Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-B, pp. 763–773
DOI : 10.47974/JDMSC-1953

Chaotic map-based selective image encryption via diffusion and confusion

Mrinal Paliwal *
Punit Soni †
Rajender Kumar §
Department of Computer Science and Engineering
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab
India

Ankur Goyal ‡
Department of Computer Science and Engineering
Symbiosis Institute of Technology
Symbiosis International Deemed University
Pune
Maharashtra
India

Meena Malik @
Bhavna Goyal #
Department of Computer Science and Engineering
University Centre for Research & Development
Chandigarh University
Mohali
Punjab
India

* *E-mail:* mrinal.paliwal@chitkara.edu.in (Corresponding Author)
† *E-mail:* punit.soni@chitkara.edu.in
§ *E-mail:* kumar.rajender@chitkara.edu.in
‡ *E-mail:* ankur_gg5781@yahoo.co.in
@ *E-mail:* meenamlk@gmail.com
# *E-mail:* Bhawna.e9244@cumail.in

Abstract

Industrial diversification and Technology have a drastic impact on the day-to-day life and economic growth of the country. Sharing multimedia content over the network has drastically increased. The multimedia data can be just social media images or some highly confidential data. There is a high demand for secure image transmission over networks in the age of the Internet and other transmission mediums. Since images are high-volume data, care must be taken to ensure that the security does not become computationally very expensive. To overcome these problems, we propose a method to encrypt the images selectively using a chaos map. Selective encryption is the process of encrypting an image so that only a piece of it is visible while the remainder is encrypted. This decreases the computational cost of the algorithm to a great extent. Selective encryption consists of two parts, public and private. The public part of the image is visible to everyone but the private part is only visible to the authorized user. The chaotic map is used for encrypting the image and providing security to the algorithm. Confusion and diffusion are used for key generation using pixel value substitution and scrambling. We use PSNR, histogram analysis, and correlation coefficient to verify the result.

Subject Classification: *68U10, 94A08.*

Keywords: *Selective image encryption, Chaos map, Confusion and diffusion, Cryptography.*

1. Introduction and Literature Review

With a large amount of images being exchanged over the internet, it has become very important to ensure the security of the images during transmission. The conventional cryptographic methods, such as "linear feedback shift register (LFSR)", "advanced encryption standard (AES)", "international data encryption algorithm (IDEA)", and "data encryption standard (DES)", etc., which are used to encrypt textual data, invariably fail in case of images [1].

Traditionally, there are two types of encryption techniques used in images-pixel value substation and pixel value scrambling. Arnold transform, Josephus traverse, and chaos map are few of the encryption methods that have been developed in the past ("Guan et al., 2005[2]; Zhang et al., 2005[3]; Fang et al., 2007[4]; Fang and Tong, 2007[5]; Li et al., 2006[6]; Pareek et al., 2006[7]; Liu and Liu, 2007[8]"). All these algorithms give better results than the traditional algorithms. These algorithms use pixel-scrambling encryption techniques. However, the computational cost of these algorithms is very high and the elapsed time for image encryption is also high[9].

An image encryption algorithm secures images with a fully layered encryption scheme; this method encrypts the entire image content. However, in the event of selective encryption, a portion of the image's content is not encrypted. Because the selective encryption algorithm encrypts only a portion of the image, it takes less time to execute. As a

result, partial encryption is another name for selective encryption [10] [11]. The capability of the encrypted bit-stream to be precisely decoded and proven, in conjunction with the encrypted and un encrypted quantities of the compressed bit-stream, is an critical characteristic of selective encryption. This is achieved by using standard decoders. As a result, format-compliant encryption is another name for selective encryption [12] [13] [14]. The chaotic encryption is quick; there for it is frequently used in conjunction with more established encryption techniques. Chaos maps have been employed extensively in the field of data encryption and secure communication in recent years [15].

2. Proposed Encryption Algorithm

In this paper, a novel encryption technique is proposed which uses selective encryption techniques to ensure that the perceptual information about the image is retained. This light encryption is helpful in two ways – computational cost is reduced; secondly, there are many real-life multimedia applications where it is required to maintain the perceptual information.

A. *Selective Encryption Technique*

Selective encryption is a technique of selectively encrypting the images. Selective encryption is more challenging because the image should be partially encrypted which results in some issues to be addressed. Confidentiality and security are the main issues related to selective encryption. The first step of the selective encryption algorithm of the suggested algorithm makes use of a Henon map for encryption.

