QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

Image Encryption Based on Partitioning and Rearranged Pixels Position

Dr. Jamila H. Al-A'meri
Computer Science Dept., College of Science, AL-Mustansiriyah University - Iraq
Dr.jameelahharbi@uomustansiriyah.edu.iq
Salah T. Allawi
Computer Science Dept., College of Science, AL-Mustansiriyah University – Iraq
Salahta1970@gmail.com
May M. Abbas
Ministry of Higher Education and Scientific Research, Legal and Administrative Directorate – Iraq
May.M.Altaie@gmail.com

ARTICLE INFO

Article History:
Received: 9 March 2017
Accepted: 1 April 2017
Published: 10 April 2017
DOI:
10.25212/lfu.qzj.2.2.31

Keywords:
Data protection,
Image encryption,
Image Decryption,
Random number ,
LFSR.

ABSTRACT

Protect important information transmitted via the channels of communication it's one of the important area. Today, especially with the increasing use of the Internet in the process of transferring this information you had to find ways to protect this information for fear of being captured by unauthorized people to look at it. The image and what it contains is one of the fore mentioned knowledge that should be protected. In our paper a new method is suggested for protecting information of colored image by rearranging the distribution of image pixels. This way depends on the image partition into four equal parts where each data stored in a 1-D array, then the data of these parts are re-arranged through random numbers generated by using LFSR to produce a new (2-D) array combines the data of the four-part. Finally, the new array is converted to another color space YCbCR and the result will be representing the stego image.

1. INTRODUCTION

Internet is used to get quicker transmission of large amount of essential and important data, because internet contains numeral points of attack, it faces a large number of attacking types, to avoid unauthorized access this information should be protected, thus many data protection methods like (Encryption, Watermarking, Masking Data, etc.) are done[1]. Protecting digital images has become very important because of the Internet fastness in the digital world at this time. Protection of digital images drawn a lot of interest nowadays, and several image encryption techniques suggested to make better safety of images [2]. Where nobody can read encrypted text without decrypting. The changing method of the modified data into its native plaintext is defined Decryption, for it can be read easily [3]. Algorithm of encryption image is divided into three groups [4]:

1- Visual transformation based algorithm,
2- Position permutation based algorithm,
3- Value transformation based algorithm.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

This paper consists of the following parts:

Part 1- Provide general information about the subject of image encryption.

Part 2- View previous research that has been done within this topic.

Part 3- Review the way it has been used in this research.

Part 4- Explain some of the points that have been got out from work.

2. LITERATURE SURVEY

M. A. B. Younes and A. Jantan [5]. Proposed Blowfish forward algorithm depending on the Selection and choosing of image transformation and a well-defined encryption and decryption. In their algorithm is divided main image into groups that reconstructed into a changed image. Blowfish algorithm is used to encrypt transformed image. The correlation was decreased between image elements by using the suggested method.

Y. Rajput and A, K. Gulve [6]. are suggested method to make better a secure image can be obtain from the scheme encrypt. The suggested method is classified into 3 steps. Firstly, the single digit number from the original image calculated if it can be partitioned. Secondly, bit rotation, reversal & for each block of the image is done. Thirdly, the extended hill cipher method is used upon an output of second step. The receiver can be generating the original image if he has suitable decryption key.

A. Gupta, N. Tiwari, M. Chawla and M. Shandilya [7], are introduce image encryption methods which gather the idea of block based on pixel treatment and transformation. The suggested technique contains two phases:

1- Block based matrix transformation for pixel place treatment was applied.

2- Applying a bit moving method which alters the data of every pixel.

S. P. Nichat and S. S. Sikchi [8], are introduced a hybrid model for image encryption gathers chaotic function and genetic algorithm. Their technique is contains two phases:

1- Secure images is built using chaotic function and secret key.

2- Using the result images as seed value for genetic algorithm.

In their suggested way used genetic algorithm to have a better result. The best cipher image is chosen on finding the correlation entropy and coefficient. Also the best cipher image in case of having highest entropy and lowest correlation coefficient.

