EASR

Engineering and Applied Science Research

https://www.tci-thaijo.org/index.php/easr/index

Published by the Faculty of Engineering, Khon Kaen University, Thailand

Selective colour image encryption using Hénon chaotic system with a keyless substitution cipher

Ashish Kumar[1] and NS Raghava*[2]

[1]Department of Information Technology, Delhi Technological University, Delhi, India
[2]Department of Electronics and Communication Engineering, Delhi Technological University, Delhi, India

Received 3 July 2019
Revised 19 August 2019
Accepted 10 September 2019

Abstract

Security is a continuous process of protecting the resources of a computer system from hackers or attackers. Multimedia comes in the form of text, image, audio and video, and all are very important modes of communication that gives users more ways to express their feelings. In traditional cryptography, encipherment and decipherment take more processing time to secure bulky data with a high order of complexity in data storage, as well as in the transmission of multimedia-oriented applications. Therefore, selective encryption reduces computational costs, overhead and size of data in the encipherment process, which is always advantageous for all the parties involved in communication. In this paper, we propose a region-based selective image encryption to secure information in an efficient manner to achieve reduced encryption time. Secrecy of unnecessary information within an image is not required for both the ends in communication. Here, security summarised as aggregated chaos-based coding with most significant bit diffusion and recentness keyless substitution cipher at the pixel level on the ROI image obtained by a hybrid region growing method. This technique significantly reduces the storage space and transmission costs. Experimental results confirm it is a more secure and fast encryption method for large sized images.

Keywords: Hénon chaotic map, Image encryption, Diffusion, Region-Based encryption

1. Introduction

Digital images are a significant source of information among all multimedia applications in terms of storage, as well as in transmission [1-2]. When a sender or any host is connected to a subnet and it sends multimedia to any other host, secrecy of information over the communicated channel is an important concern. Information is passed from various layers of TCP/IP when it comes to the network layer. Routers play an important role to directing packets to the intended user [3]. The sensor nodes have limited computation, communication and storage capabilities. As a result, it requires high security in the transmission medium, because eavesdroppers can monitor the traffic with mal-intentions and can easily eavesdrop to gain useful information. In such cases, information should be in a non-readable format and moreover, it should be difficult for the cryptanalyst to generate original information from the cipher image.

Image segmentation is an emerging field of image processing, which is very helpful to determine non-overlapping homogenous regions of an image. Many researchers are participating in image processing and usually focus upon certain portions of an image called the foreground (the remainder is called the background) having a unique and specific nature. Object segmentation is particularly important in computer vision applications, such as medical image analysis, video surveillance, content-based image retrieval, and information security, among other applications.

In images, secrecy of unnecessary information within an image is not required for all the legitimate users. Therefore, it is possible to encrypt only foreground details. This technique is called Region-based encryption. It is defined by segmentation and encryption simultaneously. Considering the limitations of over-segmentation and under-segmentation of the classical region based object segmentation, object segmentation is done by an automatic edge constrained seeded region growing method. In this paper, nearest edge pixels are used to solve the problem of over-segmentation and under-segmentation, where a center window containing some part of the object and threshold value with a seed selection is calculated on the basis of an input image [4].

Medical images are used to diagnose the health of a patient before treatment. Compressed and low resolution images may be the origin of some incorrect diagnosis, so this is a constraint since diagnosis and treatment of the patient should be based on high quality and lossless compressed images, which hold important data than lossy or compressed images might not [5]. When a medical report or information of a patient is exchanged between medical personnel for further diagnosis, they do not want to reveal their patient's

*Corresponding author. Tel.: +9197 1172 4842
Email address: nsraghava@dce.ac.in

doi: 10.14456/easr.2020.6

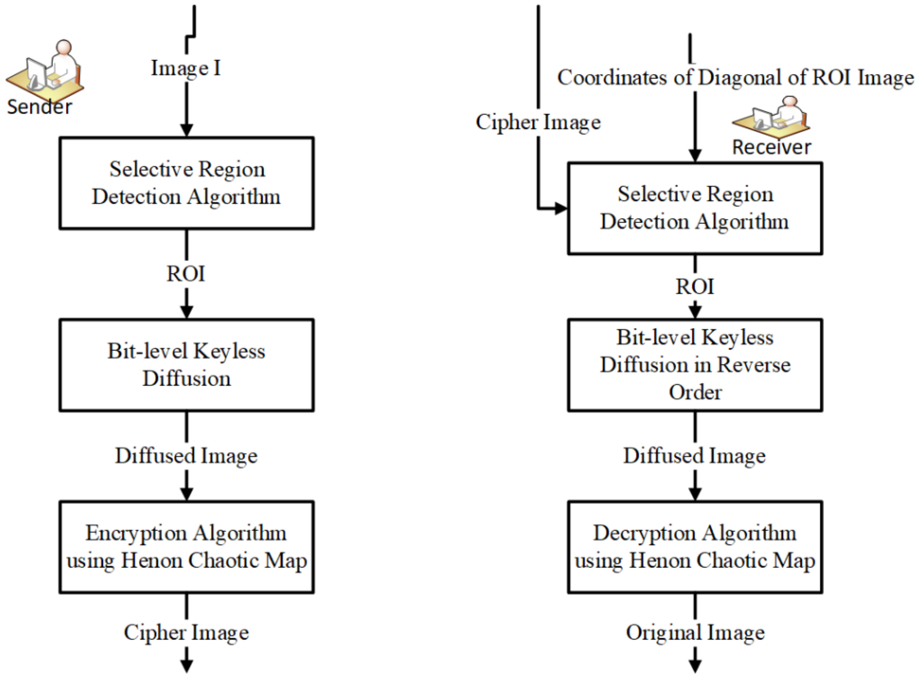

Sender
Image I
Selective Region Detection Algorithm
ROI
Bit-level Keyless Diffusion
Diffused Image
Encryption Algorithm using Henon Chaotic Map
Cipher Image
Coordinates of Diagonal of ROI Image
Cipher Image
Receiver
Selective Region Detection Algorithm
ROI
Bit-level Keyless Diffusion in Reverse Order
Diffused Image
Decryption Algorithm using Henon Chaotic Map
Original Image

Figure 1 Architecture of the proposed algorithm

sensitive information. In this particular case, the medical technician will only send relevant information that is encapsulated with hidden information of the patient by region based selective image encryption. Region-based selective image encryption methodology is also required for the military and defense sectors of any country so that sensitive information within an image can be sent in encrypted or cipher mode.

In this paper, the presented algorithm is suitable for digital colour images. In the first phase, a sensitive region of an image is segmented and then the region of interest (ROI) of an image is introduced in a bit level keyless substitution method, where each pixel value is substituted. After that, a diffused image is passed to the next module of the proposed algorithm, where it is encrypted using Hénon chaotic system with a symmetric key cryptographic approach. In the complete process, sensitive details of image, i.e., the ROI is encrypted, while the remainder section of the image, region of background (ROB), remains in its original form.

