Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Selective Image Encryption with Diffusion and Confusion Mechanism

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

Abstract— In recent years, With the wide development in communications networks and applied the e-government in most field depending on the internet and its technologies, with the development in the hackers ability to intruder the communication channels. Consequently, cryptographic techniques are required to accomplish a sufficient level of security, integrity, confidentiality as well as, to prevent unauthorized users from accessing of important information during storage, recovery and transmission of data.. In this paper, a novel and efficient selective image encryption scheme has been suggested depending on the diffusion and confusion mechanesim. Color transformation applied to convert from RGB to the YCbCr color space.On Y component a selective encryption algorithm is performed to protect the sensitive data. further the confussion process is adopted by using two dimension Arnold cat transformation to make more distortion of the relationship among adjacent pixels of Y image and to hide the statistical structure of pixels. Scrambling process depend on row_columm method applied independently on Cb and Cr components .Then to diffuse the correlation between crypto-image and plain-image we using 2D Baker on scrambling CbCr channels and Henon Chaotic map on encrypted Y channel . 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. Also the cipherd image has information entropy and correlation coefficients close to ideal value.

Keywords— Image encryption techniques; 2D Arnold cat map; Chaotic theory; selective encryption; 3D logistic map.

I. INTRODUCTION

Resentlly, with the rapid development of internet technologies and communication networks, cryptographic techniques are required in order to accomplish a high level of security, integrity, confidentiality and to prevent unauthorized access of sensitive information during storage or transmission over an insecure channels like the Internet. a real time applications such as medical images, teleconference, video live streaming, satellite images and surveillance camera are obviously require selective encryption methods for secure transmission via networks[1]. Selective digital image encryption technique based on chaotic map is a wonderful and novel method to protect the content of multimedia such as digital image,audio and video. In this approach some of multimedia data remains unencrypted but the effect is that total image pixels are encrypted in order to significant reduction of encrypting and decrypting processing time which is an essential factor in wireless and portable multimedia systems[2]. In this paper we presented image encryption scheme combining selective image encryption with chaotic theory system based on 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 proposed system for fast and secure digital image encryption Firstly involved color transformation from RGB color space to the YCbCr space. selective encryption algorithm applied in Y-component values which in the range [16 235] then to increase the secure and more pixels shuffling in suggested encrypted method Arnold cat mapping is a suitable candidate for this purpuse. Finally, Henon map applied on Y channel to add more difussion of image. while improved 2D Baker transform is essentail for encrypting the scrambling CbCr components separately. The Baker 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 by cryptanalysis and experimental results are explained. Finally, Section 5 involved the conclusion of the paper.

II. LITERATURE SURVEY

Selective Image encryption depend on chaotic mapping system 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 building fast and secure image transmission system. Rodrigues et al. [5] have proposed new approach of selective or partial encryption of human face images based on discrete cosine transform and AES stream cipher use Variable Length Coding(VLC)method of the Huffman’s vector, they found that it can be cipher an image without disturbing the compression rate. Rajinder et.al[6] makes security comparison between full and selective image encryption techniques using fidelity criteria such as correlation, entropy and histogram analysis, they found that selective methods provide great level of protection since they reduced the encryption process time.In 2011Shrivastava proposed an algorithm to encrypte the stream of data based on 2D Arnold's cat transform to shuffle the pixels value by selecting control paramter seperatly to encrypte and decrypte the data of image as well as, the confussion performed by using 2D baker map to generate the sequence of encryption keys. All the expermintal analysis show the effectivness and securityof proposed encryption method [7].

III. Proposed Technique

The aim of this work is to design and implement a novel fast 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. Moreover, image encryption provide an easy and inexpensive scheme of encryption and decryption of digital data to all authorized users. Fig(1) below depicts the main algorithm executed in this paper and included two approaches Selective encryption and Chaotic encryption.

