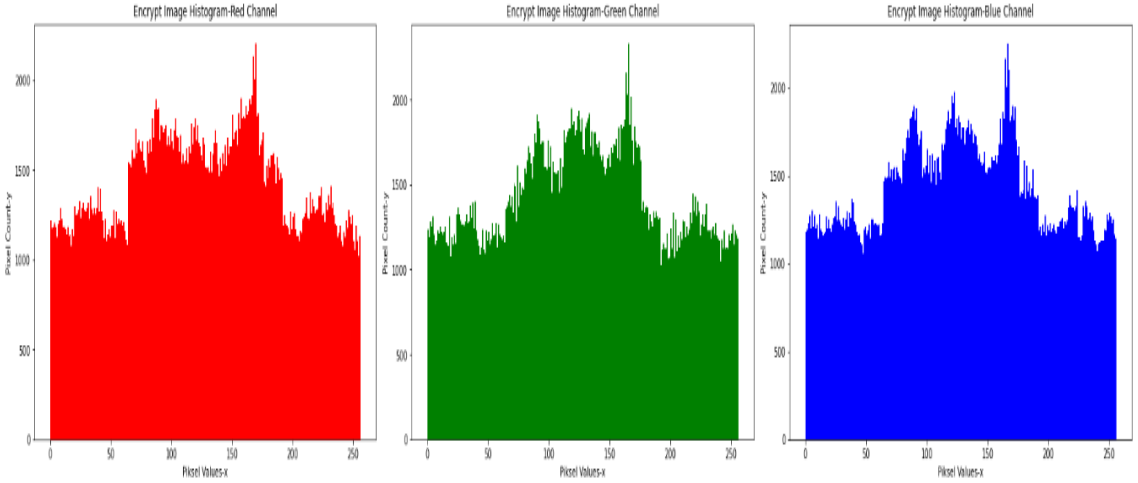
(a) ***(b)*** ***(c)***

Figure 7. (a) *Red channel* ***(b)*** *Green channel* ***(c)*** *Blue channel histogram plot of encrypted image for Tent map*



(a) ***(b)*** ***(c)***

Figure 8. (a) *Red channel* ***(b)*** *Green channel* ***(c)*** *Blue channel histogram plot of original image for Henon map*

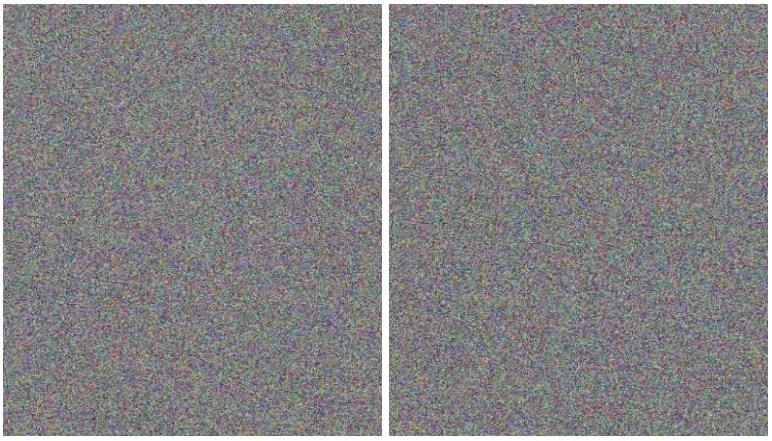


(a) ***(b)*** ***(c)***

Figure 9. (a) *Red channel* ***(b)*** *Green channel* ***(c)*** *Blue channel histogram plot of encrypted image for Henon map*

