Journal of Theoretical and Applied Information Technology
15th November 2018. Vol.96. No 21

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMAGE ENCRYPTION ALGORITHM BASED ON RC4 AND HENON MAP

[1]DENA S. ALANI, [2]SALAH A. AL IESAWI

[1,2]Department of Computer Science, College of Computer Science and Information Technology, University of Anbar, Iraq

E-mail: [1]denaalani83@gmail.com, [2]salaheng1996@gmail.com

ABSTRACT

In network-based technology like multimedia applications, different encryption techniques are used to protect the confidential data from unauthorized access and provide highly secured data transmission. Due to the large data size and high correlation between pixels, special encryption techniques are used for digital images instead of traditional ciphers that incur significant overhead. In this paper, a new encryption algorithm is proposed using chaotic Henon map with the RC4 algorithm. In the first step, a new basis is presented to reduce the amount of data required to present the image. In the second step, the combination of the RC4 algorithm and the chaotic Henon map function is used to generate sub-keys with N rounds. The sub-key is generated to encrypt one block in each round, so that N of rounds is equal to N of the blocks for the compressed image. The results of using different metrics such as statistical analysis and key sensitivity tests show that the proposed encryption scheme provides an efficient and secure way for real-time image encryption and transmission**.**

Keywords: *Image Compression, DCT, Image encryption, Chaotic Henon Map, RC4*

1. INTRODUCTION

The encryption of digital images is very important to ensure the security for the information that should not be accessed or used by other users. Many genuine applications, for example, medical imaging system, video conferencing, military image databases, remote sense, remote learning, cable TV, etc. require reliable, fast and robust security system to store and transmit advanced information and digital images. The requirements to fulfill the security needs of digital images have led to the development of good encryption techniques. The image encryption process is achieved by transforming the information and making it unreadable by using an algorithm and a special key [1]. Traditional cryptographic algorithms like RSA, DES, AES, etc. exhibit a low level of security and they are prone to different security attacks. These standard encryption algorithms were not efficient enough for secure communication of images and videos. Recently, many chaos-based techniques have been developed to overcome the limitations of such traditional encryption algorithms. The process can be partial encryption or full encryption that uses transformation maps, which appear to be random but are actually deterministic. The chaos-based techniques is based on full encryption, and it is hard to break and understand by any adversary. Moreover, it is fast and easy to implement [2]. Most of the researchers in the field of image transmission have utilized two major techniques; the compression and the encryption. These techniques are supposed to offer secure, reliable and efficient transmission. The techniques are used in three orders: (1) compression followed by encryption (CE), (2) encryption followed by compression (EC), and (3) join compression and encryption (JCE) [3]. Modern cryptography has used chaos system as it has the advantage of being very sensitive to a small change in initial value. In this paper, chaos Henon Map (CHM) combines with

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RC4 algorithm to derive N of sub keys to encrypt N of image blocks. This paper is organized as follows. Section 2 explains related works. Section 3 explains image compression and encryption, chaotic, chaotic based in encryption methods and Chaotic Henon Map. Section 4 explains the proposed image compression and encryption algorithm. Section 5 shows the results, and Section 6 offers the study conclusion.

2. RELATED WORKS

Prominent researchers in the field of image encryption carried out many researches and proposed many algorithms in chaotic image encryption. According to some chaotic functions, several algorithms are utilized to manipulate them and scatter the position of pixels. In [4 - 6], Chaotic Henon Map was proposed to be used in pixel shuffling. Two chaotic image encryption schemes were presented by Yen, and Guo [7-9] where the pixels of the image are rearranged by utilizing a chaotic system method to randomly generate a binary sequence. Kadir, et al. [10], have presented external private key for encrypting the chaotic image. The algorithm of image encryption was based on 80-bits and 2 chaotic logistic maps. The external secret key is utilized for providing various weights to its bits to generate initial conditions for two (CLM). The first CLM map is used to generate the numbers ranging from 1 to 24. The initial condition of the second CLM is modified using the numbers produced by the first CLM. Also in this system, the process of producing the keys required a time. Ukur, et al. [11], presented encryption algorithm for digital color images utilizing the combination of RC4 algorithm and chaotic logistic map. In the proposed algorithm, the external key is converted to the initial values, then that initial values of CLM function are used to generate pseudo-random numbers and XOR-ed the byte streams of plain-image with a stream of pseudo-random numbers during the encryption process. Atan, et al. [12], presented a new image encryption scheme that is based on Ikeda and Henon chaotic maps. Techniques of the shuffling and diffusion are the most frequently used in image encryption. The sequences produced from Ikeda Map are used to shuffle the image rows and columns, then the sequences of Henon map are used to change the gray levels of pixels. After that, the pixels are shuffled again using Ikeda Map. Many experimental tests are utilized to evaluate the developed algorithm.

