MATHEMATICAL MODELING AND COMPUTING, Vol. 11, No. 3, pp. 883–892 (2024)

Color image encryption using chaotic-based cryptosystem

Mamat A. R.[1], Mohamed M. A.[1], Abidin A. F. A.[1], Mohamed R. R.[2], Sambas A.[1,3], Rusyn V.[4], Lisnichuk A. Ye.[5], Markovych B. M.[5]

[1] *Universiti Sultan Zainal Abidin Gong Badak, 21300 Kuala Nerus, Terengganu Darul Iman, Malaysia*
[2] *Universiti Tenaga Nasional, 43000 Kajang, Selangor, Malaysia*
[3] *Universitas Muhammadiyah Tasikmalaya, Jl. Tamansari No.KM 2.5, Mulyasari, Kec. Tamansari, Kab. Tasikmalaya, Jawa Barat 46196, Indonesia*
[4] *Yuriy Fedkovych Chernivtsi National University, 2 Kotsjubynsky Str., Chernivtsi, 58012, Ukraine*
[5] *Lviv Polytechnic National University, 12 S. Bandera Str., 79013, Lviv, Ukraine*

(Received 14 March 2024; Revised 26 September 2024; Accepted 28 September 2024)

This paper presents research on a proposed project involving image encryption using a chaotic-based cryptosystem. The purpose is to create an image encryption environment with additional features derived from chaos theory. This cryptosystem applies the element of uncertainty and sensitivity to initial conditions. The encryption uses a symmetric key; generating a key is based on a chaotic map — a nonlinear mathematical function that exhibits uncertainty and randomness based on initial values. Any change in the initial conditions affects the function's outcome. Furthermore, this encryption aims to create a secure image-sharing environment over a public network, as image or text data can be intercepted or eavesdropped on by unauthorized users. A comparison based on image histogram analysis, pixel changes between the original and encrypted images, and encryption and decryption calculations were performed, demonstrating that the plain image differs from the encrypted image.

Keywords: *chaos theory; Rossler system; chaotic cryptosystem; image encryption; RGB.*
2010 MSC: 34A34, 65P20, 94A15, 94A60 **DOI:** 10.23939/mmc2024.03.883

1. Introduction

Data sharing has been the key to the success of many networked applications. In fact, the input and output data from a process need to be treated with the highest sensitivity, especially when dealing with applications involving government agencies such as military and police. The consequences of any compromise can be disastrous. This has triggered computer scientists and mathematicians to come up with the idea of masking the real message via cryptography. Cryptography is a multidisciplinary approach, formed from a combination of several academic disciplines (mathematics, computer science and electrical engineering). In order to work in this new field, the challenge is to propose a new cryptosystem that increases the security and reduces the potential for hackers to steal information [1]. Existing mathematical-based cryptosystems can be generalized into symmetric [2] and asymmetric systems [3, 4] which were founded over pure mathematics concepts. Only recently, a chaotic-based cryptosystem relying on chaotic theory was created. The chaotic system bears some properties such as sensitivity to initial conditions, topologically mixing and dense periodic orbit [5] making it a good candidate for cryptosystem [6]. A study of chaos is traced back to that of a non-linear dynamical system, which was largely applied to model real-world phenomena with the ability to predict future behavior. Many physical systems are known to be chaotic, while others were designed to be chaotic [7–16].

This research was partially funded by the Ministry of Education of Malaysia, grant number FRGS/1/2020/STG06/UNISZA/02/2 and Center for Research Excellence & Incubation Management, Universiti Sultan Zainal Abidin.

© 2024 Lviv Polytechnic National University

Chaos was made possible for cryptography and has been greatly studied for cryptography technique [17, 18]. Some studies found that earlier cryptosystems are either inefficient in terms of performance or weak in the scale of computational complexity and security [19–21]. In order to develop a secure image encryption technique, an encryption scheme relies upon a chaotic system for key generation (for encryption), and the key is then used as a chaotic sequence for offering pixel value confusion/diffusion, and finally, an arithmetic calculation (for decryption) is required to obtain the plain image from encrypted image and key generation from the chaotic sequence.

In this work, the development of image encryption using a chaotic-based cryptosystem is demonstrated and this cryptosystem uses a three-dimensional chaotic Rossler system [22],

$$\begin{cases} \dot{x} = -y - z, \\ \dot{y} = x - ay, \\ \dot{z} = b + z(x - c). \end{cases} \tag{1}$$

The chaotic behavior of the system for parameter values $a = b = 0.2$ and $c = 5.7$ is shown in Figure 1.