Advantages of the proposed algorithm include that:

- A minimum number of bits are required for encryption. Hence, the computational cost of encryption is decreased.
- The proposed architecture ensures that various users from different spaces can only view a certain portion of an image.
- This algorithm can be used in two ways depending upon the user's requirements, whether sender wants to send an encrypted ROI image along with foreground details or choose to send only the ROI encrypted part of an image.

The paper is organized as follows. Section 2 discusses related work. Section 3 introduces the proposed algorithm. Experimental results and comparisons are presented in Section 4. Section 5 provides conclusions and future directions for work.

2. Related work

Numerous researchers are continuously working on segmentation techniques as well as in cryptography. A variety of techniques and algorithms have been developed to build fast and secure image transmission systems. Mahmood and Dony [6] proposed a technique that applied segmentation based encryption to medical images achieving faster processing time. Liu [7] proposed a method of selective image encryption. He has proposed an efficient selective encryption scheme to protect the privacy of an image and achieve access control of a JPEG 2000 code stream. A secret key along with a mapping function is used to generate a table to encrypt the selected DWT code in the entropy coding stage of the JPEG 2000 coding standard.

Ravishankar and Venkateshmurthy proposed an architecture where sensitive regions are not detected automatically since such regions are marked by the user [8]. The proposed selective region-based image encryption technique also has a further advantage. After completing the permutation and segmentation processes, the regions are encrypted individually. Spatially localized and boundary finding approaches are found in the segmentation domain [9], where monochromatic images are tested using discontinuity measures. Susan et al. proposed an algorithm for segmenting out the region of interest by integrating the edge information to decrease the imperfections of the seeded region growing technique [4].

3. Region based selective encryption algorithm

The proposed algorithm acts at two levels to achieve better processing times than previous methods. In the proposed method, first, a region of interest is found using the extended segmentation approach. Then, this sensitive information is encrypted with the help of a Hénon chaotic system. A procedure for doing this is given in Figure 1.

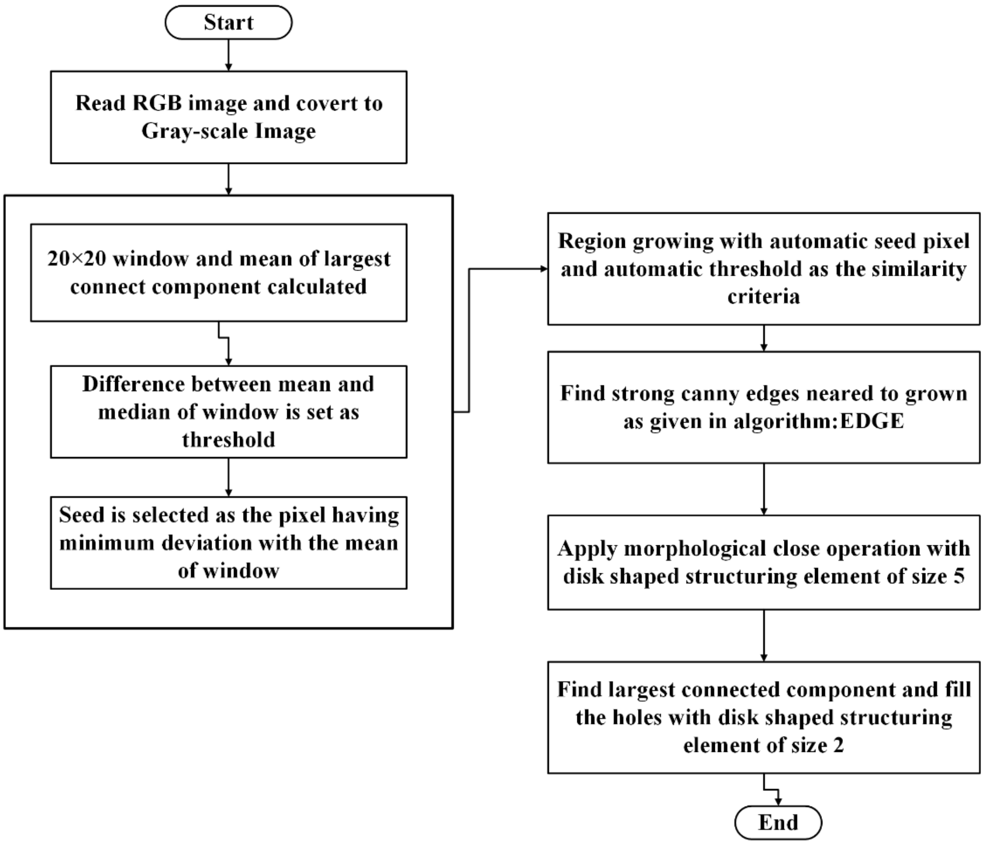

Start
Read RGB image and covert to Gray-scale Image
20×20 window and mean of largest connect component calculated
Difference between mean and median of window is set as threshold
Seed is selected as the pixel having minimum deviation with the mean of window
Region growing with automatic seed pixel and automatic threshold as the similarity criteria
Find strong canny edges neared to grown as given in algorithm:EDGE
Apply morphological close operation with disk shaped structuring element of size 5
Find largest connected component and fill the holes with disk shaped structuring element of size 2
End

Figure 2 Flow chart: Adaptive ROI based segmentation

3.1 Segmentation of an image

3.1.1 Calculate automatic threshold and initial seed

a) A 20 × 20 window *W* is chosen across the center pixel to start the automatic phase of the method.

Threshold determination is done from the window *W*.

b) Find the largest connected component of this window and the mean of the grey pixels in the largest connected component. Absolute distance between the mean of window and median of all the window pixels gives the threshold to decide whether a neighbour pixel is included in a region or not.

Threshold, $T = \left| Mean_w - Meadian_w \right|$ (1)

c) Automatic initial seed selection from the window and calculate deviation of pixel values in the window from the mean,

$$Dev = \left| W_{(x,y)} - Mean_w \right| \quad (2)$$

Find the coordinates (x, y) in the window where deviation is minimum and embed this window back into the actual image to obtain the initial seed coordinates.

