International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Image Encryption Based on Pixel Shuffling with 3D Chaotic System

Asia Mahdi Naser Alzubaidi

Computer Science Department, College of Science, Karbala University, Karbala, Iraq

Abstract: ***In recent years, with the fascinating development of internet technologies and wireless communication networks such as computer and mobile networks. all types of multimedia data such as digital image, Audio, text and video can be reached in easily way over internet. Due to this, cryptographic techniques are required to accomplish a sufficient level of security, integrity, confidentiality as well as, to prevent unauthorized access of important information during data storage and transmission. To meet this challenges, a novel and efficient color image encryption chaos-based scheme has been suggested in order to confuse the relation between adjecent pixels by alter the position of image pixels using block image scrambling by iteratively dividing it to sixteen blocks and rotate each one in to clockwise direction with 90 angle.then, apply 2D Arnold cat map with row_colunm wise methods to make more distortion of the relationship among connected pixels of original image by hide the statistical structure of pixels. The second part of proposed method is to diffuse the relation between plain and encrypted images by change the gray scale value of original image pixels using 3D logistic chaotic function.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 such as frequency analysis attack. Moreover the encrypted images have entropy near to ideal rate and correlation coefficients close to 0 value. the experimental results and numerical analysis demonstrates the security, flexibility, correctness, effectiveness, Reliable and robustness of the proposed cryptosystem.***

Keywords: Row-Column wise; 2D Arnold cat map; Image encryption;Chaotic theory; 3D logistic map.

1. Introduction

Nowdayes, with the rapid development of internet technologies and communication networks,cryptographic techniques are required in order to achieve high level of security and to prevent unauthorized access of sensitive information during storage or transmission over an insecure channels like the Internet. 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[1]. 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 this paper we presented image encryption scheme based on chaotic theory system that combined confusion and diffusion mechanisms due to their intrinsic features such as Pseudo-randomness behavior, sensitive to initial condition, non-linear dynamic system and unpredictable manners which make them very desirable for encryption [3]. The approach use uniform shuffling based block and pixels of image by dividing the plain image in to sixteen blocks and rotate them with clockwise direction.then, appling Arnold cat transform and row wise followed by column wise to disturb the connection between image pixels. Also,the 3D logistic map used to diffusion the relationship among encrypt-image and original-image and consequently the proposed algorithm for encryption became more secure from cryptanalytic attacks[4]. The rest of this research is described as follow: Section 2 shows the related works of image encryption. In section 3, an image encryption scheme based on 3D logistic transform is depicted and discussed in details. In Sections 4, the security of the new algorithm is assessed.

2. Literature Survey

Image encryption based on chaotic mapping problem has been widely studied in the previous works of digital image processing. Actually, various techniques and widespread algorithms have been suggested and implemented in the purpose of constructing fast and secure image transmission or storage system. Rakesh et al. [5] have proposed new method for image security using a corporation of image compression and image encryption mechanisms. the method used image scrambling based row-column and block shuffling using Arnold cat transform then, twice encryption is achieved on the scrambled image based chaotic mapping to make more confidently. The experimental analysis shows that the encrypted image has entropy value near to ideal value and small correlation coefficients. In[6] suggested method for image encryption based confusion and diffusion mechanism and using 3D Logistics Chaotic function to provide more security of system. They found that if doing little change in the initial values of secret keys it will leads to huge change in the encrypted result and decrypted image. Nizam et al. [7] have suggested improved Pixel chaotic shuffling method to encrypt color image by using pixels permute before achieving the column-wise and row-wise scrambling. Many tests have been performed to assess the security of the UACI analysis and information entropy, the proposed algorithm result a high performance over the existing algorithm. Zhang et al. [8] find an efficient image encryption based confusion and diffusion architectures to confuse the relationship among ciphered and original images. Using Arnold cat map to change the position of image pixels in spatial domain then applying Lorenz chaotic function to defuse the image. The experimental analysis demonstrates key space is large enough to resist the

statistical and structural attacks such as brute force and plaintext attacks. moreover, the distribution of gray scale values of encrypted image shows random behavior.

3. Materials And Methods

The aim of this work is to design and implement a novel and highly secure method which is essential for confidentiality and can be applied in real time systems and also to solve the problems of some previous chaotic image encryption schemes. Fig (1) below depicts the main algorithm executed in this paper and included two approaches confusion and diffusion architectures.

