



SEMARAK ILMU
PUBLISHING
202101256166(003314878-P)

International Journal of Advanced Research in Computational Thinking and Data Science

Journal homepage:

<https://semarakilmu.com.my/journals/index.php/ctds/index>

ISSN: 3030-5225



Chaotic Encryption Scheme for Double Grayscale Images using Sprott B Hyperchaotic Map

Syahidatul Shafiqah Ramlee¹, 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:

Sprott B hyperchaotic map; double images; cipher image; excellent quality; noise-like visual

ABSTRACT

Image encryption become more significant since most of our data are communicated and stored as digital image form. To warrant high confidentiality, cipher image must be the produced in excellent quality to avoid any information leakage related to the original image. Since image has become one of the most used tools in information exchanges, large production and storage of cipher images are highly demanded, and this scenario could affect the production of high-quality cipher images. While most of existing encryption for images are for single image, processing multiple images simultaneously comes in handy as a fitting fast action to realize the convenience of encryption, storage, and transmission of multiple images. Inspired by those idea, we proposed a new chaotic encryption scheme using Sprott B hyperchaotic map. Using this scheme, two grayscale images are encrypted to produce a single cipher image. The encryption begins with the process of combining two images and encrypting the combined image using the hyperchaotic map. One cipher image will be produced representing and carrying information of the combination of the two images. Our experiments demonstrated significant enhancement offered by the scheme, while maintaining the quality of the recovered plain image. The proposed scheme yields cipher image with excellent quality in terms of noise-like visual of which the information of the images is concealed. While the proposed scheme satisfies the requirements of producing cipher images with excellent quality, it also achieves the credibility to decrypt the cipher image and restoring the plain image exactly similar to the original image.

1. Introduction

In this digital era, our data and information are stored and communicated through the Internet. Thus, cryptography plays more crucial role in protecting and maintaining security in cyber realm. Without cryptography, our data and information might be exposed to various kinds of attacks such as the ransomware attacks which are currently one of cybersecurity's greatest and most alluring threats [1]. Encryption and decryption are required to ensure the confidentiality of our data and

* Corresponding author.

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

information. For security and efficiency purposes, encryption and decryption algorithms must be selected and executed properly [2]. As long as the data can be digitalized, then encryption and decryption algorithms can be deployed. Most of the encryption and authentication systems use private and public-key cryptography [3].

Distributed computing ought to keep up with information trustworthiness and mystery to help with information security. By and by, there are very few copyright and information security chances. The way that anybody can see the information when it is communicated 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. As of now there are not many devices and strategies for safeguarding information put away in the cloud.

Image encryption is one of the cryptosystem techniques in cryptography. It is a method to encode and generate secret images known as cipher images using encryption algorithms in attempt to prevent access from unauthorized parties. A cipher image should be generated to be completely hidden and unreadable. This is to prevent information leaks as to secure the integrity of the images. Only the parties who own the key to the encryption algorithm will have the access to the images [4]. The procedure in image encryption is to convert a plain image, which is the readable image, to a cipher image, the unreadable image. The conversion can only be performed using a key known as secret key or private key. The procedure to recover the cipher image back to its readable image is known as the decryption of the cipher image. The same key used in the encryption will be used again in the decryption to decrypt the cipher image [5].

On the other hand, chaotic map is roughly defined as a system with chaotic behaviours. The concept behind chaotic theory is unpredictable and random. It is dependent on the controlling parameters. The arrangement of the parameters is to confuse from locating the outputs which will make it impossible to locate if the parameters in unknown [6]. The dependency on the controlling parameters makes chaotic map to be very sensitive towards any change on the parameters, thus making chaotic map an ideal scheme for image encryption [7].

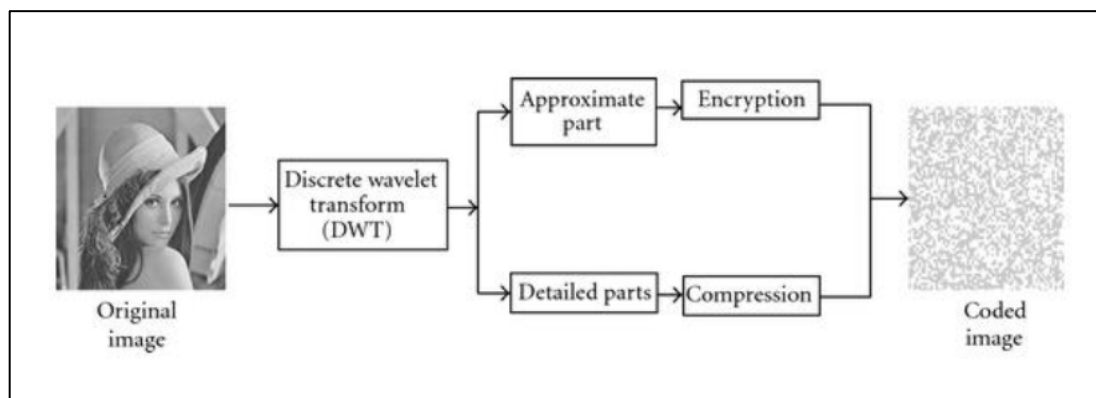


Fig 1. An example of image encryption process [7]

There are several methods developed for image encryption using chaotic maps. This paper proposed a method using Sprott B hyperchaotic map which was derived from Sprott chaotic map, which is from Lorenz chaotic map. Lorenz map is a high-dimensional chaotic map exhibiting a complex chaotic behaviour and produces chaotic sequence that is fix and precise in values [11]. In the previous study in [12], a cryptosystem of image encryption using Lorenz map is proposed. The cryptosystem is a hybrid cryptosystem based on 3D Lorenz map. The study shows that the pixel distributions of the

produced cipher image are shown to be uniform, implying that the cipher image has no resemblance to the plain image.