3.2 Seeded region growing process

The initial seed is the deciding factor for the overall segmentation by region growing technique. It decides the region of interest or object within the image [10]. The initial seed obtained above is labelled as the grown region. All eight neighboring pixels are checked for similarity criteria to determine whether or not to include them in this region. The similarity criterion is whether the Euclidean distance of seed and the pixel in question is less than the threshold of the image (as obtained by the above process). The pixel is labelled as a region that then grows based on a similarity measure.
Euclidean distance is:

$$ED = \sqrt{(seed - n_p)^2} \quad (3)$$

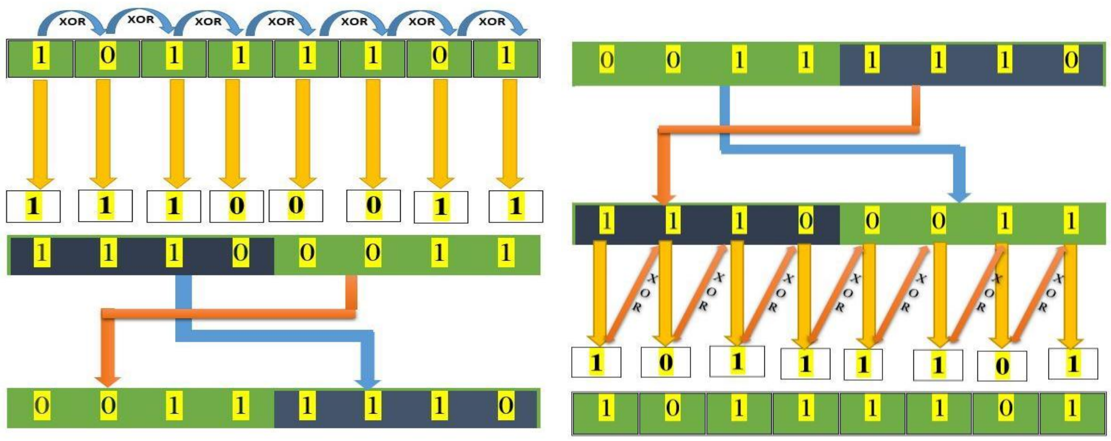
where, ED= Euclidean Distance, n_p = neighbor of the seed, p=1,2, 3,………. 8

If ED <= threshold, label the unlabeled pixel and push it onto the stack.

The grown region first calculates its distance with canny edge pixels of the image and then marks the minimum distance as the nearest strong edge pixel. Some discontinuities and holes may be present in the object. These defects are overcome by applying certain morphological operations onto the segmented image.

3.3 Perform morphological operations to refine the segmentation results

a) For a morphologically close image, perform a dilation



(a) (b)

Figure 3 Keyless substitution, (a) keyless substitution at the sender end, (b) keyless substitution at receiver's end

followed by erosion on a binary image using the same structuring element.

b) Trace region boundaries in a binary image to identify the exterior boundaries of objects in the image to produce the largest connected component. This function returns the position of border pixels in the image.

c) Structure elements of size five and size two are used for morphological closing and filling, respectively. This gives the single largest connected component in the image. The size of the morphological tools is determined through experimentation to determine the best results. The single largest connected component is the region of interest, which is further worked upon for efficient encryption.

Identify the target object and extract only the segmented area with two coordinates of diagonal. Then, further processing is applied to the segmented region. The ROI based segmentation is applied to 100 images of the 'CAR' category of the PASCAL VOC 2005 dataset [11]. It is observed that more than 95% of the images achieve accurate precision. To understand the procedure, a flow chart of the adaptive segmentation of an image is illustrated in Figure 2.

3.4 Bit level keyless substitution cipher

In gray images, each pixel is represented in an 8-bit format and they have different values to form a meaningful image. Here, a novel approach has been introduced that is based on the XORed property of gray code conversion. The first bit of a pixel will remain the same and the second bit will be generated using an XOR between the first and second bits. The complete process is repeated until all the bits of pixels are covered. Later, these eight bits are divided into two halves and the halves interchanged.

Algorithm: Keyless Substitution

```
        Pixel $P_i$= $B_1B_2B_3B_4B_5B_6B_7B_8$,
                for (i=1 to 8)
        {
        if (i=1)
        $C_i$ =$B_i$
else
        $C_i$=XOR ($B_i$ , $B_{i-1}$)
        }
```

Let one Pixel, P_i, have a bit value in 8-bit format, B_1, B_2, B_3, B_4, B_5, B_6, B_7, and B_8. Keyless substitution of a pixel will be obtained by the algorithm given below.

When pixel value is converted into bit format using a given algorithm, it is found that it is converted into other decimal values, as shown in Figure 3.

3.5 Encryption of segmented image

When any data is converted into a non-readable format and a procedure returns this original data, then this complete procedure is known as cryptography. Readable data, when converted into a non-readable form, is called encryption. In a stream cipher categorized under private key cryptography, every bit of a message is encrypted with the corresponding key, which is generated with the help of a pseudo-random key generator. Pseudo-random numbers are used for the encryption in a stream cipher.

Here, chaos theory has emerged due to its properties. The Hénon map is a non-linear dynamic system which is generally used for generating the pseudo-random sequence in various disciplines of science [12]. A two-dimensional discrete-time nonlinear dynamic Hénon chaotic map generates a pseudo-random binary sequence which is described as:

$$\begin{aligned} X_{n+1} &= 1 + Y_n - aX_n \\ Y_{n+1} &= bX_n \end{aligned} \qquad (4)$$

The initial points X_1 and Y_1 [13] work as a symmetric key for the chaotic cryptographic system in the proposed system. Since a Hénon chaotic map is deterministic, decryption of the cipher image will reconstruct the original image at receiver's end with the same initial points X_1 and Y_1. Thus, the sensitivity of the key and encryption algorithms together contributes to avoiding many types of cryptanalysis attacks. Here, the parameters, *a* and *b*, are of key significance as the dynamic behaviour of the system depends on this initial set of values [14]. Initial seeds are treated as security keys at both ends as depicted in the following procedure.

Step 1: Choose the initial values (X_1, Y_1) for the Hénon map. These seeds act as an initial secret symmetric key for the Hénon map. For every initial seed, a Hénon map generates different pseudo-random numbers.

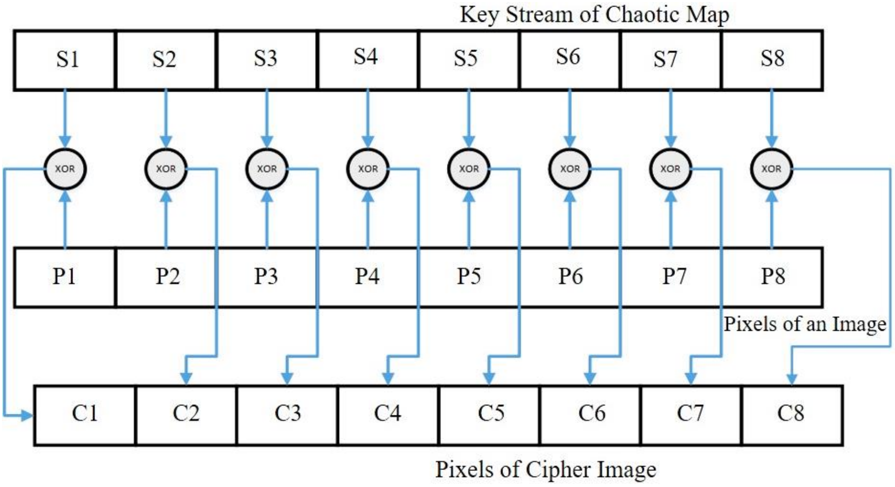


Figure 4 Diffusion based on a Hénon chaotic map

Step 2: Hénon map works as a keystream generator for the cryptosystem. The size of the sequence depends on the size of a selective image. If the selective image size is $M \times N$, then the Hénon sequence will be a size $2\times M \times N$, obtained by equation (4).