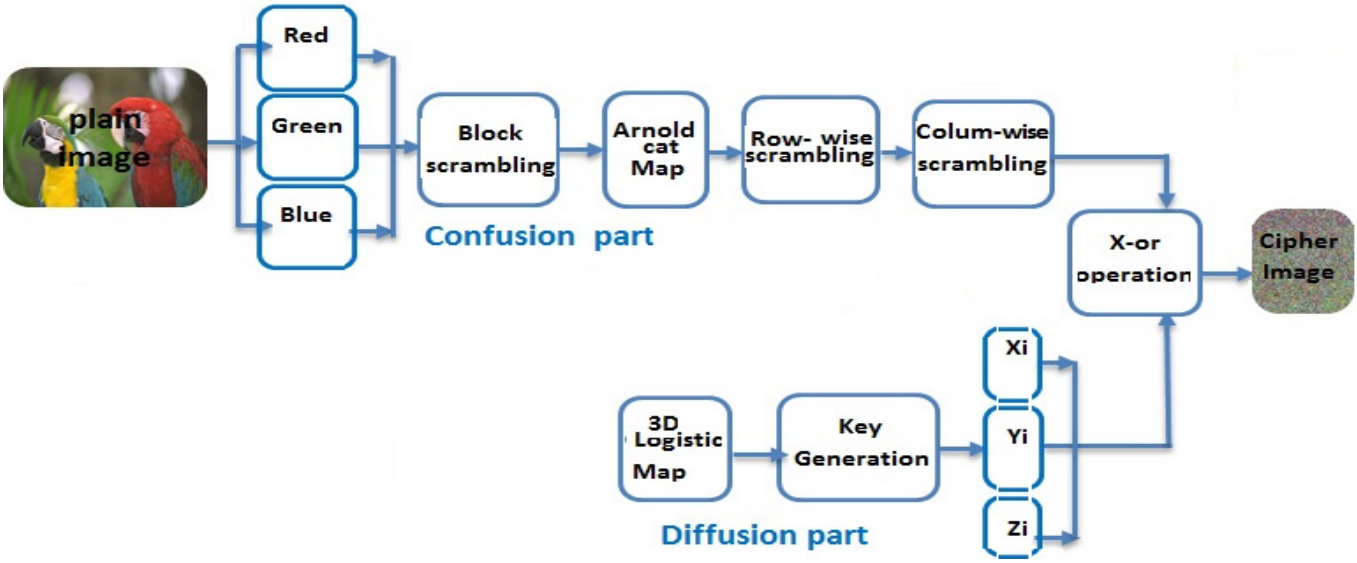


Figure 1: Block diagram of proposed Image encryption scheme

A. Block Scrambling

In encryption method we use RGB image of size 256*256*3 stored as a three dimensional matrix of pixels. block shuffling of image is useful to disturb the correlation between the neighboring pixels of image by changing the position of them so the histogram of image is the same before and after shuffling process. Actually image scrambling doing by two 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 [9].

B. Arnold Cat Map System

Arnold's Cat Map transformation use for shuffling the pixels of color image and to perform extra security of cipher system. The 2D Arnolds cat transform does not alter the gray scale value of the image pixels but it only scramble the image data as shown in equation(1) for image encryption and equation(2) for image decryption.

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & p*q+1 \end{bmatrix} * \begin{bmatrix} X \\ Y \end{bmatrix} \bmod 256 \qquad ...(1)$$

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & p*q+1 \end{bmatrix}^{-1} * \begin{bmatrix} X' \\ Y' \end{bmatrix} \bmod 256 \qquad ...(2)$$

Where:
p,q: represents the positive secret keys.
X,Y : original position of the image pixel before scrambling.
X',Y': new position of the image pixel after scrambling [6].

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 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[10].Figure(2) depict tested images after applying confusion mechanism based Block scrambling and Arnold Cat transform for one time.