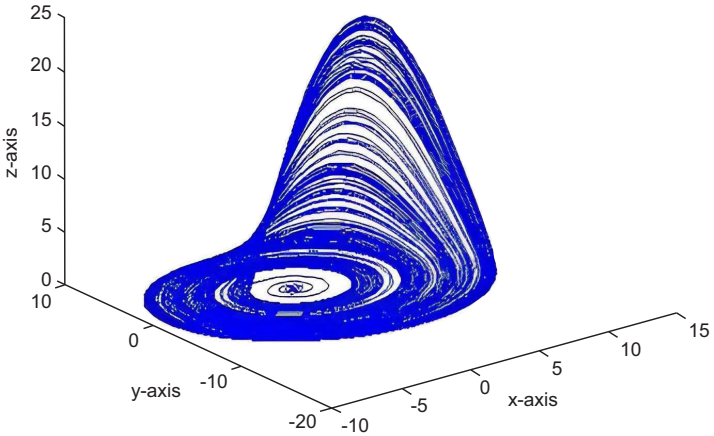

Fig. 1. Chaos attractor of the Rossler system.

Rossler system is chosen in order to obtain a three-dimensional large sequence of key generation. This key is restricted in the range of 0 to 255, to match the criteria of an 8-bit color image. Each pixel value for each channel is transformed into a decrypted value by some formula which offer confusion and diffusion properties to manipulate the original pixel. The Rossler Sequence Key Generation is performed on the basis of the y and z components of chaotic sequences of the Rossler system. The Rossler system is described in equation (1).

This paper is structured as follows. Section 1 briefly discusses the idea of image encryption based on a chaotic cryptosystem. Section 2 reviews some related works regarding chaotic cryptography in image encryption. Section 3 exposes an idea of our proposed image encryption algorithm whereas Section 4 exposes an idea for image decryption algorithm. Finally, the summary of the research is concluded in Section 5.

2. Related works

In this section, we present some of the works related to our study. It mingles around the requirement of this new encryption technique such as image encryption, chaos theory and application of chaotic maps in cryptosystems.

The first one is a proposal for a modified version of an advanced encryption standard (AES) algorithm for image encryption. The modification focuses on the ShiftRow transformations [23]. The modified version allows cyclic left shift of ShiftRow transformation to be symmetrical and varies in numbers based on row and column. The performance analysis has been recorded from the aspects of image histogram of encrypted image, information entropy analysis and correlation coefficient of two adjacent pixels in original and encrypted image [24]. This symmetric image encryption proves that new modified version of AES exhibits a significant improvement over the original AES. The timing performance was also measured, the modified AES showed some improvements in encryption time for various image sizes (pixels) of grey-scale images.

The second technique proposed, an image encryption based on a region basis and selective part of the image [25, 26]. This technique is based on previous work that uses position permutation technique

and value transformation technique [27]. Initially, a part of an image is identified and marked for selective encryption. In this region, there occurs encryption, permutation and construction of the encryption information that will be used as a header. An implementation of chaotic key algorithm was applied for both permutation and region encryption. The timing result was recorded by varying the number of block sizes. This proposal has its advantage, once the segmentation and permutation of region are completed, the regions are independently encrypted.

A third technique uses a transformation approach where the original image is divided into a number of blocks [28]. The technique comprises two stages, dividing the image into blocks of fixed size and shuffling the blocks by applying the matrix transformation, and then applying the bit rotation algorithm. This study was extended to image encryption using pixel and position manipulation technique [29] where the pixel is shuffled by block and the row is rearranged in bit-reversed order so that the position of rows seems manipulated.

All encryption techniques we surveyed have their advantages and disadvantages [30–32]. However, in the aspect of performance, the correlation between an original image and encrypted image should be reduced and the entropy increased.

3. Proposed encryption algorithm

This proposed chaos-based image encryption algorithm scheme comprises a few steps in its execution, where the image initially goes through channel separation, where encryption takes place at an individual channel with keys generated by chaotic behavior. Each encrypted channel is finally merged before transmitting to the receiving end.

Step 1: Image Channel Separation. Plain-image goes through a channel separation process to produce a file for each individual color channel. The purpose is to segregate the pixels for Red, Green and Blue Channels. An example of channel separation is shown in Figure 2.

Step 2: Chaos Sequence Key Generation. In this chaos sequence key generation, we used equation (1) from Rossler system. The purpose application of Rossler system in this encryption is to generate a chaos sequence to serve as encryption keys. Figure 3 shows a sequence of chaos key generation for 4 different color channels. Each column in the sequence represents Red, Green, Blue and also Alpha channels respectively.