The Henon function is used as:

$$\begin{aligned} X_{n+1} &= 1 - aX_n^2 + Y_n \\ Y_{n+1} &= bX_{n+1}^2 \end{aligned} \tag{1}$$

The values of a, b, c, Xn, and Yn are the input values by the user for the selective encryption algorithm. With the help of the Henon function, random numbers are generated and these values of Xn and Yn are bored with each pixel of R, G, and B channels.

$$\begin{aligned} R_{(1,1)} &= R_{(1,1)} \oplus X1 \\ G_{(1,1)} &= G_{(1,1)} \oplus Y1 \\ B_{(1,1)} &= B_{(1,1)} \oplus \mathbf{X}2 \\ R_{(1,2)} &= R_{(1,2)} \oplus \mathbf{Y}2 \end{aligned} \tag{2}$$

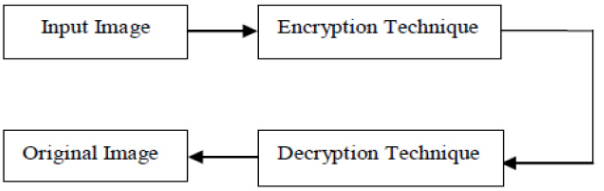


Figure 1

Selective Encryption Procedure

The detailed exiting model is available in Figure 1 for selective encryption process and the proposed selective encryption model is discussed in Figure 2 below.

The following stages are involved in implementing the selective encryption method for RGB images:

Step 1: Reading and expressing a colorful image with a "matrix A (M×N)".
Step 2: Apply the Henon function to the input matrix A and store the resultant matrix in B.
Step 3: Generate the key by applying chaos-based key generation to matrix A and perform confusion and diffusion accordingly, matrix C is got.
Step 4: Bitxor the two matrixes B and C, get a "matrix D of size M×N".
Step 5: The Selective encryption procedure is completed and a colored selective encrypted picture is developed.

B. *Chaos-Based Key Generation*

The first step will be to calculate four variables K1, K2, K3,and K4. The value of X_n and Y_n will be obtained from e.q(1). The value of Xn and Yn will be multiplied and divided by 256 to form the variable K1. The variable K2 could be created through multiplying the value of Yn via Xn+1 and dividing with the aid of 256. K3 could be formed by way of multiplying and dividing the values of Xn+1 and Yn+2 with the aid of 256. The variable K4 could be created by means of taking the mod of Yn+2 and 255. Variables could be produced the usage of the subsequent regulations:

$$\begin{aligned} K_1 &= (X_n * Y_n) / 256 \\ K_2 &= (Y_n * X_{n+1}) / 256 \\ K_3 &= (X_{n+1} * Y_{n+2}) / 256 \\ K_4 &= \mathrm{mod}(Y_{n+2}, 255) \end{aligned} \tag{3}$$

Those variables will generate the values, with the intention to be used to generate the important thing inside the subsequent step of the set of rules.

C. *Confusion and Diffusion*

The method of hiding the plain image is confusion. By breaking down the first pixel in the image's red channel (represented by variable K1), the first pixel in its green channel (represented by variable K2), the first pixel in its blue channel (represented by variable K3), and the remaining pixels (represented by XORing), confusion is achieved in this procedure.

$$\begin{aligned} R_{(1,1)} &= R_{(1,1)} \oplus K1 \\ G_{(1,1)} &= G_{(1,1)} \oplus K2 \\ B_{(1,1)} &= B_{(1,1)} \oplus K3 \\ R_{(1,2)} &= R_{(1,2)} \oplus K4 \end{aligned} \tag{4}$$

Until every pixel in the R, G, and B channels has been bit XORed, the operation will proceed. Following confusion, the diffusion process is applied; during this process, the output bits must intricately depend on the input bits. This is accomplished by this algorithm by conducting the diffusion process in two stages, namely vertical and horizontal diffusion.