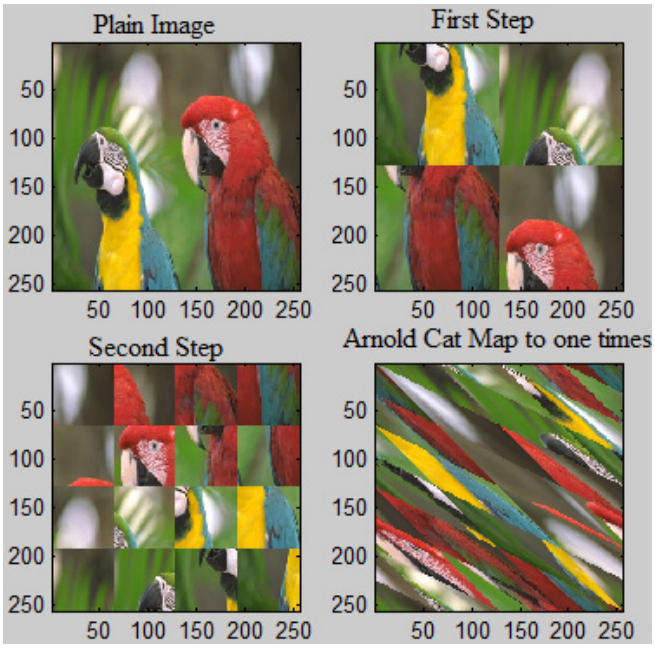


Figure 2: Confusion based Block with Arnold Transform

C. Row- Column Wise Scrambling

Actually, the main aim of image shuffling is to decrease the relationship of adjacent pixels location and gray values until they are unrelated for each other. although the image is scrambled, the pixels of it will remain have same gray values. Therefore, by use information entropy and graphical shape of encrypted image histogram, cryptanalysis can perform statistical and structural attacks which lead to make the system vulnerable. The row wise shuffled image is the movement of a row set to the summation of values on that row and can performs by using equation(3).

$$I'(X, Y) = I((X + R(X)) \mod 256, Y)$$

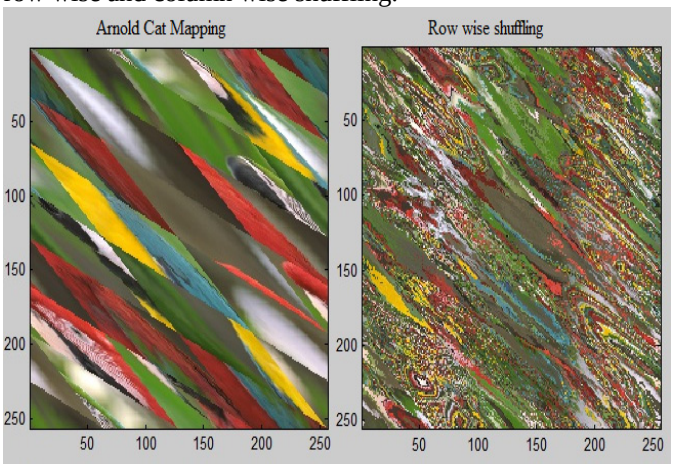
$$R(X) = \sum_{Y=0}^{256} I(X, Y) \quad ...(3)$$

Where:
I(X,Y): the original image coordinate.
I'(X,Y): row wise shuffled image coordinate.
R(X) : summation of all elements in x row of I image.
While, column wise shuffled image is the displacement of a column set to the summation of elements in that column as shown in equation(4).

$$I'(X, Y) = I(X, (Y + C(Y)) \mod 256)$$

$$C(Y) = \sum_{X=0}^{256} I(X, Y) \quad ...(4)$$

Where C(y) is the summation of all values in the Y column[5]. Figure(3) depict one of test images after applying confusion technique based Arnold Cat mapping, row wise and column wise shuffling.