Sprott chaotic map is a variant from Lorenz chaotic map. Compared to Lorenz map, Sprott map exhibits richer dynamic [13]. In previous study Xie *et al.*, [14], proposed a cryptosystem of image encryption with the implementation of ordinary Sprott map. Their study stated that the produced cipher image from Sprott map has pixel distribution that is random and distributed evenly. Sprott B map is a variant from Sprott map which considered special for it has the closest attractor to Lorenz map [15]. In the study proposed in [16] of which Sprott B map is used in the image encryption, Sprott B map has resulted to a very simple chaotic system yet is so rich and complex in dynamics. The study shows that pixel distribution of the produced cipher image from the method is uniform. From the Sprott B map, Ye *et al.* [9] has proposed an image encryption using the map but improved which make the chaotic state of their map to reach hyperchaotic state. The chaotic behaviour is even more hyper and extreme compared to the ordinary Sprott B map.

Images has been one of the most used multimedia in information exchanges, which demands the increasing production of cipher images. Processing multiple images can be the course of action to satisfy the demands for large production. To produce cipher images, processing two or more images simultaneously is a proper way to realize the convenience of encryption, storage, and transmission of multiple images [17]. In Yu *et al.*, [18], an encryption algorithm for double images based on spatiotemporal chaos and DNA operations is proposed. The study stated that the developed double image encryption has improved the encryption security and speed. Then, a double image encryption based on compression by combining hyperchaotic map and compressive sensing is proposed in [19]. Their developed encryption algorithm for double images was shown to has high transmission efficiency, as well as high-rate production of good quality cipher image and has effective decryption for favourable image recovery.

In this paper, we proposed an encryption method for double images using a hyperchaotic map which was inspired from Sprott B chaotic map. The method is aimed to enhance the quality of the cipher image by encrypting double grayscale images using the hyperchaotic map, to make the cipher image more noised and unreadable, in order to disguise the visual information of the plain images. The proposed method starts by the process of combining two plain images using XOR functions and only then be proceeded to the encryption step with the hyperchaotic map.

This study embarks on few objectives including to develop a cryptosystem for encrypting double grayscale images using Sprott B hyperchaotic map, to analyse the performance of the quality of the cipher images, and to study whether the recovered image is the same as the original image after being processed by the proposed double image encryption. The importance of this study is to improve the reliability of the developed cryptosystem in producing a good quality cipher image. In addition to that, the cryptosystem is designed to maintain the original quality of the plain image after recovered by the decryption step in cryptosystem. This study will involve demonstration on only grayscale images, with dimension fixed to be in square shape which all four sides are of equal length.

2. Methodology

The proposed encryption scheme of double images encryption involves the use of two plain images, Image 1 and Image 2. The images are of the same dimension with width, W , are the same as the height, H . The images will be read as a grayscale image consisting of black and white pixels with value 255.

2.1 Combining Two Images

The scheme begins with the combination process of the two images. The combination process is operated using XOR function. Image 1 is operated with Image 2. Table 1 shows the return statement of the function on the pixels of a grayscale image.

Table 1

XOR operation on grayscale image

Image 1	Black (0)	Black (0)	White (1)	White (1)
Image 2	Black (0)	White (1)	White (1)	Black (0)
XOR Operation	Black (0)	White (1)	Black (0)	White (1)

2.2 Generating Hyperchaotic Sequence

A hyperchaotic map from Sprott B is used in the encryption process of the cryptosystem. The map consists of five control parameters initialized on three state variables. The algorithm is given by:

$$f'(x) = ayz, \tag{1}$$

$$f'(y) = bx - cy, \tag{2}$$

$$f'(z) = d - exy - f(xy), \tag{3}$$

where $x, y, z \in \mathbb{R}$ are representing the state variables, and $a, b, c, d, e \in \mathbb{R}^+$ are representing the control parameters [9].

The proposed algorithm takes three parameters a, b , and c from the map and initialized on two state variables x and y . The selected value of each is as:

Initial state variables: $x = 0.1, y = 0.1$

Control parameters: $a = 1, b = 0.9, c = 1.7$

The same hyperchaotic sequence generated using the same stated selected values are used for the decryption process.

2.3 Encrypting Combined Image

Encryption process is operated on the combined image by the XOR operation. The pixel of combined image is randomized and scattered using the generated hyperchaotic sequence. The dimension of the combined image has the width equal to the height. The dimension of the combined image should be $H \times H$. The image after randomization is reshaped into the initial dimension of $H \times H$. The cipher image is produced.

2.4 Decrypting Cipher Image

Decryption process is operated on the cipher image by reversing the steps of the encryption process using the same hyperchaotic sequence. The pixel of the cipher image is scattered to a reverse randomization and restored back to the original position. The image after the reverse randomization is reshaped into the initial dimension $H \times H$.

2.5 Separating Decrypted Image

The decrypted image is the recovered image of the combined image. To recover the two plain images, the decrypted image will be separated from the combination using the same operation to

combine them which is the XOR function. To recover one of the images, the decrypted image will be operated with the other one image. In other words, Image 1 will be recovered by Image 2 and vice versa.