1) *Horizontal Diffusion*: Each pixel in horizontal diffusion is bitXORed, row-wise, with the pixel adjacent to it. Beginning with the second red channel pixel, the first red channel pixel and the second red channel pixel are bitXORed, and the outcome is substituted with the second red channel pixel. The three channels are also dispersed horizontally.

$$\begin{aligned} R_{(i,j+1)} &= R_{(i,j+1)} \oplus R_{(i,j)} \\ G_{(i,j+1)} &= G_{(i,j+1)} \oplus G_{(i,j)} \\ B_{(i,j+1)} &= B_{(i,j+1)} \oplus B_{(i,j)} \end{aligned} \tag{5}$$

2) *Vertical Diffusion*: It starts with the Red channel. The final pixels of the G and B channels are bit XORed with the second-last pixel of the R channel in vertical diffusion, bit XORing the channel as a whole. The entire channel is bitXORed by bit XORing the second-to-last pixel of the G channel with the final pixels of the R and B channels, appropriately.

$$\begin{aligned} R_{(i\text{-}1,j)} &= R_{(i\text{-}1,j)} \oplus G_{(i,j)} \oplus B_{(i,j)} \\ G_{(i\text{-}1,j)} &= G_{(i\text{-}1,j)} \oplus R_{(i,j)} \oplus B_{(i,j)} \\ B_{(i\text{-}1,j)} &= B_{(i\text{-}1,j)} \oplus R_{(i,j)} \oplus G_{(i,j)} \end{aligned} \tag{6}$$

Image obtained with the Chaos-based key generation will act as a key and this key will be bored with the selectively encrypted image, to increase the security of the encrypted image. Hence the cipher image will have a private part and a public part. The key and the cipher image will be transmitted through the channel.

$$\begin{aligned} R_{(i,j)} &= R_{key(i,j)} \oplus R_{(i,j)} \\ G_{(i,j)} &= G_{key(i,j)} \oplus G_{(i,j)} \\ B_{(i,j)} &= B_{key(i,j)} \oplus B_{(i,j)} \end{aligned} \tag{7}$$

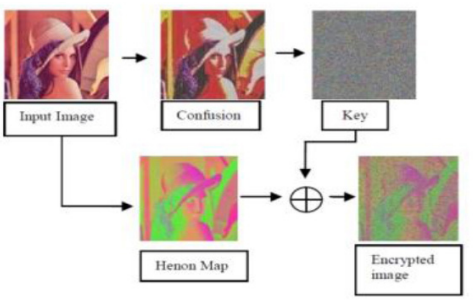


Figure 2

Proposed Selective Image Encryption Method

A. *Decryption Algorithm*

The decryption part involves the selectively encrypted image i.e Chaos based key generation (IIB) and selectively encrypted image (Cipher image). Input will be a selectively encrypted image, the image obtained by Chaos-based key generation will act as a key for decrypting the image. Apply the Henon function (II) with the same input values, which were selected at the time of encrypting the image. The encrypted image is bitXORed with the chaos image to recover the original image. Suppose C_i is the cipher image, and C_k is the key image; the output image will be generated according to the following formula:

$$\begin{aligned} R_{(i,j,1)} &= C_{i(i,j,1)} \oplus C_{k(i,j,1)} \\ G_{(i,j,1)} &= C_{i(i,j,2)} \oplus C_{k(i,j,2)} \\ B_{(i,j,1)} &= C_{i(i,j,3)} \oplus C_{k(i,j,3)} \end{aligned} \tag{8}$$

The decryption technique for the cipher image using the proposed algorithm is as follows:

Step 1: Reading a cipher image and expressing it with a matrix E of size M×N.

Step 2: Apply the Henon function to the image E; the input value will be the same as used in encryption.

Step 3: Apply the Chaos-based key B, Bit xor B, and E; the resultant will be a matrix F of M×N.

Step 4: The decryption process is completed and the resultant image F is the final output image, which will be the same as the input image.

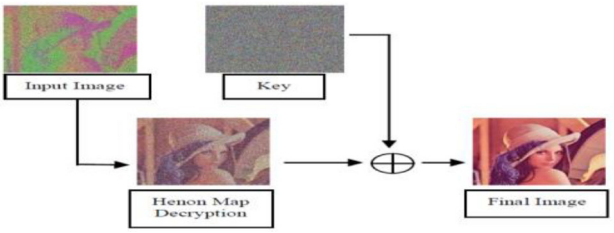


Figure 3

Proposed Decryption Procedure

3. Simulated Experiment

In this section, we conduct experiments to verify the suggested algorithm's practicability and security. Figure 3 shows a Lena image of size 256 × 256, which will be the input image for this algorithm. The initial values that are given to the Henon map (II) are X0=89, Y0=90, a=0.25, b=3 and c=4. Figure 6 shows the decryption procedure. The selective encrypted image in Figure 4(b) is obtained after applying the selective encryption algorithm in Figure 4(a) and the final output image is shown in Figure 4(b). Experimental result shows that there are similarities between the