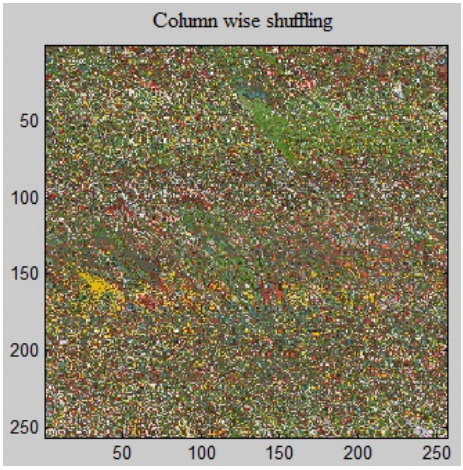


Figure 3: Row - Column wise shuffled Image

D. 3D Logistic Function

In this paper, 3D logistic map have been suggested for diffusion technique to increase the security of encryption method.The 3D Logistic map described in equation(5).

$$X_{i+1} = \lambda X_i(1 - X_i) + \beta Y_i^2 X_i + \alpha Z_i^3$$
$$Y_{i+1} = \lambda Y_i(1 - Y_i) + \beta Z_i^2 Y_i + \alpha X_i^3$$
$$Z_{i+1} = \lambda Z_i(1 - Z_i) + \beta X_i^2 Z_i + \alpha Y_i^3 \quad ...(5)$$

Three quadratic coupling constant factors are presented to strengthen the difficulty and security of 3D Logistic map[6]. The system provide chaotic behavior for $3.53<\lambda<3.81$, $0<\beta<0.022$, $0<\alpha<0.015$ and generate chaotic sequences X,Y and Z in the range [0, 1].

E. Key Generation

We represent the color image (RGB) with matrix of dimension (256*256*3) where 256 represents both rows and column values of image. To achieve chaotic image encryption we need to separate RGB matrix of color Image to their R,G,B components each equal to the dimension of (1*65536) elements. For encryption system we first generate keys sequence by using 3D logistic map that needs three secret factors λ,β,α such λ =3.8414991, β=0.022 and α =0.015 with initial value of x0 = 0.976, y0 = 0.677 and z0 = 0.973 represented as a secret keys to generate the next keys of Xi, Yi and Zi using equation(5). The values of keys sequence lie among interval of [0 1] table (1) show some key samples in this range. so we need to convert them to values in range [1 256] using equation(6) to perform the X_OR operation with the scrambled image. Table (2) illustrates some key samples in this interval.

$$X_i = \text{floor}(10^{14}(X_i) \mod 256) \quad ...(6)$$
$$i = 1,2,3,...,65536$$

Table 1: Sample of key values in [0 1]

0.9760	0.1136	0.3889	0.9158	0.3271
0.8460	0.5129	0.9781	0.0872	0.3212
0.8381	0.5327	0.9748	0.1082	0.3764
0.9171	0.2972	0.8215	0.5649	0.9539
0.1898	0.5946	0.9282	0.2754	0.7724
0.6774	0.8545	0.4909	0.9644	0.1649

Table 2: Sample of key values in [1 256]

0	140	50	19	52
227	104	73	184	221
28	84	184	204	30
40	42	24	153	167
162	70	7	112	7
253	50	235	180	202

