International Journal of Mathematics and
Computer Science, **17**(2022), no. 1, 183–194

An RGB Color Image Double Encryption Scheme

Thammarat Panityakul[1], Mahwish Bano[2],
Tasneem M. Shah[3], Dulyawit Prangchumpol[4]

[1]Division of Computation Science
Faculty of Science
Prince of Songkla University
Hat Yai, Songkhla 90110, Thailand

[2]Department of Mathematics
Air University
Islamabad, Pakistan

[3]Department of Mathematics
Preston University
Islamabad, Pakistan

[4]Department of Information Technology
Faculty of Science and Technology
Suan Sunandha Rajabhat University
Bangkok 10300, Thailand

email: thammarat.p@psu.ac.th, mahwish@mail.au.edu.pk,
dr.tasneem@preston.edu.pk, dulyawit.pr@ssru.ac.th

(Received June 18, 2021, Accepted August 6, 2021)

Abstract

In this paper, we present an encryption technique for an RGB color image involving Markov matrices and chaotic map. We use Henon's chaotic map in the given algorithm to shuffle the image pixels. The Henon's map is the simplest two dimensional mapping exhibiting

Key words and phrases: Encryption time, decryption time, MSE, PSNR, Markov matrices, Henon map.
AMS (MOS) Subject Classifications: 68P25.
Corresponding author: Dulyawit Prangchumpol (dulyawit.pr@ssru.ac.th)
ISSN 1814-0432, 2022, http://ijmcs.future-in-tech.net

chaotic behaviors and is being used due to its low dimensions and chaotic behavior. The Model RGB color image is encrypted using a random Markov matrix key. A chaotic map is applied to the image and that image is then used as a key for further encryption of a previously encrypted image by shuffling the pixels. Basically, we use a random Markov matrix as a key and then produce a sub key using the Henon's map.

