



International Journal of Advanced Research in Computational Thinking and Data Science

Journal homepage:
<https://karyailham.com.my/index.php/ctds/index>
ISSN: 3030-5225



Colour Image Encryption and Decryption using Arnold's Cat Map and Henon Map

Siti Nurul Hatikah Mohammad¹, Arif Mandangan^{1,*}

¹ Mathematics Visualization Research Group, Faculty of Science and Natural Resources, Universiti Malaysia Sabah, Jalan UMS, 88400 Kota Kinabalu, Sabah, Malaysia

ARTICLE INFO

Article history:

Received 29 February 2024

Received in revised form 20 March 2024

Accepted 25 March 2024

Available online 15 April 2024

Keywords:

Arnold's cat map; Henon map; chaotic; quality image cipher

ABSTRACT

Image encryption plays a crucial role in securing sensitive visual information during transmission and storage. Throughout the encryption and decryption phases of images, the utilized ciphers exhibit substandard quality, resulting in the persistence of the original image. Consequently, the issues at hand stem from a deficiency in the quality of cipher image, thereby compromising the confidentiality level to an unsafe extent. This research explores the application of chaotic maps, specifically the Arnold Cat Map and Henon Map for the encryption and decryption of digital colour images. The encryption process involves applying the Arnold Cat Map and Henon Map to permute and diffuse pixel values, enhancing the confusion and diffusion properties essential for robust encryption. The study provides insights into the decryption efficiency and the ability to recover the original image from the ciphered version. This research contributes to the body of knowledge in colour image encryption techniques and offers a novel approach leveraging chaotic maps. The findings emphasize the importance of selecting suitable chaotic maps and their parameters to achieve a balance between security and image quality.

1. Introduction

Data and information are considered as valuable assets nowadays. When communicated, the way that anybody can see the information to an outside climate is the major issue. Data the elevated degree of safety vital for legitimate information security and protection isn't given by cloud specialist organizations [1]. To provide security, encryption and authentication systems are adopted by using the technology in private and public-key cryptography [2]. Data and information are communicated in various forms, including images.

The existence of digital images in contemporary applications, ranging from medical imaging and remote sensing to personal conferencing, emphasizes the importance of securing this visual data against unauthorized access and manipulation [3]. The exchange of information over public networks, such as the internet, requires the use of encryption methods to protect the confidentiality

* Corresponding Author.

E-mail address: arifman@ums.edu.my

and integrity of the transmitted image [4]. In the field of image encryption and decryption, the choice of cryptographic algorithm plays an important role in determining the security posture of the transmitted image. On the other hand, chaos theory is branch of mathematics with interdisciplinary area of scientific study that engrossed on underlying patterns and deterministic laws of dynamical systems that are highly sensitive to initial conditions [5]. Chaotic dynamics has sparked a lot of interest in mixing equipment and other process equipment both experimentally and numerically. In chaos theory, chaotic mixing is a process by which flow tracers develop into complex fractals under the action of a fluid flow [6].

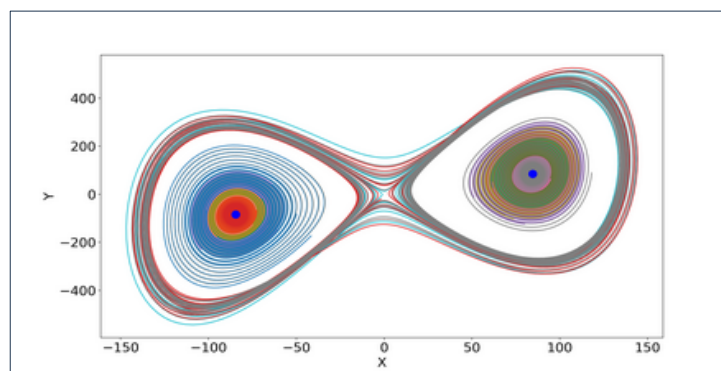


Fig. 1. Chaos production where period-doubling as the parameter r increases [7]