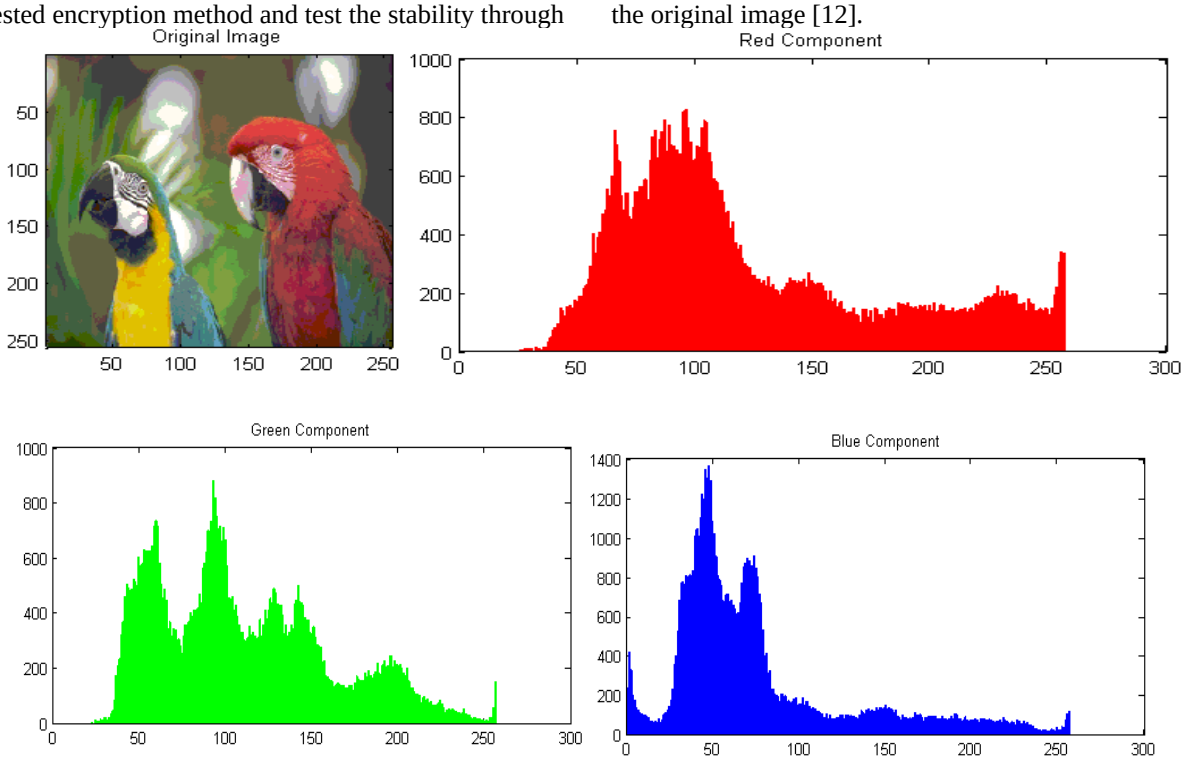
4. Experimental Analysis And Results

A good quality encryption scheme should be robust against all types of attack, involved security attack and statistical attack. the proposed procedure implements in some color images of size 256*256*3 pixels to demonstrate the

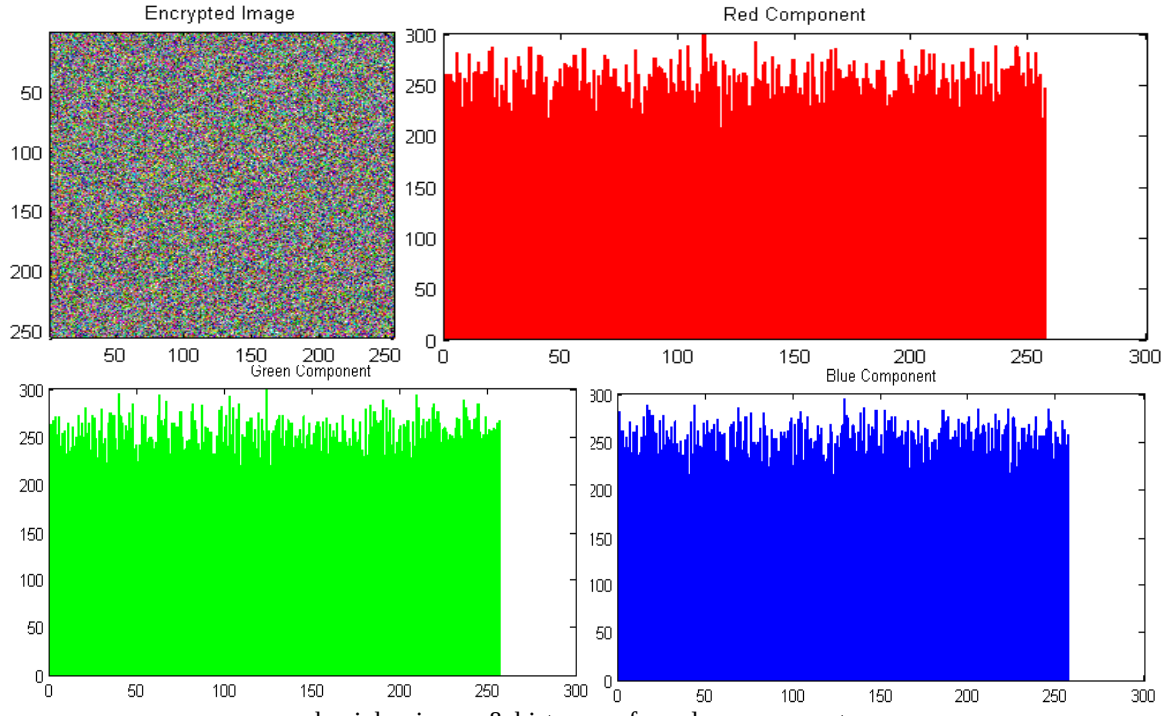
efficiency of presented technique[11]. for instance the graphical shape of histogram of encrypted image must be flat distributed to avoid the statistical attacks, and the key range of key sequences necessity be big enough to evade brute force attacks.