1 Introduction

Data security has developed as a considerable worry in our present computerized time. The headways in the new transmission innovations demand a requirement for explicit techniques of security instruments particularly in the information correspondence. System security is critical as the amount of information being moved across the web is expanding. With the fast development and rise in technology over the past few decades, a lot of advancements were made in cryptography as well. Many cryptographic algorithms have been introduced adding to the qualitative and quantitative aspects of existing knowledge of cryptography. Each of these techniques has an edge over the other in some way, in meeting the growing need of security. Images are most frequently used data and therefore providing image security is the utmost need of the hour. Image encryption is harder than text encryption due to bulk data and high level of data redundancy. As a lot of confidential data is transferred through images so many algorithms are constructed for image encryption. It is necessary to study novel and safer cryptosystems to meet the current safety requirements in the area of image encryption [11]. An encryption algorithm makes sure that only the authorized party is able to decrypt the image back to its original form. Nowadays, the mainly used image encryption techniques involve pixel transformation, digital image encryption that relies on random sequence, digital image encryption based on image compression coding, and digital image encryption utilizing an image key. Chaos technology is also being widely used for image encryption because it cannot be easily cracked. A randomness encryption technique based on chaos theory provides high security features. A lot of new efficient chaotic image encryption techniques are brought up in recent times. Chaotic systems are frequently being applied to image encryption because of their properties such as random like behavior and sensitivity to initial conditions [11]. In the field of chaotic encryption, the most important element to study is chaotic maps which often occur in the study of dynamic nonlinear systems. The behavior of chaotic maps is governed by some particular mathematical equation. They are very sensitive to the initial conditions and the slightest change in the initial conditions leads to significant changes in the output and seem to be random and disorderly but actually they follow some sort of pattern. The output of the chaotic systems having properties of randomness is used to induce confusion and diffusion properties in the cryptosystem. Confusion applies to forming the connection of the key with the cipher data as convoluted whereas diffusion shows that the repetition in the statistics of the original data is depleted in the statistics of the cipher data. Diffusion means that the output bits are dependent, in a complex manner, on the input bits. Generally, the change in one bit of the original text changes the cipher text altogether in a random way, especially in case of a good cipher. Confusion works on making the key undetectable even if the intruder has an abundance of original data and cipher data pairs using the same key. Hence every element of the cipher data depends on the complete key and in various manners on various bits of the key. Therefore, altering a single bit of the key will result in a complete change of the cipher text. There are mainly three basic aspects of the technique which are modified for different algorithms of image encryption: chaotic mapping, use of the mapping, and structure of algorithm. Classical one-dimension chaos, particularly the Logistic map and Arnold map [12], is generally utilized to encrypt images. However, due to limitations linked to a small secret key space and uncertain security of one dimensional chaotic systems, researchers are now leaning towards working with higher dimensional chaotic systems [13]. To enhance the security and reliability of chaotic encryption science, some researchers have expanded the two dimensional chaotic encryption schemes to develop chaotic encryption techniques in three-dimensional space and higher multidimensional space [5]. Despite better chaotic properties and highly complex dynamics of higher dimensional chaotic systems, there are some downsides to them as they require a large amount of hardware resources and in some cases are not effective real time techniques [20]. The chaos encryption technology based on high dimension space proposed by some scholars has problems of poor uniformity of pixels in the process of encryption, the difficulty of confusion processing, and the low efficiency of encryption and decryption process. Both substitution and permutation processes were utilized to improve the encryption techniques structured on the traditional logistic map [10], the Gray code [16] and a two dimensional hyper-chaos discrete nonlinear dynamic system with the Chinese Reminder Theorem [21]. Zhang et al. [18] proposed a scheme to shuffle the image pixel through permuting plane by expanding and shrinking. Moreover, Sethi and Vijay [9] gave another scheme based on two phases to encrypt the image. Furthermore, sub-keys were generated using four different chaotic maps in [8], and the logistic map and the Arnold's Cat Map were applied in [15], [17], etc. Besides the chaotic systems, the non-chaotic methods have also shown to be effective and important in carrying out the confusion diffusion schemes. These sorts of techniques generally enhance the complexity of the algorithm to protect against the cryptanalysis. Likewise, a two dimensional substitution-permutation structure was developed using the Latin Squares Technique by Wu et al. [14]. Pareek et al. [7] proposed a technique in which the image was first divided into non-overlapping blocks and each block was then scrambled using a zigzag-like algorithm. In addition, Al-Husainy [2] divided the image into a set of n-bit vectors first and then each vector was substituted by the XOR of that vector with the previous vector and finally permuted by right rotating its bits circularly. On the contrary, after dividing the image into non-overlapping blocks, Pareek et al. [6] performed every encryption round by using the round key to change the size of the block. Within the same block, a permutation was performed using a zigzag-like algorithm. The combination of chaotic and non-chaotic algorithms displayed good results in many cryptosystems. Li and Liu [4] used the 3D Arnold Map and a Laplace-like equation to carry out permutations and substitutions, respectively. Fouda et al. [3] proposed a technique where a linear chaotic map gave rise to pseudo random numbers which were used to produce the coefficients of a Linear Diophantine Equation (LDE). Large permutations were created from the solution of LDE and were used to shuffle the image pixels. Zhang and Xiao [20] used a coupled logistic map, self-adaptive permutation, substitution-boxes and combined global diffusion to perform the encryption. In this paper, a double encryption technique is proposed. An encryption procedure similar to that of Al-Laham [1] technique is carried out initially. In particular, the random key generated in the proposed technique is the double random Markov matrix. Then a second key is produced from the two dimensional Henon chaotic map to introduce chaos and randomness in the technique.

2 Encryption-decryption parameters

To determine the effectiveness of the proposed image encryption-decryption algorithm, the following parameters must be taken into account:
2.1 **Encryption time.** The time required for the encryption process.

2.2 **Decryption time.** The time required for decryption process.
2.3 **Mean square error.** It is measure of quality of the algorithm. In an efficient algorithm, the mean square error value of original and decrypted image is zero whereas the mean square error value of the original and encrypted images is large. The mean square error is given as

$$MSE = \frac{1}{MN}\sum_{m=1}^{N}\sum_{n=1}^{M}[I(m,n) - D(m,n)]^2,$$

where I is the original image and D is the decrypted image.
2.4 **PSNR.** For an ideal encryption, the PSNR between the original image and the encrypted image must be very low and between the original image and the decrypted one must be close to infinity (zero errors).
2.5 **Entropy.** Entropy is the measure of degree of randomness. For image encryption, we want the cipher image pixel values to be highly random. A good cipher image will have an entropy value close to 8. The entropy is given by