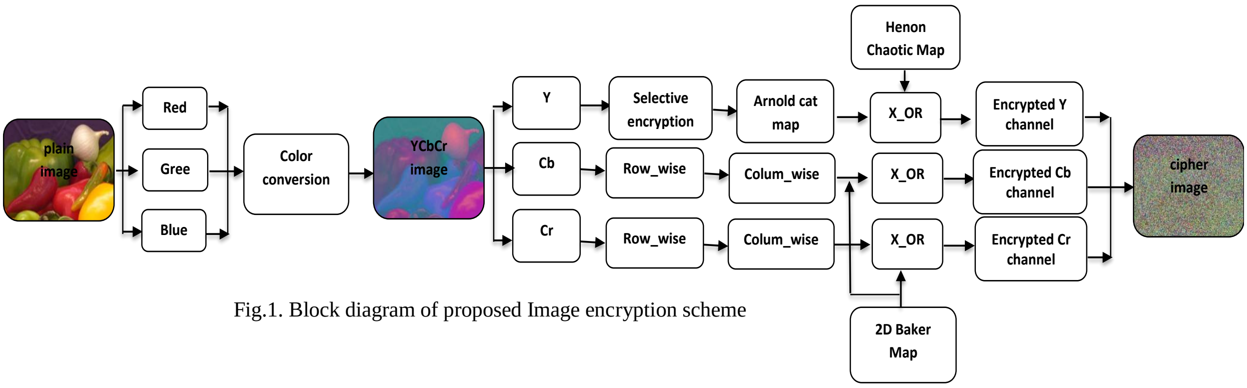


Fig.1. Block diagram of proposed Image encryption scheme

A. Image Conversion

RGB color space is one of best widely used for handling and storing the data of image due to high connection between the red, green and blue components. Actually, RGB color space mixes the chrominance and luminance components so it can't use in color analysis and segmentation methods based on color criteria. While, YCbCr Color model is widely used in processing of video information since it separate between luminance and chrominance components. Y denoted the luma part with values range [0 255] and can be calculating as weighted sum of RGB values. Cb component obtained from the difference between blue and luma component with values range [0 255] and Cr is the difference among red and Y model [8] with values also in range [0 255]. As shown in equation(1) and equation(2).

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.500 \\ 0.500 & -0.410 & -0.081 \end{bmatrix} * \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad ..(1)$$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 1.000 & 0.000 & 1.400 \\ 1.000 & -0.343 & -0.711 \\ 1.000 & 1.765 & 0.000 \end{bmatrix} * \begin{bmatrix} Y \\ Cb-128 \\ Cr-128 \end{bmatrix} \quad ..(2)$$

B. 2D 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; it only shuffles the data of image and it given in equation(3) for image encryption and equation(4) for image decryption.

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & p*q+1 \end{bmatrix} * \begin{bmatrix} X \\ Y \end{bmatrix} \bmod 256 \qquad ...(3)$$

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & p*q+1 \end{bmatrix}^{-1} * \begin{bmatrix} X' \\ Y' \end{bmatrix} \bmod 256 \qquad ...(4)$$

Where:
p,q: represents the positive secret keys.
X,Y : original position of the image pixe before scrambling.
X',Y': new position 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 [9]. 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 (2) show an example of Y component image, selective encryption and shuffled Y image with iteration of 10.

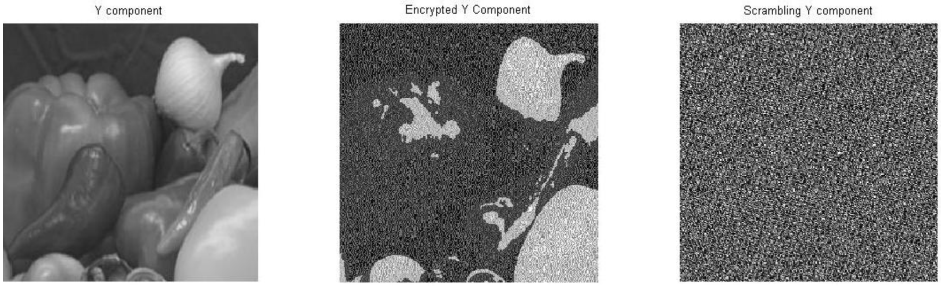


Fig2: Encryption and Scrambling of Y component

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(5).

$$\mathrm{I}'(\mathrm{X},\mathrm{Y}) = \mathrm{I}((\mathrm{X}+\mathrm{R}(\mathrm{X})) \bmod 256, \mathrm{Y})$$

$$\mathrm{R}(\mathrm{X}) = \sum_{Y=0}^{256} I(X,Y) \qquad \ldots(5)$$

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(6).

$$\mathrm{I}'(\mathrm{X},\mathrm{Y}) = \mathrm{I}(\mathrm{X},(\mathrm{Y}+\mathrm{C}(\mathrm{Y})) \bmod 256)$$

$$\mathrm{C}(\mathrm{Y}) = \sum_{X=0}^{256} I(X,Y) \qquad \ldots(6)$$

Where C(y) is the summation of all values in the Y column[10]. Figure(3) shows the effect of this method with Cb channel.