3. IMAGE COMPRESSION & ENCRYPTION

3.1 Image Compression

The idea of image compression is to minimize the size of image to the least size possible with accepted quality by reducing the amount of data required to represent the image [13]. Image compression is a very important method used to decrease the time required for image transmission, and allow more images to be stored in a given memory space. The purpose of image compression is to represent an image in the fewest number of bits without losing the essential information of the original image. Information of an image can be compressed if it is redundant. There are different methods to compress, but all of these methods depend on the basic principle by which one "Eliminates or reduces redundant data from the image". The term redundancy refers to unnecessary image pixel values and all forms of duplication. There are three primary types of data redundancies in an image [14]:

1- Inter-pixel redundancy which occurs due to high correlation ratio between picture elements.

2- Psycho-visual redundancy which exists because of the nature of the human eye.

3- Coding redundancy which occurs as a result of using frequencies that are lower than the optimal code words.

In general, there are two types of compression techniques according to the way of redundancy removal: Lossy and Lossless

1- Lossless technique: there is no loss of information, and the original image can be reconstructed perfectly from the compact image.

2-Lossy technique: in this technique, information removed during the compression process cannot be retrieved. Yet, this technique has several advantages [15]:

1- Reduce transmission time.

2- Increase the storage space.

Journal of Theoretical and Applied Information Technology
15th November 2018. Vol.96. No 21

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3- Reduce transmission errors due to fewer bits transferred.

4- Provide a level of secure transmission due to compressing and encoding the image.

3.2. Image Encryption

Image encryption is an art and a mechanism for protecting image information from undesirable persons by hiding the information and converting it into non-recognizable form while being transmitted and stored [16].

In fact, the basic aim of image encryption is to provide secure transmission for the image over the internet. The image pixels have specific characteristics like huge capacity, high correlation ratio, and much higher redundancy ratio. This imposes specific requirements on any technique and encryption algorithm. In general, the technique that is mostly used to secure image is shuffling the original image data and converting it to non-clear form. Many ways are used to secure the image information such as watermarking, steganography, compression and cryptography.

To secure the image perfectly, two techniques are employed according to the approach used to structure the encryption system [17]:

-*Chaotic based image encryption methods*

-*Non-chaotic based image encryption methods*

In this paper, chaotic based encryption methods is used**.**

3.3 Chaotic

Chaos is defined as a phenomenon that happens in nonlinear systems. It depends on initial condition and on exhibiting random behavior [18].

3.3.1 Chaotic based image encryption methods

In the architecture of the chaotic system used in image encryption and decryption, two important processes are used: Confusion and Diffusion.

Confusion is defined as the process used to scramble the position of picture elements (pixels) without changing the values of the pixels.

Diffusion is defined as the process used to change the pixel values of the original image by the random sequence produced from chaos system. In chaotic systems, diffusion and confusion depend on initial value conditions and the control parameters with *N* rounds to generate the random sequence [19].

3.3.2 Chaotic Henon Map (CHM)

Henon map is a simple type of discrete chaotic system proposed by the French astronomer scientist Michelas as a simplification of the Lorenz chaotic system [20]. It was obtained by thinking about stretch and folding. The model of Henon is a two-dimension plane that is able to stretch, fold and reverse. It displays chaotic behavior for the dynamic systems. The map takes the form shown in fig (1) [21]. The mathematical model is represented in two equations and written in the following form:

$$X_{n+1} = 1 - aX_n + Y_n \quad (1)$$

$$Y_{n+1} = bX_n \quad (2)$$

Where

x_n, y_n represent initial values.

$a = 1.4, b = 0.3$.

X_{n+1}, Y_{n+1}: Take the values between (0, 1)

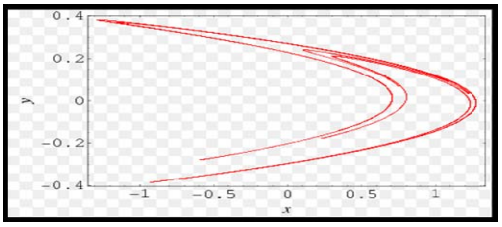
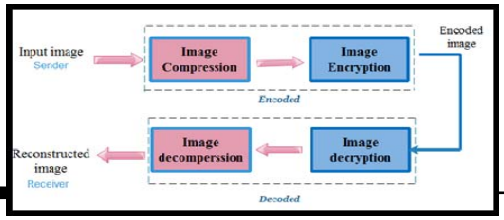


Fig1. Henon Map

But if the two parameters (a) and (b) take other values, the Henon map may converge to a periodic orbit.

