International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

Color Image Encryption and Decryption using Pixel Shuffling with Henon Chaotic System

Asia Mahdi Naser Alzubaidi
Computer Science Department, College of Science
Karbala University
Karbala, Iraq

Abstract*—Nowadays, with the incredible development of internet technologies and wireless communication networks such as computer and mobile networks, all kinds of multimedia data like digital image, Audio, text and video can be accessed in easily way on internet. As a result, cryptographic techniques are required to accomplish a certain level of security, integrity, confidentiality and as well as, to prevent unauthorized access of sensitive information during data storage and transmission. In this research, a novel and efficient color image encryption and decryption schemes has been suggested based on image pixels scrambling by iteratively dividing it in sixty four blocks and rotate each one in clockwise direction with 90 angles. Then applied two dimensions Arnold cat mapping to make more distortion of the relationship among adjacent pixels of original image by hide the statistical structure of pixels. Actually, the location of the image pixels is again reordered back to their original location in decryption operation. Image encryption is performed by using Henon mapping system to diffuse the correlation between crypto-image and plain-image. The presented encryption Algorithm As mentioned in this work has been tested and analysis on some color images and the results showed a significant security and validity to resistance the statistical and differential attacks

Keywords—*Image shuffling; Arnold cat map; Cryptography; Chaotic theory; Encryption system; Henon Map; Decryption algorithm; Confusion and Diffusion.*

I. INTRODUCTION

With the wide reach of the multimedia data via internet and wireless networks, the secrecy of information during transmission has become an important and central issue especially for digital images. Due to image powerful attribute such as vast data capacity, the great redundancy and great correlation among pixels of image. Digital encryption is one of essential technique to ensure secrecy transmission of images and videos data [1]. The main aim of image encryption system is to convert the image data from readable form to obscured form in an open network so that the plain image is kept protect. Digital image encryption can ubiquitous in diverse set of applications such as military field, archaeological applications, medical imagery, video surveillance, confidential transmission and in daily life styles likes financial records [2]. Among this popular application of multimedia, researchers have been presented many kinds of digital image encryption schemes and all working to keep the content of image from accessing of all unauthorized users. In recent few years, many techniques have been proposed for real time protect of image transmission via Internet and communication networks including image chaotic based system, data processing Based methods, key generation based encryption algorithms, etc. Among those Chaotic system based on confusion and diffusion mechanisms is widely used and superior performance in cryptography system due to their intrinsic features such as Pseudo-randomness behavior, sensitive to initial condition, non-linear dynamic system and unpredictable manners[3]. In this paper a new approach is presented for fast and secure digital image ciphering. Firstly, the proposed system scrambling the position of image pixels by iteration dividing the two dimension image into blocks and rotate each block in clockwise direction with 90^{o} angle to decorrelate the relations between image pixels. Secondly, to increase the secure and more pixels shuffling in suggested encrypted method Arnold cat mapping is a suitable candidate for this object. Finally, the scrambling image is encrypted depend on Henon's chaotic method, the chaotic mapping system is designed to diffusion the relationship among encrypt-image and original-image. The most important clue to be achieved in the proposed algorithms is not to be losing the image data during the decryption process, so that the plain image is rebuild from cipher image in much easier way [4]. The rest of this research is arranged as follows: Section II shows the related works of image encryption. In section III, an image encryption method based on 2D Arnold cat map and Henon chaotic mapping is proposed and discussed also, we discuss the method of scrambling based on both image shuffling and the main attribute of the Arnold cat map. In Sections IV, the security of the new algorithm is assessed via cryptanalysis and experiment results are explained. Finally, Section V involved the conclusion of the paper.