Step 3: Experimental analysis concludes that the obtained sequence is not normalized and does not come under the image intensity values. A two-dimensional Hénon chaotic map generates sequences and stores them as a single array by applying element multiplication between X and Y matrices. These sequences are normalized and decimal values are then converted into [0, 255] values using equation (5).

$$G = |(\mathrm{X}.\times\mathrm{Y})| \times 10^6$$
$$G = mod(G, 255) \quad (5)$$

Step 4: The Hénon sequence is then reduced by combining each sequence value into one byte-oriented value. This pair of bits of the keystream is XORed with a pixel in bitwise fashion and next key value of keystream is XORed with next pixel of an image. The procedure goes on until all the pixels of an image are XORed with the keystream of the Hénon Chaotic system [15]. Figure 4 illustrates the working procedure of the Hénon chaotic map.

Step 5: Encryption is done by a bitwise Exclusive-OR (XOR) operation between pixels and the sequence generated in step 4. An obtained *ROI* encrypted image is combined with the foreground to make a complete image with selective encryption.

3.6 Decoding algorithm at receiver's end

At the receiver's end, the cipher image is further processed for decryption and a secret key is transmitted through a secure channel that applies the Hénon chaotic system to generate the deterministic sequence. These sequences are applied to the cipher image in the process to obtain the original image. An ROI selective encrypted segment is attached with foreground details of an image and sent to the receiver along with the diagonal coordinates of the ROI image. Since the chaotic system behavior is deterministic, reconstruction of the image using the same key (X_1, Y_1) at the decryption end gives a diffuse image. Later, this diffused image is passed using a bit level keyless substitution to rearrange it in a manner exactly reverse of the way done for encryption, as discussed in Section 3.1 Finally, the original digital colour image is reconstructed at the receiver's end.

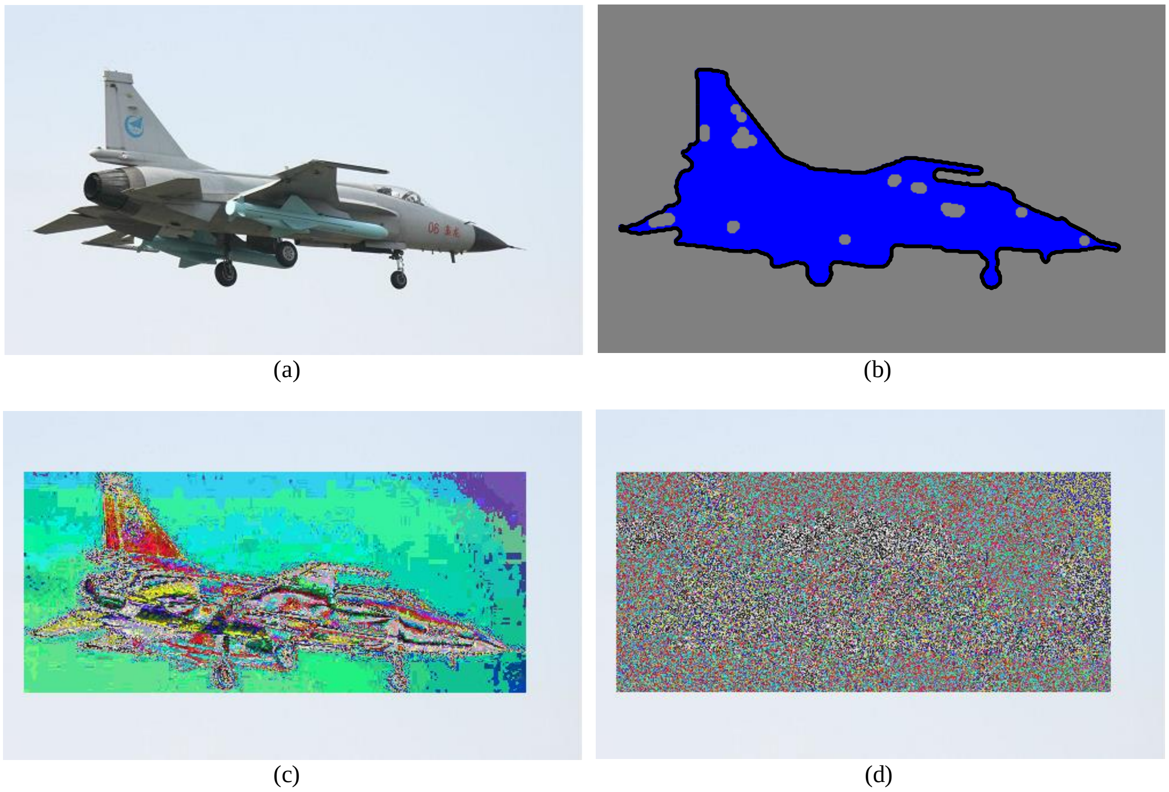
4. Experimental results

The proposed framework has been applied to several colour images. Excellent results demonstrate the effectiveness and efficiency of the proposed cryptosystem. MATLAB 7.9 software was used for implementing the proposed algorithm. Here, an input image of size 156×507 is shown in Figure 5(a). The dynamic behaviour of the system depends on the values of *a* and *b*. These sets of values are of key significance to create the chaotic behavior of Hénon system. It was found in experiments that the initial parameters for Hénon map are best chosen as a=1.4 and b=0.3 to make the system chaotic [14]. In the implementation of the process, a secret symmetric key for encryption is a combination of X_1=0.01 and Y_1=0.02 that is assigned here. Figure 5(b-c) illustrates the growing region of the input image and diffused image after keyless substitution, respectively. The image is shown in Figure 5(c) is used as the input for the next module and an encrypted image is obtained by applying the methodology of Section 3.5. The image is transmitted to receiver's end and the main aim is to decrypt the received image using the secret key and known algorithm. Experimental results of the decryption process are shown in Figure 6. This is the original decrypted image at the receiver's end.

4.1 Histogram analysis

A histogram can be used as a graphical representation of pixel intensity values. There are 256 different possible intensities for a grey image or a single color channel. So the graphical representation of the histogram will display 256 intensities and the distribution of pixels amongst those intensity values. On the basis of the histogram, it can be concluded that cipher image is well encrypted and it has more variation than original color image histogram. Visual representation of histogram of original image, as well as diffused image, encrypted image, and decrypted image, are given in Figure 7.

