

## Multi Facial Blurring using Improved Hénon Map

Saparudin<sup>\*1</sup>, Ghazali Sulong<sup>2</sup>, Muhammed Ahmed Saleh<sup>2</sup>

<sup>1</sup> Faculty of Computer Science, Sriwijaya University, Indralaya, Sumatera Selatan, Indonesia.

<sup>2</sup> Digital Media and Games Centre of Excellence (MaGIC-X), Faculty of Computing, Universiti Teknologi Malaysia, Skudai, Johor, 81310, Malaysia.

\*Corresponding author, e-mail: Saparudin1204@yahoo.com<sup>1</sup>, ghazali@utmpace.edu.my<sup>2</sup>, hasibat2003@yahoo.com<sup>3</sup>

### Abstract

Generally, full encryption is applied on the entire image to obscure the faces. However, it suffers in overhead, speed and time. Alternatively, selective encryption can be used to encrypt only the sensitive part of the image such as human faces. This paper proposes a new encryption algorithm using enhanced Hénon chaotic map to conceal the faces. This technique involves three steps: face detection, encryption and decryption. Experiments have been performed to evaluate security such as histogram, sensitivity and statistical analysis, and results reveal that the proposed method provides high security with entropy and correlation close to ideal values.

**Keywords:** selective image encryption, face detection, face blurring, hénon map, chaotic system

### 1. Introduction

The protection of private or personal data is essential to provide an efficient work environment. This is because networks have become essential to growing multimedia applications and there is a need for data security techniques to safeguard valuable data from unauthorized access. The confidentiality of data is provided by encryption, which renders the data unreadable by unauthorized persons. Encryption can be applied to different types of data. However, each type has its own inherent characteristics. For example, images represent a significant type of data because of their wide scale use. Images have their own characteristics as they contain a large amount of data and neighbouring pixels have strong correlations meaning that the value of each pixel can be reasonably predicted from its neighbouring pixels, thus the requirement for different encryption methods. Current encryption algorithms encrypt the entire image including the background, which may be considered irrelevant or less important. Also, the algorithm requires extra overhead [1].

Selective encryption is one of the new ways of securing content from unauthorized users. In selective encryption, the main goal is to reduce the amount of data to be encrypted while obtaining the required level of security. Selective encryption has the additional feature of preserving some of the functionalities of the original bit stream. A common approach is to divide the content in two public and private in selective encryption parts, protected part is made as small as possible [2].

This paper presents a new selective encryption technique based on improved Hénon chaotic map to obscure facial images. The process involved three parts namely face detection, encryption and decryption. The rest of the paper is organized into sections. Section 2 is the related work of the study which is followed by methodology in section 3, while the results of the experiments are explained in detail in section 4. The summary and concluding remarks are given in section 5.

### 2. Related Work

Hénon chaotic map [3] has some characteristics, such as ergodicity, randomness and the sensitivity of initial conditions and control parameters, these makethequality is improved and the defect of data redundancy is reduced also. In 2009, [4] presented a new image encryption algorithm based on Hénon's chaotic system in order to meet the requirements of secure image transfer. Shuffling positions and changing the grey values of image pixels were combined to change the relationship between the cipher-image and the original-image. First, Arnold's cat

map was used to change the positions of the image pixels. Second, the shuffled-image was encrypted pixel by pixel using Hénon's chaotic system. The authors improved the equations of Hénon map by merging the two equations into one equation. This improved equation works like the original two Hénon map equations.

Four years later, [5] presented a novel image encryption technique based on a Hénon chaotic map. Chaos-based image encryption techniques are one of the more promising encryption algorithms. They provide very efficient and fast image encryption due to their deterministic nonlinear systems that exhibit extreme sensitivity to initial condition and random like behaviours.

In same year, [1] presented three distinct image encryption techniques for colour images. Two of the three techniques use a selective encryption algorithm and the first technique uses Region Based Selective Image Encryption. This algorithm encrypts part of the bit-stream using a well\_proven ciphering technique. A watermark message is added during this process along with a decryption key that the receiver uses to decrypt the bit-stream and decompress the image. In principle, there is no difference between the original image and the encrypted image.

