EUROPEAN ACADEMIC RESEARCH
Vol. II, Issue 4/ July 2014

Impact Factor: 3.1 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Selective Image Encryption with 3D Chaotic Map

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. All kinds of multimedia data such as digital image, Audio, text and video can be accessed in easily way over internet. Due to this, cryptographic methods 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. In this paper, a novel and efficient selective image encryption and decryption schemes has been suggested based on 3D logistic chaotic map. 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 confusion 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. Encryption scheme is performed on Y encrypted and scrambling channel with CbCr components by using 3D logistic 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. Also the ciphered image has information entropy close to ideal value and correlation coefficients near to 0 value.

Key words: Image Encryption Techniques; 2D Arnold Cat Map; Chaotic Theory; Selective Encryption; 3D Logistic Map; Confusion and Diffusion.

1. Introduction

Recently, 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(Abeer et al. 2013). 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 (Panduranga et al. 2013). 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 (Shubo et al, 2009). 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 purpose. Finally, improved 3D logistic transform is essential for encrypting the scrambling Y channel with CbCr components separately. The 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 (Pawan et al, 2012).The rest of this research is described as follow: Section 2 and 3 shows the related works of image encryption. In section 4, an image encryption scheme based on 3D logistic transform is depicted and discussed in details. In Sections 5, the security of the new algorithm is assessed by cryptanalysis and experimental results are explained. Finally, Section 6 involved the conclusion of the paper.

2. Background

Today, with the rapid evolution of communication networks and fastening on multimedia information in the digital world, the secrecy of data has become a central issue during transmission via insecure channels. Diverse digital image encryption techniques have been presented to increase the secrecy, integrity, confidentiality of these images. Actually, all image ciphering methods attempt to alter the original image to deformed image that is difficult to understand. On the other hand, image decryption try to reconstruct the plain image from the ciphered one by follow the reverse process of encryption steps.

3. 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,2006).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. (Panduranga et al.2013) describe selective encryption in two methods to secure only selected portion of medical and satellite images, the first way is very useful if the selected portion of image is known while the second encryption scheme is suitable when region of interest is found in image.(Rajinder et al,2013)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. (Abeer et al. 2013)In this research, a novel image encryption method based on 3D chaotic algorithm execute the diffusion and confusion operations. The experimental analysis show that the presented scheme provide high security level, they resistance to different types of attacks such as force attack, chosen-cipher text attacks and differential attack with encryption ratio equal to (6.25 %) and well-matched with compression process.

4. 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.

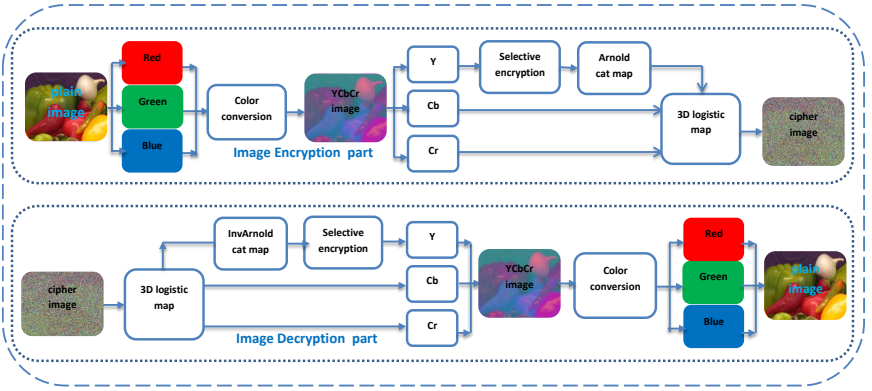

Figure (1) Block diagram of proposed Image encryption scheme

The block diagram of proposed method involved steps are:

4-1 Color 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 [16 235] and can be calculating as weighted sum of RGB values. Cb component obtained from the difference between blue and luma component with values range [16 240] and Cr is the difference among red and Y model (Amanpreet et al, 2012) with values also in range [16 240]. As shown in equation (1) and equation (2). Figure (2) show example of color conversion.