3. Result and Discussion

Analysis for the proposed cryptosystem is tested and conducted on four different grayscale images with respective different dimensions. Table 2 shows the four plain images: Apple, Lena, Barbara, and Baboon.



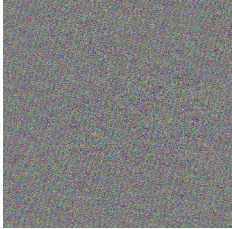

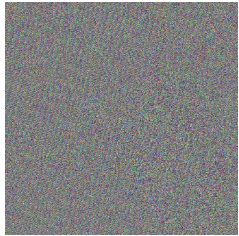
Table 2
 The Four Plain Images

			
Image: Apple(1116 x 1116)	Image: Lena (512 x 512)	Image: Barbara (512 x 512)	Image: Baboon (637 x 637)

3.1 Encryption Outputs

Using Sprott B hyperchaotic map, two images undergo the process of encryption simultaneously and produce one cipher image. Each plain image in Table 2 will be combined and encrypted together with the other images, respectively. In other words, each image will act as Image 1 while the other image acts as Image 2.

Table 3
 Cipher images produced by Apple as Image 1

Image 1	Image 2	Cipher Image
		
		

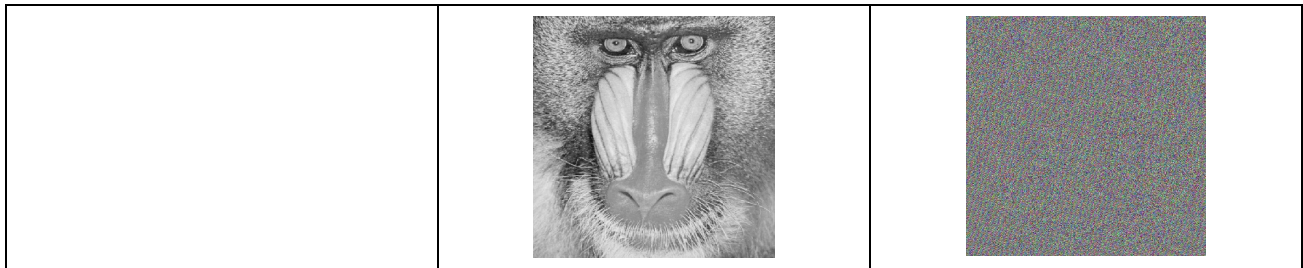


Table 3 until Table 6 show the cipher images produced by all the combination of the images. Table 3 shows the cipher images generated from the combination of the images when image Apple acts as Image 1 while the other images (Lena, Barbara, and Baboon) act as Image 2. Furthermore, Table 4 shows the cipher images generated from the combination of the images when image Lena acts as Image 1 while the other images (Apple, Barbara, and Baboon) act as Image 2. Finally, Table 5 shows the cipher images generated from the combination of the images when image Barbara acts as Image 1 while the other images (Apple, Lena, and Baboon) act as Image 2.

Table 4
 Cipher images produced by Lena as Image 1



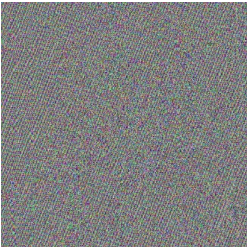

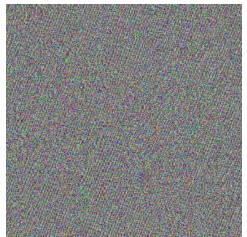
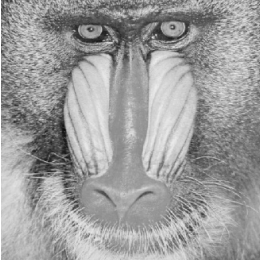

Image 1	Image 2	Cipher Image
		
		
		

Table 5
 Cipher images produced by Barbara as Image 1



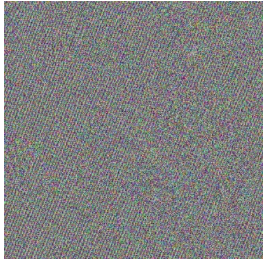

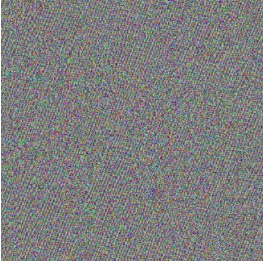
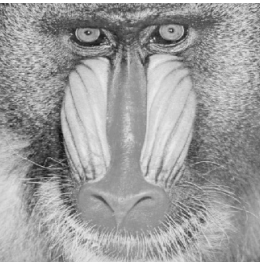

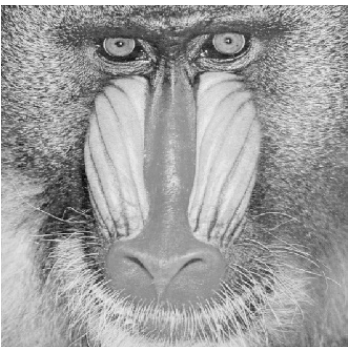

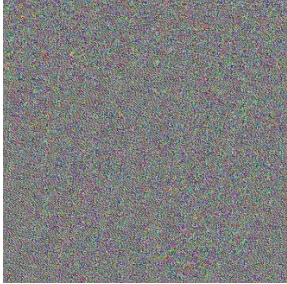

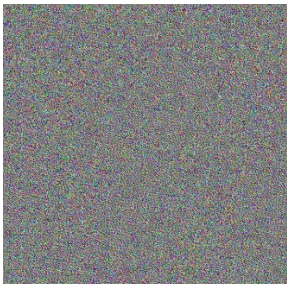
Image 1	Image 2	Cipher Image
		
		
		

Table 6
 Cipher images produced by Baboon as Image 1

Image 1	Image 2	Cipher Image
		
		



3.2 Decryption Outputs




The decryption process or recovery process is conducted on each of the produced cipher images shown in Table 3 until Table 6. Each of the cipher images will and should produce three distinct recovered plain images for the first image and one recovered plain image for each of the second images. Table 7 until Table 10 show all the recovered images.