Following that, [6] introduced two different methods for selective image encryption. The first method divides an image into sub-blocks and then selected blocks are manually sent to the encryption process. The second method automatically detects the positions of objects and then selected objects are sent to the encryption process. Morphology techniques are employed to detect the positions of objects in the images. These two approaches were specifically developed to encrypt medical and satellite images.

Finally, [7] proposed an image encryption technique that selects facial areas and encrypts them using RGB pixel regrouping of an image of  $m \times n$  size. As a result, it is difficult for off-the-shelf software to restore the encrypted image. This technique is useful for law enforcement agencies to reconstruct a face from pictures or videos related to abuse cases.

### 3. Proposed Method

First, feature extraction is performed using Viola Jones with best feature selection using AdaBoost algorithm then applying Cascaded classifier to detect one or more front faces rapidly. Second, encrypting and decrypting human faces. The process utilizes Hénon map but with some improvements.

The proposed method improved Hénon map using Sine function on the  $x$ -axis and Tangent function on the  $y$ -axis which also includes the frequency  $w$  to control the Hénon chaotic signal. These parameters used distorted signals from unauthorized users to decrypt the signal due to specific characteristics such as nonperiodicity, ergodicity, and randomness. The proposed method used four initial values, four parameters and two frequencies as given by the following equations:

$$x_{i+2} = 1 - ax_{i+1}^2 + b \sin(wx_i) \quad (1)$$

$$y_{n+2} = 1 - ay_{n+1}^2 + b \tan(wy_n) \quad (2)$$

where:  $a > 0$ ,  $|b| < 1$ ,  $n = 0, 1, 2, \dots$

#### 3.1 Encryption process

**Input:** detected faces

**Output:** encrypted faces

**Step1:** generate the secret key by using equations 1 and 2.

**Step2:** Separate the image colors into three component matrices Red, Green, and Blue.

**Step3:** encrypt the human faces using BitXOR operation based on the secret key obtained from step 1 and the color component matrices acquired in step 2 as seen in Figure 1.

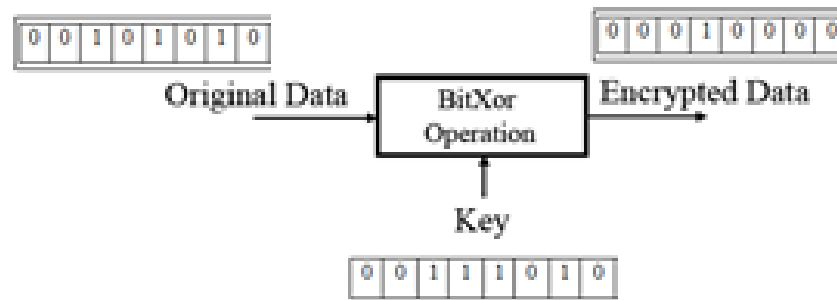


Figure 1. XOR Encryption

After protecting the image from unauthorized access by encrypting the human faces, the next step is to decrypt the secure image by using decryption algorithm which works similar to the encryption phase except it is done in a reverse manner.

#### 4. Experimental Results and Discussion

This part employed two different images. The first image sample is standard image database USC-SIPI (Lena). The second is an internet image for Nasser football player URL (<http://www.alrmaa.com>) used to test the proposed method on multi facial encryption. Hénon map, improved Hénon map and chaos system algorithms have been tested on color image 512X512 pixels. The results of these processes are as shown in Table 3 and Table 4. Here we can conclude that the cipher images resulted from all the three algorithms under chaotic map operation of mode display a vivid figure of the original image.

However, the encryption for improved Hénon map gives a better cipher. The encrypted images do not show any clue of the original image because this method are changed the value of pixel through the equations (1),(2) of proposed method. As a result, the cipher image is more chaotic and random. It should be noted here that the processing time is very fast because the algorithm is encrypt just only the multi-facial humans. Table 1 presents execution time between the entire image and the area of interest in the image in the encryption and decryption respectively, and the proposed method reduced the execution time with high security. Security analysis such as histogram, sensitivity, and statistical properties were examined by calculating entropy and the correlation of two adjacent pixels in the ciphered image as discussed in the next section. And also we have compared the different algorithm of selective encryption technique based on their result analysis.