Encryption at sender end

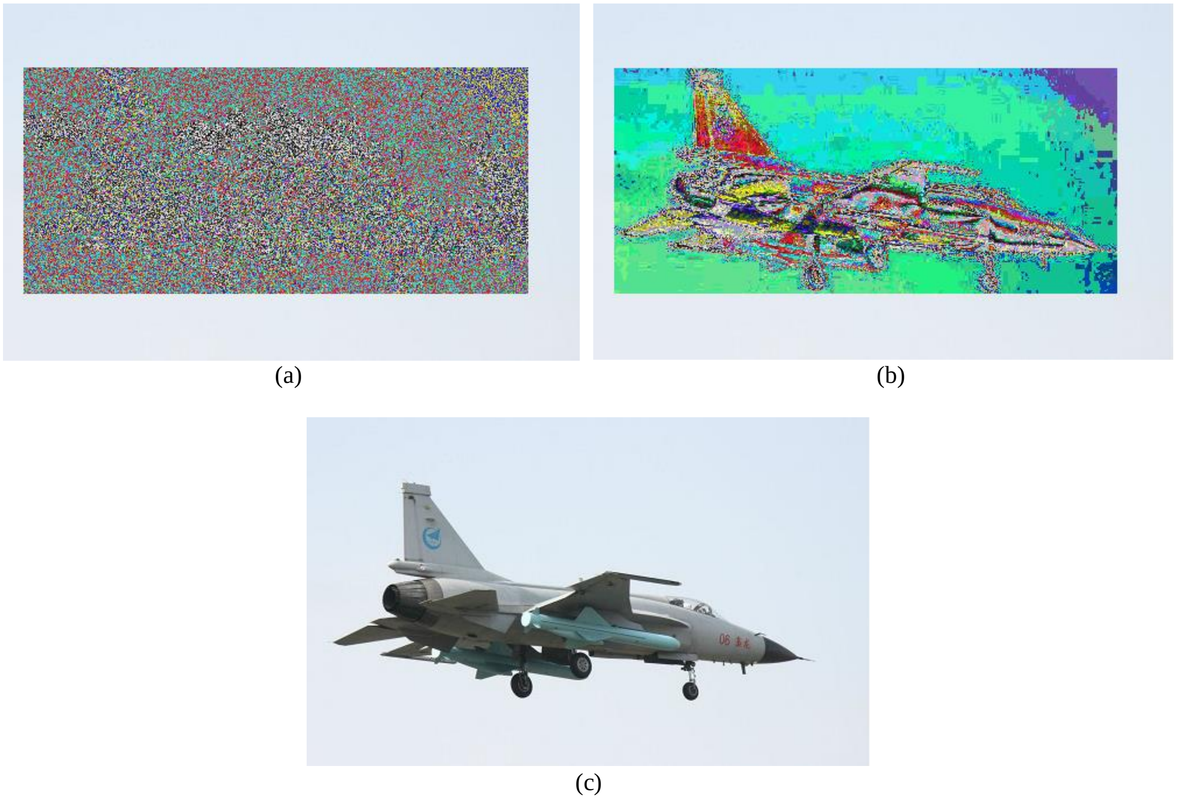


(a) (b)

(c) (d)

Figure 5 Encoding by system: (a) input image (b) segmented image (c) diffused image using keyless substitution (d) encrypted image

Decryption at receiver end



(a) (b)

(c)

Figure 6 Decryption by system: (a) encrypted image (b) diffused image after decryption and (c) original image