4. THE GENERAL PROPOSED MODEL

The general proposed model consists of two parts: first part is related to image encoding, and the second part is related to image decoding as shown in figure (2).



ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig 2. Block diagram of the general proposed model

A. Image compression

In image compression, the proposed model is based on Dct and Shift coding to minimize the size of the image and eliminate redundancy and less important data. Figure (3) shows the steps of image compression and decompression

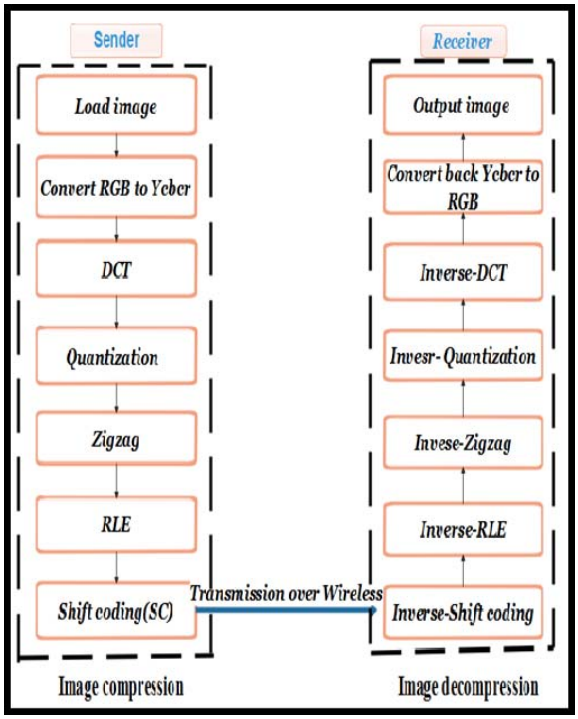


Fig 3. The Proposed Image Compression& Decompression

The steps of image compression can be listed as the follows:

Step1: Load image.

Step2: Convert RGB color space to YCbCr color space.

Step3: Apply Discrete Cosine Transform (DCT) on 8x8 blocks.

Step4: Quantization lowers the high frequencies that represent the least important information.

Step5: Apply Zigzag scan to convert a 2-D matrix to one dimension matrix and to group important data in the top of the one dimension matrix.

Step7: Shift coding is used to decrease the number of bits needed to represent the data after RLE.

Step6: Use RLE to encode the large run of repeating zeros that are generated after quantization and zigzag stage

Decompression

In the decompression technique, the processes used in the compression techniques are perfectly reversed starting with inverse shift coding and ending with converting YCbCr to RGB.

B. The proposed Encryption Method

The proposed image encryption model combines RC4 algorithm with chaotic Henon Map to generate N of the keys so that each produced key (256) bytes is used to encrypt one block (256) bytes of the compressed image. Fig (4) shows the structure of the model. Each generator has two inputs. The first generator has an initial S (256), which represents a vector containing the values from 0 to 255, and a secret key that is input by the user for encryption and decryption. Also, the other generators have two inputs, a produced key 256 bytes from the previous generator, and a generated key that is produced from the previous PRGA of RC4. In this model, chaotic Henon Map was added between two stages of RC4 to increase the strength and randomness of encryption keys.

The proposed model includes:

1. The number of rounds is equal to the number of blocks of the compressed image.

2. The number of generated keys is equal to the number of blocks of the compressed image.

3. The length of each block of the compressed image is 256 bytes.

4. The length of each generated key is 256 bytes.

5. The type of encryption in this model is stream cipher, but the process of keys generation is block.

6. The encryption process is XOR.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The image in the computer represents a two-dimensional matrix, then during the compression process, the image is converted into a one-dimensional matrix. The compressed image is then divided into blocks where length of each block is 256 bytes. As shown in Fig (6), the proposed image encryption model consists of four main processes. These processes are the *Key generator (KSA), Generation chaotic Henon, PRGA, XOR_ed generated key and a block of image.*

1. *Key generator* is similar to KSA of RC4, but the produced key of the generator returns as input to the generator again. The Key generator has two inputs: S (256), which represents a vector containing the values from 0 to 255, so that S [0] = 0 and S [255] = 255, and secret key ***K***, which is input from the user. The locations of the state are permutated according to the value of the secret key. The operation that is used in the generator is the swap, so that S[i] is swapped with another location in S according to the value of location K[i]. The produced key has two uses: as feedback (as input) to the generator of keys in the next round, and as a converter to x_0, y_0 , which is used as input for Chaotic Henon map. To increase randomness and strength of the key against attack, Henon Map is used.