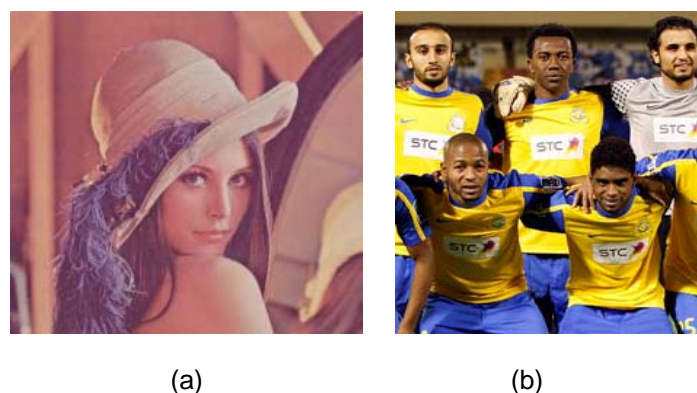


Figure 2. Test Image: (a) Lena (b) Football

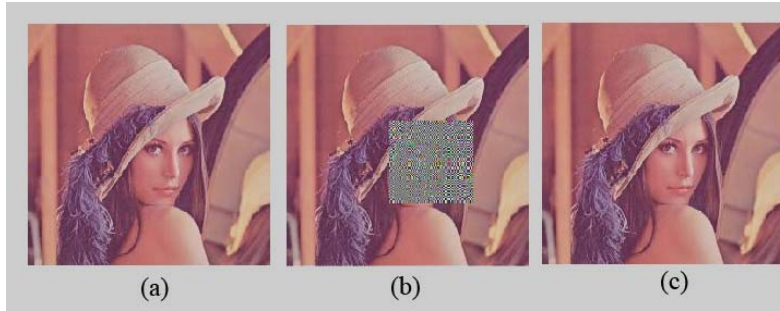


Figure 3. Partial encryption of Lena: (a) original (b)encrypted image (c)decrypted image

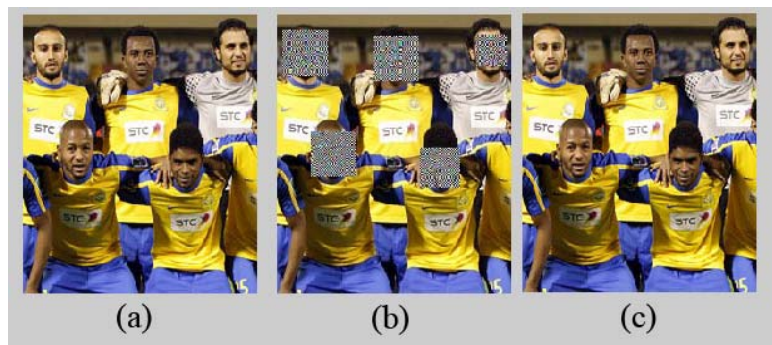



Figure 4. Partial encryption of five faces: (a)original image (b)encrypted image (c)decrypted image

Table 1. Execution time for all images and facial part of the image

Image	Execution Time	
	Encrypt and decrypt all image	Encrypt and decrypt part of image
	1.493323 seconds	0.483053 seconds

#### 4.1 Security Analysis

The security of the proposed technique was analyzed using standard histogram procedures including sensitivity for initial value, entropy, and adjacent correlation.

**Histogram Analysis:** The first security evaluation of the proposed method has been tested by comparing the histograms of encrypted image and plain image. The results of this evaluation are illustrated in Figure 5. The proposed method has shown more distributed frequency and more unrecognizable encrypted images, good statistical properties and more robust against statistical attack.