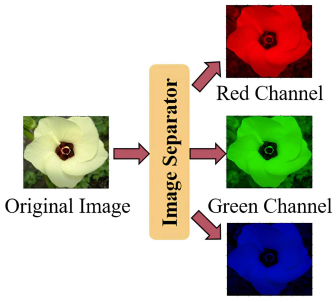

Fig. 2. Image channel separation.

rosslersequence.txt

```
1.067662475317391974 -6.7932351343874826 1.020842774913646188 1.01
1.13544578387638012 -6.8058188539698392 1.021653119338823267 1.02
1.20334370889404219 -6.8177486761322994 1.022433892158506739 1.029999999999999999
1.27134998153515966 -6.8290221757826171 1.023187740277564334 1.040000000000000001
1.33945828351889906 -6.839636985974086 1.023917116641636239 1.050000000000000003
1.4076622495593557 -6.8495907985045541 1.024624296692631303 1.059999999999999998
1.47595546965463431 -6.8588813644929809 1.025311393403736 1.070000000000000007
1.544331491237797 -6.8675064949349309 1.025980371023347573 1.080000000000000002
1.61278382120178898 -6.8754640612382918 1.026633057645171276 1.089999999999999997
1.68130592780934851 -6.8827519957403798 1.027271156710739274 1.100000000000000001
1.74989124249790706 -6.8893682922074957 1.027896257540684231 1.11
1.81853316158857681 -6.8953110063178995 1.028509844982142627 1.12
1.88722504790750112 -6.9005782561290898 1.029113308251563663 1.13
1.95596023232709448 -6.9051682225301976 1.029707949044880319 1.140000000000000001
1.0247320152340218 -6.9090791496802302 1.030294988980380536 1.14999999999999999
1.0935336679301508 -6.9123093454328357 1.030875576433629762 1.16
1.1623584339721502 -6.9148571817482081 1.031450792818379252 1.170000000000000001
1.2311995304549004 -6.916721095092691 1.032021658362491615 1.179999999999999999
1.3000501492434182 -6.9178995868265991 1.032589137423476036 1.19
1.3689034581575803 -6.9183912235807208 1.033154143384205088 1.200000000000000001
1.4377526021135414 -6.9181946376219345 1.033717543165742603 1.209999999999999999
1.506590704225403 -6.9173085272083377 1.034280161390910988 1.22
```

Fig. 3. Rosslers' chaos sequence generation.

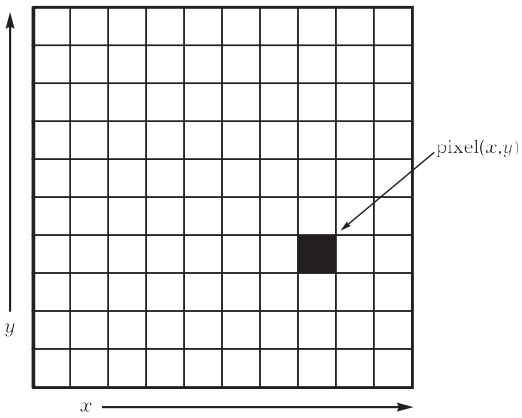

Fig. 4. Pixels illustration.

The key provided by this equation will be used throughout the processes of encryption and decryption. The encryption will take place pixel-by-pixel for each R, G, and B channels. Figure 4 shows an illustration where the encryption happened. Based on Figure 4, consider x as the row and y as the column, the encryption occurs in every image channel(x, y) where every single pixel is affected in this encryption.

Step 3: Channel Encryption. For this part, we will see how Red, Green, Blue and Alpha channels are affected by this encryption with Alpha channel taking the value of each pixel from original image. Figure 5 shows an example of encryption for the three separate channels,

$$\text{Encryption} = (\text{RosslerSequenceChannel} * 256) * (\text{NextChannel} - \text{RosslerSequenceChannel}). \tag{2}$$

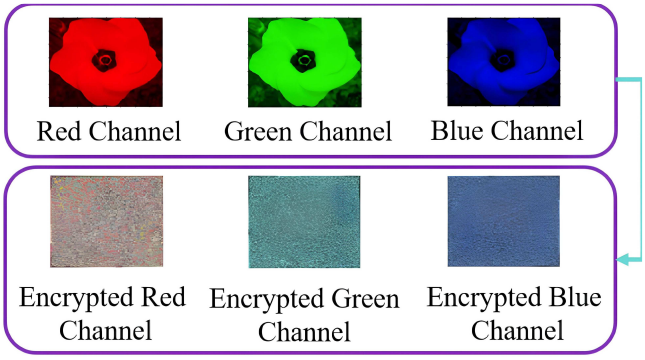

Fig. 5. Concept for encryption image channels.