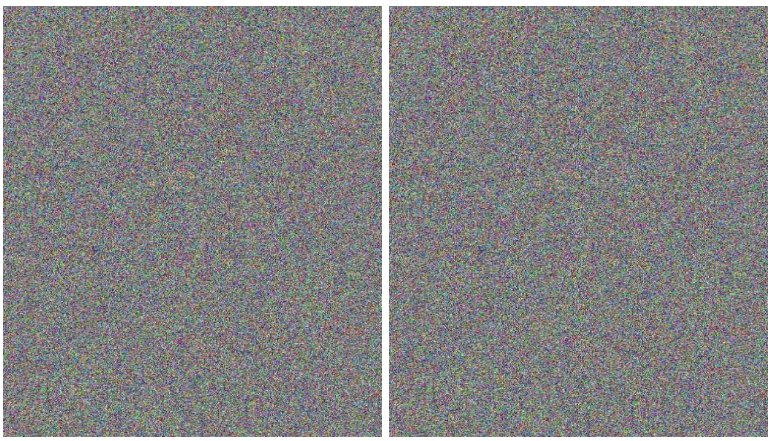
B. KEY SENSITIVITY ANALYSIS

A robust encryption system should be sensitive to small modifications to encryption and decryption keys. During the encryption phase, the encrypted image resulting from a minor change in the encryption key should be significantly different from the real encrypted image.



(a) ***(b)***

Figure 10. (a) *Image encrypted with key 0.52* ***(b)*** *Decrypted image with key 0.520000001 for Tent map*



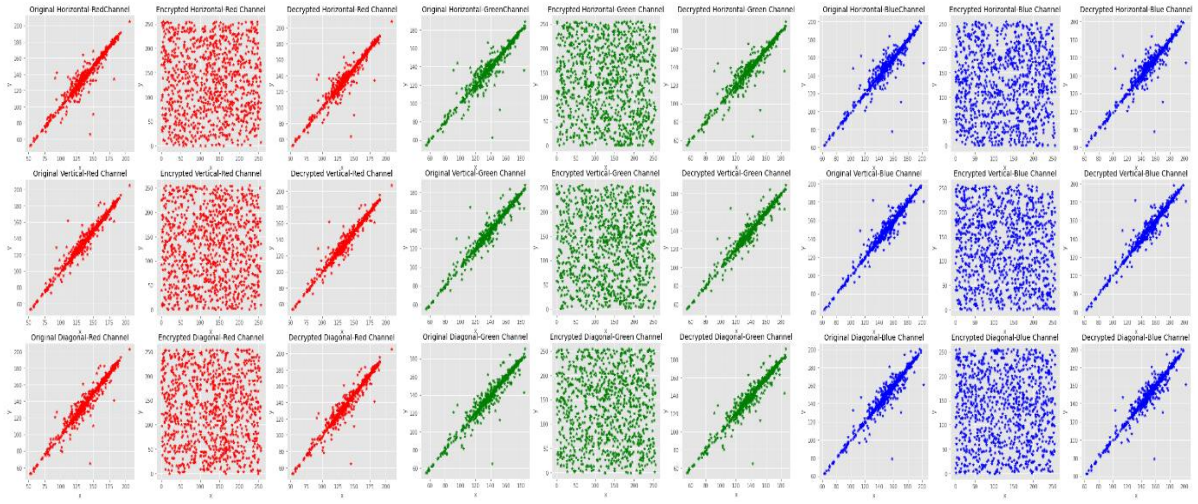
(a) ***(b)***

Figure 11. (a) *Image encrypted with key (0.1, 0.1)* ***(b)*** *Decrypted image with key (0.1, 0.10000001) for Henon map*

Similarly, when decryption is conducted using the new key obtained with a very small change in the decryption key, there should be no statistical similarities between the newly produced plain image and the plain image. Encryption and decryption tests closely related to keys demonstrate that the system is sensitive to the smallest variation in secret keys. Figure 10 illustrates the images, which are image encrypted image with keys 0.52 and decrypted image with key 0.520000001 for Tent map. Figure 11 shows image encrypted with keys (0.1, 0.1) and decrypted image with key (0.1, 0.10000001) for Henon map.