3. Proposed Method

The proposed Image Encryption Based on Partitioning and Rearranged Pixels Position (IEBPRPP) method is suggested to protect information of colored image by rearranging the distribution of image pixels. The framework of IEBPRPP method is classified into two parts; image encryption and image decryption as it will be shown below:

A- Encryption Part

The IEBPRPP method is illustrated in Fig.1. First step includes entering cover image (RGB) used in the IEBPRPP method. Second step: partitioning the cover image into four equal parts, and then converting the pixels value of each part into new 1-D array.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

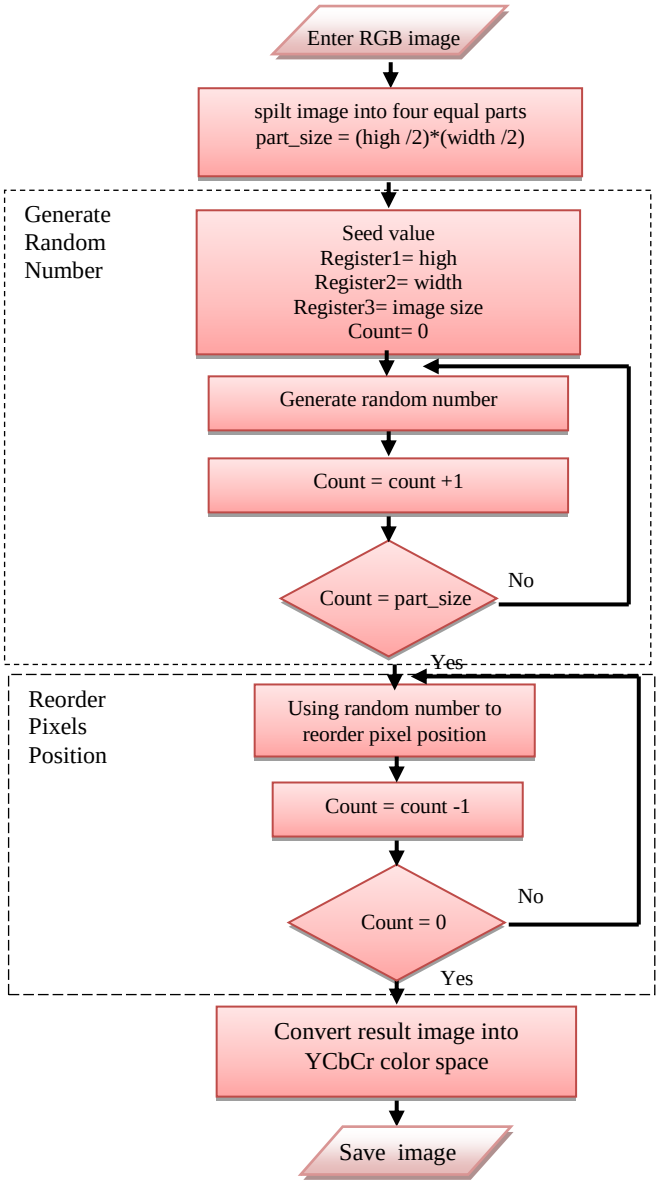


FIGURE1. Proposed method outline (Encryption Stage)

Third step, is generate a set of random numbers by using LFSR. The length of sequence bits that will be generated by using LFSR and then convert it to random number depending on the size of any part of cover image (part image =(high/2)*(width/2)) therefore this length will be changed with each cover image that has a new size. LFSR consists of three registers that have different primary lengths (29, 31, 37) respectively with different connecting function. Initial values of registers based on the original image (height, width and size of image). These numbers are stored in a new 1-D array where the size is equal to any part of sub square partition see Fig.2.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

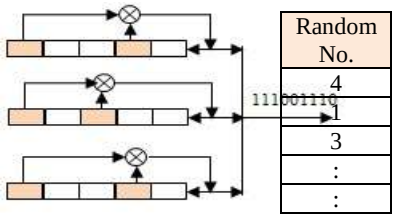


FIGURE 2. Generate random number

Each number indicates the pixel location that will be called from the four respectively to be rearranged in a new array, whose size is equal to the size of the main image see fig. 3. Fourth step, after the rearrangement of all the pixels complete the result image will be converting to another color space (YCbCr) and then the result represent encrypted image.