A. Histogram Analysis

Image histogram demonstrates how pixels in an image are distributed so is an effective criterion to assess the efficiency of suggested encryption method and test the stability through statistical attacks. Figure (4) depicts the histograms of Red, Green and Blue components of original and encrypted images. From all figures, it is obviously that there is a perceptual difference in graphical representation of all color's channels histogram and fairly uniform distribution of frequencies values among 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].



a. Plain image & histogram for color components



b. cipher image & histogram for color components

Figure 4: Plain &cipher image with histogram for color components

B. Correlation Analysis

It is well known that the correlation coefficient among the neighboring pixels of an encrypted image is a suitable factor 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[12]. Three utilities are need to calculate the correlation coefficient these are respectively as in formula (7).

$$E(X) = 1/256 \sum_{i=1}^{256} (x_i)$$

$$D(X) = 1/256 \sum_{i=1}^{256} (X_i - E(X))^2$$

$$\text{cov}(X,Y) = 1/256 \sum_{i=1}^{256} (X_i - E(X))((Y_i - E(Y)) \quad ...(7)$$

Then for both plain image and 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 hand, if the coefficient is close to zero then the pixels are not related.

$$CR_{XY} = \text{cov}(X,Y) \Big/ \sqrt{D(X)} * \sqrt{D(Y)} \quad ...(8)$$

where x and y represent color intensity of two contiguous pixels in the cipher or original image. tables (3) and table(4) presents correlation coefficients to plain and cipher images respectively and for five famous images in image processing applications.

Tables 3: correlation coefficient for plain images

Direction / Images	Horizontal	Vertical	Diagonal	Anti-Diagonal
Baboon	0.9459	0.9397	0.9083	0.9062
Lena	0.9717	0.9853	0.9570	0.9686
Pepper	0.9784	0.9824	0.9618	0.9666
Cat	0.9669	0.9680	0.9503	0.9514
Onion	0.9953	0.9959	0.990	0.9928

Tables 4: correlation coefficient for encrypted images

Direction / Images	Horizontal	Vertical	Diagonal	Anti-Diagonal
Baboon	0.0033	-0.0043	0.0037	0.00009
Lena	-0.0020	0.00008	-0.000002	-0.0024
Pepper	0.0025	0.0036	-0.0039	0.00001
Cat	-0.0061	-0.0011	0.0024	0.0033
Onion	-0.0014	0.0027	0.0022	0.0016

C. NPCR and UACI Factors

There are two criteria to assess the differences among the original image and the encrypted image, the Number of Pixels Change Rate (NPCR) and the Average Changing Intensity (UACI). Equation (9) gives the mathematical formula of the NPCR measure.

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

$$\text{Dif} = \begin{cases} 1 & \text{I(i, j) } \sim= \text{I'(i, j)} \\ 0 & \text{I(i, j) } = \text{I'(i, j)} \end{cases} \quad ...(9)$$

Where:
I(i,j) represent the original image
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 plain 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. Equation (10) shows the mathematical expression of the UACI measure.

$$\text{UACI} = \frac{1}{65536}\left[\sum_{i=1}^{256}\sum_{j=1}^{256} \frac{|I(i,j) - I'(i,j)|}{256}\right] * 100\% \quad ...(10)$$

UACI measures the intensity rate of differences between the original image and ciphered image.

Tables 5: NPCR & UACI for original &encryption images

IMAGES	NPCR	UACI
Baboon	0.9962	30.1206
Lena	0.9959	32.9299
Pepper	0.9962	31.8801
Cat	0.9961	34.2639
Onion	0.9964	37.7531

In general, the NPCR and UACI of the suggested scheme being all close to unity and a good obvious that the encryption image scheme has a highly confidential security[11].