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 0.257 & 0.504 & 0.098 \\ -0.148 & -0.291 & 0.439 \\ 0.439 & -0.368 & -0.071 \end{bmatrix} * \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad ..(1)$$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 1.164 & 0.000 & 1.596 \\ 1.164 & -0.392 & -0.813 \\ 1.164 & 2.0017 & 0.000 \end{bmatrix} * \begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} \quad ..(2)$$

Figure (2) example of color conversion

4-2 Selective Image Encryption Based Chaos map

Selective image encryption approach based on chaotic function is a wonderful technique for image encryption can ubiquitous various set of real-time applications where privacy is essential issue (Lahieb et al 2013).The main objective of selective encryption techniques is to reduce the overhead involved in transmission of digital data via secure channels and to enhance the efficiency of the network with the help of Chaos based key Generation due to their powerful features such as Pseudo-random behavior, sensitive to initial condition, and ergodicity, non-linear dynamic system (Pavithra et al 2013) In this paper 3D logistic map have been suggested for diffusion technique to increase the security of encryption technique. The three-dimensional Logistic map is described in equation(3).

$$
\begin{aligned}
X_{i+1} &= \lambda X_i(1-X_i) + \beta Y_i^2 X_i + \alpha Z_i^3 \\
Y_{i+1} &= \lambda Y_i(1-Y_i) + \beta Z_i^2 Y_i + \alpha X_i^3 \\
Z_{i+1} &= \lambda Z_i(1-Z_i) + \beta X_i^2 Z_i + \alpha Y_i^3 \qquad \ldots(3)
\end{aligned}
$$

Three quadratic coupling constant factors are presented to strengthen the difficulty and security of 3D Logistic map[4]. 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 in the range [0, 1].

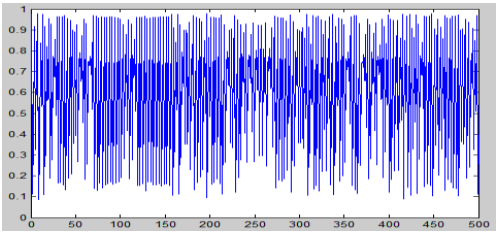

Figure 3: Plot of X component of 3D logistic map

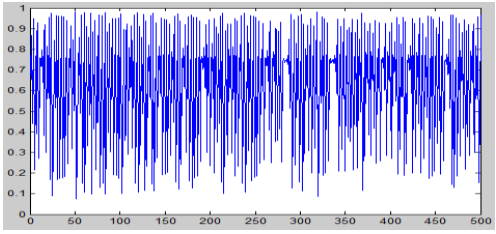

Figure (4) Plot of Y component of 3D logistic map.

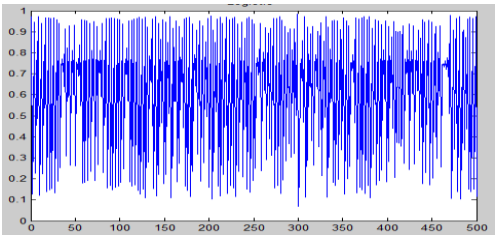

Figure (5) Plot of Z component of 3D logistic map

4-3: 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 (4) for image encryption and equation(5) for image decryption.

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

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} 1 & \mathrm{p} \\ \mathrm{q} & \mathrm{p}*\mathrm{q}+1 \end{bmatrix}^{-1} * \begin{bmatrix} \mathrm{X}' \\ Y' \end{bmatrix} \bmod 256 \qquad \ldots(5)$$

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 (Vikas et al, 2012) Actually, for iterating it to many times it will return to original look. This means 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 (6) show an example of Y component image, selective encryption and shuffled Y image with iteration of 2. Next of confusion process we use 3D logistic map System for diffusion and for enhancing the security (Ramesh et al, 2013).

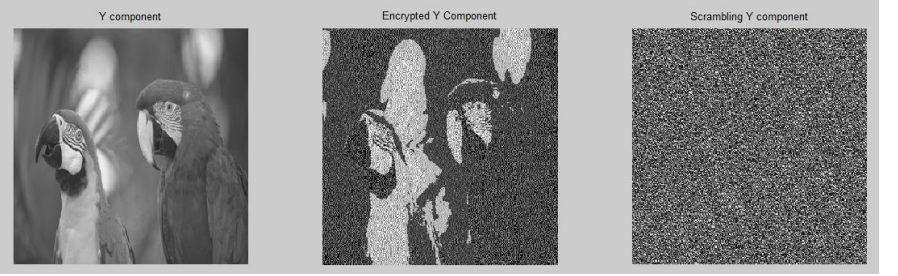

Figure (6) Encryption and Scrambling of Y component

4-4 Key Generator

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 selective image encryption we need to perform color transformation by Separate RGB matrix of color Image to R,G,B components and then convert them to YCbCr model using (1). the results would be three matrices each equal to the dimension of (1*65536) elements. To generate keys to achieve diffusion process we use 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. The values of keys sequence lie among interval of [0 1] table (1) show some key samples. so we need to convert them to values of interval [1 256] to perform the X_OR operation by using (6). table (2) illustrate some key samples in this interval.

$$X_i = \text{floor}(X_i * 256.0) \quad \ldots(6)$$
$$i = 1,2,3,\ldots,65536$$

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

249	29	99	234	83
216	131	250	22	82
214	136	249	27	96
234	76	210	144	244
48	152	237	70	197
173	218	125	246	42

4-5 Image Encryption

Image encryption performs by diffusion or substitute the shuffled image of Y component and 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(Manjunath et al 2011)figure(7) depict the encryption image for each components of YCbCr image.