$$H(x) = -\sum_{I=1}^{n} p_i \log_2 p_i.$$

3 Fundamental knowledge

3.1 **Markov matrices.** A Markov matrix, also known as a stochastic matrix or probability matrix, is used to represent steps in a Markov chain. Each input of the Markov matrix represents the probability of an outcome. A right stochastic matrix means each row sums to 1 whereas a left stochastic matrix means each column sums to 1. In a doubly stochastic matrix, both the rows and the columns sum to 1. The Markov matrix provides a complete way to understand the probabilities of each step in a Markov chain and is a useful tool in almost any field that requires formal analysis.
3.2 **Henon's map.** A Henon's chaotic system is a 2-D dynamic system described as:

$$x_{i+1} = 1 - ax_i^2 + y_i, y_{i+1} = bx_i \text{ for } i = 1, 2, 3, \ldots.$$

Here a and b are initial parameters. Each point (x_n, y_n) is mapped to a new point (x_{n+1}, y_{n+1}) through the Henon's map. The initial conditions x_0 and y_0 and the parameters a and b serve as the key, making it hard to predict the data.

4 The proposed Image Encryption technique

The technique that is proposed in this paper uses two keys. First, a Markov matrix is used to encrypt the original RGB color image and then a second key produced by Henon map is used. A Henon map will enhance the security of the previously encrypted image by shuffling pixels of the image.

4.1 **Encryption algorithm.** The following steps are performed for the encryption of RGB color image:

- Input original RGB color image.
- Extract its red, green and blue components.
- Change the three dimensional image to a one dimensional array.
- Resize the array into two square dimensional matrices.
- Generate and save the random Markov key.
- Multiply the Markov key with the matrix obtained in step IV.
- Obtain a second key from Henon's map and apply it to step VI.
- Get the encrypted image.

4.2 **Decryption algorithm.** In the decryption process, the steps explained in above the flowchart are reversed.

5 Simulation results

In this section, some security analysis results are discussed. The outcomes of the algorithm at the encryption and decryption stages are illustrated. The original image used as a test and its red, green and blue components are shown in Figure 1.

Matlab codes were implemented various times on images of different sizes. The time taken by the suggested technique to encrypt and decrypt the images of various sizes is measured. The results are given in Table 1.

Table 1: Encryption-decryption times and total time required for the technique implementation on images of different size.

Image size	Encryption time(sec)	Decryption time(sec)	Total time (sec)
200*300*3	0.356398	0.182998	0.539396
225*225*3	0.857358	0.266689	1.124047
768*512*3	2.700832	1.790966	4.491798

In addition, each time the results are displayed on images of different sizes they displayed that the mean square error of original image and decrypted image is zero. That means the original and decrypted images came out identical, as can be seen from Figure 2 to Figure 4.

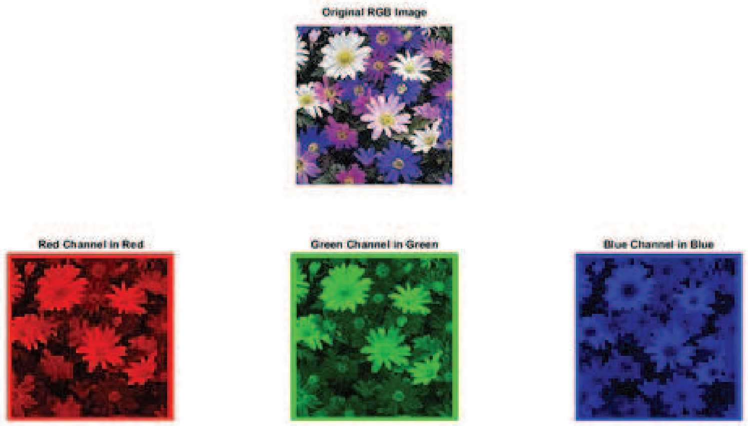

Figure 1: Original RGB image and its red, green, blue components.

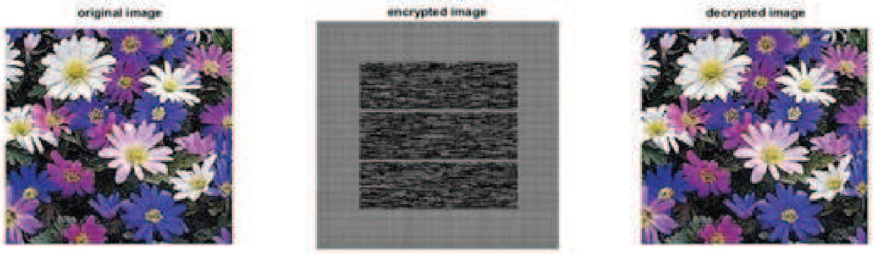

Figure 2: Original 225*225*3 size image, its encrypted and decrypted images.