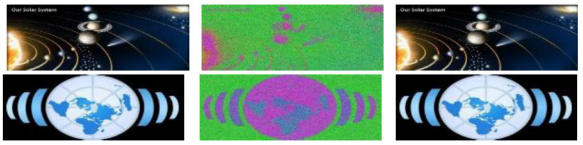


Figure 4

(a) Original Image (b) Selective Encryption (c) Final image

original image and the encrypted image as shown in Figure 4, for this purpose, we have calculated the PSNR value and histogram of input and output image to verify the result.

B. *Security Analysis*

(1) "The peak signal-to-noise ratio (PSNR)".

The PSNR is frequently used to assess how well lossy compression codecs reconstruct images, or how well they compress images. In this instance, the original data—that is, an array stream—is the signal, while the error brought about by compression is the noise. As a rough measure of human perception of reconstruction quality, PSNR is used to compare the compression codecs; hence, in certain instances, a reconstruction with a lower PSNR may seem more similar to the original than one with a higher PSNR (in general, a greater PSNR would suggest a higher-quality reconstruction).

As a result, lower PSNR levels indicate more security. PSNR value for selective encryption is between 20 and 30 dB. Figure 5 shows the PSNR value of 24 images of red, green, and blue channels, the PSNR value ranges from 10 to 25 PSNR.

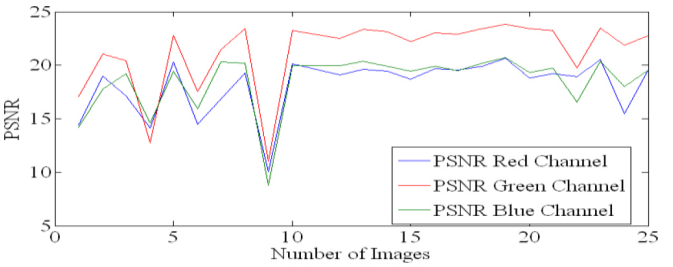


Figure 5

PSNR value of RGB channel

(2) Correlation Coefficient

A linear relationship involving two neighboring pixels was used in tests to compare the statistical aspects of the novel and encrypted images in a horizontal, vertical, and diagonal manner. Adjacent pixels in natural images taken with natural data have a high association. The magnitude and direction of a linear combination of two random variables are represented by the correlation coefficient, or "r."

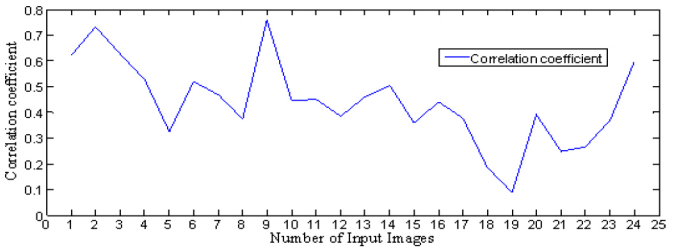


Figure 6

Graph showing the correlation coefficient of different images

The Figure 6 shows the correlation coefficient of 24 images. The correlation coefficient is calculated between the input image and the selectively encrypted image. The value of the correlation coefficient lies between 0.1 to 0.8. This shows that the selectively encrypted image and input image have some relations in between.

(1) Histogram Analysis

The figure illustrates a histogram analysis example. We have the secret key and the 256 × 256-pixel image of Lena. We are attempting to differentiate between the input and output images using histogram analysis. Figure 7 shows the histogram of the input image, the selectively encrypted image, and the output image. With the help of histogram analysis, we can prove that the output image and the input image are the same as the histogram of both the images are same.