II. RELATED WORK

Image encryption depend on chaotic mapping system problem has been widely studied in the prior works of digital image processing. Actually, various techniques and widespread algorithms have been suggested and implemented in the purpose of building fast and secure image transmission system. In [5], Chen at el. introduced a symmetric gray scale image encryption scheme based on chaotic cat mapping to scramble the position of image pixels. The experimental tests and analysis of proposed algorithm that carry out on various images demonstrating the high level of security and rapidity of the novel image encryption algorithm and also, it suitable for encryption the

real time images through internet and transmission networks. In[6] showed an image encryption technique depend on Arnold cat map with Henon's chaotic system to encrypt image pixel by pixel and to perform the requirement of protect and fast of image transfer via networks. The experimental results and analysis of chaotic system shows that the spreading of gray scale of the cipher image exhibits a pseudo-random manners. In 2011 some researcher performed experimental results showed that this method is more suitable for image encryption application especially for wireless communication [7]. In [4] the suggested system perform diffusion or permutation method on pixel by pixel of image data to move information from original position to a new position and to hide the statistical structure of image while, confusion or substitution method has been done through byte sequence generated by using Henon map. The resulted test showed that the increasing in confusion and diffusion processing will increased the security of proposed encryption method.

III. PROPOSED CRYPTOSYSTEM

Actually, the main aim of image encryption is to provide an easy and inexpensive scheme of encryption and decryption of digital data to all authorized users. Figure (1) below depicts the main algorithm executed in this research and included encryption and decryption process use RGB image of 256*256*3 stored as a three dimensional matrix of pixels.

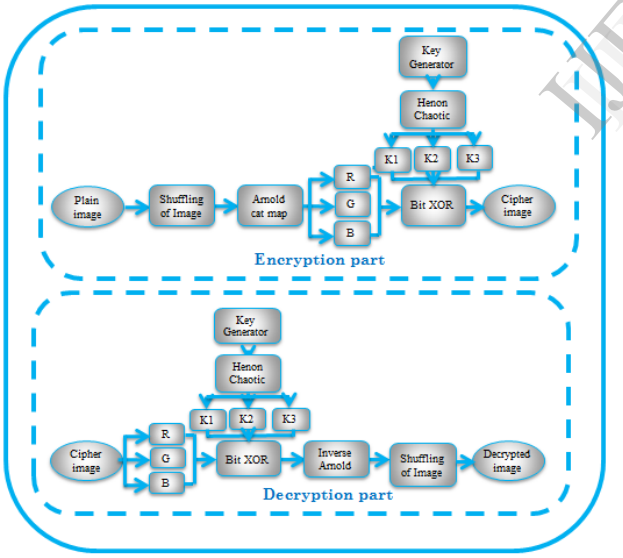


Fig.1. Block diagram of proposed Image encryption scheme

A. *Image Shuffling*

RGB image scrambling is useful to disturb the correlation between the neighboring pixels by changing the position of it and not changes of pixel value so the histogram of image is stable at the beginning of the encryption and the decryption process. Shuffling of image pixels is done in three steps.

First step: Divide image in quadrant and rotate each one with 90 in clockwise direction.
Second step: Divide each quadrant into four sub-quadrants and rotate them with 90 and the result is 16 block of image.

Third step: Divide each block again to four blocks and rotate each one with 90 and the result is 64 blocks of image [4]. An example of image scrambling shown in figure (2).

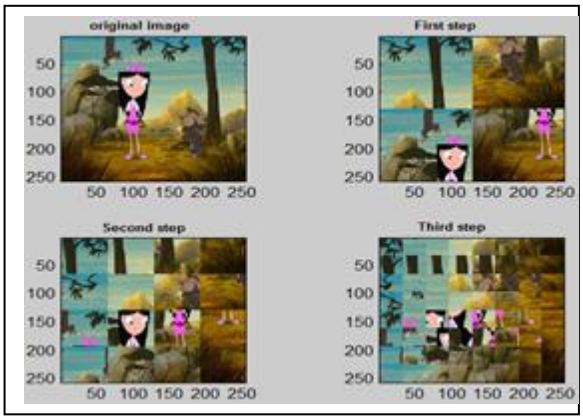


Fig .2 .Example of image shuffling

B. *Arnold Cat Map System*

Arnold's Cat Map transformation use for scrambling the pixels of color image and to perform extra security of cipher system. The 2D Arnolds cat Map does not change the intensity value of the image; it only shuffles the data of image and it given in (1).

$$x' = (x + p * y) mod\ 256$$
$$y' = (q * x + (b * q + 1)y) mod\ 256 \quad (1)$$

Where:

p,q: represents the positive secret keys.
x,y : represents the original location of the image pixel before scrambling.
x',y': represents the new location of the image pixel after scrambling.