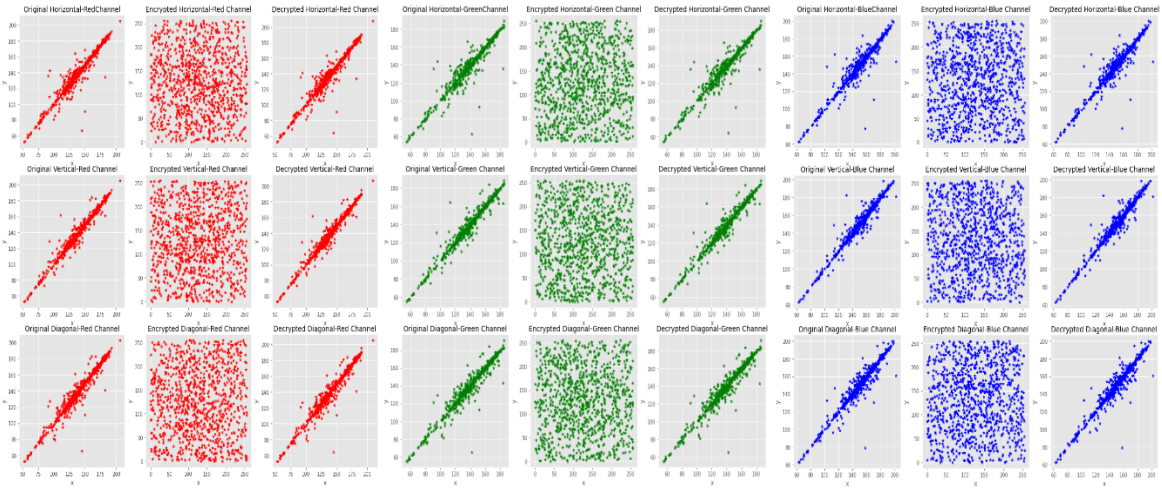
C. CORRELATION ANALYSIS

The concept of correlation shows the direction and magnitude of the linear relationship between two random variables in probability theory and statistics [17]. A statistical measure that determines the strength of the association between the relative movements of two variables is the correlation coefficient. The correlation coefficient indicates the magnitude and direction of the relationship between two independent variables. This coefficient has a range between (-1) and (+1). Positive values represent a direct linear relationship, whereas negative values represent an inverse linear relationship. The correlation coefficient is equal to zero if there is no linear relationship between the variables.



(a) ***(b)*** ***(c)***

Figure 12. (a) *Correlation scatter plots of the red channel original, encrypted and decoded image* ***(b)*** *Correlation scatter plots of the green channel original, encrypted and decoded image* ***(c)*** *Correlation scatter plots of the blue original, encrypted and decoded image for Tent map*



(a) ***(b)*** ***(c)***

Figure 13. (a) *Correlation scatter plots of the red channel original, encrypted and decoded image* ***(b)*** *Correlation scatter plots of the green channel original, encrypted and decoded image* ***(c)*** *Correlation scatter plots of the blue original, encrypted and decoded image for Henon map*

The correlation coefficients between neighbouring pixels in a plain image are large and approach one. Typically, in encrypted images, it is small and close to zero. A good encryption system should eliminate the associations between neighbouring pixels in the original image as much as possible in the encrypted image. Figs. 12 and 13 depict the graphical representation of the correlation coefficient analysis performed on both Tent and Henon map. The figures clearly show that the linear pixel relationship in the plain image does not exist in the encrypted image. Table 3 compares the correlation coefficients of the images encrypted using chaos-based confusion in this study's encryption technique. This table also contains comparisons of the correlation coefficients calculated according to the horizontal, vertical, and diagonal neighbourhoods of the encrypted and decrypted image.

Table 3. *Horizontal, vertical and diagonal correlation values of the original and encrypted image*

Chaotic system	Channel	Original horizontal correlation	Original vertical correlation	Original diagonal correlation	Encrypt horizontal correlation	Encrypt vertical correlation	Encrypt diagonal correlation
Henon Map	Red	0.976304	0.988193	0.980054	-0.022306	0.034636	0.024162
	Green	0.972751	0.986124	0.977173	0.055811	0.000389	-0.003229
	Blue	0.967131	0.983732	0.971970	0.031365	-0.031104	0.045122
Tent Map	Red	0.976304	0.988193	0.980054	0.002077	0.008482	-0.038856
	Green	0.972751	0.986124	0.977173	-0.048824	0.021482	0.010142
	Blue	0.967131	0.983732	0.971970	0.045343	-0.082980	-0.014627

Table 4. *Encryption and decryption times*

Embedded boards	Time	Tent Map	Henon Map
Jetson TX2	Encryption time (Second)	32.4822	31.1366
	Decryption time (Second)	32.6289	30.9536
Jetson Nano	Encryption time (Second)	45.1846	48.0252
	Decryption time (Second)	48.6594	43.1396

The encryption and decryption time of the system by encryption using both chaotic maps on embedded systems are presented and compared. According to Table 4, the embedded system board of the Jetson TX2 encrypts the images on both chaotic maps in less time. Compared to other chaotic maps, Henon map in the encryption part performed on Jetson TX2 and Tent map in the encryption part performed on Jetson Nano encrypt data in less time. Similarly, when the decryption components are analysed, the application using the Henon map for both embedded system boards is decrypted in a shorter time.