In cryptography, chaos theory is used for the development of deterministic nonlinear systems, that can be used to create random numbers for the encryption scheme based on chaotic map [8-10]. In this paper, we discovered the synergies between the Arnold Cat map and the chaotic Henon map, exploring their combined potential to improve encryption and decryption processes. The Arnold Cat map, known for its permutation properties, was used for confusion technique to rearrange pixel values, while the Henon chaotic map introduced dynamic elements to further increase the quality of cipher image [11]. The combination of these two chaotic Maps offers a new approach to strengthen the security of image encryption. By leveraging their distinctive properties, this study aims to address existing challenges in image encryption, such as the vulnerability of traditional algorithms to attacks and the need for improved visual inspection methods to assess the quality of encrypted images. Through these research efforts, the aim is to contribute to the advancement of image encryption techniques, with a particular focus on improving the quality of encryption and decryption processes. The combined exploration of Arnold and Henon is to achieve a robust cipher image, thereby improving the overall security framework for digital images in a wide range of applications.

In the study by Jithin and Syam [12] have proposed a color image encryption algorithm by combining Arnold maps, DNA sequence operations and Mandelbrot sets. This encryption mechanism is applied separately to the three channels (RGB) of a color image with a corresponding chaotic map. The method was also tested and the results obtaining the cipher image has a good quality due to the indicated change values. Generated cipher images are unlikely to be decrypted by an attacker because encryption is done using a random sequence of chaotic maps and large spaces of keys can eliminate brute force attacks.

In the paper Hu *et al.*, [13], a new color image encryption based on improvements to Henon maps called 2D-HHMSC to improve security and efficiency has been proposed. To prevent the algorithm from brute-force attacks, two hash functions were used to generate the parameters and prefix values of the Arnold Cat map and the 2D-HHMSC that generated the main column. This method can also prevent against common attacks and show solidity and reliability. The increased level of security and

efficiency of image encryption is reflected from this method, making it suitable for use in real-world applications. Furthermore, Ghorbani *et al.*, [14] has proposed a new Color Image encryption using Ribonucleic Acid (RNA) and Henon maps. In the permutation phase, 2D Henon maps are used to reshuffle pixel positions using initial values computed first by secret keys and subsequently by RNA recombination. Not only that, but the algorithm is also proposed and fully described in three phases, namely preparation, permutation, and diffusion. The results show that the proposed algorithm is sensitive to small changes in normal images and resistance to different attacks.

Therefore, the cryptosystem to be used in this study is by combining Arnold Cat map algorithm and Henon map for the purpose of encryption and decryption of images. The Arnold Cat map is a chaotic model map used for confusion while the Henon map is intended for diffusion. It is because, confusion techniques are not safe enough as past studies have shown that the distribution of Pixels will be the same as the original image [15]. In addition, the use of diffusion techniques is safe enough based on pixel diffusion, but the resulting image still looks dim. Hence, image encryption based on chaotic with the combination of confusion and diffusion methods will give higher quality and has two layers of security.

2. Methodology

2.1 Confusion using Arnold's Cat Map Algorithm

Arnold Cat Map (ACM) is a technique that will be used for confusion regarding the encryption and decryption of colour images. This map was chosen because it is a chaotic model used to randomize the pixel positions of an image. Confusion is the first pixel manipulation process performed using the system encryption of this image. Mathematically, this concept works by stretching and distorting the square shape and then rearranging it to shape the same [16]. The confusion technique in the selected ACM is the purpose to change the position of the image pixels randomly so that it does not look exactly like the original image. It works by randomizing the position of the pixels without changing the Pixel value itself. This technique is applied using the following formula in Equation (1):

$$\begin{bmatrix} x_{n'} \\ y_{n'} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \text{mod } N \quad (1)$$

At the beginning of the formation of the ACM, three parameters are required, namely, p , q , and the number of repetitions, which are all positive numbers and are obtained from the compilation number of the secret key. It can be defined as in Equation (2):

$$\begin{bmatrix} x_{n'} \\ y_{n'} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \text{mod } N \quad (2)$$

where $p, q \in \mathbb{R}^+$ are parameters,

N = Image size or dimension,

$x_{n'}$ and $y_{n'}$ = Pixel position, and

x_n and y_n = New pixel position.