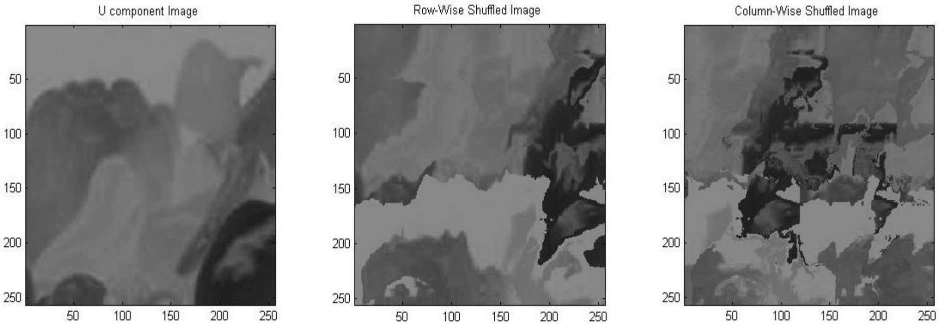


Fig3: Row_columm wise of Cb component

D. Henon Chaotic Map

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 (7).

$$X_{i+1} = 1 - aX_i^2 + Y_i$$

$$Y_{i+1} = bX_i \qquad \ldots(7)$$

Where:
a,b: represented the control parameters such a=0.43 and b=1.79.

x0, y0: represented the initial secrete keys such x0=0.01 and y0=0.02.
xi+1,yi+1: represented the sequence of other keys.
i:in the range[0 256*256].
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[11].

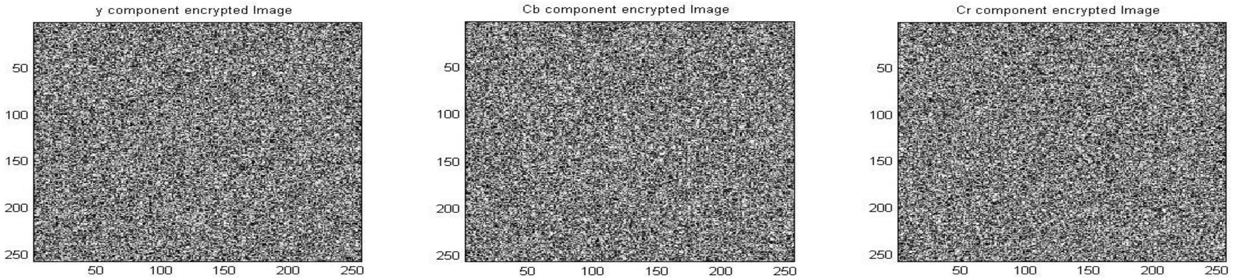
E. Baker Map Based Chaotic System

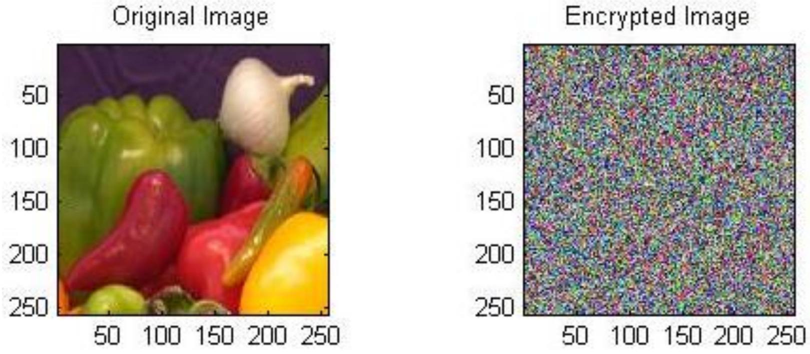
The Baker Map is a concept of chaotic map that discretized, generalized and parameterized of chaotic function to generate the encryption key sequences in cryptography system. Actually, it understood by its effect on the space of functions defined on the unit square, the operation of it comes from dividing the domain of unit square in to halves or thin strips and each two halves are stacked and compressed to each other by vertically compressing the right half of the unit square and converting it to the left half of the unit square simultaneously by extending it horizontally. In general 2D Baker map vertically compresses the first half and stretching it horizontally then puts it along the x-axis. Then it compresses the second strip and places it above the first compressed strip.so it can be used of any number of strip [7]. The baker's map formula in the unit square explain in the equation(7).