The values for the mean square error (MSE) and the peak signal to noise ration (PSNR) for the three test images are given in Table 2. The readings show that PSNR is close to infinity between original and decrypted image which is ideal for an efficient encryption-decryption algorithm.

Table 2: MSE and PSNR values of different size images.

Image size	MSE	PSNR
200*300*3	0	Infinity
225*225*3	0	Infinity
512*768*3	0	Infinity

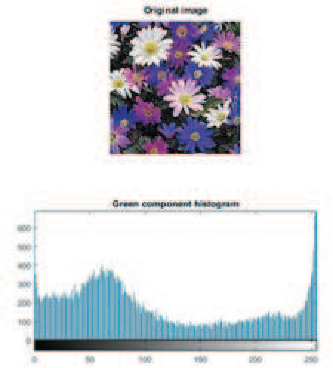

Figure 3: Original 225*225*3 image and its RGB component histograms.

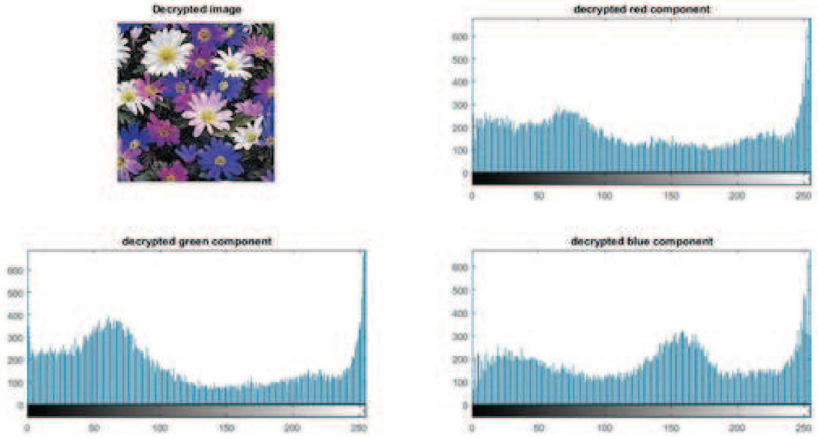

Figure 4: Decrypted 225*225*3 image and its RGB component histograms.

Table 3: Entropy of images of different sizes.

Image size	Entropy
200*300*3	7.5639
225*225*3	7.0603
512*768*3	6.9453

From Table 3, we conclude that the information entropy indicates that it is difficult to conduct a successful attack because the values of the information entropy for the cipher-images are close to a theoretical value of 8.

6 Conclusion

An RGB color image encryption technique based on a chaotic map wass proposed. The color image was doubly encrypted with two keys. Initially, the identity of the image was hidden by an operating random Markov matrix key and changing the pixel values of the image. Then randomness was introduced in image pixels through the simple 2-D Henon chaotic mapping. The analysis was done on a personal computer with Intel Celeron 2.16 GHz processor and 4 GB RAM, while the implementation was performed using MATLAB 2017. The results were measured for three different color images with different sizes.

Table 4: Encryption-decryption times of images based on Al-Laham's technique

Image size	Encryption time(sec)	Decryption time(sec)	Total time (sec)
200*300*3	0.395506	0.285005	0.680511
225*225*3	0.858185	1.079542	1.937727
768*512*3	2.848969	2.699534	5.548503

From Tables 1 and 4, it is obvious that the proposed technique is faster than the Al-Laham technique.

Table 5: Entropy values of images based on Al-Laham's technique

Image size	Entropy
200*300*3	0.2531
225*225*3	0.8032
512*768*3	1.027

The proposed technique is better than Al-Laham [28] in providing higher security due to randomness. Also entropy of the encrypted image was not calculated in Al-Laham [28]. The entropy values with Al-Laham technique in Table 5 calculated for these images is close to zero while the entropy of images encrypted through proposed technique is close to the ideal value. The results have shown following achievements:

- The technique enables to decrypt the message with 100% accuracy, since the MSE is zero.
- Fast speed in encryption phase.
- Fast speed in decryption phase.
- The PSNR and histogram analysis also show the efficiency of the technique.
- The higher entropy values indicate the higher level of randomness given by this algorithm, which provides higher security.
- This technique also ensures high security through separate encryption of the components with a random Markov matrix key.