2. *Generation of Chaotic Henon*

Converting the produced key from the generator to the initial value for X_0, Y_0 for Henon map, the length of the produced key is 256 bytes. The process divides the produced key into two parts so that X_0 takes the values from 0 to 127, and Y_0 takes the values from 128 to 255. Then, the values of X_0, Y_0 which are obtained from the key are converted from integer numbers to real numbers, Also Y_0 . Then, apply X_0 and Y_0 on equation (1), (2) to calculate X_n , Y_n

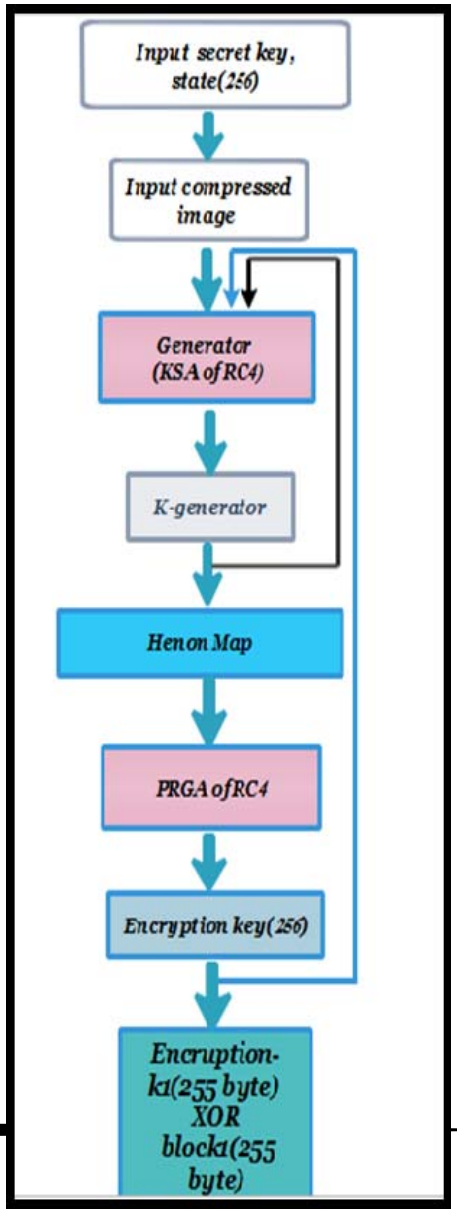
$$X_{n+1} = 1 - 1.4 x_n + y_n$$

$$Y_{n+1} = 0.3\, y_n$$

After that, "X_n"and "Y_n" will act as "X_0", and "Y_0" to calculate $X_{n+1}$and so on. The X_n obtained from Henon equation represents one byte, also Y_n represents one byte. So, to generate an encryption key of length 256 byte from Henon map, a loop from 0 to 255 is involved. The loop increases by 2 every time. After x_n value and Y_n value are converted back into integer number, X_n, Y_n will be multiplied with 255 and then the result will be modulo with 255 and takes the absolute value of the result. The final result of X_n will be stored in array K_out [i]. And Y_n will be stored in K_ out [i+1], where I =0, 1 ...255. This process will be repeated until K_ out [255] is filled.

3. *PRGA:* in this stage, locations of K_ out [256] are swapped to produce a generated key. This process needs loop through all locations of K_ out [i]. K_ out [i] is swapped with another location in K_ out according to scheme dictated by current configuration of K_ out.

4. *XOR_ed generated key and a block of image.* The generated key [255] is XOR block1of the compressed image [255]. The previous steps are for a N of rounds so that the N equals the number of blocks of the compressed image.



Journal of Theoretical and Applied Information Technology
15th November 2018. Vol.96. No 21

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig 5. The proposed system for image encryption

The Steps of the Proposed Encryption Algorithm

Step1: Input the compressed image and secret key (K)

Step2: Use secret key *K* and initial S [256] as input to the Generator.

Step3: Swap each location of S [i] with another location in S according to the value of location K [i]

Step4: Generate the produced key [256] bytes from the Generator

Step5: The produced key is a feedback to the generator, and also use the produced key as an input to Chaotic Henon Map (CHM)

Step6: Use the produced key to create initial value X_0 and Y_0 for Eq. (1), (2).

Step7: Apply Eq. (1), (2) of Chaotic Henon Map (CHM) by using X_0 and Y_0 to produce key. The length of key is 256 bytes. These are used as input to PRGA.

Step8: PRGA takes the key [256] bytes from the Henon Map, and changes the arrangement of its locations depending on the key itself to produce the first key for encrypting the first block of the compressed image.

Step9: XOR_ed first encryption key with the first block of the compressed image

Step10: First encryption key is a feedback to the generator.