The general encryption formula used is shown in equation (2). This encryption requires variables from the Rossler Sequence and pixel values from each channel. We expand the equation for each channel into the following:

$$\begin{aligned}
\text{EncryptedRedChannel} &= (\text{RosslerSeqRedChannel} * 256) \\
&\quad * (\text{GreenChannel} - \text{RosslerSeqRedChannel}), \\
\text{EncryptedGreenChannel} &= (\text{RosslerSeqGreenChannel} * 256) \\
&\quad * (\text{RedChannel} - \text{RosslerSeqGreenChannel}), \\
\text{EncryptedBlueChannel} &= (\text{RosslerSeqBlueChannel} * 256) \\
&\quad * (\text{AlphaChannel} - \textit{RosslerSeqBlueChannel}), \\
\text{EncryptedAlphaChannel} &= (\text{RosslerSeqAlphaChannel} * 256) \\
&\quad * (\text{BlueChannel} - \text{RosslerSeqAlphaChannel}).
\end{aligned} \tag{3}$$

Let us use the pixel value at $(1, 1)$ from Figure 6 and apply in detailed formula presented in equation (3).

By using the data from the first line of Rosslers' Chaos Sequence Generation shown in Figure 3 and the channel values taken from Figure 6, we come to the following values,

$$\begin{aligned}
\text{EncryptedRedChannel:}\ & (1.0676625 * 256) * (137 - 1.0676625) = 36855, \\
\text{EncryptedGreenChannel:}\ & (-6.7932353 * 256) * (226 - (-6.7932353)) = -403448, \\
\text{EncryptedBlueChannel:}\ & (1.0208428 * 256) * (125 - 1.0208428) = 66033, \\
\text{EncryptedAlphaChannel:}\ & (1.01 * 256) * (255 - 1.01) = 31734.
\end{aligned} \tag{4}$$

This process takes place for every single pixel for each channel in the image, where the performance of encryption depends on how much pixel is being processed in order to encrypt the image.

Fig. 6. Pixel $(1,1)$ representation for `Lena.png`.

Step 4: Image Channel Merger. After each pixel has been encrypted, the encrypted image for each channel will look like Figure 7. Then all three image channels will be merged together to create an encrypted image in a complete RGB Channels as shown in Figure 7.

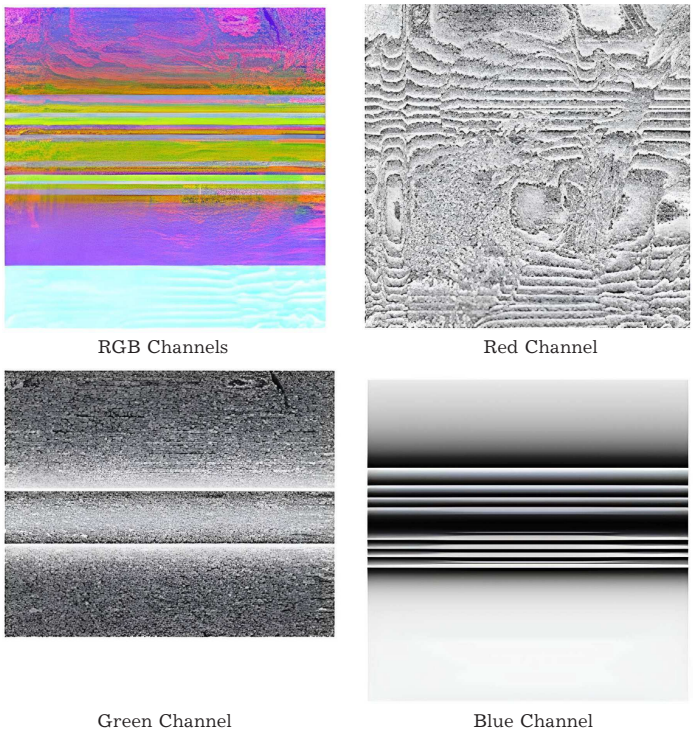

Fig. 7. `Lena.png` after encryption in 3 different channels.

Step 5: Cipher-Image and Key Distribution. As the process for Image Channels Merger is completed, the user will obtain two files, the encrypted images and the key. These two are compulsory in order to decrypt the encrypted image by the receiver. Figure 8 illustrated a general understanding of the encryption process.

Fig. 8. Overview for cipher-image and key distribution.

4. Proposed decryption algorithm

Decryption is a reverse process in order to acquire the original image from an encrypted image using the key that has been distributed. Since this cryptosystem is based on symmetric key encryption, the encrypted image can only be decrypted using the key as used for encryption. The steps required in the decryption process are, acquiring the encrypted image accompanied with the key that has been distributed, image channel separation, reverse channel encryption, and image channel merging to recover the original image.

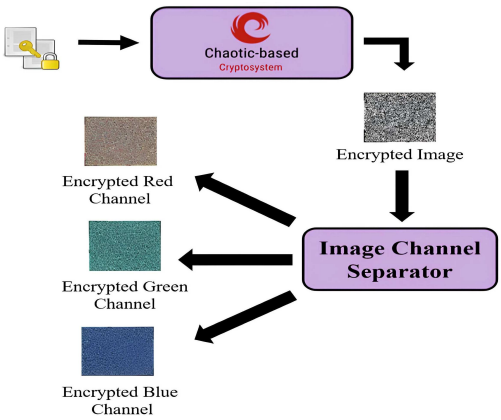

Fig. 9. Operation for input cipher-image, key and image channel separation.

