Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.1 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

Comp Page 54 - 62 Mohammed .H

Image Encryption Using Columnar Transportation Technique and Bits Reversing

Mohammed Hasan Abdulameer
Department of computer science,
Faculty of education for girls, university of kufa, Iraq

Recived : 26\11\2017 **Revised : 30\11\2017** **Accepted : 14\12\2017**

Available online : 26/1/2018

DOI: 10.29304/jqcm.2018.10.1.351

Abstract

Security has become very important aspect during data transmission and storage. Cryptography is used to maintain security. Columnar Transportation Technique is one of the most common methods that used in image encryption. In this paper, we proposed an encryption technique based on columnar Transportation and bits reversing, and named the method (CTR). Different colored images are used in the experiments. Experimental results showed that the proposed method is a secure and effective as a color image encryption method.

Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.1 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

I. Introduction

Security of images has gained much attention for many years, and the "illegal data access has become big issue and widespread in communication networks. So that, data security in storage and transmission of digital images is extremely needed, such as in transmitting medical images, military images transmissions, and confidential video conferencing [1][2][3]. Digital images, nowadays it's a very popular for using in computers and other digital devices. For image processing applications, it is always worth to minimize the computational time and storage. There are many studies and techniques to encrypt images which were achieved great results [4][5]. However, the classical cipher methods are still slow to process image and video data in commercial systems. An algorithm to enhance the security in transmission digital images was proposed by Rodriguesa et al [6] .Their approach was based on Advanced Encryption Standard (AES) stream ciphering applied in the Huffman coding. Their proposed structure permits decryption of an explicit area of image and that led to a substantial decrease in processing time in encrypting and decrypting process. Moreover, it provides a steady bit rate and retain the JPEG bit-stream acquiescence. To reflect a high level security and features of parallel processing with better image encryption and non-distortion, Ammar et al [1] introduced a new method as an image encryption technique. It was established on a non-traditional random number generators and a residue number system (RNS) sequence, which are clustered as a chaotic system. Acharya et al [7] have proposed an advanced of hill cipher named as (AdvHill) encryption algorithm which uses an involuntary key matrix.[7]. Their proposed method was an effective against plaintext attacks. Singh and Nand [8] introduced an approach where the image file is considered as a stream of bits. These are constructed as grids of variable sizes.

Their proposed method transforms each grid into encrypted grid by applying Helical and columnar transposition. This paper proposes an approach called (CTR) to simulate analyzing and ciphering the entire image by re-ordering the data of image matrix; using Columnar Transportation technique and bits reversing in order to choose an effective key as one of available ciphering/deciphering keys.

I. The proposed Methodology

The general block diagram of the proposed methodology is illustrated in the figure (1) below:

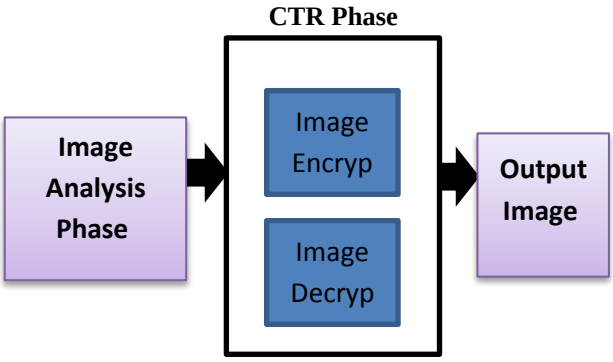


Figure (1): the proposed Methodology.

1. **Image Analysis phase**: it is the first phase in the proposed methodology which comprises many steps as described in the following flowchart:

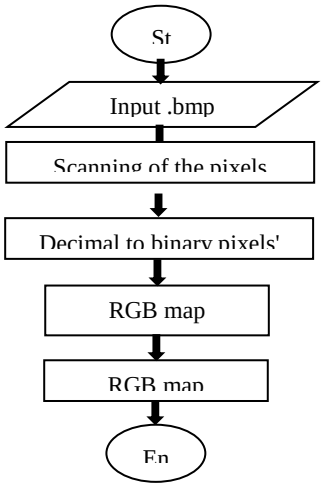


Figure (2): flowchart of the image analysis steps

a) **Input .bmp image:** In this processing step, each image is mapped into the popular type of bitmap (24 bit for each pixel (RGB)) which is used in most operating systems such as windows. We used different sizes of the applied image from the dataset such as (768×512) [9] as shown in the table (1).