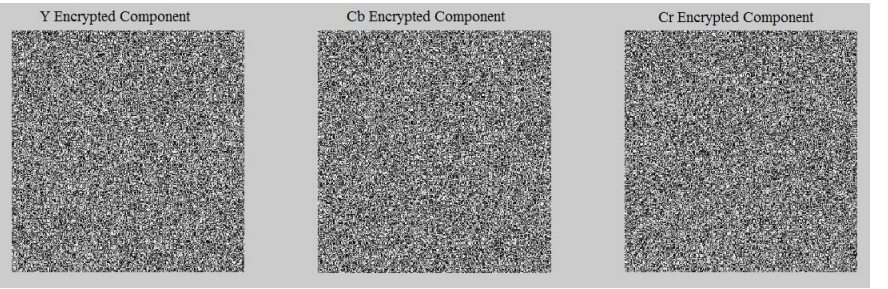

Figure (7) YCbCr Encrypted Components

5. 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.

5-1 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(8)shows the test image with R, G and B histogram while figure(9) depict the encrypted image with components histogram 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 (Manjunath et al 2011).

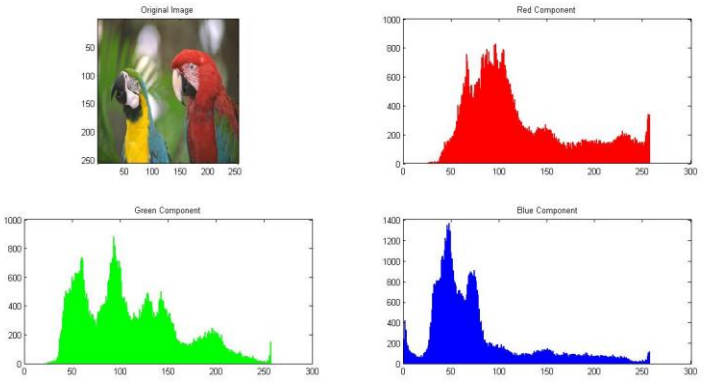

Figure (8) Original Image with Components Histogram

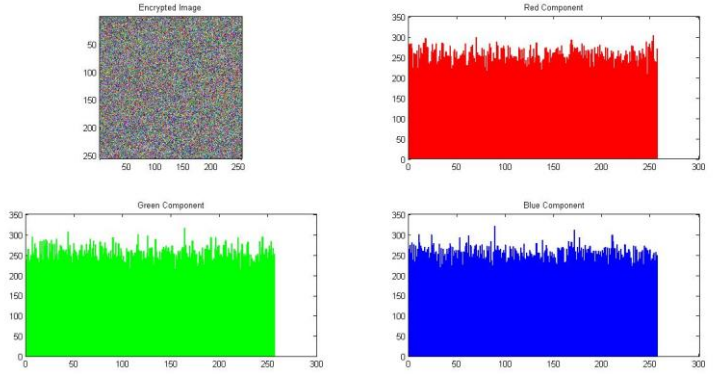

Figure (9) Encrypted Image with Components Histogram

5-2 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(Osama et al,2013)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.

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

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

Table (3) correlation coefficient for plain images

Direction / Images	Horizontal	Vertical	Diagonal	Anti-Diagonal
Baboon	0.9027	0.8830	0.8335	0.8293
Lena	0.9522	0.9763	0.9280	0.9480
Pepper	0.9672	0.9739	0.9422	0.9500
Cat	0.9669	0.9680	0.9503	0.9513
Onion	0.9928	0.9937	0.9861	0.9514

Tables (4) correlation coefficient for Encrpted images

Direction / Images	Horizontal	Vertical	Diagonal	Anti-Diagonal
Baboon	0.0081	0.0024	0.0031	-0.0019
Lena	-0.0104	0.0197	0.0027	0.0025
Pepper	0.0034	-0.0072	0.0016	0.0043
Cat	-.00021	-0.0323	0.0049	0.0071
Onion	0.0036	-0.0430	0.0031	-0.0083

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.