After applying 2D Arnold cat transformation for several iterations, the relationship between the neighboring pixels is entirely destroy and the original image seems deformation and meaningless [8]. Actually, for iterating it to many times it will return to original look. this mean that Arnold cat map is a periodic transform. After image shuffling the statistical features are same for encrypt image and original image to increase the security of encryption system. Figure (3) show an example of plain image and shuffled image with iteration of 5 and their Grayscale histogram. Next of confusion process we use Henon Chaotic map System for diffusion and for enhancing the security [9].

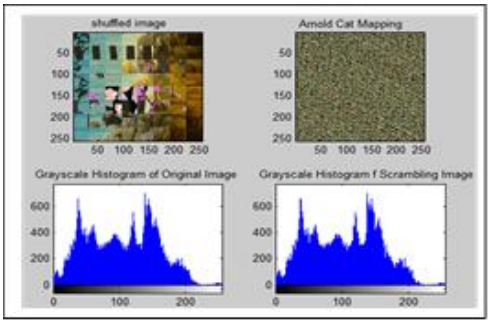


Fig.3. Example Arnold Cat Map

C. Henon Chaotic System

Henon map system regards as the most known and commonly used of dynamical systems that reveal chaotic behavior. Actually, Henon map introduces uniform distribution of pixels of digital image and is a discrete time transform takes initial condition (x0,y0) as a secrete value in 2D real plane and map it to next point by using (2).

$$x_{i+1} = 1 - a\,x^2{}_i + y_i$$
$$y_{i+1} = b x_i \quad i = 1,2,3\ldots \qquad (2)$$

Where:

a,b: represented the control parameters.
x0, y0: represented the initial secrete keys.
xi+1,yi+1: represented the sequence of other keys.

Henon system exhibits chaotic behaviors such as sensitivity property means it dependent to initial secrete key (x0,y0) this cause the system have values of control parameters a,b but slightly differing to initial condition values, and Ergodicity feature means that a large set of identical systems which only vary in their initial conditions will be distributed after adequate discrete time on the attractor accurately the same way as the sequence of iterations of one single system[10].

D. Key Generator

We represent the color image (RGB) with matrix of dimension (256*256*3) where 256 represents both rows and column value of color level. To perform color image encryption we need to Separate RGB matrix of color Image and then convert each component of R,G,B matrix into single array vector of (1*65536) elements. For encryption system we first generate keys sequence by using Henon map of equation (2) with matrix equal to the dimension of (1*196608) elements. There are two secret factors a, b such that a=0.43 and b=1.79 with initial value of x0=0.01 and y0=0.02 represented as a secret keys to generate the next keys. The values of keys sequence lie among interval of [-1 1] Table (1) show some key samples. so we need to convert them to values of interval [1 256] by using (3). Table (2) illustrate some key samples in this interval [11].

$$newkey = (key * 1000)\ mod\ 256 \qquad (3)$$

Table(1) Sample of keys value in [-1 1]

0.0100	1.0199	-0.4532	1.0185	-0.5881
-1.2678	-0.8686	-0.4365	0.4727	0.5562
1.2388	-1.1136	-0.3646	0.4798	0.5684

Table(2) Sample of keys value in [1 256]

10	252	59	250	180
12	155	75	217	44
215	166	147	224	56

E. Encryption of Image

Image encryption performs by diffusion or substitute the shuffled image blocks through changing the value of each component of R, G, and B pixels through exclusive X_OR operation with the sequence key values dedicated for each component[12].