Step 11: Go to step 3

Step 12: Repeat the previous steps for N of rounds, until N > the number of blocks of the compressed image then stop. The following figure represents the image encryption scheme in details.

Decryption Method

In this process, the same key that was keyed in by the user in the encryption process is used in the decryption process to generate the key (256) bytes that decrypts the first block (256) bytes of the encrypted image. The first generated key is used as an input to the system again to generate the key and to decrypt the second block of the image until generating a N of the decryption key that is equal to the N of blocks image to finally get the plain image.

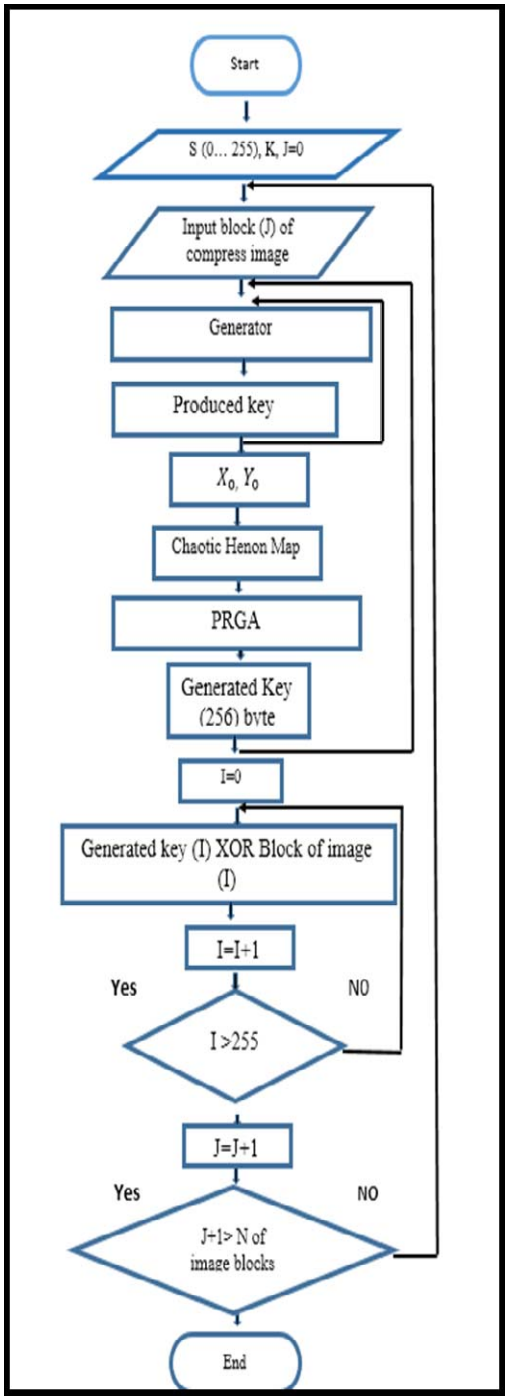


Fig 6. Flowchart of encryption image

Journal of Theoretical and Applied Information Technology
15th November 2018. Vol.96. No 21

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. RESULTS AND DISCUSSION

A. Results of Test Image Compression

Image compression algorithm was applied on 7 images as shown in Fig (7). The type of images used are BMP with different sizes on PC computer with VB language, and the operating system is window 7. CR and PSNR are calculated. Table 1 shows the results of CR, PSNR. The compression algorithm was compared with standard JPEG and the results are shown in Table 2. The results show that the proposed compression algorithm was better and faster than JPEG standard.

Table1. *Result of CR & PSNR*

NO	Size of tested images in KB		*CR*	*PSNR*
1	Baboon	44.3	1:9.57	31.68
2	Lenna1	192	1:15.93	35.88
3	Girl child	28.8	1:12.01	34.02
4	Flower	19.6	1:20.11	38.54
5	Lenna2	34.6	1:17.15	40.78
6	Boy child	51.8	1:11.49	31.47
7	Blue sky	5.41	1: 6.86	36.60

B. Result of Test Image Encryption

1. Key space analysis

Key space size is defined as the total number of various keys that can be generated and used for encryption. Attributes of good encryption algorithm are sensitive to the secret key which has to be large enough to resist attacks. In our proposed algorithm, the length of generated key is 256 byte, and the key space size can be up to 256^{256}. Thus, the key space is large enough to impede various attacks [22].