Step 1: Input Cipher-image, Key and Image Channel Separation. The first step shown in Figure 9 is about collecting encrypted images, and a symmetric key accompanied with. The validation process takes a turn where a header from the key will recognize their encrypted image. After that, the image channel separation process will be executed before the decryption algorithm is executed.

Step 2: Reverse Channel Encryption. Equation (5) shows the reverse encryption (decryption) calculation where the calculation can retrieve the original pixel that has been encrypted using equation (2),

$$\begin{aligned}\text{Decryption} = {} & \text{EncryptedNextChannel}/(\text{RosslerSequenceNextChannel} * 256) \\ & + \text{RosslerSequenceNextChannel}.\end{aligned} \tag{5}$$

This decryption requires variables from the Rossler Sequence and encrypted pixel values from each channel. We expand the equation for each channel into the following:

$$\begin{aligned}\text{DecryptedRed} &= \text{EncryptedGreen}/(\text{RosslerSeqGreen} * 256) + \text{RosslerSeqGreen}, \\ \text{DecryptedGreen} &= \text{EncryptedRed}/(\text{RosslerSeqRed} * 256) + \text{RosslerSeqRed}, \\ \text{DecryptedBlue} &= \text{EncryptedAlpha}/(\text{RosslerSeqAlpha} * 256) + \text{RosslerSeqAlpha}, \\ \text{DecryptedAlpha} &= \text{EncryptedBlue}/(\text{RosslerSeqBlue} * 256) + \text{RosslerSeqBlue}.\end{aligned} \tag{6}$$

A further calculation that uses variables from encrypted channel values produces the following,

$$\begin{aligned}\text{DecryptedRedChannel}: & -403448/(-6.7932353 * 256) + (-6.7932353), \\ \text{DecryptedGreenChannel}: & \ 36855/(1.0676625 * 256) + (1.0676625), \\ \text{DecryptedBlueChannel}: & \ 31734/(1.01 * 256) + (1.01), \\ \text{DecryptedAlphaChannel}: & \ 66033/(1.0208428 * 256) + (1.0208428).\end{aligned} \tag{7}$$

When the decryption process is done for all channels, it produces 3 images in 3 different channels.

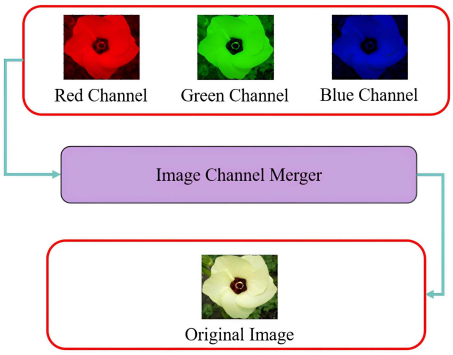

Fig. 10. Operation for Image Channel Merger.

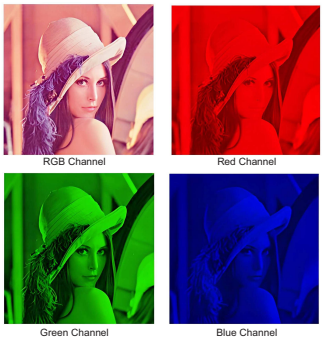

Fig. 11. Lena.png after Decryption in 3 Different Channels.

Step 3: Image Channel Merger and Plain-image. From the decryption process, the 3 channels are merged to create a single plain image which must be identical to the original image. The idea is to produce a plain image with RGB channels merged as shown in Figure 10.

Back to the decryption performed on `Lena.png`, Figure 11 shows the outcome of the decryption process. After individual channels have been merged, it produces the Lena.png in RGB channels intact together as a plain image.

5. Image analysis for encrypted image

This section discusses the two types of image analysis, image channel analysis and image histogram analysis.

5.1. Image channel analysis

In this analysis, the purpose is to observe how much the encryption process affects the pixel formation for each channel. The image to be analyzed is the encrypted image shown in Figure 12. The image channel analysis is performed in the ImageJ application. The result of the image analysis is shown in Figure 13. This analysis proved that every single encryption that occurred in the channels does not have any correlation between each pixel in different channels.