Table 6 shows the cipher images generated from the combination of the images when image Baboon acts as Image 1 while the other images (Apple, Lena, and Barbara) act as Image 2. Next, Table 7 shows the recovery of the of the first plain image, image Apple, from the cipher images generated from the encryption between the original plain image Apple (as Image 1) with the other three plain images, Lena, Barbara, and Baboon (as Image 2). Alongside is shown the recovery of the plain images of Image 2, including image Apple, Lena, and Baboon.

Table 8 shows the recovery of the of the second plain image, image Lena, from the cipher images generated from the encryption between the original plain image Lena (as Image 1) with the other three plain images, Apple, Barbara, and Baboon (as Image 2). Alongside is shown the recovery of the plain images of Image 2, including image Apple, Barbara, and Baboon. Moreover, Table 9 shows the recovery of the of the third plain image, image Barbara, from the cipher images generated from the encryption between the original plain image Barbara (as Image 1) with the other three plain images, Apple, Lena, and Baboon (as Image 2). Alongside is shown the recovery of the plain images of Image 2, including image Apple, Lena, and Baboon. Finally, Table 10 shows the recovery of the of the last plain image, image Baboon, from the cipher images generated from the encryption between the original plain image Baboon (as Image 1) with the other three plain images, Apple, Lena, and Barbara (as Image 2). Alongside is shown the recovery of the plain images of Image 2, including image Apple, Lena, and Barbara.

Table 7

Recovered images of Apple as Image 1

		
Recovered Apple generated with Lena	Recovered Apple generated with Barbara	Recovered Apple generated with Baboon



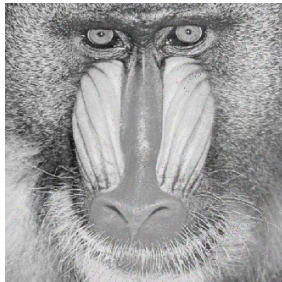



		
Recovered Lena	Recovered Barbara	Recovered Baboon

Table 8
 Recovered images of Lena as Image 1

		
Recovered Lena generated with Apple	Recovered Lena generated with Barbara	Recovered Lena generated with Baboon
		
Recovered Apple	Recovered Barbara	Recovered Baboon

Table 9
 Recovered images of Barbara as Image 1

		
Recovered Barbara generated with Apple	Recovered Barbara generated with Lena	Recovered Barbara generated with Baboon


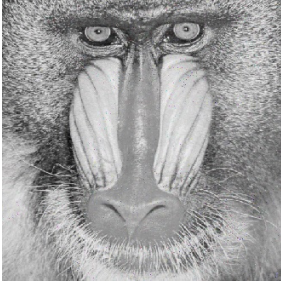
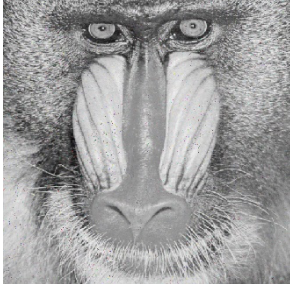
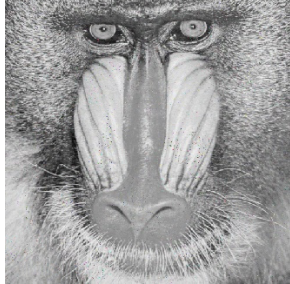



		
Recovered Apple	Recovered Lena	Recovered Baboon

Table 10
 Recovered images of Baboon as Image 1

		
Recovered Baboon generated with Apple	Recovered Baboon generated with Lena	Recovered Baboon generated with Barbara
		
Recovered Apple	Recovered Lena	Recovered Barbara

3.3 SSIM Measurement

In general, the measurements by Structural Similarity Index Measurement (SSIM) indicate the similarities between two images. The range value of SSIM is [0, 1]. The larger and closer the value to 1, the higher the similarity between the images. Indicating there is little to no difference between the images. The computation of SSIM is as follow [20]:

$$SSIM = \frac{(2Mv_x Mv_y + c)(2Cv_{xy} + c')}{((Mv_x)^2 + (Mv_y)^2 + c)((Sv_x)^2 + (Sv_y)^2 + c')}, \quad (4)$$

where Mv_x and Mv_y are mean value of x and y respectively, Sv_x and Sv_y are the value for standard deviation of x and y respectively, and Cv_{xy} is the covariance value of x and y . Being $c = (kL)^2$ where $k = 0.01$ and $L = 2^n - 1$, whereas $c' = (k'L)^2$ where $k' = 0.03$ and $L = 2^n - 1$ with both n as the number of bits per pixel.