- No loss of data information.
- Almost impossible to hack.

Acknowledgments: The authors would like to thank Suan Sunandha Rajabhat University for scholarship support.

References

[1] M. M. Al-Laham, Encryption-decryption RGB color image using matrix multiplication. International Journal of Computer Science and Information Technology, **7**, no. 5, (2015), 109–119.

[2] M. A. F. Al-Husainy, A novel encryption method for image security, International Journal of Security and Its Applications, **6**, no. 1, (2012), 1–8.

[3] J. A. E. Fouda, J. Y. Effa, S. L. Sabat, M. Ali, A fast chaotic block cipher for image encryption. Communications in Nonlinear Science and Numerical Simulation, **19**, no. 3, (2014), 578–588.

[4] Z. Li, X. Liu, The image encryption algorithm based on the novel diffusion transformation. In 2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering, **5**, (2010), 345–348.

[5] L. Liu, S. Xiao, L. Zhang, M. Bi, Y. Zhang, J. Fang, W. Hu, Digital chaos-masked optical encryption scheme enhanced by two-dimensional key space, Optics Communications, **398**, (2017), 62–66.

[6] N. K. Pareek, V. Patidar, K. K. Sud, Substitution-diffusion based image cipher. International Journal of Network Security and Its Applications, **3**, no. 2, (2011), 149–160.

[7] N. K. Pareek, V. Patidar, K. K. Sud, Diffusion-substitution based gray image encryption scheme, Digital signal processing, **23**, no.3, (2013), 894–901.

[8] G. A. Sathishkumar, D. N. Sriraam, Image encryption based on diffusion and multiple chaotic maps, arXiv preprint arXiv:1103.3792, (2011).

[9] N. Sethi, S. Vijay, Comparative image encryption method analysis using new transformed-mapped technique. In Proceedings of the Conference on Advances in Communication and Control Systems, (2013), Atlantis Press.

[10] A. N. K. Telem, C. M. Segning, G. Kenne, H. B. Fotsin, A simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network. Advances in Multimedia, (2014).

[11] X. Wang, N. Guan, H. Zhao, S. Wang, Y. Zhang, A new image encryption scheme based on coupling map lattices with mixed multi-chaos. Scientific reports, **10**, (2020), 1–15.

[12] C. Wang, X. Wang, Z. Xia, C. Zhang, Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm, Information Sciences, **470**, (2019), 109–120.

[13] X. Wang, H. Zhao, L. Feng, X. Ye, H. Zhang, High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices. Optics and Lasers in Engineering, **122**, (2019), 225–238.

[14] Y. Wu, Y. Zhou, J. P. Noonan, S. Agaian, Design of image cipher using latin squares. Information Sciences, **264**, (2014), 317–339.

[15] R. Ye, A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Optics Communications, **284**, no. 22, (2011), 5290–5298.

[16] M. Zanin and A. N. Pisarchik, Gray code permutation algorithm for high-dimensional data encryption. Information Sciences, 270, (2014), 288-297.

[17] W. Zhang, K. W. Wong, H. Yu, Z. L. Zhu, An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion, Optics Communications, **285**, no. 9, (2012), 2343–2354.

[18] W. Zhang, K. W. Wong, H. Yu, Z. L. Zhu, A symmetric color image encryption algorithm using the intrinsic features of bit distributions, Communications in Nonlinear Science and Numerical Simulation, **18**, no. 3, (2013), 584–600.

[19] Y. Zhang, D. Xiao, Self-adaptive permutation and combined global diffusion for chaotic color image encryption. AEU-International Journal of Electronics and Communications, **68**, no.4, (2014), 361–368.

[20] Y. Zhou, L. Bao, C. P. Chen, A new 1D chaotic system for image encryption. Signal processing, **97**, (2014), 172–182.

[21] H. Zhu, C. Zhao, X. Zhang, A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem, Signal Processing: Image Communication, **28,** no. 6, (2013), 670–680.