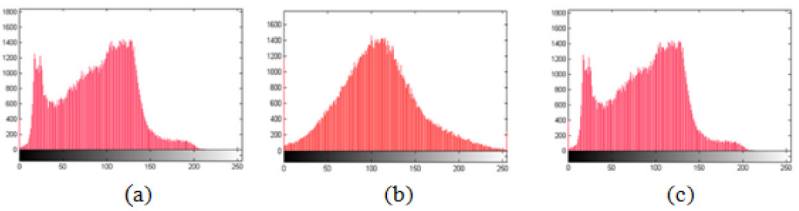
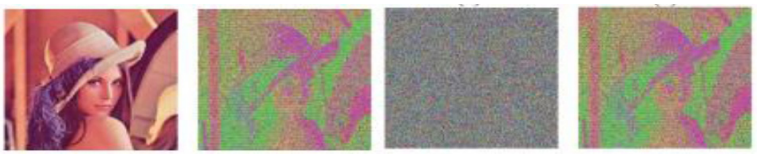


Figure 7

(a) Histogram of the input image (b) Histogram of Selectively Encrypted Image (c) Histogram for Output Image

(4) Key Sensitivity

The algorithm's feature known as key sensitivity states that even a small change in the key should produce an entirely new image. The image



(a) (b) (c) (d)

Figure 8

Key sensitivity test. (a) Input image (b) Encrypted image (c) Wrong key (d) Final image

should be decrypted by the algorithm using a particular key. The algorithm's sensitivity to initial conditions has been demonstrated. To evaluate whether there are any visual connections between the decrypted data and the one with the proper key, the data is slightly modified and the data is decrypted. Figure 8(a) displays the input image for this test, and Figure 8(b) displays the encrypted image. The input key to this algorithm is the wrong key Figure 8(c). Then the resultant of this algorithm will be a different image and not the original image.

5. Conclusion

This study defines a careful image encryption technique by confusion and diffusion utilizing a chaos map. Using a key image, the new algorithm may carry out the selective encryption technique. Using chaotic functions, the approach presented in this paper can be extended to selective video encryption. Colored images may be efficiently processed using this approach.

References

[1] Menezes A J, Oorschot PCV, Vanstone SA. Handbook of applied cryptography. Boca Raton(FL) : CRCPress (1997).

[2] Guan, Z.H., Huang, F.J., Guan, W.J., Chaos-based image encryption. Phys. Lett. A346, 153–157 (2005).

[3] Zhang, L. H., Liao, X. F., Wang, X. B., An image encryption approach based on chaotic maps. Chaos, SolitonsFract. 24(3), 759–765 (2005).

[4] Fang, Z. J., Lu, X., Wei, W. M., Wang, S. Z., Image scrambling based on bit shuffling of pixels. J. Optoelectron. Laser 18(12), 1486–1488 (2007).

[5] Fang, Z. Y., Tong, W. Q., Image scrambling algorithm based on chaos mapping. ModernComput. 10, 51–53 (2007).

[6] Li, Y., Fan, Y. Y., Hao, C. Y., Information hiding technology based on image second-scrambling. J. Image Graph.11(8), 1088–1091 (2006).

[7] Pareek, N. K., Patidar, V., Sud, K. K., Image encryption using chaotic logistic map. Image Vision Comput. 24 (9), 926–934 (2006).

[8] Liu, Z.J., Liu, S.T., Double image encryption based oniterative fractional Fourier transform. Opt. Commun. 275, 324–329 (2007).

[9] Guodong Ye, Image scrambling encryption algorithm of pixel bit based on chaos map,‖ Pattern Recognition Letters 31, 347–354 (2010).

[10] H. Chengand X. Li, Partial encryption of compressed images and videos, ‖IEEETrans. Signal Process. Vol. 48(8) 2439–2451, 2000 (2010).

[11] H. Kiya, O. Watanabe, A. Nakazaki, A scalable encryption method allowing backward compatibility with JPEG 2000 images: Proceedings of the IEEE International Symposium on Circuits and Systems, pp. 6324–6327 (2005).

[12] Khan, J.S. and Ahmad, J., Chaos-based efficient selective image encryption. *Multidimensional Systems and Signal Processing*, pp.943-961 (2019).

[13] Cun, Qiqi, Xiaojun Tong, Zhu Wang, and Miao Zhang. "Selective image encryption method based on dynamic DNA coding and new chaotic map." Optik 243 : 167286 (2021).

[14] Tandon, R., & Gupta, P. K., A novel and secure hybrid iwd-mask algorithm for enhanced image security. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science), 14(2), 384-394 (2021).

[15] Bhardwaj, Rupali, and Divya Khanna. "Enhanced the security of image steganography through image encryption." In 2015 Annual IEEE India Conference (INDICON), pp. 1-4. IEEE (2015).