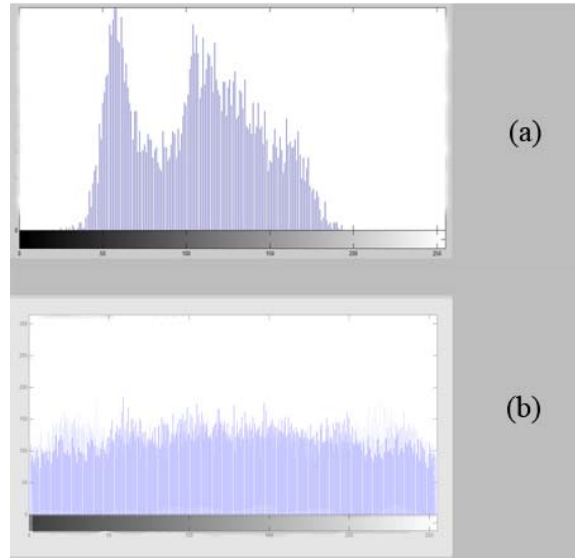


Figure 5. Histogram analysis of Lena(a)original image (b)encrypted image

**Sensitivity:** Another test with respect to secret key is the key sensitivity test that indicates how much an encrypted image is sensitive towards the change in the key. For a secure cryptosystem, a decryption algorithm will not decrypt cipher image correctly, even if there is a one bit difference between key. It means that large key sensitivity is required for highly secure cryptosystems. An ideal image encryption should be sensitive with respect to the secret key such that a single bit change in the key should produce a completely different encrypted image [8].

The experimental results of this research demonstrated that the encryption algorithm was very sensitive to the secret key because it depends on four initial values. Any small change in any value, even if the rate of change was 1 bit may result in faulty decryption. The different analysis of faulty tests is summarized in Table 2.

Table 2. Face decryption error with faulty initial value for Lena image

	Initial value	Fault decryption image
1	Initial value fault decryption with x axes	
2	Initial value fault decryption with y axes	
3	Initial value fault decryption with both x, y axes	

**Entropy:** Information density, or entropy, is a method for measuring uncertainty in a series of numbers or bytes. In technical terms, entropy measures the level of difficulty or the probability of independently predicting each number in the series.

In order to analyze the entropy of image encryption, each pixel color is represented by 8 bits. If entropy is evaluated in the aforementioned case, the entropy obtained is 8. In general, the entropy value of the source is smaller than the ideal value. However, when images are encrypted for a source, its entropy should be 8 bits ideally. In case if entropy is less than 8 bits, then there exists a certain degree of predictability. For a cryptosystem to resist the entropy attacks, the entropy of the cryptosystem should be close to the ideal value [9], [10].

The entropy evaluation of the proposed method is 7.9995 in table 3, its close to ideal entropy.

Table 3. Entropy analysis between authors

Entropy Analysis for Lena image	
Authors	Entropy values
[15]	7.9993
[1]	7.9936
Proposed Method	7.9995

**Correlation coefficient:** Correlation determines the relationship between two variables. In other words, correlation is a measure that computes the degree of similarity between two variables. The correlation coefficient is a useful measure to judge encryption quality of any cryptosystem. An image cryptosystem is said to be good, if encryption algorithm hides all attributes of a plain image, and encrypted image is totally random and highly uncorrelated [11]. If encrypted image and plain image are completely different then their corresponding correlation coefficient must be very low, or very close to zero. If the correlation coefficient is equal to one, then the two images are identical and they are in perfect correlation. In case of perfect correlation (the correlation coefficient is equal to 1), an encryption process completely false because the encrypted image is same as the plain image. When the correlation coefficient is -1 then encrypted image is negative of original (plain) image. In short, the correlation coefficient between an image and it is 1, the correlation coefficient between an image and totally unrelated image is zero, and correlation coefficient between an image and its negative is -1 [12]-[16]. The security of the proposed technique as evaluated by examining the correlation coefficients depending on vertical, horizontal, and diagonal of the adjacent pixels in plain image and encrypted image. Table 4 presents the performance comparison of the proposed method with the previous works of these parameters [1],[16].

Table 4. Correlation Coefficient values between Authors

Correlation Coefficient Analysis for Lena image			
Author	Adjacent pixel with Diagonal		
	R	G	B
[16]	0.02428	0.04041	0.011095
Proposed Method	0.0038	0.0031	0.0019
Author	Adjacent pixel with horizontal and vertical		
	Horizontal	Vertical	
[1]	-0.0495	0.0697	
Proposed Method	-0.0376	0.0535	

## 5. Conclusion

This paper presented a facial encryption technique and proposed a new color image encryption algorithm based on improved Hénon chaotic map. The encryption process was applied to all RGB channels. These channels go through the two dimensional Hénon chaotic map to produce a random bit-stream. In order to produce the encrypted image bitXOR operation is executed between the random key and the original pixel values of all channels (RGB). The proposed scheme has multi-dimensional keys to resist all possible brute-force types of attack.