F. Decryption of Encrypted Image

To reconstruct the plain image we follow the reverse process of encryption steps. Because the chaotic system attribute is deterministic therefore, in reconstruction process of original image we use the same sequence key values through exclusive operation with cipher image to give the shuffled image. We can get the rotating image blocks by using inverse of Arnold Mapping which is described in(4).[8]

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}^{-1} * \begin{bmatrix} x' \\ y' \end{bmatrix} \qquad \ldots(4)$$

Then the shuffled image blocks are further rearranged by rotating in counter clockwise with angle of 90o to obtain the original image. figure(4) depicted the test image after decryption, scrambling and restore parts with their grayscale histogram.

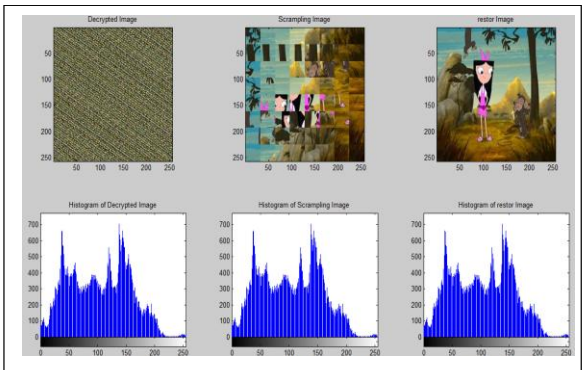


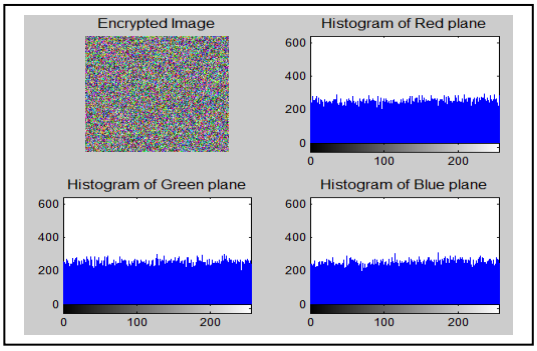
Fig (4) example of decryption part images with grayscale Histogram

IV. EXPERIMENTAL ANALYSIS AND RESULTS

To evaluate the effectiveness of suggested technique, we have performed several of experiments wither in statistical or security analysis including histogram analysis for both plain and encrypted images, Number of Pixels Change Rate (NPCR) to measure the total differences between the cipher images and the original images, unified average changing intensity (UACI), key space with sensitivity analysis and correlation coefficients analysis.

A. *Statistical Analysis*

To test the effectiveness of proposed encryption method and the stability through statistical attacks, the graphics histogram is performed for the whole color components R, G, B of the original image. Figure(5)shows the test image in both encrypted and decrypted parts using the proposed method. From all the figures, it is obviously shows that there is a perceptual difference for graphical representation of all color's channels histogram and fairly uniform distribution of frequencies values imong the plain image and it encrypted image pixels. Therefore histogram criteria can't give any clue to statistical cryptanalysis for breaking the encryption scheme so it is a good method for hide any countenance of the original image[12].



b. cipher image & histogram for colour components

Fig (5) Example of plain and encrypted images with Histogram

It is well known that the correlation coefficient among the neighboring pixels of an encrypted image is a useful measure to evaluate the encryption effectively of any cryptosystem. Any image encryption system regards as good encryption procedure, if it disguise all attributes of a plain and ciphered image pixels are totally random behavior and highly uncorrelated in horizontal, main-diagonal, vertical and anti-diagonal orientation. Three utilities are need to calculate the correlation coefficient these are respectively as the following formulas[13].

$$E(X) = \frac{1}{N}\sum_{i=1}^{256}(x_i) \qquad \ldots(5)$$

$$D(x) = \frac{1}{N}\sum_{i=1}(x_i - E(x))^2 \qquad \ldots(6)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{256}(x_i - E(x))((y_i - E(y)) \qquad \ldots(7)$$

Then for both the plain image and the encrypt image, correlation coefficient of the adjacent pixel variable is calculated using equation (8). The value of CR is near to the one If the Adjusted pixels are closely correlated. On the other side, if the coefficient is close to zero then the pixels are not related.

$$CR_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad \ldots(8)$$

where x and y represent color intensity of two contiguous pixels in the cipher or original image. Tables (3) presents correlation coefficient for both plain and cipher images.