$$Ba\ker(X,Y)=\begin{cases}(2X,Y/2) & \text{for } 0\le \mathrm{X}\ge 1/2\\(2-2\mathrm{X},1-\mathrm{Y}/2) & \text{for } 1/2\le \mathrm{X}\ge 1\\ \end{cases} \qquad ...(7)$$

F. Image Encryption Part

Image encryption performs by diffusion or substitute the shuffled image of Y component and scrambling Cb ,Cr components through changing the value of each of Y, Cb, and Cr pixels through exclusive X_OR operation with the sequence key values dedicated for each component[2].figure(4) depict the encryption image for each component of YCbCr image and figure (5) original test image and YCbCr encrypted image.


y component encrypted Image
Cb component encrypted Image
Cr component encrypted Image
50
100
150
200
250
50
100
150
200
250



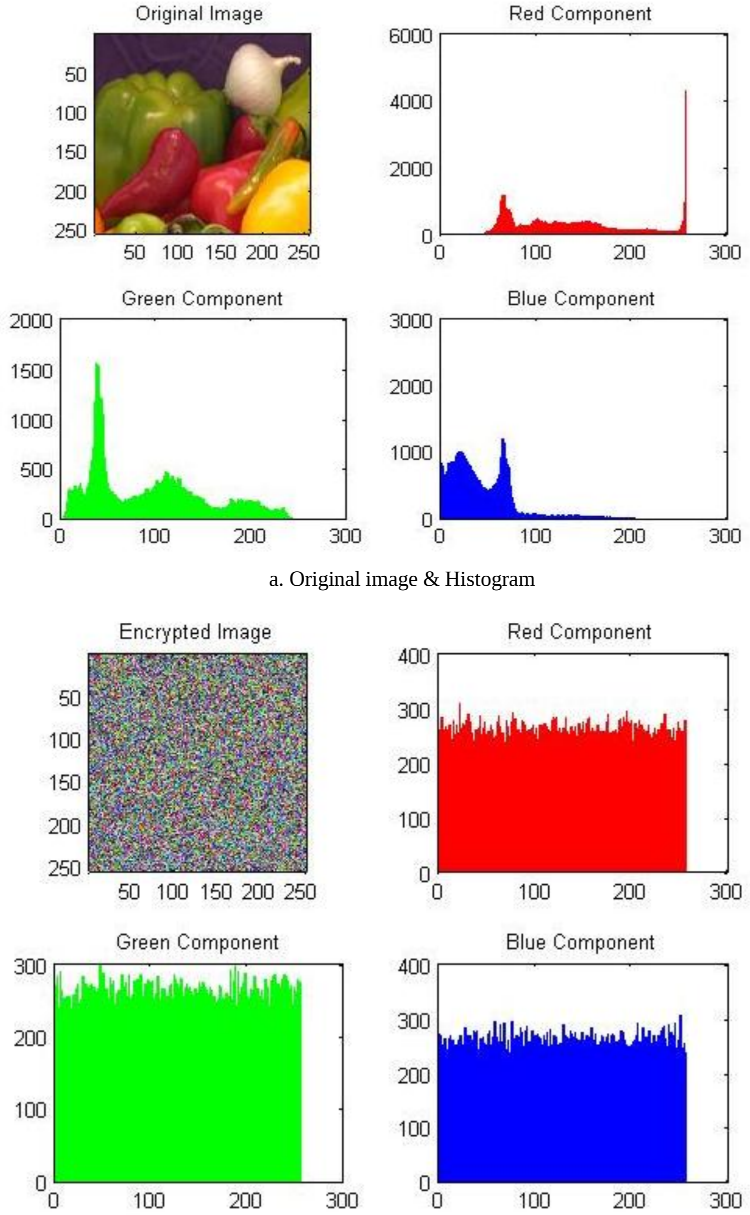
Fig(5)original & YCbCr Image Encryption

IV. Experimental Analysis And Results

To evaluate the efficiency of suggested technique, we have performed several 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), entropy for original and cipher images and correlation coefficients analysis.