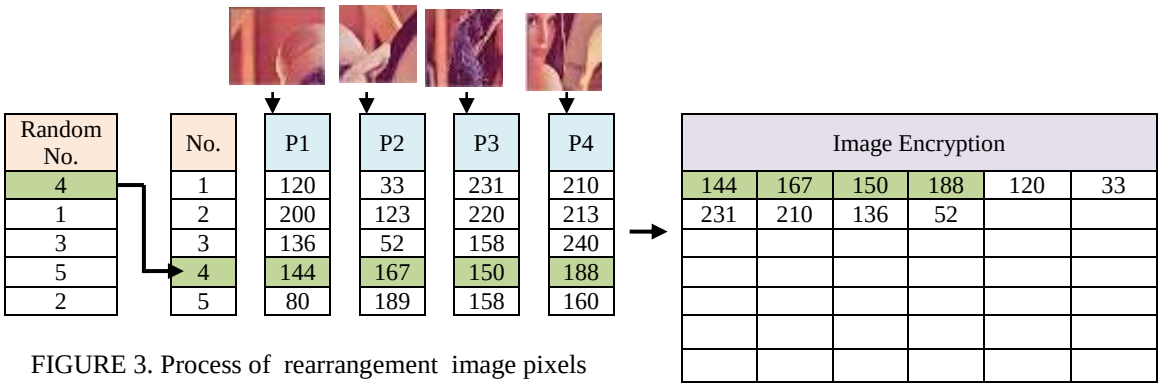


FIGURE 3. Process of rearrangement image pixels

The algorithm is illustrating the main steps of encryption image:

1. Enter color Image (RGB).
2. Partitioning the image into four equal parts.
3. Constructing four 1-D arrays to store pixels value of the parts.
4. Generating random numbers by using LFSRs.
5. Depending on the random number, reordering pixels position for all parts.
6. Constructing a new 2-D array to store pixels value after reordering (encrypted image).
7. Convert the encrypted image into another color space YCbCr.
8. Save the Image encrypted.

B- Decryption Part

Decryption part of IEBPRPP method is consists of four steps: First step: input the encrypted image (YCbCr). Second step: conversion the encrypted image from YCbCR to RGB color space. Third step: constructing 2-D array to store the pixels value of encrypted image. Fourth step: using the same initial values in encryption side to produce random numbers. Then reconstructing four equal arrays their sizes are equal to quarter part of the whole image. Relying upon the random numbers, the pixels are rearranged into their original positions in the four arrays. Finally the image has been reconstructed from the four parts that were obtained, see fig.4.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

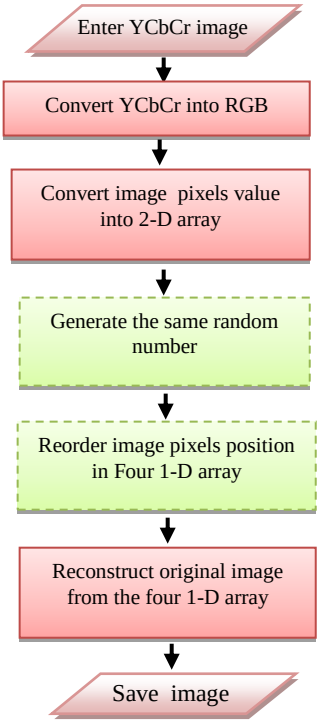


FIGURE4. Proposed method outline (Decryption Stage)

The algorithm is illustrating the main steps of decryption image:

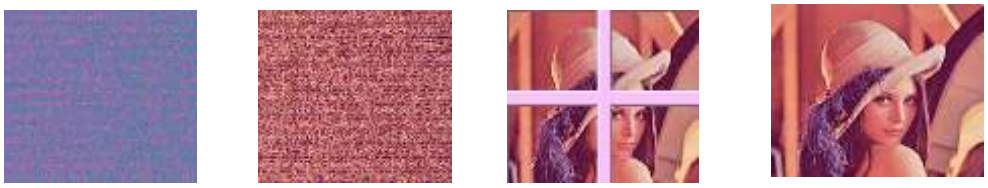
1. Entering encrypted image (YCbCr).
2. Convert image from (YCbCr) into RGB
3. Constructing new 2-D arrays to store all the pixel values of the encrypted image.
4. Generating the same random numbers by using LFSRs
5. Using the random number to getting back the data of the four 1-D arrays.
6. Reconstructing the original image from the four 1-D arrays.
7. Save the result image.