2. *Sensitivity analysis*

A robust encryption system must be sensitive to the original image and the key; therefore, we tested the sensitivity to the key using an encrypted image, which is obtained by the key that is different from the original in one bit. Two measurements are used to test sensitivity of the key: *NPCR & UACI* [23]

Table2. Result of compression JPEG & the proposed compression method

No	*Standard JPEG*		*The proposed image compression Method*	
	CR	*Comp/ time (Sec)*	*CR*	*Comp/ time (Sec)*
1	1:4.68	1.10940	1:9.57	0.00726
2	1:7.40	1.11532	1:15.93	0.00553
3	1:6.63	0.43903	1:12.01	0.00269
4	1:9.19	1.11197	1:20.11	0.00539
5	1:7.81	1.75489	1:17.15	0.00858
6	1:6.38	1.73723	1:11.49	0.00900
7	1:9.59	0.27755	1:16.86	0.00109

Fig 7. Samples of tested images

Journal of Theoretical and Applied Information Technology
15th November 2018. Vol.96. No 21

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- *NPCR*: is checking the no. of the pixels, which is different between encrypted images E1, E2. NPCR that is the shortcut to the number of pixels changes rate and is defined in the following form:

$$NPCR\ (E1\ E2) = \frac{\sum_{ij} D(i,j)}{z} \times 100\ \% \qquad (3)$$

Where

$$Dij = \begin{cases} 0 & , \ if\ E1(i,j) = E2(i,j) \\ 1 & , \ if\ E2(i,j) \neq E2(i,j) \end{cases}$$

$$z = W \times H$$

- *UACI:* is used to calculate the average intensity of variation between the encrypted image and the original image.

UACI is defined by equation (4)

$$UACI = \frac{1}{z} \left[\sum_{ij} \frac{|E1(i,j) - E2(i,j)|}{255} \right] \times 100 \qquad (4)$$

Hence, E1, E2 are representing 2 encrypted images for the same original image, which has a single modified pixel.

A) Key sensitivity

In the proposed encryption model, 7 samples of color images with different sizes were used to encrypt via ("f1278hswdgky121") as key, and then the same samples of the images were encrypted with a little difference in the key. The results of NPCR and UACI for encrypted images with changing one character in the key are shown in table 3, while the results of the encrypted images with changing 2 characters in the key are shown in table 4.

The results in Table 3 and Table 4 of NPCR and UACI for the encrypted image show that more than 99% of pixels of the encrypted image are different when making a simple change in the key of the proposed system. It also shows high key sensitivity.

Table 3. NPCR & UACI for encrypted images with changing 1 character in the key

Original Images	NPCR	UACI
Lenna1	99.5785	33.5174
Baboon	99 5471	33.4869
Girl Child	99.6051	33.6857
Flower	99.5318	33.7340
Lenna 2	99.5908	33.3403
Boy child	99.5694	33.3670
Blue sky	99.6226	33.6026

Table 4. NPCR & UACI for encrypted images with changing 2 characters in the key.

Original Images	NPCR	UACI
Lenna1	99. 6596	33.5053
Baboon	99.6201	33.4735
Girl Child	99.6525	33.3694
Flower	99.6277	33.5603
Lenna 2	99.7033	33.4707
Boy child	99.6298	33.5217
Blue sky	99.8284	33.7081

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. Resistance to known-plaintext and chosen-plaintext attacks

In our model, we have compressed the image to eliminate the correlation between the pixels of the original image, and remove redundant data, which attackers use to know the original image. Then the compressed image was divided into blocks; each block was encrypted with a different key, and each key was generated from the previous one. So attackers cannot get any helpful information to know the original image by encrypting several special standard images. The attacks suggested in [24, 26] become inactive in this system.

4. The entropy

The most important attribute for randomness is the entropy, which is calculated according to Eq. 5:

$$H(s) = \sum_{i=0}^{2^n-1} P(s_i) \log_2 \frac{1}{p(s_i)} \quad (5)$$

For a correct random when the source is represented by 2^n symbols, the entropy H(s) must be n, or near to (n). In gray image, the pixel can take 2^n possible to represent data. So the entropy for a correct random must be 8 or closer to 8. Entropy values for the encrypted images are ordered in Table 5. The resulting values are much nearer to 8. That proves that the encryption model is secured against attackers. The proposed algorithm is compared with another two algorithms suggested in [26], and the results of the comparison were arranged in Table 6. The results prove that the proposed model is better.

Table 5. *Results of entropy for encrypted images*

Encrypted images	Entropy values
Girl child	7.97396
Lenna 1	7.9849
Baboon	7.9906

Table 6. *Results of entropy for encrypted image "Lenna1"*

Algorithms	Entropy values
Baptista's	7.926
Wong's	7.969
The proposed	7.984

Table 6 shows the comparison between the proposed algorithms and two other algorithms for image encryption, which were used in previously published research. The comparison is based on entropy measurement, which represents the most outstanding characteristic of randomness. The comparison was executed using standard image Lena1. The results proved that the proposed algorithm is better.