5-3 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.

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

$$\mathbf{Dif} = \begin{cases} \mathbf{1} & \mathbf{I(i,j) \sim= I'(i,j)} \\ \mathbf{0} & \mathbf{I(i,j) = I'(i,j)} \end{cases} \qquad \ldots(9)$$

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.

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

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

Tables (5)NPCR & UACI for original

Images	NPCR	UACI
Baboon	0.9974	40.7375
Lena	0.9975	41.3395
Pepper	0.9945	43.4811
Cat	0.9945	42.6224
Onion	0.9908	47.9474

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(Abeer et al 2013).

5-4 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 decrease 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 (11).

$$\text{entropy} = \sum_{i=1}^{256} P(i) * \log_2 \frac{1}{P(i)} \qquad ...(11)$$

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 (Dhanashri et al,2014).

5-5 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.

Table(6), shows the results of entropy information and MSE for the proposed cryptosystem(Dhanashri et al,2014).

Tables (6) MAE & entropy of encryption

Images	MAE	Entropy
Baboon	111.1948	7.9824
Lena	118.9794	7.9788
Pepper	76.0246	7.9769
Cat	96.3513	7.9797
Onion	73.6917	7.9859

6. Conclusion

This article presents the concept of selective encryption technique for Y panel and full encryption Technique for scrambling Y ,Cb and Cr channels based on 3D logistic chaotic function. All steps of encryption and decryption system were simulated using MATLAB. 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.

BIBLIOGRAPHY:

Abeer, M.Y. and M. M. Ali. 2013. "A Selective Image Encryption Based on Chaos Algorithm." *Journal of Karbala University* 11(1): 136-149.

Amanpreet, K. and B.V. Kranthi. 2012. "Comparison between YCbCr Color Space and CIELab Color Space for Skin Color Segmentation." *International Journal of Applied Information Systems (IJAIS)* 3(4): 30-33.

Dhanashri, M.T. and N.B. Sambre. 2014. "Blowfish Encryption Using Key Secured Block Based Transformation." *International Journal of Engineering Sciences & Research Technology* (IJESRT) 3(3): 1774-1780.

Lahieb, M.J. and G. B. Sulong. 2013. "A Review of Color Image Encryption Techniques." *International Journal of Computer Science (IJCSI)* 10(6.1): 266-p275.

Manjunath, P. and K. L. Sudha. 2011. "Chaos image encryption using pixel shuffling with henon map." *Elixir Elec. Engg*. 38: 4492-4495.

Osama, M. A., N. A. El-Fishawy, E. M. Nigm, and O.S. Faragallah. 2013. "A Proposed Encryption Scheme based on Henon Chaotic System (PESH) for Image Security." *International Journal of Computer Applications* 61(5).

Panduranga, H. T. and S.K. Kumar. 2013. "Selective image encryption for Medical and Satellite Images." *International Journal of Engineering and Technology (IJET)* 5(1): 115-p121.

Pavithra, C. and B. Vinod. 2013. "Analization and Comparison of Selective Encryption Algorithms with Full Encryption for Wireless Networks." *International Journal of Engineering Trends and Technology (IJETT)* 4(5): 2083-2088.

Pawan, N.K. and M. Narnaware. 2012. "3D Chaotic Functions for Image Encryption." *IJCSI International Journal of Computer Science Issues* 9(3.1): 323-328.

Rajinder, K. and E.K. Singh. 2013. "Comparative Analysis and Implementation of Image Encryption Algorithms." *International Journal of Computer Science and Mobile Computing (IJCSMC)* 2(4): 170 – 176.

Ramesh, K.Y, B. K. Singh, S.K. Sinha, and K. K. Pandey. 2013. "A New Approach of Color Image Encryption Based on Henon like Chaotic Map." *Journal of Information Engineering and Applications* 3(6).

Rodrigues, J.M., W. Puecha, and A. G. Bors. 2006. "Selective Encryption of Human Skin in Jpeg Images." *Image Processing, IEEE Xplore* 1981 - 1984.

Shubo, L., J. Sun, and Z. Xu. 2009. "An Improved Image Encryption Algorithm based on Chaotic System." *Journal of Computers* 4(11): 1091-1100.

Vikas, C., P. Trivedi, and R.K. Pandey. 2012. "Novel Image Encryption of Color Image based on Henon Chaotic Systems and its Analysis." *International Journal of Computer Applications* 57(14).