Direction	Original image	Cipher image
Horizontal	0.9616	-0.0071
Vertical	0.9956	0.1304
Diagonal	0.9243	0.0018
Anti-diagonals	0.9296	-0.0011

It is clearly depicts that the correlation coefficient for the cipher image is very small and near to zero value. This demonstrates that the suggested encryption algorithm leads to a more secured encryption.

B. *Security Analysis*

For high secure, encryption algorithm should resist toward most known attacks, very much sensitive to encryption key values, moreover the key space should be large enough to make the brute force attacks infeasible since Randomness is the intrinsic attribute of Henon map. The experimental tests in proposed scheme to the sensitivity of the secret keys involved make a slight change in original secret keys by replace it from xkey(1)=0.01 and ykey(1)=0.02 to xkey(1)= 0.01000001 and ykey(1)= 0.02000001. As a consequence, it was not conceivable to obtain the original image at decrypted part as shown in figure (6).

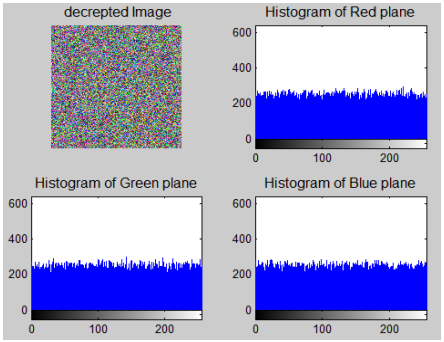


Fig (6) Example of decrypted image with colour planes Histogram

there are two tests to assess the differences between the original image and the decrypted image, the Number of Pixels Change Rate (NPCR) and the Average Changing Intensity (UACI). Equation (8) gives the mathematical equation of the NPCR measure.

$$NPCR = \frac{\sum_{i=1}^{256}\sum_{j=1}^{256} Dif(i,j)}{65536} * 100\% \qquad \ldots(8)$$

$$Dif(i,j) = \begin{cases} 1 & I(i,j) \sim = I'(i,j) \\ 0 & I(i,j) \quad = I'(i,j) \end{cases}$$

Where I(i,j) represent the original image and I'(i,j) represent the encrypted image. NPCR value indicates the different average of the number of pixels of the encrypted image when only one pixel of the original image is adapted. It is obviously that NPCR value should be as big as possible to reach the performance of an ideal digital image encryption scheme and after calculated it using equation 8 for two test images found values of 98.8510 and 98.9014 respectively. While Equation (9) shows the mathematical expression of the UACI measure.

$$UACI = \frac{1}{65536}\left[\sum_{i=1}^{256}\sum_{j=1}^{256}\frac{|I(i,j) - I'(i,j)|}{256}\right] * 100\% \quad ...(9)$$

UACI measures the intensity rate of differences between the original image and ciphered image and after calculated it for tested images found their values are 29.9160, 29.1745 respectively. In general, the NPCR and UACI of the suggested scheme being all close to unity are a good obvious that the encryption image scheme has a highly confidential security[14].