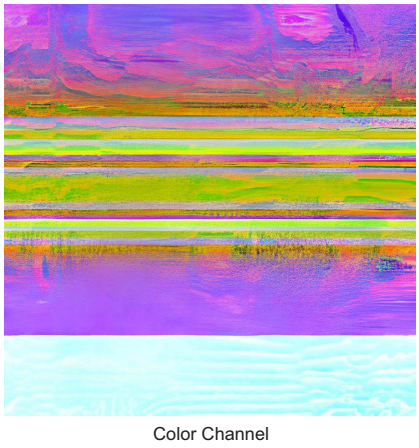

Fig. 12. Encrypted Image of `Lena.png`.

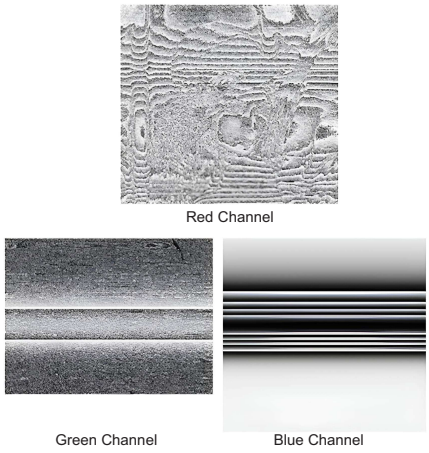

Fig. 13. Encrypted Channels of `Lena.png`.

5.2. Image histogram analysis

Image histogram analysis is the practice of studying and analyzing the context of the image via pixel density value. The pixel density is measured by the tonal value from 0 to 255 and how frequently does it occurs in the image. The purpose is to show that the Histogram for the original image and the encrypted image do not match in terms of pixel density and tonal value frequency. Figures 14 and 15 show the histogram analysis of the grayscale version of `Lena.png` for the original image and encrypted image respectively.

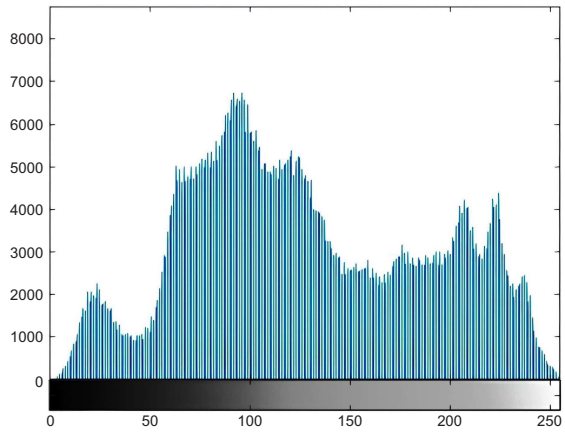

Fig. 14. Original Image — Grayscale Histogram Analysis.

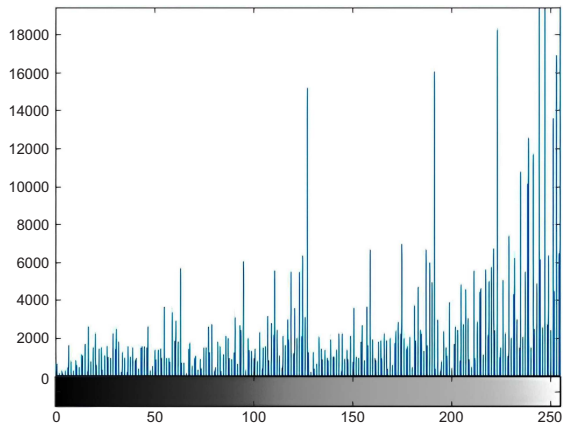

Fig. 15. Encrypted Image — Grayscale Histogram Analysis.

It is observable that there are no major similarities found in both histograms. Moreover, image histogram analysis for RGB channels is also performed. Figures 16 and 17 show the histogram for RGB channels for the original image and the encrypted image, respectively.

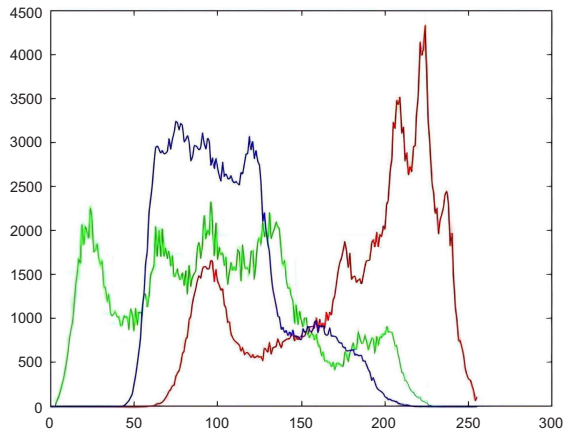

Fig. 16. Original Image — RGB Channels Histogram Analysis.