2.2 Diffusion using Henon Map Algorithm

Henon maps are used to perform diffusion techniques for image encryption and decryption. The aim is to eliminate the correlation between the two regular images and cipher image that require no

change in the 1-bit regular image or at least half of the image-cipher bits should also occur changes [17]. It is a discrete dynamical system that shows good chaotic characteristics. Equations (3) and (4) define the Henon map:

$$x_{n+1} = 1 - \alpha x^2 + y_n \quad (3)$$

$$y_{n+1} = 1 - \beta x_n \quad (4)$$

where x_n and y_n = Current point position, and
 x_{n+1} and y_{n+1} = Position of the next point.

The slightest changes that occur on and in the initial conditions will have a significant impact on the formed map. The classic Henon map uses values and that causes the values to be chaotic. When changes occur to both values, it will cause a change in the properties of the resulting map that will cause it to no longer be chaotic.

2.3 Analysis Quality Image

2.3.1 Mean Squared Error (MSE)

MSE is the mostly deployed metric for measuring image quality. It is a full reference metric and values closer to zero are better. The error that occurs is due to the difference between the estimator and budget results. MSE for cipher image and the original image as $g(n, m)$ and $\hat{g}(n, m)$ can be defined as in Equation (5) [18]:

$$MSE = \frac{1}{M \times N} \sum_{n=1}^M \sum_{m=1}^N [\hat{g}(n, m) - g(n, m)]^2 \quad (5)$$

where $\hat{g}(n, m)$ = Values of plain image,
 $g(n, m)$ = Values of cipher image,
 $M \times N$ = Size of plain image,

2.3.2 Peak signal-of-noise-ratio (PSNR)

PSNR is used to calculate the ratio between the maximum possible signal power and the power of noise that interferes and affects the quality of the image. PSNR will be calculated as the logarithmic term of the decibel scale because the signal has a very wide dynamic range. This dynamic range varies between the largest and smallest values that may change according to their quality. A higher PSNR value means that the data loss in the decrypted image is zero, and this indicates that the decrypted image is identical to the original image. This indicates the high efficiency of encryption techniques. The following Equation (6) is used to calculate PSNR [19]:

$$PSNR = 10 \log_{10} \left[\frac{peakVal^2}{MSE} \right] \quad (6)$$

where $peakVal$ (peak value) is the maximum in the image data. If it is 8-bit integer data, then the value for $peakVal$ is 255.

2.3.3 Structural Similarity Index Measure (SSIM)

SSIM and it is a metric used to quantify the similarity between two images. SSIM deliberates luminance, contrast, and structure, providing a more comprehensive assessment of image quality compared to traditional metrics like Mean Squared Error (MSE). The SSIM index is calculated using the following formula in Equation (7):

$$SSIM(x, y) = \frac{(2 \mu_x \mu_y + c_1)(2 \sigma_{xy}^2 + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (7)$$

where μ_x = the average of x ,
 μ_y = the average of y ,
 σ_x^2 = the variance of x , and
 σ_y^2 = the variance of y .

3. Results

In this section, we provide some experiments and tests that used as measurement objectives to obtain more reliable and accurate results. The tests carried out were image quality analysis, histogram analysis, differential attack analysis, and entropy analysis. The analysis of metric methods such as SSIM, PSNR and MSE used in this test aims to assess the level of cipher image quality produced by the proposed system. Not only that, but histogram analysis also aims to assess the quality of the cipher image. Histograms offer a clear visual representation of the distribution of data and help users quickly understand the shape, spread, and trend of the resulting data. Whereas the analysis of different attacks will be evaluated using NPCR and UACI tests to check the difference between plain-text image and cipher image because small changes in plain-text image will have a significant effect in the resulting cipher image. Information entropy analysis, in turn, is used to measure the average amount of uncertainty associated with image data. An analysis of the proposed encryption and decryption system of images will be carefully discussed.