V. CONCLUSION

In this article, a suggested color image ciphering technique depend on 2D Henon like chaotic system is presented. The proposed method used confusion schemes for scrambling the positions of pixels of the colored images in two stages firstly, by dividing the original image to 64 blocks and rotate each one in clockwise with 90o . Secondly, using 2D Arnold Cat mapping to apply more scrambling of blocked image pixels. Shuffling mechanism combined with diffusion mechanism for encrypting the scrambling image by changing the gray values of the image pixels. The suggested cryptosystem scheme employed on any RGB component. The chose channel goes via 2D dimensional Henon chaotic map to produce a sequence of random values that use bit XOR operation with the shuffled pixel value of selected channel to produce the encrypted image and to increase its resistance to all possible type of attacks such as the arithmetical and differential attacks. The experimental results and numerical analysis show that the presented cryptosystem appropriate to provides an effective way for image encryption and achieve more flexible, Reliable, and higher encryption quality.

ACKNOWLEDGMENT

We would like to thank anonymous referees for their constructive comments.

REFERENCES

[1] NOOR.D.S,"Encryption and Decryption Digital Image Using Confusion System", European Academic Research,Vol. I, Issue 11/ February 2014.

[2] W.Puech,"Image Encryption and Compression for Medical Image Security",published in "IPTA'08: 1st International Workshops on Image Processing Theory, Tools and Applications,Tunisie",mar 2009

[3] H. Asadollahi, M.Saberi Kamarposhti, E.Moosavian Jandaghi,"Image Encryption using Cellular Automata and Arnold Cat's map",Australian Journal of Basic and Applied Sciences, 5(8): 587-593, 2011.

[4] N. S. Raghava , A. Kumar,"Image Encryption Using Henon Chaotic Map With Byte Sequence",International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR),Vol. 3, Issue 5, Dec 2013.

[5] G. Chen , Y.Mao , C. K. Chui ,"A symmetric image encryption scheme based on 3D chaotic cat maps",Chaos, Solitons and Fractals 21 ,pages 79–761, Elsevier Ltd 2004.

[6] C.Wei-bin, Z. Xin ,"Image encryption algorithm based on Henon chaotic system",Image Analysis and Signal Processing IEEE xplore,pages 94 - 97,11-12 April 2009.

[7] Manjunath Prasad,K L Sudha,"Chaos Image Encryption using Pixel shuffling",D.C. Wyld, et al. (Eds): CS & IT 02, pp. 169–179,CSCP 2011.

[8] V. Chaturvedi, P. Trivedi, R.K. Pandey," Novel Image Encryption of Color Image based on Henon Chaotic Systems and its Analysis", International Journal of Computer Applications (0975 – 8887) Volume 57– No.14, November 2012.

[9] R.K.yadava, B.K.singh*, S.K.sinha*, K. K.pandey,"A New Approach of Colour Image Encryption Based on Henon like Chaotic Map",Journal of Information Engineering and Applications ,Vol.3, No.6, 2013.

[10] Z. Lv, Lei Zhang, J.Guo,"Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed Dynamics System",ISBN 978-952-5726-07-7 (Print), 978-952-5726-08-4 (CD-ROM)Proceedings of the Second Symposium International Computer Science and Computational Technology(ISCSCT '09) Huangshan, P. R. China, 26-28, pp. 191-194,Dec. 2009.

[11] P.Tian-gong**,** L.Ta-yong**,"** A New Algorithm of Image Encryption Based on 3D Arnold Cat**",** Advanced Engineering Forum Vol. 1,pp 183-187, Sep. 2011.

[12] M. Prasad, K.L.Sudha, "Chaos image encryption using pixel shuffling with henon map", Manjunath Prasad et al./ Elixir Elec. Engg. 38, pp4492-4495, August. 2011.

[13] O.M.Abu Zaid,Nawal A. El-Fishawy,E. M. Nigm,O.S. Faragallah,"A Proposed Encryption Scheme based on Henon Chaotic System (PESH) for Image Security",International Journal of Computer Applications (0975 – 8887)Volume 61– No.5, January 2013.

[14] A.M.Yousif,M.M.Ali," A Selective Image Encryption Based on Chaos Algorithm", Journal of KerbalaUniversity , Vol. 11 No.1 Scientific . 2013