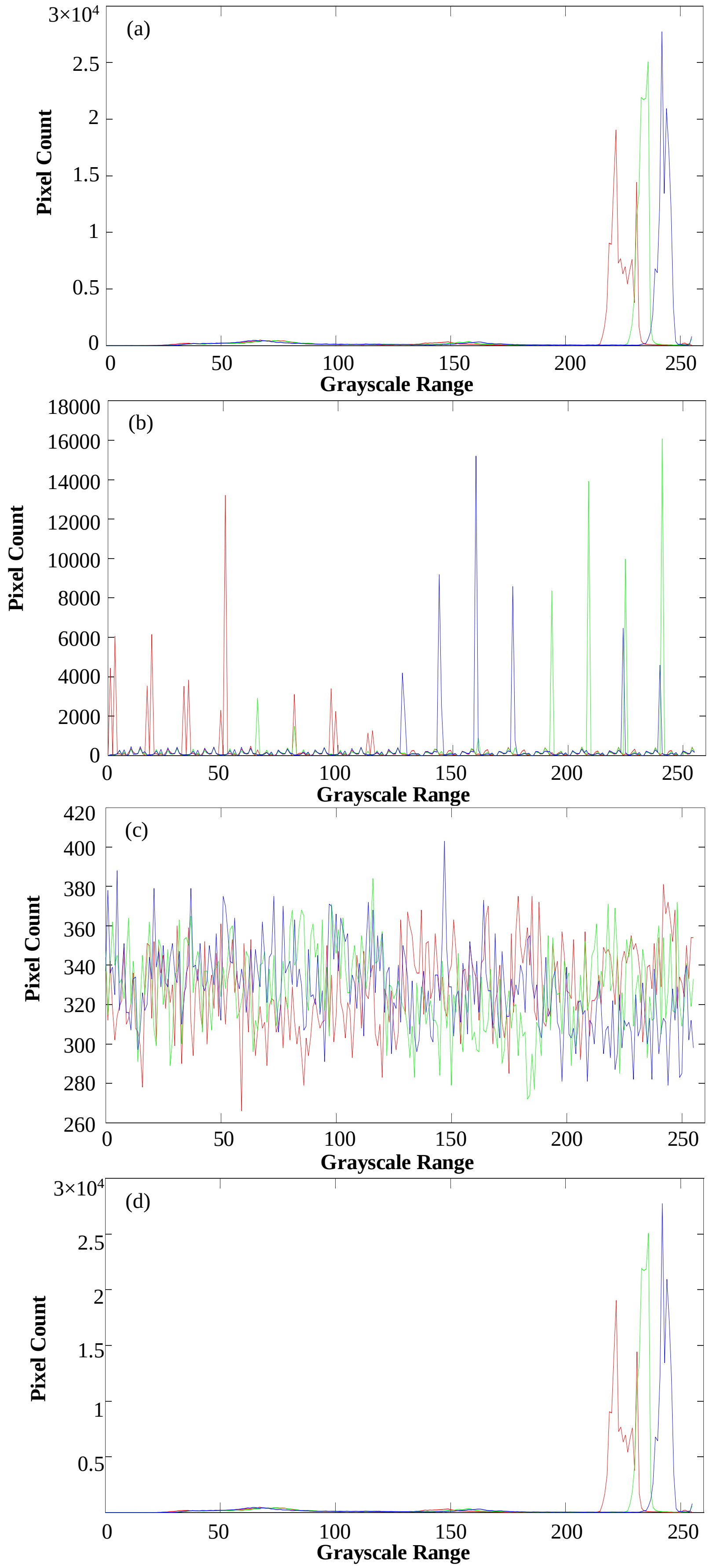
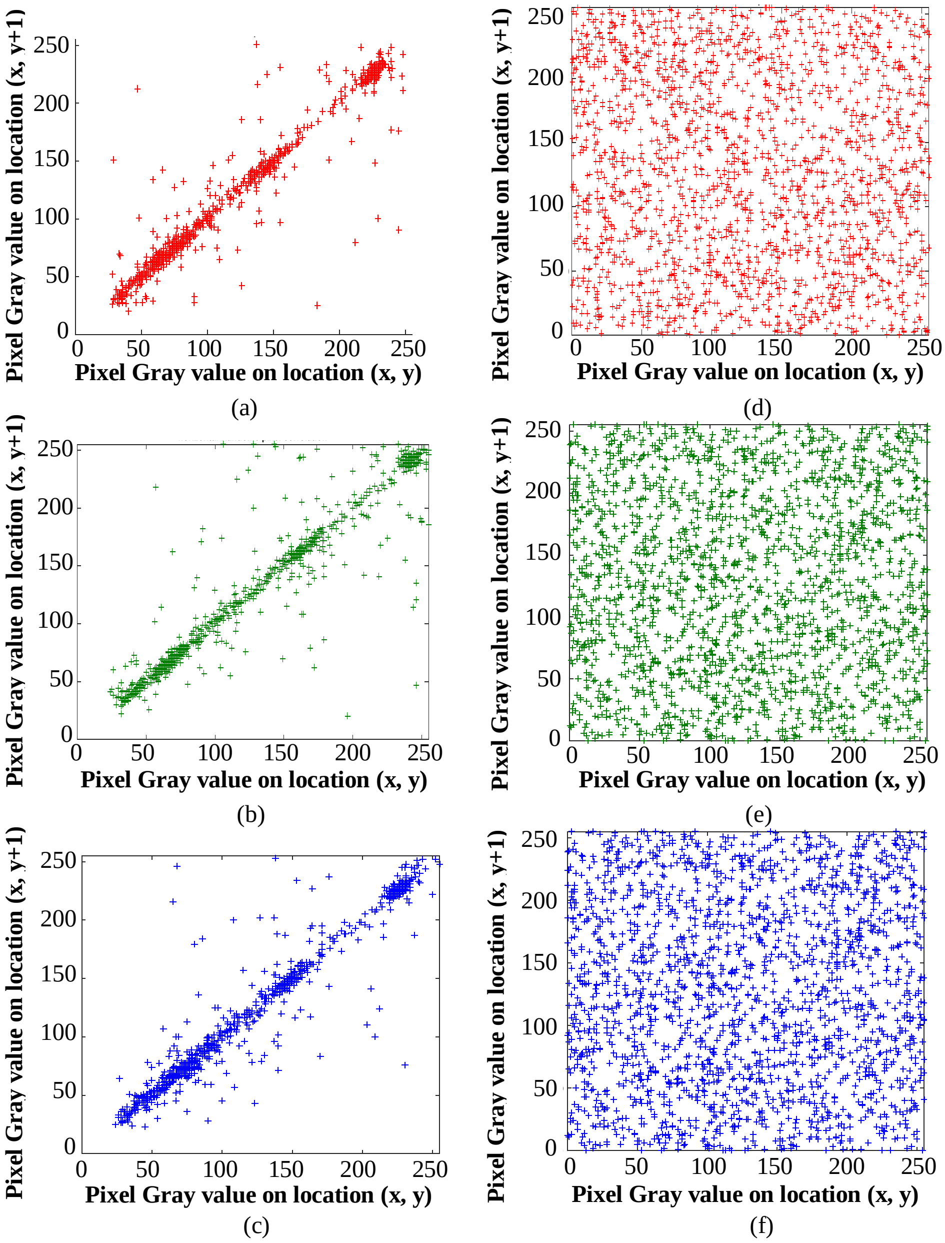


Figure 7 Histogram of ROI images (a) original image, (b) segmented image using bit level keyless substitution, (c) encrypted region using MSB based encryption using Hénon chaotic map and (d) decrypted image



(a) (d) (b) (e) (c) (f)

Figure 8 Correlation plot of two adjacent plain-image pixels in segmented image in horizontal direction for the (a) green channel, (b) red channel, and (c) blue channel. Correlation plot of two adjacent pixels of the cipher-image obtained by the proposed scheme from the (d) green channel (e) red channel (f) blue channel

4.2 Correlation analysis

Correlation is used to find the relationship between two variables or two different datasets. In image processing, correlation between every two adjacent pixel pairs of an image is usually very high, which indicates that pixels are strongly connected with their neighboring pixels within an image [16]. Correlation is calculated in an image with pixels in the horizontal, vertical, and diagonal directions. Here, correlation analysis represents horizontal correlation in all the channels of original color image and it is also calculated in the cipher image, as well as shown in Figure 8. Correlation between pixel values is calculated using the following equations:

$$D(r) = \frac{1}{N}\sum_{i=1}^{N}[r_i - E(r)]^2 \qquad (6)$$

$$Cov(r,s) = \frac{1}{N}\sum_{i=1}^{N}[r_i - E(r)][S_i - E(s)] \qquad (7)$$

$$r_{r,s} = \frac{Cov(r,s)}{\sqrt{D(r)}\sqrt{D(s)}} \qquad (8)$$

where r_i and s_i are 8-bit values of two contiguous pixels. N represents the total number of pixel pairs.

Table 1 shows a correlation of 2000 randomly selected pairs of adjacent pixels. It can be observed that correlation of cipher image is approximately equal to 0 while the correlation of plain image is nearly 1. This shows that the proposed algorithm is secure against all types of statistical attacks.