3.1 Input Image

Several images with different dimensions and sizes were used as input sample of a plain image that is often used in the field of image processing as in Table 1.

Table 1
 Sample input image with corresponding details

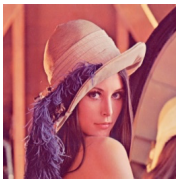

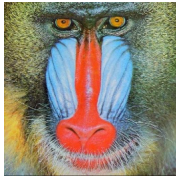





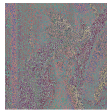
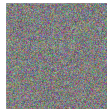


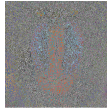


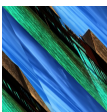
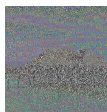



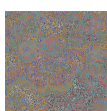

Image	Details	Image	Details
	Format: PNG File Size: 462 KB Dimension: 512 x 512		Format: JPG File Size: 41.9 KB Dimension: 512 x 512
	Format: PNG File Size: 65.0 KB Dimension: 512 x 512		Format: PNG File Size: 286 KB Dimension: 384 x 384
	Format: JPG File Size: 59.5 KB Dimension: 512 x 512		Format: JPG File Size: 40.5 KB Dimension: 800 x 800

Image encryption and decryption algorithms need to be tested with a variety of input images to ensure their effectiveness and security. Using images with different characteristics helps assess how well the algorithms perform under various conditions, such as different resolutions, aspect ratios, and colour depths. Other than that, If the image encryption and decryption system involve user interaction, testing with diverse sample images can help ensure a smooth user experience. Users may upload images of different sizes and formats, and the system should handle them seamlessly without sacrificing security or performance.

3.2 Colour Image Encryption

This encryption and decryption process was carried out using several samples of images-ordinary with a square resolution. The system is capable of encrypting and decrypting various sizes and dimensions of images, but it is necessary that they be in a square shape. Table 2 shows the colour image encryption results of the proposed system. The results shown for the Arnold Chaotic images and Henon Chaotic images are the result of the image encryption process before the merger and applying XOR operation. When the two Chaotic images are combined and the XOR operation is applied, it will produce high-quality ciphers without the shadow of the original image as can be seen in Table 2.

Table 2
 Sample output for colour image encryption

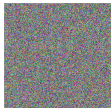
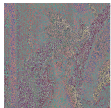







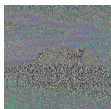
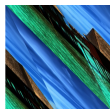
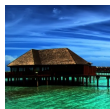

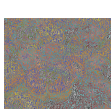


1. Plain Image	2. Arnold Chaotic Image	3. Henon Chaotic Image	4. Cipher Image
			
			
			
			

The encrypted image would still be a colour image, but its content would be transformed in such a way that it becomes unreadable without the decryption key. This transformation could involve scrambling the pixel values, applying mathematical operations, or using cryptographic techniques to obscure the image data. The encrypted image would typically retain the same file format as the original image (e.g., JPEG, PNG). However, the content of the file would be entirely different due to the encryption process.

3.2 Colour Image Decryption

Table 3 below will show the decryption results of colour images for the proposed system using several input image samples. The decryption process is the reverse of the encryption process, in which the ciphers are decrypted using the Henon map first and followed by the Arnold Cat map. The primary output of image decryption is the original image that was encrypted. After decryption, the image data is restored to its original form, and the resulting image is identical to the input image before encryption.

Table 3
 Sample output for colour image decryption

5. Cipher Image	6. Henon Chaotic Image	7. Arnold Chaotic Image	8. Plain Image
			
			
			
			

3.3 Analysis Quality Image

Tests were performed between plain image and cipher image, as well as plain image and decipher image as can be seen in Tables 4 and 5. The calculation of PSNR, SSIM, and MSE between the original image and the cipher image helps assess the quality of the cipher image and the effectiveness of the encryption process itself. The higher the PSNR and SSIM, and the lower the MSE, the better the encryption algorithm in retaining the original information during encryption. The most immediate aspect to assess is how the cipher image looks visually. A high-quality cipher image should appear as random noise or pseudo-random patterns without any recognizable structure or content. If the cipher image exhibits patterns or recognizable features, it might indicate weaknesses in the encryption algorithm.