Table (1): Some images sizes used in the proposed method

127×128
549×523
581×461
768×512

b) Scanning pixels: In this step, the method scans the entire coordination of the image through the width and the height in order to get the original data matrix**.**

c) Decimal to Binary pixels form: In this stage, the method converts all the pixels' values from decimal into binary form concurrently with the previous step.

d) RGB pixels map division and buffering: In this step, each pixel's value divided into three parts of colors binary matrixes named as color names R, G, and B.

The general equations for the previous steps are:

$$I_{Size(n*m)} = \begin{matrix} n = I_{width-1} \\ m = I_{high-1} \end{matrix} \quad (1)$$

To convert the decimal form of value to the binary form

$$I_{RGB}(r.c) \sum_{i=0}^{n} \sum_{j=0}^{m} I(r.c) \quad (2)$$

And for each pixel in equation 2, we get the binary form of it based on equation 3

$$I_{Bin}(r.c) = \sum_{k=1}^{24} \begin{matrix} \text{if } I_{rgb}(r.c) \bmod 2=0 \\ \text{else } I_{rgb}(r.c) \bmod 2=1 \\ I_{rgb}(r.c)=I_{rgb}(r.c) \text{ div } 2 \end{matrix} \begin{matrix} \text{if K}\leq 8: I_R(0) \text{and if K}\leq 16: I_G(0) \text{ and if K}\leq 24: I_G(0) \\ \text{if K}\leq 8: I_R(1) \text{and if K}\leq 16: I_G(1) \text{ and if K}\leq 24: I_G(1) \end{matrix} \quad (3)$$

$$I_{Binary\ of\ RGB}(r.c) = I_{Binary\ of\ R}(r.c) + I_{Binary\ of\ G}(r.c) + I_{Binary\ of\ B}(r.c) \quad (4)$$

2. CTR method phase:

There are two main procedures for this phase, the CRT image encryption for ciphering each input image and the CRT image decryption for deciphering each input image that is ciphered.

Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.1 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

2.1. **Image Encryption:**

The general flowchart of CTR image encryption as shown in figure (3):

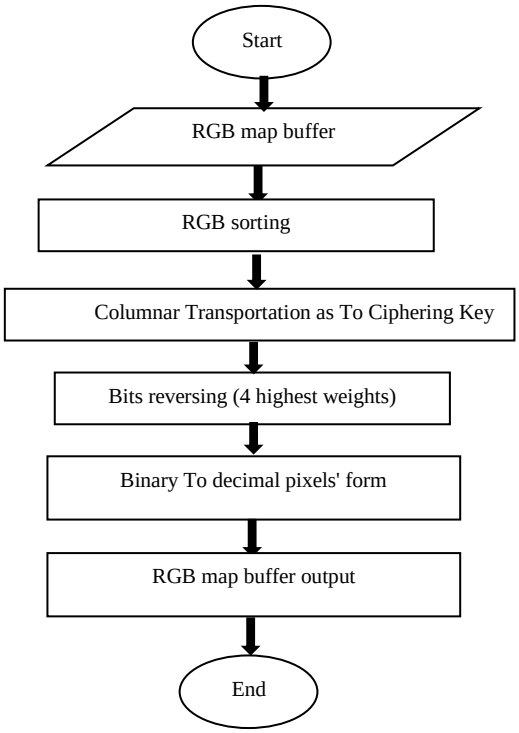


Figure (3): flowchart of CTR image encryption

A. **RGB sorting step:** this step starts with sorting all pixels' data by organize the 24 bits for each pixel into (3*8) array in order to convert them to ciphering key in Columnar transportation using equation 5:

$$I_{RGB\ Sort}(n.m) = \sum_{i=0}^{n}\sum_{j=0}^{m}\sum_{k=1}^{3}\sum_{l=1}^{8} I_{Binary\ of\ RGB}(k.l) \quad (5)$$

B. **Columnar transportation**: Re-arrange the 8' columns of the binary array as to the applied ciphering key (length is: 8) for each pixel sorted in equation 5 by applying equation 6:

$$P_{RGB\ Sort} = \sum_{k=1}^{3}\sum_{l=1}^{8} P_{Columnar\ Transport}(k.l) \quad (6)$$

C. **Bits reversing (4 highest weights)**: It is a significant step in the proposed method that reverse the last 4 bits' positions values (5,6,7,8) from 1 to 0 and verse vise for each pixel sorted in equation 6 by applying equation7 below:

$$P_{Bit\ inverse} = \sum_{k=1}^{3}\sum_{l=5}^{8} \begin{matrix} if\ P(k,l)=1, then\ P(k,l)=0, \\ Else\ P(k,l)=1 \end{matrix} \quad (7)$$