Table 1 Correlation analysis of an encrypted ROI

Image	Orientation	Red Channel	Green Channel	Blue Channel
Plain Image	Horizontal	0.962	0.9683	0.985
	Vertical	0.9015	0.9466	0.9621
	Diagonal	0.87	0.91	0.9402
Cipher Image	Horizontal	0.0141	0.0304	-0.00278
	Vertical	-0.0094	0.0034	-0.0083
	Diagonal	0.0159	-0.00170	0.0014

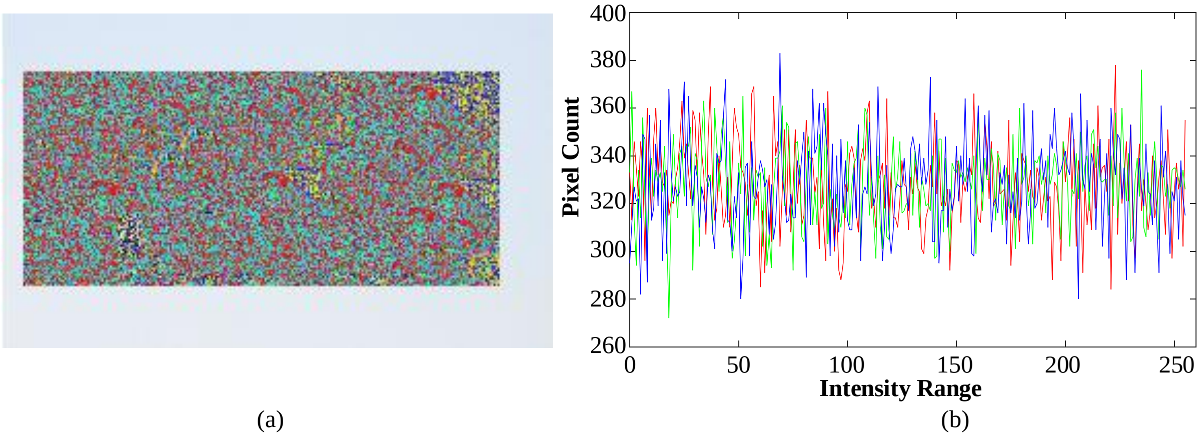


Figure 9 Key sensitivity test (a) image after applying the wrong symmetric key, and (b) intensity range of the corresponding segmented image

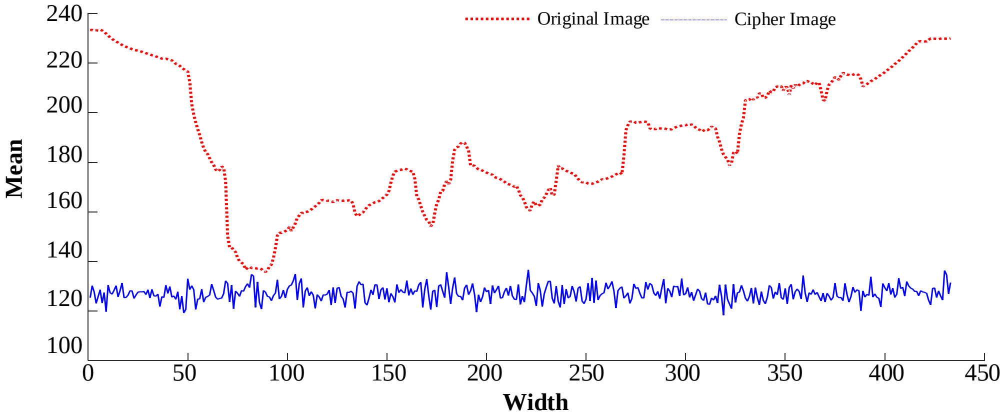


Figure 10 Mean value analysis

4.3 Key sensitivity test

For secure encryption, the key should be sensitive to a large keyspace and resist all kinds of brute force attacks. To test the sensitivity of the key involved, a tiny variation is done in the original secret key by changing it from x(1)=0.01 and y (1)=0.02 to x’(1)=0.010001 and y’(1)=0.020001. As a result, it was not possible to obtain the original image at the receiver’s end without knowing the secret key, as shown in Figure 9. A failed decryption image is shown in Figure 9(a) with its corresponding intensity range in Figure 9(b). Comparing these results with the correct decrypted image and its intensity range, it is clear that the decrypted image with the wrong key is completely different, and its intensity range is still balanced.

4.4 Mean value analysis

Mean value analysis is an important measure to check the correctness and level of secrecy of a cipher image. It is a calculation of the vertical distribution of mean pixel values of an image until the width of an image is reached [17]. The mean value of input plain image varies along the width of the image. On the other side, a cipher image in mean value visual representation that remains consistent along with the width of the image as shown in Figure 10. It can also be seen that the mean distribution of the cipher image is very close to each other and is uniform in the distribution graph of mean values. The mean is calculated using equation (9), where A is an image having N scalar observations.

$$\mu = \frac{1}{N}\sum_{i=1}^{N} A_i \qquad (9)$$

4.5 Comparative analysis with the existing techniques

There are several ROI based encryption techniques, usually classified into two domains, i.e., spatial and transformed domain.

Table 2 Comparative analysis of different ROI encryption schemes

Scheme	Parameter for the encryption process	Domain	Purpose	Encryption Module	Module for ROI	Image Type	Test performed	Remark
[18]	JPEG2000 Code stream	Wavelet domain	To secure medical images.	AES with CFB mode	Precincts Selection	Grayscale images	PSNR	Less than 10% of the data is encrypted.
[8]	Pixels of ROI	Spatial Domain	Speeds up the encryption process and enhances confidentiality	Permutation and value transformation	Manual selection as per the user, i.e., fixed-size block	Grayscale images	Encryption time	Regions are encrypted independently
[19]	Blocks of ROI	Spatial Domain	To secure biometric images i.e., iris images	Logistic Map and Arnold map	Edge-based detection	Grayscale images	Computational time analysis	Encryption time is less than 1 second
[20]	DWT coefficients	Transform Domain	Confidentiality	AES S BOX, Cat map, and Logistic map	cAP band	Grayscale images	Time, Entropy, key space, Histogram, speed analysis, correlation, NPCR and UACI	Two-layer security and the complete image is ciphered
[21]	Blocks of an image	Spatial domain	Confidentiality	Arnold Map, PRN and AES	Entropy-based sensitive block selection	Grayscale and color images	Entropy, Histogram, ID, Correlation, NPCR,UACI analysis, Encryption time	Two layer security and complete image is ciphered
[22]	Coefficients, JPEG2000 Code stream	Transform domain	Confidentiality for medical images	Invert MSB, AES	Decomposition of image using wavelet	Grayscale Images	PSNR	Two schemes are designed
[23]	Pixel of ROI	Spatial domain	Confidentiality	Blowfish symmetric cipher	Edge detected using the Prewitt detector	Color Images	Encryption time and ROI ratio	Based on Edge based and face detection
[24]	All pixels of an image	Spatial domain	Confidentiality	Lorenz and sine map	Sobel edge detection operator	Grayscale Images	Differential attack, Histogram, key sensitive analysis, PSNR	Entire image is encrypted based on importance
[25]	Pixels of ROI	Spatial domain	Compression, integrity and encryption	Chaos-based encryption and Huffman coding	arbitrarily	Grayscale Image	PSNR, Entropy, Correlation analysis	MAC is used to provide Integrity
Our scheme	Pixels of ROI	Spatial domain	To secure object-oriented images	Hénon chaotic map with Key-value transformation	Automatically by the proposed algorithm	Color images	Entropy, correlation analysis, mean value analysis, histogram analysis, key sensitivity test	Size is not fixed of the region. It is adaptive as per the region

In the spatial domain, an image is treated as a collection of pixels and ROI is identified by image processing techniques. In the transform domain, highly significant coefficients are incorporated in the encryption technique. Thus, ROI techniques [8, 18-25] are different in several aspects, which is presented in Table 2. A brief comparison of the proposed algorithm with existing techniques is done and it achieves a balanced amount of security and robustness. The proposed work is applied to medical and standard images. Information entropy is always obtained near eight, which shows that proposed algorithm is adaptive and efficient to object based images.