Table 4
 Plain image VS Cipher image

9. Image	10. Metric Methods		
	PSNR	SSIM	MSE
Lenna	11.3845	0.0197	1.0
Baboon	11.8622	0.0186	1.0
House	9.9071	0.0166	1.0
Pepper	11.8825	0.0218	1.0

Table 5
Plain image VS Decipher image

11. Image	12. Metric Methods		
	<i>PSNR</i>	<i>SSIM</i>	<i>MSE</i>
Lenna	29.551	0.9769	0.0
Baboon	29.810	0.9826	0.0
House	30.245	0.9778	0.0
Pepper	29.540	0.9404	0.0

Based on the result in Table 4 and 5, a low SSIM value compared to the original image indicates significant dissimilarity, suggesting effective encryption. However, if the SSIM value is unexpectedly high or close to 1, it may indicate potential weaknesses in the encryption process, as the cipher image resembles the original image too closely. Next, a high PSNR value indicates high similarity between the original and cipher images, which is undesirable for encryption. A low PSNR value suggests effective encryption, as the noise introduced by encryption obscures the original content. Lastly, a high MSE value suggests effective encryption, as it indicates a significant difference between the original and cipher images.

3.4 Analysis Histogram

This encryption and decryption study uses histograms to make quality comparisons between the original image and the resulting cipher image. Through histogram analysis, the distribution of pixel intensity in the image can be clearly seen. A significant change in the distribution of pixel intensity could indicate there is an impact from the proposed encryption process. The results of the histogram analysis of the cipher image show a uniform distribution of the Pixel frequencies as in Table 6. An even distribution of pixel intensity across the histogram indicates that the encryption process has maintained a certain degree of randomness. This is desirable in image encryption because it shows the lack of visible patterns that could potentially be attacked by an enemy. The presence of noise in the histogram may indicate the introduction of random variations during the encryption process. Although some noise levels can be expected, excessive noise can affect the visual quality of the decrypted image.

3.5 Analysis and Comparison

The cipher images produced for the proposed system has better quality than the existing system as can be seen in Table 7. It is because, the visibility of the original image on the existing system during the encryption process of coloured images still can be seen. Some encryption algorithms may prioritize security over image quality, leading to perceptual differences between plain image and cipher image. However, it is important to make a balance between security and image quality based on the needs of a particular application.