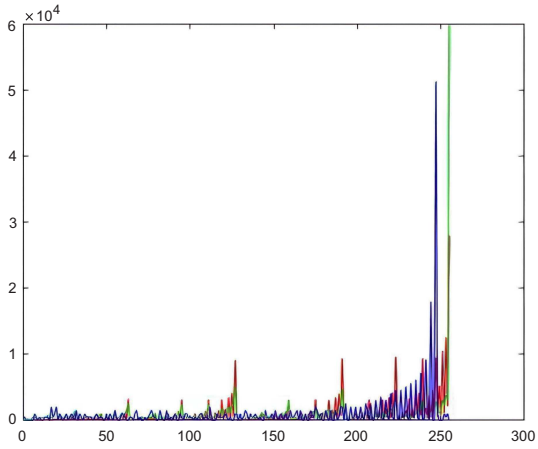

Fig. 17. Encrypted Image — RGB Channels Histogram Analysis.

6. Conclusion

This research focuses on the study of image encryption using a chaotic-based cryptosystem to ensure the confidentiality of the image is retained. We implemented the Rossler Equation where we use the Rossler Sequence to generate numbers to be used as variables to encrypt each color channel of an image. The result reveals the contribution of this paper.

[1] Li C., Lin D., Lu J. Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. IEEE MultiMedia. **24** (3), 64–71 (2017).

[2] Heron S. Encryption: Advanced Encryption Standard (AES). Network Security. **2009** (12), 8–12 (2009).

[3] Vahdati Z., Yasin S. M., Ghasempour A., Salehi M. Comparison of ECC and RSA Algorithms in IOT Devices. Journal of Theoretical and Applied Information Technology. **97** (16), 4293–4308 (2019).

[4] Mohamed M. A. A Survey on Elliptic Curve Cryptography. Applied Mathematical Sciences. **8** (154), 7665–7691 (2014).

[5] Liu Y., Chen L. A Survey of Chaos Theory. Chaos in Attitude Dynamics of Spacecraft. Springer, Berlin, Heidelberg (2013).

[6] Baptista M. S. Cryptography with chaos. Physics Letters A. **240** (1–2), 50–54 (1998).

[7] Chlouverakis K. E, Sprott J. C. Chaotic hyperjerk systems. Chaos, Solitons & Fractals. **28** (3), 739–746 (2005).

[8] Rusyn V., Mujiarto, Mamat M., Azharul M., Mada Sanjaya W. S., Sambas A., Dwipriyoko E., Sutoni A. Computer Modelling of the Information Properties of Hyper Chaotic Lorenz System and its Application in Secure Communication System. Journal of Physics: Conference Series. **1764** (1), 012205 (2021).

[9] Sambas A., Vaidyanathan S., Bonny T., Zhang S., Sukono F., Hidayat Y., Mamat M. Mathematical Model and FPGA Realization of a Multi-Stable Chaotic Dynamical System with a Closed Butterfly-Like Curve of Equilibrium Points. Applied Sciences. **11** (2), 788 (2021).

[10] Rusyn V., Subbotin S., Sambas A. Simple autonomous security system based on Arduino UNO platform and fingerprint scanner module: A study case. CEUR Workshop Proceedings. **2864**, 262–271 (2021).

[11] Pehlivan I., Uyaroglu Y. A new chaotic attractor from general Lorenz system family and its electronic experimental implementation. Turkish Journal of Electrical Engineering. **18** (2), 171–184 (2010).

[12] Rusyn V. Modeling and Research Information Properties of Rucklidge Chaotic System Using LabView. 2017 10th Chaotic Modeling and Simulation International Conference. 739–744 (2017).

[13] Sambas A., Mohammadzadeh A., Vaidyanathan S., Ayob A. F. M., Aziz A., Mohamed M. A., Nawi M. A. A. Investigation of chaotic behavior and adaptive type-2 fuzzy controller approach for Permanent Magnet Synchronous Generator (PMSG) wind turbine system. AIMS Mathematics. **8** (3), 5670–5686 (2023).

[14] Rusyn V., Mohamad M., Titaley J., Nainggolan N., Mamat M. Design, Computer Modelling, Analysis and Control of the New Chaotic Generator. Journal of Advanced Research in Dynamical & Control Systems. **12**, 2306–2311 (2020).

[15] Sambas A., Vaidyanathan S., Zhang S., Zeng Y., Mohamed M. A., Mamat M. A New Double-Wing Chaotic System with Coexisting Attractors and Line Equilibrium: Bifurcation Analysis and Electronic Circuit Simulation. IEEE Access. **7**, 115454–115462 (2019).

[16] Rusyn V., Khrapko S. Memristor: Modeling and Research of Information Properties. 11th Chaotic Modeling and Simulation International Conference. 229–238 (2019).

[17] Pecora L. M., Carroll T. L. Synchronization in chaotic systems. Physical Review Letters. **64** (8), 821–825 (1990).