Table 11 shows the measured SSIM values between the original plain images of Image 1 and the cipher images, as well as between the original images of Image 1 and the recovered images of Image 1. It shows between Image 1 and the cipher image generated with the corresponding Image 2, the

minimum SSIM value is 0.00592 and the maximum is 0.00887. All the values for cipher images are small and very close to 0.00 which indicates that the cipher image has little to no resemblance to the original Image 1. The small resemblance between the images is what is aimed for the cipher image to be considered as good in quality. The cipher images are very different from the plain images. While the SSIM value between the original Image 1 and recovered Image 1 which decrypted from the cipher image generated with the corresponding Image 2, the obtained minimum value is 0.95061 and the maximum is 0.99134. All the measured values are large and very close to 1.00 which indicates that the recovered Image 1 has little to no difference to the original Image 1. The recovered images are very similar and the same as the original images.

Table 11
 SSIM measured on original Image 1 to cipher image and to recovered Image 1

Images 1	Image 2	Size	SSIM	
			Cipher Image	Recovered Image
Apple	Lena	1116 x 1116	0.00856	0.95286
	Barbara		0.00844	0.96315
	Baboon		0.00887	0.95061
Lena	Apple	512 x 512	0.00592	0.99134
	Barbara		0.00683	0.98884
	Baboon		0.00877	0.98546
Barbara	Apple	512 x 512	0.00707	0.98963
	Lena		0.00786	0.98493
	Baboon		0.00742	0.97959
Baboon	Apple	637 x 637	0.00659	0.97716
	Lena		0.00787	0.96730
	Barbara		0.00843	0.96740

3.4 PSNR Measurement

In general, the measurements by Peak Signal to Noise Ratio (PSNR) indicate the noise difference between the images. The range value of PSNR starts from 0. The larger the value, the smaller the difference between the images. A value of 30-40 indicates good quality, 20-30 indicates moderate quality, and below 20 indicates poor quality. The computation of PSNR is as follow [21] :

$$PSNR = 20 \times \log_{10} \frac{MaxPixel}{MSE} \tag{5}$$

where *MaxPixel* is the maximum supported pixel value which is 255 and *MSE* is the mean squared error defined as:

$$MSE = \frac{1}{H \times W} \sum_{i=0}^{H-1} \sum_{j=0}^{L-1} [Q_{ij} - Z_{ij}]^2, \tag{6}$$

where $H \times W$ is the dimension of the image (with the width W is the same to the height H), Q_{ij} is the pixel value of the plain image and Z_{ij} is the pixel value of the decrypted image.

Table 12 shows the measured PSNR between the original plain images of Image 1 and the cipher images, as well as between the original images of Image 1 and the recovered images of Image 1. It shows between Image 1 and the cipher image generated with the corresponding Image 2, the

minimum PSNR value measured is 7.65498 and the maximum is 7.69565. The values between the images are all far below 20, indicating that the measured image is poor in quality and has massive differences from Image 1. The measured PSNR that results of poor quality is what is aimed for the cipher image to be considered as good. The more the cipher image is different from the plain image, the better the quality of the cipher image. Indicating that the cipher image has no resemblance to the Image 1, thus satisfying the purpose of cipher image concealing the information of plain image. While the PSNR value between the original Image 1 and recovered Image 1 which decrypted from the cipher image generated with the corresponding Image 2, the obtained minimum value is 33.01274 and the maximum is 33.46223. All the measured values are in the range of 30 to 40, the range value for image of good quality, indicating that the recovered Image 1 are the same in appearance to the original Image 1.

Table 12
 PSNR measured on original Image 1 to cipher image and to recovered Image 1

Image 1	Image 2	Size	PSNR	
			Cipher Image	Recovered Image
Apple	Lena	1116 x 1116	7.65498	33.21831
	Barbara		7.66322	33.44797
	Baboon		7.66719	33.19455
Lena	Apple	512 x 512	7.69565	33.36967
	Barbara		7.66763	33.46223
	Baboon		7.66149	33.40936
Barbara	Apple	512 x 512	7.67977	33.16189
	Lena		7.67220	33.06742
	Baboon		7.66196	33.01274
Baboon	Apple	637 x 637	7.66450	33.15353
	Lena		7.66117	33.08787
	Barbara		7.66029	33.09649

3.5 Histogram Test

In general, a histogram of an image represents the pixel distribution of the image. It shows the obvious statistical characteristics of the image. The histogram of a cipher usually appears to be evenly distributed or uniform in shape, indicating the pixels of all intensity are equally distributed. Table 13 shows the histogram of the four original plain images shown in Table 2. Table 14 shows the histogram of all cipher images generated from the encryption when image Apple acts as Image 1 which is shown in Table 3. Table 15 shows the histogram of all the cipher images shown in Table 4 generated from the encryption when Lena acts as Image 1.

Furthermore, Table 16 shows the histogram of all the cipher images shown in Table 5 which was generated from the encryption when Barbara acts as Image 1. Table 17 shows the histogram of the cipher images shown in Table 6 which were generated from the encryption when Baboon acts as Image 1. Roughly to look at, the histograms of the cipher image are uniform in shape. The pixels of the cipher images are evenly distributed. Compared to the histogram of the plain images in Table 13, while the plain images have distinct shapes with visible peak and troughs, all the histogram of the cipher image from Table 14 to Table 17 appear to be uniform and very different from that of the plain images. This indicates that the plain images and the cipher images are not similar at all.