4. Experimental Results

The proposed method is implemented on color images. Figs. (5 and 6) are illustrated the result of IEBPRPP method (encrypted and decrypted). The result of the images are analyzed the performance by using some types of visual observation.

Figure 5. Encrypted image

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)



a) stego image b) Encrypted image c) reconstruct image d) original image

Figure 6. Decrypted image

4.1. Number of Pixel Change Rate (NPCR):

NPCR is known as the different value of pixels of original and encrypted images. By regarding two images P(i, j) and C(i, j), an array X(i, j) means X(i, j) = 0, if P(i, j) = C(i, j), else X(i, j) = 1. If the output is equal to zero both images are same otherwise equal to one [9]. The value of NPCR is calculated by using the mathematical methods found in the eq. 1.

$$NPCR = \left(\frac{\sum i,j\ X(i,j)}{H * W} \right) * 100\% \qquad (1)$$

Where: W and H are the image width and height.
Encrypted and original images gave NPCR value as shown in table 1. Through applying the proposed method it is clear that the obtained NPCR values are different from one image to another.

TABLE1. Showing the difference of NPCR value

Encryption method	NPCR Value %
Suggest method	100
R. Venkatesan [9]	99.5468
K.Bhoopathy Bagan [10]	98.4754
Jean-Yves Chouinard [11]	99.5850
C.W. Liao [12]	99.5400

4.2. Unified Average Changing Intensity (UACI)

The (UACI) shows the rate of intensity variation of original and encrypted images. NPCR focuses on the unlimited value of pixels that alters rate in different attacks, as the UACI optimal value UACI is around 33% [9]. The UACI is computed by using the eq. 2.

$$UACI = \frac{1}{W * H}\left[\sum_{i,j} \frac{P(i,j) - C(i,j)}{255}\right] 100\% \qquad (2)$$

Where: p(i,j) and c(i,j) are two images.
H and W the height and width of the images.
Table2 shows The UACI value of the encrypted and main images and a compares with the ways which are already found.

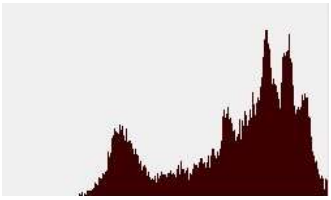
QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

TABLE2. The comparison value of UACI

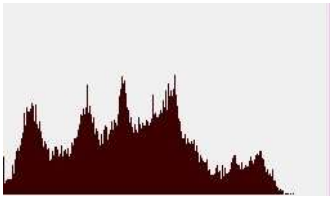
Encryption method	UACI Value %
Suggest method	24.3333
R. Venkatesan [9]	28.8065
K.Bhoopathy Bagan [10]	32.2128
Jean-Yves Chouinard [11]	28.6210
C.W. Liao [12]	28.2700

4.3. Histogram Analysis

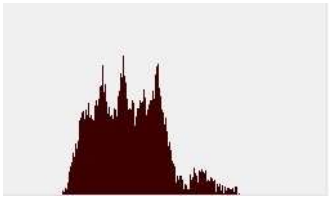
Graphical show of the many times of pixels in an image likes a function of their intensity values which is known histogram image. The degree for the variation of inspecting between encrypted and main images visually at pixel level is done by Image histogram is a. Fig 7 shows The histogram of the result of process image encrypted fig.5.