[18] Lawande Q. V., Ivan B. R., Dhodapkar S. D. Chaos based cryptography: a new approach to secure communications. BARC Newsletter. **258**, 1–12 (2005).

[19] Alvarez G., Li S. Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption. Communications in Nonlinear Science and Numerical Simulation. **14** (11), 3743–3749 (2009).

[20] Cheng H., Li X. Partial encryption of compressed images and videos. IEEE Transactions on Signal Processing. **48** (8), 2439–2451 (2000).

[21] Rhouma R., Belghith S. Cryptanalysis of a new image encryption algorithm based on hyper-chaos. Physics Letters A. **372** (38), 5973–5978 (2008).

[22] Gaspard P. Rossler systems. Encyclopedia of Nonlinear Science. **231**, 808–811 (2005).

[23] Kamali S. H., Shakerian R., Hedayati M., Rahmani M. A new modified version of Advanced Encryption Standard based algorithm for image encryption. 2010 International Conference on Electronics and Information Engineering, V1-141–V1-145 (2010).

[24] Li S., Zheng X., Mou X., Cai Y. Chaotic encryption scheme for real-time digital video. Proceedings of SPIE – The International Society for Optical Engineering. **4666**, 149–161 (2002).

[25] Ravishankar K. C., Venkateshmurthy M. G. Region based selective image encryption. International Conference on Computing & Informatics. 1–6 (2006).

[26] Van Droogenbroeck M., Benedett R. Techniques for a selective encryption of uncompressed and compressed images. Advanced Concepts For Intelligent Vision Systems (ACIVS), Ghent, Belgium. 90–97 (2002).

[27] Yen J.-C., Guo J.-I. A New Chaotic Image Encryption Algorithm. IEEE Int. Conf. Circuits and Systems. **4**, 49–52 (2000).

[28] Gautam A., Panwar M., Gupta P. R. A new image encryption approach using block based transformation algorithm. International Journal of Advanced Engineering Sciences and Technologies. **8** (1), 90–96 (2011).

[29] Agung K., Fatmawati, Suprajitno H. Image encryption based on pixel bit modification. Journal of Physics: Conference Series. **1008**, 012016 (2018).

[30] Dey S. SD-EI: A cryptographic technique to encrypt images. 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). 28–32 (2012).

[31] Nag A., Singh J. P., Khan S., Ghosh S., Biswas S., Sarkar D., Sarkar P. P. Image encryption using affine transform and XOR operation. International Conference on Signal Processing, Communication, Computing and Networking Technologies. 309–312 (2011).

[32] Delei J., Sen B., Wenming D. An Image Encryption Algorithm Based on Knight's Tour and Slip Encryption-filter. 2008 International Conference on Computer Science and Software Engineering. 251–255 (2008).

Шифрування кольорового зображення за допомогою хаотичної криптосистеми

Мамат А. Р.[1], Мохамед М. А.[1], Абідін А. Ф. А.[1], Мохамед Р. Р.[2], Самбас А.[1,3], Русин В.[4], Ліснічук А. Є.[5], Маркович Б. М.[5]

[1] *Університет Султан Зайнал Абідін Гонг Бадак, 21300 Куала Нерус, Теренгану Дарул Іман, Малайзія*
[2] *Університет Тенага Національ, 43000 Каджанг, Селангор, Малайзія*
[3] *Університет Мухаммадія Тасікмалая, Тасікмалая, Ява Барат 46196, Індонезія*
[4] *Чернівецький національний університет імені Юрія Федьковича, вул. Коцюбинського, 2, 58012, м. Чернівці, Україна*
[5] *Національний університет "Львівська політехніка", вул. С. Бандери, 12, 79013, м. Львів, Україна*

У цій роботі представлено дослідження запропонованого проекту, що передбачає шифрування зображень за допомогою хаотичної криптосистеми. Мета полягає в тому, щоб створити середовище шифрування зображень з додатковими функціями, отриманими з теорії хаосу. Ця криптосистема застосовує елемент невизначеності та чутливості до початкових умов. Шифрування використовує симетричний ключ; генерування ключа базується на хаотичній карті — нелінійній математичній функції, яка виявляє невизначеність і випадковість на основі початкових значень. Будь-яка зміна початкових умов впливає на результат функції. Крім того, це шифрування спрямоване на створення безпечного середовища для обміну зображеннями через загальнодоступну мережу, оскільки зображення або текстові дані можуть бути перехоплені або підслухані неавторизованими користувачами. Порівняння на основі аналізу гістограми зображення, зміни пікселів між вихідним і зашифрованим зображеннями, а також розрахунків шифрування та дешифрування було виконано, демонструючи, що звичайне зображення відрізняється від зашифрованого зображення.

Ключові слова: *теорія хаосу; система Росслера; хаотична криптосистема; шифрування зображень; RGB.*