D. **Binary to decimal pixels' form:** after the previous step, we convert the 24 bit of applied pixel to its decimal value for each pixel sorted in equation7 via applying equation 8 as below:

$$P_{Dec}(r.c) = \sum_{k=1}^{24} \begin{matrix} \text{if } I_{rgb}(k) = 1 \text{ then } sum = sum + p\ (initial = 1) \\ p = 2 \times p \end{matrix} \quad (8)$$

E. **RGB map buffer output:** collect all image data as in the equation 9 and saving it as ciphered image.

$$I_{decimal\ of\ RGB}(r.c) = I_{dec\ of\ R}(r.c) + I_{Bec\ of\ G}(r.c) + I_{dec\ of\ B}(r.c) \quad (9)$$

1.2 Image Decryption:

The general flowchart for CTR image decryption is illustrated in figure (4):

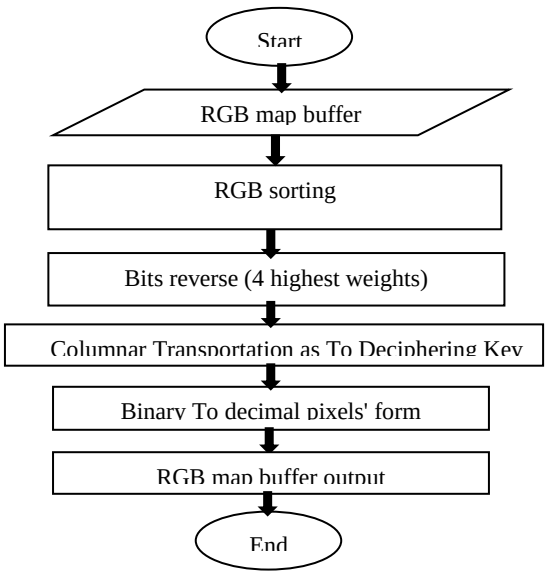


Figure (4): flowchart steps of CTR image decryption

A. **RGB sorting:** arrange the 24 bits for each pixel into (3×8) array to convert them as deciphering key in columnar transportation step as above in equation 5.

B. **Bits reverse (4 highest weights):** reverse the last 4 bits' positions (5,6,7,8) from 1 to 0 and verse vise as in explained above in equation 6.

C. **Columnar transportation**: Re-arrange the 8' columns of the binary array as deciphering key from the equation 7 above.

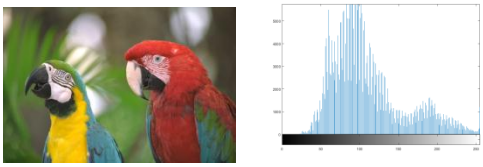
D. **Binary to decimal pixels' form:** convert the 24 bit of applied pixel into its decimal values as in equation 8.

E. **RGB map buffer output:** collect all the image data and saving it as ciphered image as in the equation 9.

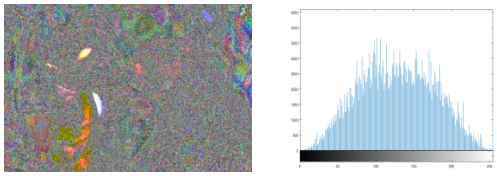
3. Output Image: it is the final phase that shows either the ciphered or deciphered image after applying CTR method procedures.

II. Implementation and Experimental results

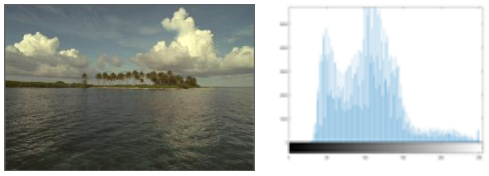
This section shows the experimental results of the proposed CTR approach for the selected images from the dataset of colored images [9]. The figures 5 and 6 present the images before and after applying CTR method.



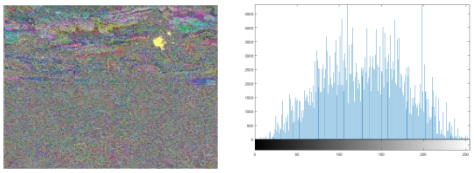
(a)Original Parrot image with histogram



(b) Parrot image after applying CTR method with histogram

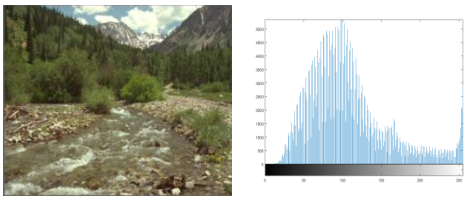


(a)Original Land image with histogram

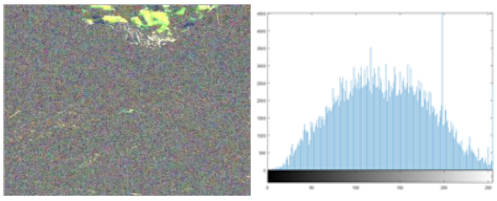


(b) Land image after applying CTR method with histogram

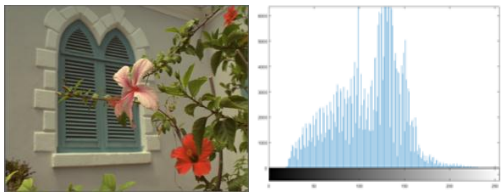
Figure (5): Two images encryption and decryption by CTR method with their histogram