The effectiveness of the proposed method was firstly evaluated by security analysis, which covered histogram, sensitivity, entropy, and correlation analysis. Histogram analysis shows that the histogram of cipher image is flat or uniformly distributed, so the algorithm is secure from frequent analysis attack and the achieved results were very promising, the best results on this dataset to date. As well, the selective encryption approach reduces the overhead of encrypting non-sensitive areas and enhanced the execution time. This study also investigated the strengths of the proposed algorithm in different environments such as multi facial encryption.

## References

- [1] Kaur, R. Comparative Analysis and Implementation of Image Encryption Algorithms. *International Journal of Computer Science & Network Security*. 2003; 13(12): 1-10.
- [2] Pisarchik, A., Flores-Carmon, N. and Carpio-Valadez, M. Encryption and Decryption of images with Chaotic Map Lattices. *Chaos: An Interdisciplinary Journal of Nonlinear Science*. 2006; 16(3): 33-38.
- [3] Ren, W., Kang, C., Li, Y., Gong, L. Chaotic Immune Genetic Hybrid Algorithms and Its Application. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11(2): 975-984.
- [4] Wei-bin, C., Xin, Z. *Image Encryption Algorithm based on Hénon Chaotic System*. IASP 2009. International Conference on Image Analysis and Signal Processing, Taizhou. 2009: 94-97.
- [5] Ramesh Kumar yadava, DBK. s., SK. Sinha, KK. Pandey. A New Approach of Colour Image Encryption Based on Hénon like Chaotic Map. *Journal of Information Engineering and Applications*. 2013; 3(6): 1-10.
- [6] Panduranga, H., NaveenKumar, S. Selective Image Encryption for Medical and Satellite Images. *International Journal of Engineering Science & Technology*. 2013; 5(2): 32- 43.
- [7] Kester, QA. A Cryptographic Image Encryption Technique for Facial-blurring of Images. *International Journal of Advanced Technology and Engineering Research (IJATER)*. 2013: arXiv: 1307.6409.
- [8] H. Liu, Z. Zhu, H. Jiang, B. Wang. *A novel image encryption algorithm based on improved 3d chaotic cat map*. The 9<sup>th</sup> IEEE International Conference for Young Computer Scientists (ICYCS 2008). 2008: 3016–3021.
- [9] R. Enayatifar. Image encryption via logistic map function and heap tree. *Int. J. Phys. Sci.* 2011; 6(2): 221-233.
- [10] Z. Han, W. Feng, L. Hui, L. Da Hai, L. Chou. *A new image encryption algorithm based on chaos system*. Proceedings of IEEE International Conference on Robotics, Intelligent Systems and Signal Processing. 2003; 2: 778–782.
- [11] I. Elashry, O. Allah, A. Abbas, S. El-Rabaie, F. El-Samie. Homomorphic image encryption. *Journal of Electronic Imaging*. 2009; 18: 033002.
- [12] H. Elkamchouchi, M. Makar. *Measuring encryption quality for bitmap images encrypted with rijndael and kamkar block ciphers*. Proceedings of the 22<sup>nd</sup>. IEEE National Radio Science Conference (NRSC' 2005). 2005: 277–284.
- [13] N. El-Fishawy and O. Zaid. Quality of encryption measurement of bitmap images with rc6, mrc6, and rijndael block cipher algorithms. *International Journal of Network Security*. 2007; 5(3): 241–251.
- [14] Abugharsa, AB., Hasan Basari, ASB., Almangush, H. A Novel Image Encryption using an Integration Technique of Blocks Rotation based on the Magic cube and the AES Algorithm. *International Journal of Computer Science Issues (IJCSI)*. 2012; 9(4): 1-12.
- [15] Massoudi, A., Lefebvre, F., De Vleeschouwer, C., Macq, B., Quisquater, JJ. Overview on Selective Encryption of Image and Video: Challenges and Perspectives. *EURASIP Journal on Information Security*. 2008: 179290.
- [16] Wang, X., Zhao, J., Liu, H. A New Image Encryption Encryption based on Chaos. *Optics Communications*. 2012; 285(5): 562-566.