Table 13
 Histogram of the original plain images

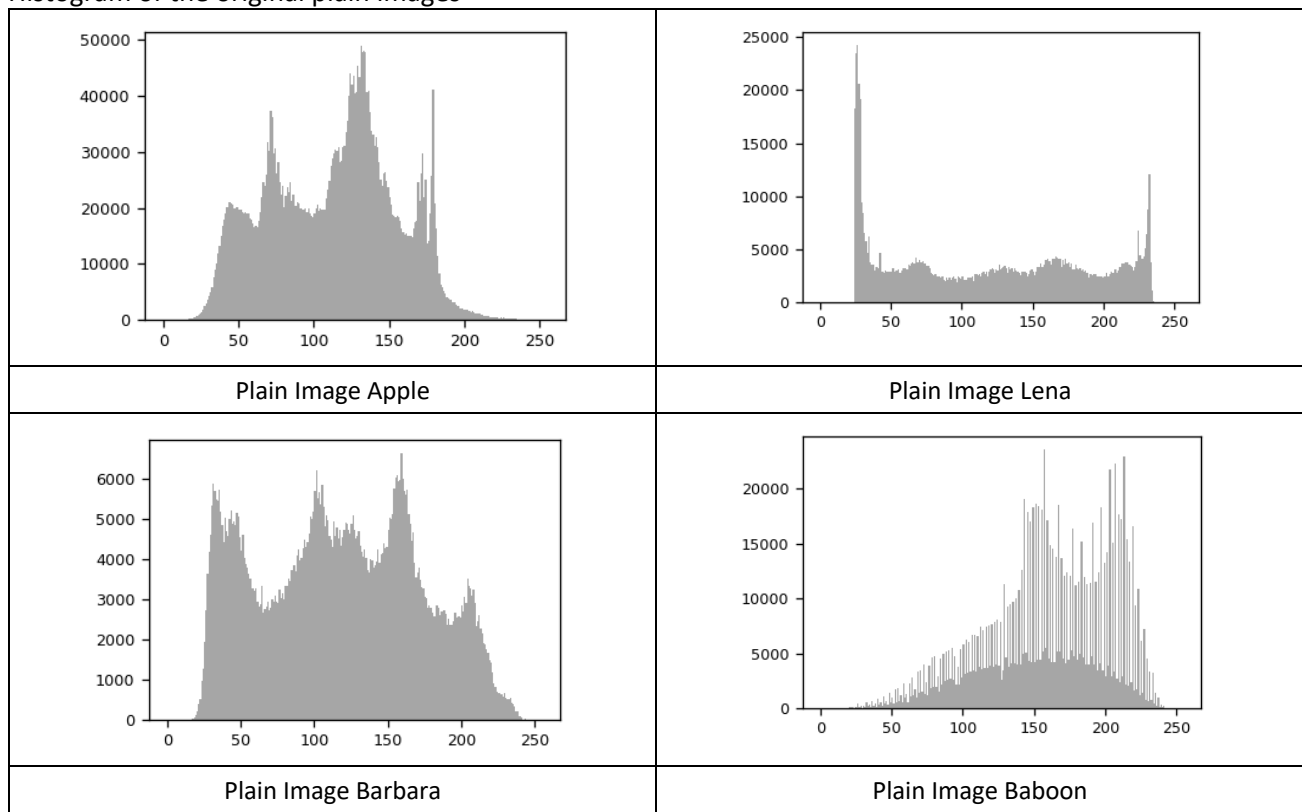


Table 14
 Histogram of cipher image in Table 3

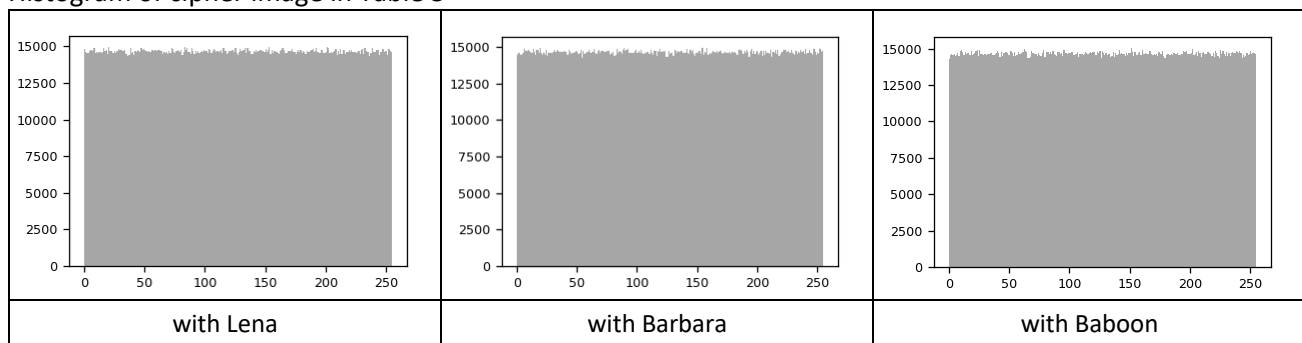


Table 15
 Histogram of cipher image in Table 4

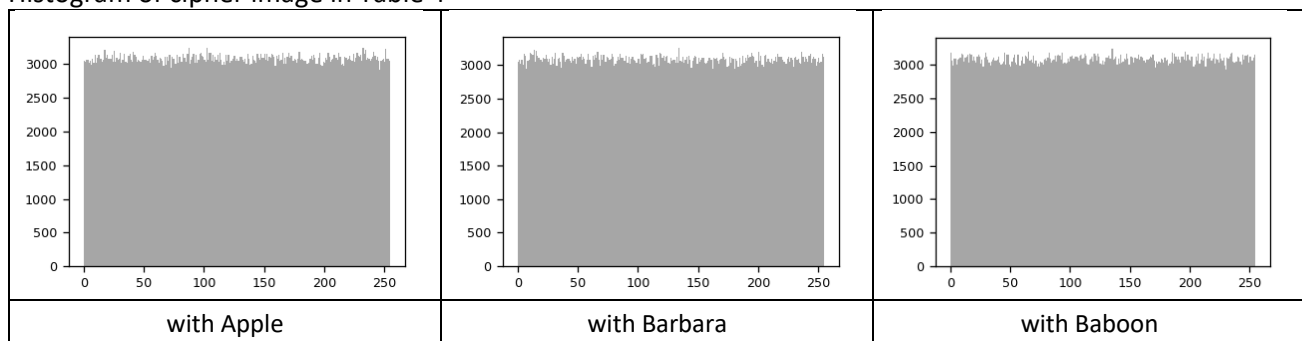


Table 16
 Histogram of cipher image in Table 5

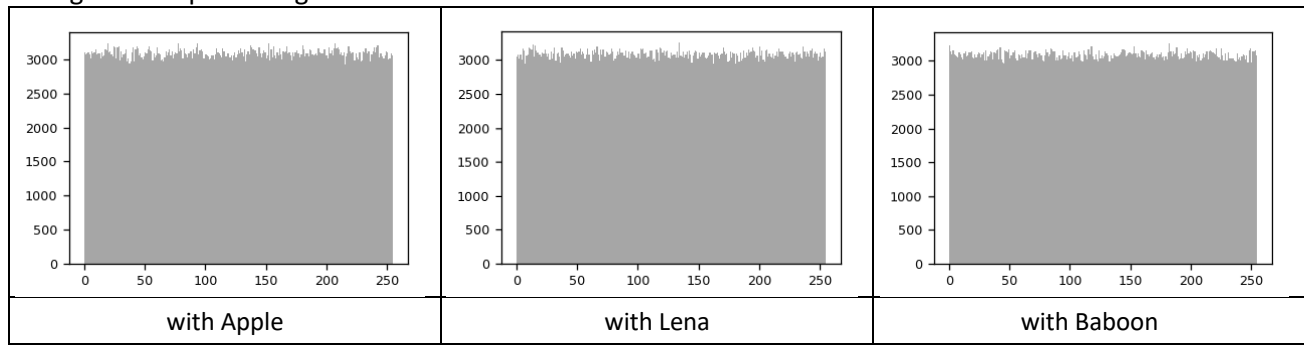
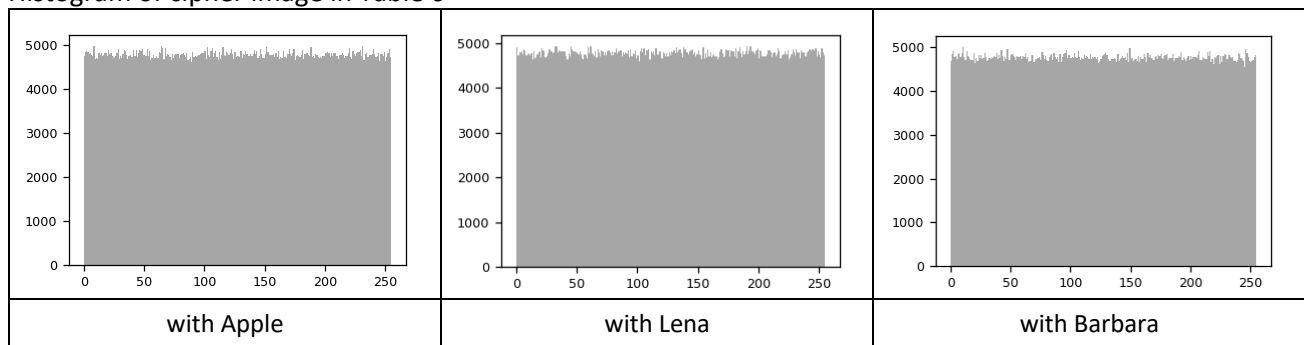


Table 17
 Histogram of cipher image in Table 6



4. Conclusion

In a nutshell, the proposed image encryption scheme has been successfully developed. The cryptosystem is markedly able to conduct both processes of combination and separation with XOR function, and the process of encryption and decryption with a hyperchaotic map of Sprott B. The analysis on the outputs using SSIM and PSNR measurements, and histogram test showed that the proposed encryption scheme is able to produce a cipher image with excellent quality of which the cipher image produced to has no resemblance to the plain image at all. To include, the scheme is also able to recover the plain images as similar to the original plain images with little to no difference from the original. This study can be further extended towards the application of a more hyper chaotic map. A map that is hyper provides such extreme randomness producing a chaotic scheme that is even more sensitive thus improving the security of the cipher image. Additionally, the implementation of encrypting double image to produce one cipher image could be operated by different operation for the combination process.

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] Zakaria, Wira Zanoramy A., Nur Mohammad Kamil Mohammad Alta, Mohd Faizal Abdollah, Othman Abdollah, and SM Warusia Mohamed SMM Yassin. "Early Detection of Windows Cryptographic Ransomware Based on Pre-Attack API Calls Features and Machine Learning." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 39, no. 2 (2024): 110-131.