D. Information Entropy

It is well known, information entropy is a concept of measuring the degree of randomness in the encryption system. Actually, for any image encryption scheme it should decreases the connect information among encrypted Image pixels and this mean rises the entropy value. also, It must fulfil a rule that the information entropy value for encrypted image should not offer any clue about the plain image. Image entropy is computed by equation(11).

$$\text{entropy} = \sum_{i=1}^{256} P(i) * \log \frac{1}{P(i)} \quad ...(11)$$

where P(i) is the probability of existence of pixel i.
Truly, the ideal entropy value of random system is equal to8.In general, if calculated entropy value is very close to ideal value this mean that the cipher system is protect upon the entropy attack[5].

E. Mean Absolute Error (MAE)

Mean absolute Error (MAE) value is the cumulative squared error between two digital images used to measure how close predictions are to the final results. The larger value of MAE means that the encryption system is more secure upon attacks. Table (6), shows the results of entropy information and MSE for the proposed cryptosystem[5].

Tables 6: MAE & entropy of encryption images

Images	Mae	Entropy
Baboon	114.9195	7.9990
Lena	117.8201	7.9992
Pepper	100.1947	7.9990
Cat	80.4215	7.9991
Onion	81.8736	7.9992

5. Conclusion

In this paper, we presented scheme for image encryption using 3D Chaotic function. The technique involves of scrambling, confusion and diffusion techniques to make it more confident. The experimental analysis and results for proposed system security includes histogram analysis, correlation analysis, mean absolute error, entropy analysis and others. The results show that the graphical shape of histogram for cipher image is uniformly distributed, so the proposed algorithm is protected from frequency analysis attack. information Entropy analysis depicts that the scheme has entropy value that is close to ideal value, so the algorithm is protect from penetrate of image information. Also, the low correlation coefficient of encrypted image is near to the ideal value 0. Thus the experimental results and numerical analysis demonstrates the security, flexibility, correctness, effectiveness, Reliable and robustness of the proposed cryptosystem.

6. Future work

1. It can increase the size of key sequence, so that brute force attack is not easy.
2. Increasing the block shuffling of image can enhance the security of algorithm.
3. The algorithm can be implemented for more image format such as bmp and make comparison.
4. Investigate the capability of proposed image encryption method to resistance some other attacks in both security and statistical analysis.
5. Consider and measure the speed performance for both encryption and decryption parts of the proposed algorithm.

7. Acknowledgment

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

References

[1] A.M.Yousif, M.M.Ali,"A Selective Image Encryption Based on Chaos Algorithm", Journal of KerbalaUniversity , Vol. 11 No.1, p136-p149 Scientific, 2013.
[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] S. Rakesh, Ajitkumar A Kaller, B. C. Shadakshari, B. Annappa,Multilevel Image Encryption,cornell university library,fep-2012.
[6] P.N.Khade, M.Narnaware,"3D Chaotic Functions for Image Encryption", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, N`o 1 p323-p328, May 2012.
[7] O.P.Verma, M.Nizam, M.Ahmad,"Modified Multi-Chaotic Systems that are Based on Pixel Shuffle for Image Encryption",J Inf Process Syst(JIPS), Vol.9, No.2, June 2013.
[8] Z.X.Zhang,T.Cao,"Chaotic-Based Image Encryption Scheme with Confusion -Diffusion Architechure",CSIE,part I,CCIS 152,p258-p263,2011.
[9] 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.
[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 (CDROM) Proceedings of the Second Symposium International Computer Science and Computational Technology(ISCSCT '09) Huangsha, P.R. China, 26-28, pp. 191-194,Dec. 2009.
[11] A.B.Abugharsa,A.S.Basari,H.Almangush,"A New Image Scrambling Approach using Block-Based on Shifted Algorithm",Australian Journal of Basic and Applied Sciences, 7(7): 570-579, 2013.
[12] NOOR.D.S,"Encryption and Decryption Digital Image Using Confusion System", European Academic Research,Vol. I, Issue 11/February 2014.

Author Profile

Asia Mahdi Naser Alzubaidi was awarded her B.Sc, and M.Sc, at University of Babylon, College of Science, Department of Computer Science in 1997 and 2002 respectively. She is an lecturer at Karbala University, Collage of Science, Computer Department. Here research interests include: Computational Geometry and Object Modeling, Image processing such as Segmentation and Steganography , Speech signal processing, Computer Graphics and Data Security.