Table 6
Histogram for plain image and cipher image

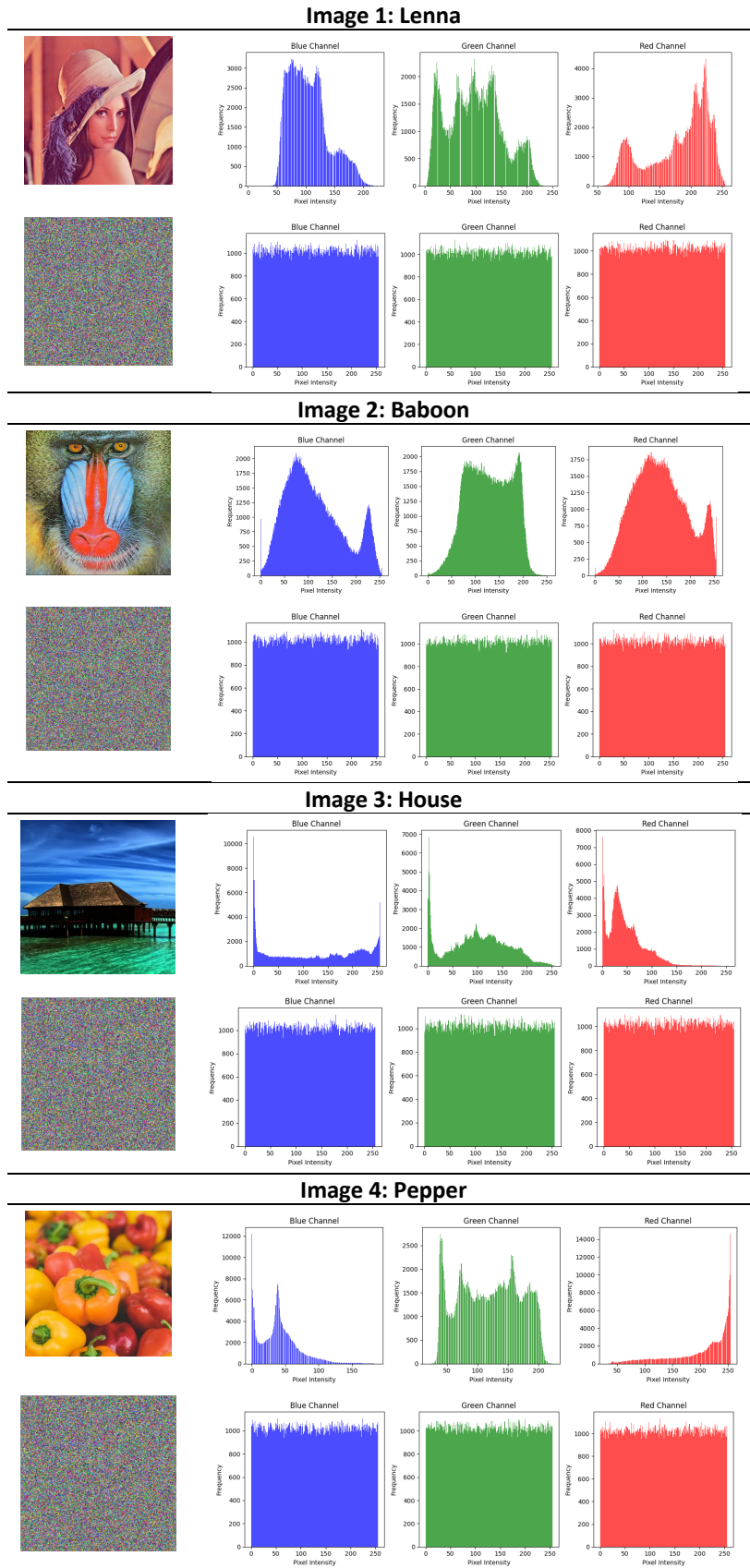

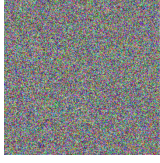
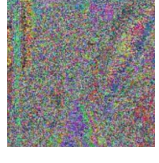

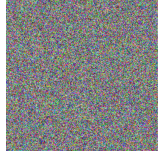
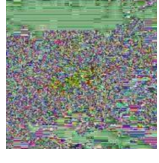


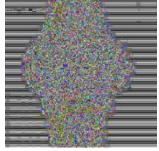


Table 7
 Comparison of cipher image between proposed system and existing system

Plain Image	Cipher Image (Proposed System)	Cipher Image (Existing System, [20])
		
		
		

3.5.1 Analysis entropy

In the context of image analysis, entropy is often used to measure the amount of information or randomness contained in an image. Higher entropy values indicate greater randomness in the pixel intensity distribution. High entropy images are difficult to predict and contain more information, while low entropy images have a more orderly or uniform intensity distribution. In this study, entropy is also used as a metric to evaluate image quality. Changes in entropy values before and after image processing operations, such as compression or encryption, can provide insights into the impact on image quality as in Table 8. It is the result for a test to compare the entropy value between the proposed algorithm and the existing algorithm.