6. CONCULUSIONS

The best method to attain a secure and fast image transmission is by using the techniques of compression and encryption. In this paper, image compression technique followed by encryption technique (CE) were used. The proposed model includes the encoding and the decoding of an image. The image encoding consists of two-parts: the first part is image compression with DCT and shift coding, and the second part is image encryption with a new encryption algorithm that is based on combining the RC4 algorithm and Chaotic Henon map to generate sub keys and encrypt each block of the compressed image with a different key. The algorithm has combined the advantages of fast encryption of RC4 algorithm and the best features of chaos maps. PSNR and CR are computed and compared with JPEG and the proposed compression method was better as shown in table 2. The key space is large enough to resist attacks. For security analysis, different methods were employed like key sensitivity analysis and Entropy information, and they have shown good results as shown in table 3 and table 4. The proposed algorithm was compared with two other algorithms and the results prove that the proposed model is better as shown in table 6. The results proved that

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the proposed image encryption model can resist different attacks.

REFERENCES

[1] Wang, X., Liu, L., and Zhang, Y, "A novel chaotic block image encryption algorithm based on dynamic random growth technique". Optics and Lasers in Engineering, 66, 10-18, 2015.

[2] Setyaningsih, E., Wardoyo, R, "Review of Image Compression and Encryption Techniques". International Journal Of Advanced Computer Science And Applications, 8(2), 83-94, 2017.

[3] Mohamed, M. A., F. W. Zaki, and A. M. El-Mohandes. "Improved Mobile WiMax Image Privacy Using Novel Encryption Techniques." (2013).

[4] Jolfaei, A., Mirghadri, A.,"An image encryption approach using chaos and stream cipher". Journal of Theoretical and Applied Information Technology, 19(2), 117-125, 2010.

[5] Sathyaprakash, K. P., Anandbabu, M. H., and Sathyanarayanan, M," An Efficient Compression and Decompression of Henon Chaotic System Based Encryption".

[6] Şekertekin, Y., Atan, Ö., "An image encryption algorithm using Ikeda and Henon chaotic maps". In Telecommunications Forum (TELFOR), IEEE, 24th (pp. 1-4), 2016.

[7] Yen, J.C and J. I. Guo, A New Chaotic Image Encryption Algorithm, Proceedings of National Symposium on Telecommunications, 1998, 358-362.

[8] Yen, J. C. and J. I Guo., A New Chaotic Mirror-Like Image Encryption Algorithm and Its VLSI Architecture, Pattern Recognition and Image Analysis, 2000, 10(2), 236-247.

[9] Yen, J. C. and J. I. Guo., Efficient Hierarchical Chaotic Image Encryption Algorithm and Its VLSI Realization, Proceedings of IEEE Vision, Image and Signal Processing, 2000, 147(2).

[10] R. Kadir, R. Shahril, M. A. Maarof, A Modified Image Encryption Scheme Based on 2D Chaotic Map, International Conference on Computer and Communication Engineering (ICCCE 2010), 11-13 May 2010.

[11] Saptarini, Ni GAP Harry, and Yosua Alberth Sir. "Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map." *ISICO 2013* 2013 (2013).

[12] Şekertekin, Yeter, and Özkan Atan. "An image encryption algorithm using Ikeda and Henon chaotic maps." *Telecommunications Forum (TELFOR), 2016 24th*. IEEE, 2016.

[13] Chaitanaya1, G., Keerthi2, B., Saleem3, A., Trinadh Rao4, A., Kumar5, K.T.P.S. "An Image Encryption and Decryption using Chaos Algorithm", IOSR-JECE, 2015.

[14] Dhawan, S.," A review of image compression and comparison of its algorithms". International Journal of Electronics & Communication Technology, IJECT, 2(1), 22-26, 2011.

[15] Rojatkar, D. V., Borkar, N. D., Naik, B. R., and Peddiwar, R. N."Image Compression Techniques: Lossy and Lossless". International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015.

[16] P.Ranta, "Adapting Media Elements of MMS Messages Using Digital Signal Processor", M.SC thesis, Helsinki University of Technology 6 November (2003).

[17] Sankpal, P. R., & Vijaya, P. A." Image encryption using chaotic maps: a survey" , In Signal and Image Processing (ICSIP), 2014 Fifth International Conference on (pp. 102-107). IEEE, 2014.

[18] Mendua, B. R. B. I.," A New Approach of Colour Image Encryption Based on Henon like Chaotic Map", Journal of Information Engineering and Applications, Vol.3, No.6, 2013.

[19] Mokhtar, M. A., Sadek, N. M., and Mohamed, A. G., "Design of image encryption algorithm based on different chaotic mapping". In Radio Science Conference (NRSC), 2017 34th National (pp. 197-204). IEEE, March, 2017.