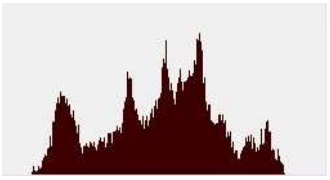
A- Red color before encrypted



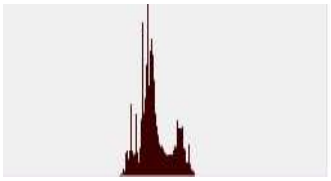
B- Green color before encrypted



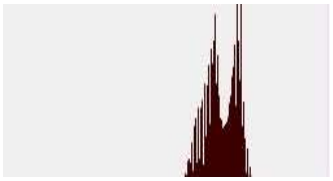
C- Blue color before encrypted



D- Red color after encrypted



E- Green color after encrypted



F- Blue color after encrypted

4.4. Noise Attack Analysis

Information transmitted over the internet is subjected to attempts by the attackers or unauthorized persons to destroy them, so that the receiver cannot understand the information sent to him after decrypted it. There is several ways to destroy this information such as:

1- Add noise
2- Cut of part of the information

In IEBPRPP method, the way of adding noise or cutting parts of the image, do not affect the clarity of the image because this noise will be distributed randomly on the image after the decryption process. This noise can be removed by using medium filter. Fig.8 illustrates adding noise and cropping parts of encryption image and the result after its decryption.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

A- Add noise B- Decryption Image C-Medium filter Image

D- Cutting parts E- Decryption Image F- Medium filter Image

FIGURE8. Add noise , decrypted image and applying medium filter

5. Conclusions

A new suggested IEBPRPP method is introduced to protect the information in color images in this paper. This method depends on fragmentation the image into four parts and rearranging pixels position through generated random numbers by using LFSRs. The initial values are taken from image data which cannot be changed if exposed for compression process. The numbers of random numbers that are generated represent 1/4 of the size of the image. One of the benefits of this method the result image can be sent to the receiver with JPEG form and the receiver can recover the original image. Another benefit is not sending any additional information with the encrypted image.

REFRENCES

[1] J. Shah, and Dr. V. Saxena "Performance Study on Image Encryption Schemes" , IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011, p 349-355

[2] V. V. Divya, S. K. Sudha, and V. R. Resmy "Simple and Secure Image Encryption", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 3, November 2012, p 286- 289

[3] R. Pakshwar, V. K. Trivedi, and V. Richhariya " A Survey On Different Image Encryption and Decryption Techniques", IJCSIT International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, p 113 – 116

[4] K. D. Patel, and S. Belani " Image Encryption Using Different Techniques: A Review ", International Journal of Emerging Technology and Advanced Engineering , Volume 1, Issue 1, November 2011, p 30-34

[5] M. A. B. Younes, and A. Jantan "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03, (Advance online publication: 19 February 2008

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

[6] Y. Rajput and A K. Gulve " An Improved Cryptographic Technique to Encrypt Images using Extended Hill Cipher", International Journal of Computer Applications, Volume 83 – No 13, December 2013, p 4-8.

[7] A. Gupta, N. Tiwari, M. Chawla and M. Shandilya " An Image Encryption using Block based Transformation and Bit Rotation Technique", International Journal of Computer Applications, Volume 98– No.6, July 2014, p 30-32.

[8] S. P. Nichat, and Prof. Mrs. S. S. Sikchi " Image Encryption using Hybrid Genetic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013, p 427- 431.

[9] T. Sivakumar, and R. Venkatesan " Image Encryption Based on Pixel Shuffling and Random Key Stream", International Journal of Computer and Information Technology, Volume 03 – Issue 06, November 2014, p 1468- 1476.

[10] G. A. Sathishkumar and K. B. Bagan, "A novel image encryption algorithm using pixel shuffling and BASE 64 encoding based chaotic block cipher, WSEAS Transactions on Computers, Vol. 10, No. 6, pp169-178, 2011.

[11] K. Loukhaoukha, J.Y. Chouinard, and A. Berdai, "A secure image encryption algorithm based on Rubik's cube principle", Journal of Electrical and Computer Engineering, Vol. 20, No. 12, pp113, 2011.

[12] C. K. Huang, C. W. Liao, S. L. Hsu, and Y. C. Jeng, "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system", Telecommunication Systems, Vol. 52, pp563– 571, 2013.