Table 8
 Entropy value for plain, cipher and decipher image

13. Image	14. Entropy Value		
	Plain Image	Cipher Image (Proposed system)	Cipher Image (Existing system)
Lenna	6.835	7.925	7.24
Baboon	6.884	7.923	6.82
Watch	5.642	9.106	4.25

3.5.1 Analysis differential attack

A differential attack is a type of cryptanalytic attack that exploits the difference between plain-text and cipher-text. The objective of a differential attack is to infer information about a cryptographic key or encryption algorithm by analysing how differences in input (plain-text) affect differences in output (cipher-text). A good image encryption algorithm will produce a high NPCR value to ensure that most of the image is affected by encryption. At the same time, a low UACI value indicates that changes are not visually noticeable, contributing to the security of the algorithm. In this study, NPCR and UACI results were presented in percent and compared between the proposed system and existing system as shown in Table 9.

Table 9
NPCR and UACI percentage comparison between proposed system and existing system

Image	Proposed System		Existing System	
	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)
Lenna	99.610	50.014	99.601	33.122
Baboon	99.603	50.025	98.621	33.657
Watch	99.608	49.995	98.611	33.641

4. Conclusions

It can be concluded that the encryption and decryption of color images using Arnold Cat's map and Henon's map makes it easier for recipients to receive sensitive information or image personalities. The system has chosen a chaotic system to overcome issues related to sensitive data. Thus, a system of encryption and decryption of color images based on these two Chaotic Maps was successfully built. Several tests and experiments were carried out, including image quality analysis, differential attack analysis and information entropy analysis to evaluate and measure the quality of the resulting cipher image to be of better quality thus enhancing system security. Encryption and decryption of color images using this both chaotic map is a combination of techniques capable of producing high-quality cipher images without the appearance of the shadow of the original image. Through this research, the process of encryption and decryption has been studied more closely. However, this study can be implemented by adding other techniques to improve efficiency in terms of time or using color images with various resolutions.

Acknowledgement

All authors would like to thank anonymous reviewers for all their constructive comments and recommendations for the betterment of this paper. This study is financially supported by Universiti Malaysia Sabah through the Research Grant SBK0508-2021.

References

- [1] Gopalakrishnan, Rajasree, and Retnaswami Mathusoothana Satheesh Kumar. "Cloud Security System for ECG Transmission and Monitoring Based on Chaotic Logistic Maps." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 39, no. 2 (2024): 1-18. <https://doi.org/10.37934/araset.39.2.118>
- [2] Aung, Pyi Phyoo, Nordinah Ismail, Chia Yee Ooi, Koichiro Mashiko, Hau Sim Choo, and Takanori Matsuzaki. "Data Remanence Based Approach towards Stable Key Generation from Physically Unclonable Function Response of Embedded SRAMs using Binary Search." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 35, no. 2 (2024): 114-131. <https://doi.org/10.37934/araset.32.3.178189>
- [3] Thanki, Rohit, Surekha Borra, Rohit Thanki, and Surekha Borra. "Technical Information." *Medical Imaging and its Security in Telemedicine Applications* (2019): 11-21. <https://doi.org/10.1007/978-3-319-93311-5>
- [4] Anthony-Claret Onwutalobi. "Overview of Cryptography". *SSRN Electronic Journal*. (2016)
- [5] Mashuri, Adib, Nur Hamiza Adenan, Nor Suriya Abd Karim, Siew Wei Tho, and Zhaofeng Zeng. "Application of Chaos Theory in Different Fields-A Literature Review." *Journal of Science and Mathematics Letters* 12, no. 1 (2024): 92-101. <https://doi.org/10.37134/jsml.vol12.1.11.2024>
- [6] Ghosh, Indranil, Md Sazzad Hossien Chowdhury, and Suazlan Mt Aznam. "Numerical treatment on a chaos model of fluid flow using new iterative method." *Journal of Advanced Research in Fluid Mechanics and Thermal Sciences* 96, no. 1 (2022): 25-35. <https://doi.org/10.37934/arfmts.96.1.2535>
- [7] Shen, Bo-Wen, Roger A. Pielke, Sr., Xubin Zeng, Jong-Jin Baik, Sara Faghih-Naini, Jialin Cui, and Robert Atlas. "Is Weather Chaotic?: Coexistence of Chaos and Order within a Generalized Lorenz Model", *Bulletin of the American Meteorological Society* 102, 1 (2021): E148-E158. <https://doi.org/10.1175/BAMS-D-19-0165.1>
- [8] Mohamadi, Housseem Eddine, Laaziz Lahlou, Nadjia Kara, and Aris Leivadreas. "A versatile chaotic cryptosystem with a novel substitution-permutation scheme for internet-of-drones photography." *Nonlinear Dynamics* (2024): 1-36. <https://doi.org/10.1007/s11071-024-09306-3>