[20] Khan, J., Ahmad, J., and Hwang, S. O., "An efficient image encryption scheme based on Henon map, skew tent map and S-Box", In Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on (pp. 1-6). IEEE, 2015.

[21] Chapaneri, S., Chapaneri, R.," Chaos based image encryption using latin rectangle scrambling". In India Conference (INDICON), Annual IEEE (pp. 1-6). IEEE, 2014.

[33] Sun, F., Lü, Z., & Liu, S. "A new cryptosystem based on spatial chaotic system. *Optics Communications"*, *283*(10), 2010. 2066-2073.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[32] Wu, Y., Noonan, J. P., and Agaian, S. "NPCR and UACI randomness tests for image encryption". Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), 31-38, 2011.

[24] Saptarini, Ni GAP Harry, and Yosua Alberth Sir. "Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map." *ISICO 2013* 2013 (2013).

[25] Soleymani, Ali, Md Jan Nordin, and Elankovan Sundararajan. "A chaotic cryptosystem for images based on Henon and Arnold cat map." *The Scientific World Journal* 2014 (2014).

[26] Zhang, G., Liu, Q. "novel image encryption method based on total shuffling scheme". Optics Communications", 284(12), 2775-2780, 2011.

Journal of Theoretical and Applied Information Technology
15th November 2018. Vol.96. No 21

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

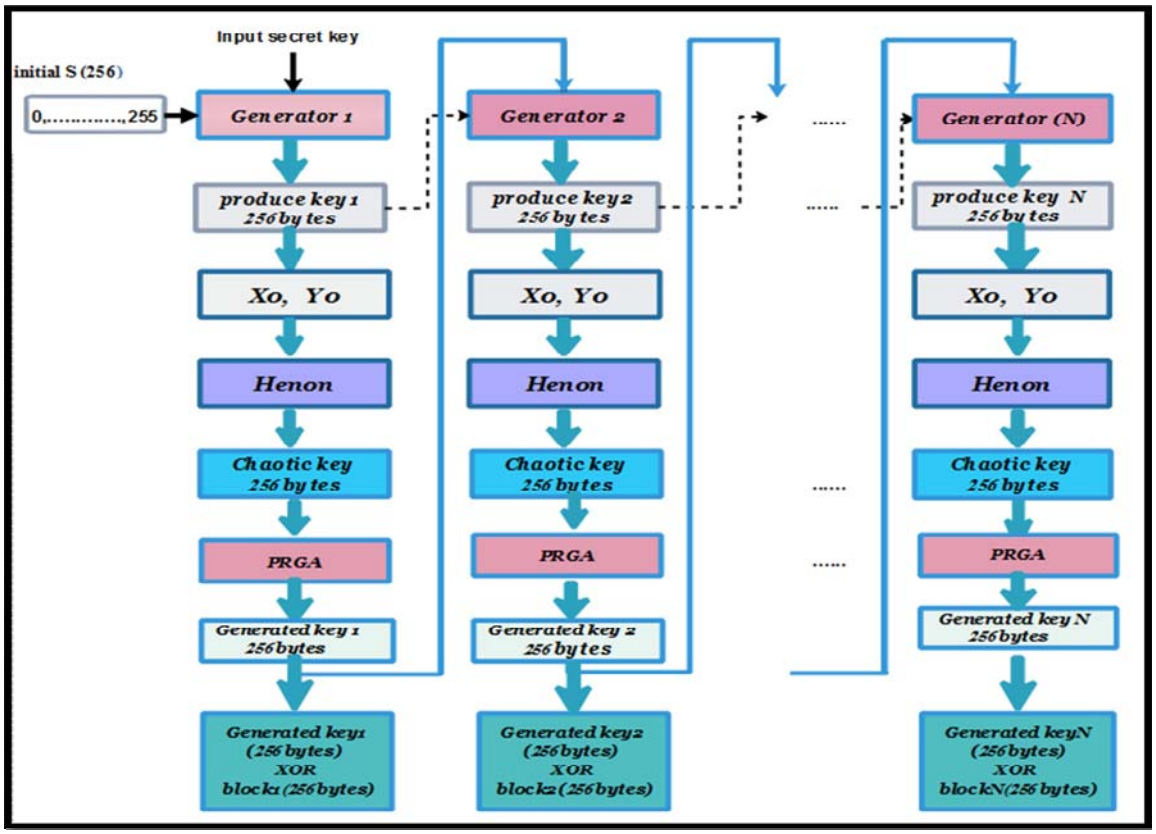


Fig 4. The Structure Of Proposed Image Encryption Method