A. *Histogram Analysis*

To assess the efficiency of suggested encryption method and test the stability through statistical attacks, the graphics histogram is performed for the R color components of original image. Figure(6)shows the test image and encrypted of Y channel 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 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. Original image & Histogram

b. encrypted image & Histogram

Fig(6) original & cipher Image with Histogram of each panel

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[13]. Three utilities are need to calculate the correlation coefficient these are respectively as in formula(5).

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

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

$$\mathrm{cov}(X,Y) = {}^{1}\!/_{256}\sum_{i=1}^{256}(X_i - E(X))((Y_i - E(Y)) \quad ...(5)$$

Then for both plain image and encrypt image, correlation coefficient of the adjacent pixel variable is calculated using equation (6). 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.

$$CR_{XY} = \operatorname{cov}(X,Y) \Big/ \sqrt{D(X)} * \sqrt{D(Y)} \qquad \text{...(6)}$$

where x and y represent colour intensity of two contiguous pixels in the cipher or original image. figure (7) and (8) presents correlation coefficients to plain and cipher images respectively and for five famous images in image processing applications.

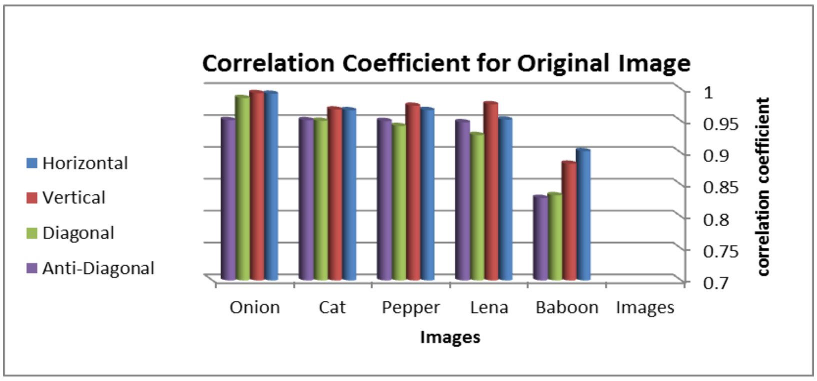


Fig (7) correlation coefficient for plain images

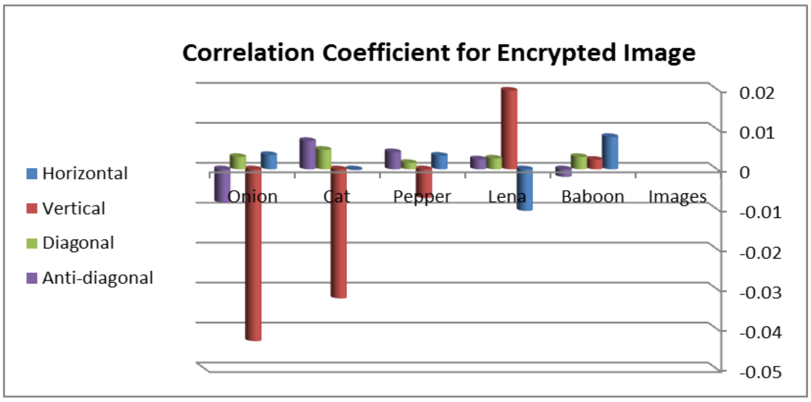


Fig (8) correlation coefficient for encryption images

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

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 (7) gives the mathematical formula of the

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

$$\text{Dif} = \begin{cases} 1 & \text{I(i, j)} \sim= \text{I'(i, j)} \\ 0 & \text{I(i, j)} = \text{I'(i, j)} \end{cases} \qquad \text{...(7)}$$

NPCR measure .

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 (8) shows the mathematical expression of the UACI measure.

$$\text{UACI} = \frac{1}{65536}\left[\sum_{i=1}^{256}\sum_{j=1}^{256}\frac{|I(i,j)-I'(i,j)|}{256}\right]*100\% \quad \text{...(8)}$$

UACI measures the intensity rate of differences between the original image and ciphered image. 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[14].