- <https://doi.org/10.37934/araset.39.2.110131>
- [2] 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>
- [3] Aung, Pyi Phyto, 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>
- [4] Aarthie, Narasimhan, and Rengarajan Amirtharajan. "Image encryption: An information security perceptive." *Journal of Artificial Intelligence* 7, no. 3 (2014): 123.
<https://doi.org/10.3923/jai.2014.123.135>
- [5] Kaur, Mandeep, Surender Singh, and Manjit Kaur. "Computational image encryption techniques: a comprehensive review." *Mathematical Problems in Engineering* 2021 (2021): 1-17.
<https://doi.org/10.1155/2021/5012496>
- [6] Manihira, Nitya Ranjan, and Alpesh Kumar Dauda. "Image encryption using chaotic maps and DNA encoding." *International Journal of Engineering Research & Technology* 10, no. 11 (2022): 1-5.
<https://doi.org/10.17577/IJERTCONV10IS11137>
- [7] Al-Maadeed, Somaya, Afnan Al-Ali, and Turki Abdalla. "A new chaos-based image-encryption and compression algorithm." *Journal of Electrical and computer Engineering* 2012 (2012): 15-15.
<https://doi.org/10.1155/2012/179693>
- [8] ElKamchouchi, Dalia H., Heba G. Mohamed, and Karim H. Moussa. "A bijective image encryption system based on hybrid chaotic map diffusion and DNA confusion." *Entropy* 22, no. 2 (2020): 180.
<https://doi.org/10.3390/e22020180>
- [9] Ghazanfaripour, Hamed, and Ali Broumandnia. "Designing a digital image encryption scheme using chaotic maps with prime modular." *Optics & Laser Technology* 131 (2020): 106339.
<https://doi.org/10.1016/j.optlastec.2020.106339>
- [10] Ye, Guodong, Min Liu, and Mingfa Wu. "Double image encryption algorithm based on compressive sensing and elliptic curve." *Alexandria engineering journal* 61, no. 9 (2022): 6785-6795.
<https://doi.org/10.1016/j.aej.2021.12.023>
- [11] Masood, Fawad, Jawad Ahmad, Syed Aziz Shah, Sajjad Shaukat Jamal, and Iqtadar Hussain. "A novel hybrid secure image encryption based on julia set of fractals and 3D Lorenz chaotic map." *Entropy* 22, no. 3 (2020): 274.
<https://doi.org/10.3390/e22030274>
- [12] Munir, Noor, Majid Khan, Sajjad Shaukat Jamal, Mohammad Mazyad Hazzazi, and Iqtadar Hussain. "Cryptanalysis of hybrid secure image encryption based on Julia set fractals and three-dimensional Lorenz chaotic map." *Mathematics and Computers in Simulation* 190 (2021): 826-836.
<https://doi.org/10.1016/j.matcom.2021.06.008>
- [13] Ouannas, Adel, Amina-Aicha Khennaoui, Samir Bendoukha, Zhen Wang, and Viet-Thanh Pham. "The dynamics and control of the fractional forms of some rational chaotic maps." *Journal of Systems Science and Complexity* 33, no. 3 (2020): 584-603.
<https://doi.org/10.1007/s11424-020-8326-6>
- [14] Xie, Zizhao, Jingru Sun, Yiping Tang, Xin Tang, Oluyomi Simpson, and Yichuang Sun. "A K-SVD based compressive sensing method for visual chaotic image encryption." *Mathematics* 11, no. 7 (2023): 1658.
<https://doi.org/10.3390/math11071658>
- [15] Zhou, Chengyi, Zhijun Li, Fei Xie, Minglin Ma, and Yi Zhang. "Bursting oscillations in Sprott B system with multi-frequency slow excitations: two novel "Hopf/Hopf"-hysteresis-induced bursting and complex AMB rhythms." *Nonlinear Dynamics* 97 (2019): 2799-2811.
<https://doi.org/10.1007/s11071-019-05164-6>
- [16] De Dieu, Nkapkop Jean, Folifack Signing Vitrice Ruben, Tsafack Nestor, Njitacke Tabekoueng Zeric, and Kengne Jacques. "Dynamic analysis of a novel chaotic system with no linear terms and use for DNA-based image encryption." *Multimedia Tools and Applications* 81, no. 8 (2022): 10907-10934.
<https://doi.org/10.1007/s11042-022-12044-6>
- [17] Man, Zhenlong, Jinqing Li, Xiaoqiang Di, Yaohui Sheng, and Zefei Liu. "Double image encryption algorithm based on neural network and chaos." *Chaos, solitons & fractals* 152 (2021): 111318.
<https://doi.org/10.1016/j.chaos.2021.111318>

- [18] Yu, Wenqian, Ye Liu, Lihua Gong, Miaomiao Tian, and Liangqiang Tu. "Double-image encryption based on spatiotemporal chaos and DNA operations." *Multimedia Tools and Applications* 78 (2019): 20037-20064.
<https://doi.org/10.1007/s11042-018-7110-2>
- [19] Huang, Wei, Donghua Jiang, Yisheng An, Lidong Liu, and Xingyuan Wang. "A novel double-image encryption algorithm based on Rossler hyperchaotic system and compressive sensing." *IEEE Access* 9 (2021): 41704-41716.
<https://doi.org/10.1109/ACCESS.2021.3065453>
- [20] Nilsson, Jim, and Tomas Akenine-Möller. "Understanding ssim." *arXiv preprint arXiv:2006.13846* (2020).
<https://doi.org/10.48550/arXiv.2006.13846>
- [21] Laiphrakpam, Dolendro Singh, Rohit Thingbaijam, Khoirom Motilal Singh, and Moatsum Al Awida. "Encrypting multiple images with an enhanced chaotic map." *IEEE Access* 10 (2022): 87844-87859.
<https://doi.org/10.1109/ACCESS.2022.3199738>