- [9] Sheela, S. J., and K. V. Suresh. "Real time region of interest based chaotic image cryptosystem for IoT applications." *Multimedia Tools and Applications* 83, no. 6 (2024): 16161-16177. <https://doi.org/10.1007/s11042-023-16093-3>
- [10] Li, Ying, Qianxue Wang, and Simin Yu. "A novel hybrid scheme for chaotic image encryption." *Physica Scripta* (2024). <https://doi.org/10.1088/1402-4896/ad3171>
- [11] Anak Agung Putri Ratna, Anak, Frenzel Frenzel Timothy Surya, Diyanatul Diyanatul Husna, I. Ketut I Ketut Eddy Purnama, Ingrid Ingrid Nurtanio, Afif Afif Nurul Hidayati, Mauridhi Mauridhi Hery Purnomo, Supeno Supeno Mardi Susiki Nugroho, and Reza Reza Fuad Rachmadi. "Chaos-based image encryption using Arnold's cat map confusion and Henon map diffusion." *Advances in Science, Technology and Engineering Systems* 6, no. 1 (2021): 316-326. <https://doi.org/10.25046/aj060136>
- [12] Jithin, K. C., and Syam Sankar. "Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set." *Journal of Information Security and Applications* 50 (2020): 102428. <https://doi.org/10.1016/j.jisa.2019.102428>
- [13] Hu, Yongsheng, Han Wu, and Luoyu Zhou. "Color image encryption base on a 2D hyperchaotic enhanced Henon map and cross diffusion." *Alexandria Engineering Journal* 73 (2023): 385-402. <https://doi.org/10.1016/j.aej.2023.04.060>
- [14] Ghorbani, Amirabbas, Morteza Saberikamarposhti, and Mehdi Yadollahi. "Using Ribonucleic acid (RNA) and Hénon map in new image encryption scheme." *Optik* 259 (2022): 168961. <https://doi.org/10.1016/j.ijleo.2022.168961>
- [15] Marsh, Ronald, and Scott Kerlin. "A Many-key Image Encryption Method Using the Lorenz System." (2013).
- [16] Hariyanto, Eko, and Robbi Rahim. "Arnold's cat map algorithm in digital image encryption." *International Journal of Science and Research (IJSR)* 5, no. 10 (2016): 1363-1365. <https://doi.org/10.21275/ART20162488>
- [17] Khalil, Noura, Amany Sarhan, and Mahmoud AM Alshewimy. "An efficient color/grayscale image encryption scheme based on hybrid chaotic maps." *Optics & Laser Technology* 143 (2021): 107326. <https://doi.org/10.1016/j.optlastec.2021.107326>
- [18] ElBeltagy, Eng Mohamed. "Image Encryption Techniques for Secure Transmission of Information." (2021).
- [19] Dawahdeh, Ziad E., Shahrul N. Yaakob, and Rozmie Razif bin Othman. "A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher." *Journal of King Saud University-Computer and Information Sciences* 30, no. 3 (2018): 349-355. <https://doi.org/10.1016/j.jksuci.2017.06.004>
- [20] Omoruyi, Osemwegie, Chinonso Okereke, Kennedy Okokpujie, Etinosa Noma-Osaghae, Obinna Okoyeigbo, and Samuel John. "Evaluation of the quality of an image encryption scheme." *TELKOMNIKA (Telecommunication Computing Electronics and Control)* 17, no. 6 (2019): 2968-2974. <https://doi.org/10.12928/TELKOMNIKA.v17i6.10488>