IV. CONCLUSION

In the article, an image encryption application based on confusion and diffusion methods using Henon and Tent maps is performed in real time on both Jetson TX2 and Jetson Nano embedded systems. It is observed that the proposed scheme efficiently encodes the plain image in the confusion and diffusion process. Security tests including histogram analysis, correlation analysis, and key sensitivity analysis have been performed and the results are presented. All experimental results show that the proposed encryption scheme is secure due to its high sensitivity to plain images. The proposed encryption scheme is easy to process and can also be applied to any images with unequal width and height. The proposed system has been examined for chaotic maps both on the Jetson TX2 and Jetson Nano embedded system boards, and the results are presented comparatively. The results obtained make the proposed scheme a potential candidate for encryption of multimedia data such as images, sounds, and even videos.

V. REFERENCES

[1] Nadhom, M., & Loskot, P., "Survey of public data sources on the Internet usage and other Internet statistics," *Data in brief*, vol. *18*, pp. 1914-1929, 2018.

[2] Belazi, A., Abd El-Latif, A. A., & Belghith, S., "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155-170, 2016.

[3] Baker, G. L., & Gollub, J. P., "Chaotic dynamics: an introduction," *Cambridge university press*, (1996).

[4] Lian, S., “Efficient image or video encryption based on spatiotemporal chaos system,” *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2509-2519, 2009.
[5] Gao, T., & Chen, Z., “Image encryption based on a new total shuffling algorithm” *Chaos, solitons & fractals*, vol. 38, no. 1, pp. 213-220, 2008.
[6] Wang, X. Y., & Yu, Q., “A block encryption algorithm based on dynamic sequences of multiple chaotic systems,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 2, pp. 574-581, 2009.
[7] Teh, J. S., Alawida, M., & Sii, Y. C., “Implementation and practical problems of chaos-based cryptography revisited,” *Journal of Information Security and Applications*, vol. 50, pp. 102421, 2020.
[8] Veena, G., & Ramakrishna, M., “A survey on image encryption using chaos-based techniques,” *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 1, pp. 379-384, 2021.
[9] Kocarev, L., & Jakimoski, G., “Logistic map as a block encryption algorithm,” *Physics Letters A*, vol. 289, no. 4-5, pp. 199-206, 2001.
[10] Tong, X. J., Wang, Z., Liu, Y., Zhang, M., & Xu, L. “A novel compound chaotic block cipher for wireless sensor networks,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 22, no. 1-3, pp. 120-133, 2015.
[11] El Assad, S., Farajallah, M., & Vladeanu, C., “Chaos-based block ciphers: An overview,” *In 2014 10th International Conference on Communications (COMM)*, pp. 1-4, IEEE, 2014.
[12] Chen, G., Mao, Y., & Chui, C. K., “A symmetric image encryption scheme based on 3D chaotic cat maps,” *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749-761, 2004.
[13] Hraoui, S., Gmira, F., Jarar, A. O., Satori, K., & Saaidi, A., “Benchmarking AES and chaos based logistic map for image encryption,” *In 2013 ACS International Conference on Computer Systems and Applications (AICCSA)*, pp. 1-4, IEEE, 2013.
[14] Hénon, M., “A two-dimensional mapping with a strange attractor*,” In The theory of chaotic attractors*, pp. 94-102, Springer, New York, 2004.
[15] Yoshida, T., Mori, H., & Shigematsu, H., “Analytic study of chaos of the tent map: band structures, power spectra, and critical behaviors,” *Journal of statistical physics*, vol. 31, no. 2, pp. 279-308, 1983.
[16] Shannon, C. E., “Communication theory of secrecy systems” *The Bell system technical journal*, vol. 28, no. 4, pp. 656-715, 1949.
[17] Bandyopadhyay, S. K., Bhattacharyya, D., & Das, P., “Handwritten signature recognition using departure of images from independence” *In 2008 3rd IEEE Conference on Industrial Electronics and Applications*, pp. 964-969, IEEE, 2008.