5. Conclusions

In this paper, the proposed algorithm is applied to various images in MATLAB and several tests were performed to find its correctness. It is estimated that the proposed algorithm gives appropriate results to get higher levels of security for images and is more space efficient and secure than previous algorithms and techniques. Statistical analysis was done on the test images, which yielded better results in all dimensions. A key sensitivity test demonstrates a small change in the symmetric key; it gives a different decrypted image which is not even near to original image. It makes system more reliable and robust against harmful activities. Sometimes, the foreground of image is an important source of information and it has to be kept secret for both communication ends. The proposed architecture ensures that various users from different spaces can only view a certain portions of an image. Experimental results show that the proposed algorithm has all the merits of an ideal cryptosystem. It is more secure and is a fast encryption module for large sized images.

6. References

[1] Le Gall D. MPEG: A video compression standard for multimedia applications. Comm ACM. 1991;34(4): 46-58.

[2] Katzenbeisser S, Petitcolas F. Information hiding. London: Artech house; 2016.

[3] Vardhana, M, Arunkumar N, Abdulhay E, Vishnuprasad PV. Iot based real time trafic control using cloud computing. Cluster Comput. 2018;(S1): 1-10.

[4] Susan S, Verma OP, Swarup J. Object segmentation by an automatic edge constrained region growing technique. 2012 Fourth International Conference on Computational Intelligence and Communication Networks (CICN); 2012 Nov 3-5; Mathura, India. USA: IEEE; 2012. p. 378-81.

[5] Ou Y, Sur C, Rhee KH. Region-based selective encryption for medical imaging. International Workshop on Frontiers in Algorithmics; 2007 Aug 1-3; Lanzhou, China. Berlin: Springer; 2007. p. 62-73.

[6] Mahmood AB, Dony RD. Segmentation based encryption method for medical images. 6th International Conference on Internet Technology and Secured Transactions; 2011 Dec 11-14; Abu Dhabi, United Arab Emirates. USA: IEEE; 2011. p. 596-601.

[7] Liu JL. Efficient selective encryption for JPEG 2000 images using private initial table. Pattern Recogn. 2006;39(8):1509-17.

[8] Ravishankar KC, Venkateshmurthy MG. Region based selective image encryption. 2006 International Conference on Computing & Informatics; 2006 Jun 6-8; Kuala Lumpur, Malaysia. USA: IEEE; 2006. p. 1-6.

[9] Kittler J. A locally sensitive method for cluster analysis. Pattern Recogn. 1976;8(1):23-33.

[10] Verma OP, Hanmandlu M, Susan S, Kulkarni M, Jain PK. A simple single seeded region growing algorithm for color image segmentation using adaptive thresholding. 2011 International Conference on Communication Systems and Network Technologies; 2011 Jun 3-5; Jammu, India. USA: IEEE; 2011. p. 500-3.

[11] Agarwal S, Awan A, Roth D. UIUC image database for car detection. 2002 [cited 2007 Mar 1]. Available from: https://cogcomp.seas.upenn.edu/Data/Car/

[12] Kumar A, Raghava N. A novel group-based cryptosystem based on electromagnetic rotor machine. Indian J Sci Res. 2017;16(2):131-6.

[13] Lin RM, Ng TY. Secure image encryption based on an ideal new nonlinear discrete dynamical system. Math Probl Eng. 2018;2018:1-12.

[14] Raghava NS, Kumar A, Deep A, Chahal A. Improved LSB method for image steganography using Henon chaotic map. J Inform Secur Appl. 2014;1(1):34-42.

[15] Jeyamala C, GopiGanesh S, Raman GS. An image encryption scheme based on one time pads-A chaotic approach. 2010 Second International conference on Computing, Communication and Networking Technologies; 2010 Jul 29-31; Karur, India. USA: IEEE; 2010. p. 1-6.

[16] Belazi A, El-Latif AAA, Rhouma R, Belghith S. Selective image encryption scheme based on DWT, AES S-box and chaotic permutation. 2015 International Wireless Communications and Mobile Computing Conference (IWCMC); 2015 Aug 24-28; Dubrovnik, Croatia. USA: IEEE; 2015. p. 606-10.

[17] Somaraj S, Hussain MA. Performance and security analysis for image encryption using key image. Indian J Sci and Tech. 2015;8(35):1-4.

[18] Brahimi Z, Bessalah H, Tarabet A, Kholladi MK. A new selective encryption technique of JPEG2000 codestream for medical images transmission. 5th International Multi-Conference on Systems, Signals and Devices; 2008 Jul 20-22; Amman, Jordan. USA: IEEE; 2008. p. 1-4.

[19] Mehta G, Dutta MK, Travieso-González CM, Kim PS. Edge based selective encryption scheme for biometric data using chaotic theory. 2014 International Conference on Contemporary Computing and Informatics (IC3I); 2014 Nov 27-29; Mysore, India. USA: IEEE; 2014. p. 383-6.

[20] Belazi A, Abd El-Latif AA, Rhouma R, Belghith S. Selective image encryption scheme based on DWT, AES S-box and chaotic permutation. 2015 International Wireless Communications and Mobile Computing Conference (IWCMC); 2015 Aug 24-28; Dubrovnik, Croatia. USA: IEEE; 2015. p. 606-10.

[21] Ayoup AM, Hussein AH, Attia MAA. Efficient selective image encryption. Multimed Tool Appl. 2016;75:17171-86.

[22] Ou, Y, Sur C, Rhee KH. Region-based selective encryption for medical imaging. International Workshop on Frontiers in Algorithmics; 2007 Aug 1-3; Lanzhou, China. Berlin: Springer; 2007. p. 62-73.

[23] Khashan OA, Zin AM, Sundararajan EA. Performance study of selective encryption in comparison to full encryption for still visual images. J Zhejiang Univ Sci C. 2014;15:435-44.

[24] Sankaradass V, Murali P, Tholkapiyan M. Region of Interest (ROI) based image encryption with sine map and lorenz system. In: Pandian D, Fernando X, Baig Z, Shi F, editors. International Conference on ISMAC in Computational Vision and Bio-Engineering; 2018 May 16-17; Palladam, India. Berlin: Springer; 2018. p. 493-502.

[25] Xiao D, Fu Q, Xiang T, Zhang Y. Chaotic image encryption of regions of interest. Int J Bifurcat Chaos. 2016;26(11):Article no. 1650193.