G. 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 thus mean increases the entropy value. also, It should fulfil a condition that on the information entropy that is the cipher image should not offer any information about the plain image. Image entropy is calculated using equation(9).

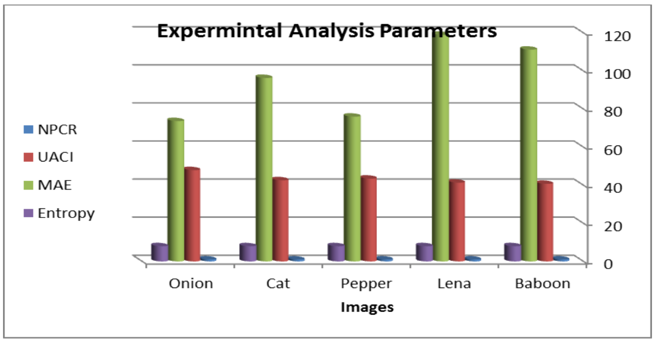
$$\text{entropy} = \sum_{i=1}^{256} P(i) * \log_2 \frac{1}{P(i)} \qquad ...(9)$$

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[15].

H. Mean Absolute Error (MAE)

Mean absolute Error (MAE) value is the a 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. Figure(9) shows the results of entropy information , MSE , NPCR & UACI Factors for the proposed cryptosystem[15].



Fig(9) MAE & Entropy &NPCR & UACI Factors of encryption images

V. CONCLUSION

This article presents the concept of selective encryption technique for Y panel and full encryption Technique for scrambling Y , scrambling Cb and scrambling Cr channels based on chaotic functions. Experimental analysis for proposed system security covers histogram analysis, correlation analysis, mean absolute error, entropy analysis and others. The results show that the graphical shape of cipher image histogram is uniformly distributed, so the proposed algorithm is secure 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.

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] H.T.Panduranga,S.K. Kumar, "Selective image encryption for Medical and Satellite Images", International Journal of Engineering and Technology (IJET), Vol. 5 No.1, p115-p121,Feb-Mar 2013.

[3] S.Liu,2,J.Sun,Z.Xu,"An Improved Image Encryption Algorithm based on Chaotic System", JOURNAL OF COMPUTERS, VOL. 4, NO. 11 p1091-p1100, NOVEMBER 2009.

[4] A.M.Yousif, M.Narnaware,"3D Chaotic Functions for Image Encryption", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1 p323-p328, May 2012.

[5] J.M.Rodriguesa,W. Puecha,A.G.Bors,"SELEC-TIVE ENCRYPTION OF HUMAN SKIN IN JPEG IMAGES", Image Processing, IEEE Xplore,P1981 - p1984,Oct. 2006.

[6] R.Kaur1, Er.K. Singh, "Comparative Analysis and Implementation of Image Encryption Algorithms", International Journal of Computer Science and Mobile Computing(IJCSMC), Vol. 2, Issue. 4, pg.170 – 176, April 2013.

[7] S.Shrivastava," A Novel 2D Cat Map based Fast Data Encryption Scheme", International Journal of Electronics and Communication Engineering,Volume 4, Number 2, pp. 217-223,2011

[8] A.Kaur, B.V. Kranthi, "Comparison between YCbCr Color Space and CIELab Color Space for Skin Color Segmentation" ,International Journal of Applied Information Systems (IJAIS),Volume 3, No.4,p30-p33, July 2012.

[9] C.Pavithra, B.Vinod,"Analization and Comparison of Selective Encryption Algorithms with Full Encryption for Wireless Networks", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 5,p2083-p2088,May 2013.

[10] S. Rakesh, Ajitkumar A Kaller, B. C. Shadakshari, B. Annappa,Multilevel Image Encryption,cornell university library,fep-2012.

[11] 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) Huangshan, P. R. China, 26-28, pp. 191-194,Dec. 2009.

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

[13] 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.

[14] 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.

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

[16] D.M.Torgalkar, N.B.Sambre, "Blowfish Encryption Using Key Secured Block Based Transformation", NTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY(IJESRT) ,Vol.3,No.3,p1774-p1780, march-2014.

[17] Mao YB, Chen G, Lian SG, A novel fast image encryption scheme based on the 3D chaotic baker map. Int. J. Bifurcat Chaos;14(10):3613-24, 2004.