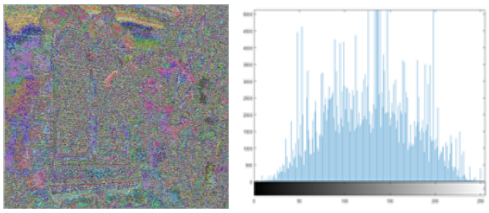
(a)Original Mount image with histogram



(b) Mount image after CTR algorithm with histogram



(a)Original Window image with histogram



(b) Window image after CTR algorithm with histogram

Figure (6): Two images encryption and decryption by CTR method with their histogram

Moreover, table 2 shows the decimal values of the cropped 5×5 pixels of Parrot image and table 3 demonstrate the RGB binary values corresponding to cropped 5×5 pixels in table 2.

Table (2): Decimal values of the cropped 5×5 pixels of Parrot image

pixels	Pix0	Pix1	Pix2	Pix3	Pix4
Pix0	١٤٩٢٩٣٣٢	١٤٩٢٩٣٣٢	١٤٩٢٩٠٧٨	١٥٠٦٠٦٦٤	١٤٩٩٤٨٧١
Pix1	١٤٩٢٩٥٨٧	١٤٨٦٣٥٣٩	١٤٩٢٩٠٧٨	١٤٩٩٤٨٧١	١٤٩٢٩٠٧٨
Pix2	١٤٩٢٩٣٣٢	١٤٨٦٣٥٣٩	١٤٩٢٩٠٧٨	١٤٩٩٤٨٧١	١٤٩٩٤٨٧١
Pix3	١٤٩٢٩٣٣٢	١٤٩٢٩٣٣٢	١٤٩٩٤٨٧١	١٥١٢٦٤٥٧	١٥١٢٦٤٥٧
Pix4	١٤٨٦٣٥٣٩	١٤٩٢٩٣٣٢	١٤٩٩٤٨٧١	١٥٠٦٠٦٦٤	١٥١٢٦٧١١

Table (3): RGB binary values corresponding to cropped 5×5 pixels in table 2.

pixels		Pix0	Pix1	Pix2	Pix3	Pix4
Pix0	R G B	٠٠١٠١١٠ ١ ١٠١١٠٠١ ١ ١١٠٠٠١١ ١	٠٠١٠١١٠ ١ ١٠١١٠٠١ ١ ١١٠٠٠١١ ١	٠١١٠١١٠ ١ ٠٠١١٠٠١ ١ ١١٠٠٠١١ ١	٠٠٠١١١٠ ١ ٠١١١٠٠١ ١ ١٠١٠٠١١ ١	١١١٠١١٠ ١ ١٠١١٠٠١ ١ ٠٠١٠٠١١ ١
Pix1	R G B	١١٠٠١١٠ ١ ٠١١١٠٠١ ١ ١١٠٠٠١١ ١	١١٠٠١١٠ ١ ٠٠١١٠٠١ ١ ٠١٠٠٠١١ ١	٠١١٠١١٠ ١ ٠٠١١٠٠١ ١ ١١٠٠٠١١ ١	١١١٠١١٠ ١ ١٠١١٠٠١ ١ ٠٠١٠٠١١ ١	٠١١٠١١٠ ١ ٠٠١١٠٠١ ١ ١١٠٠٠١١ ١
Pix2	R G B	٠٠١٠١١٠ ١ ١٠١١٠٠١ ١ ١١٠٠٠١١ ١	١١٠٠١١٠ ١ ٠٠١١٠٠١ ١ ٠١٠٠٠١١ ١	٠١١٠١١٠ ١ ٠٠١١٠٠١ ١ ١١٠٠٠١١ ١	١١١٠١١٠ ١ ١٠١١٠٠١ ١ ٠٠١٠٠١١ ١	١١١٠١١٠ ١ ١٠١١٠٠١ ١ ٠٠١٠٠١١ ١
Pix3	R G B	٠٠١٠١١٠ ١ ١٠١١٠٠١ ١ ١١٠٠٠١١ ١	٠٠١٠١١٠ ١ ١٠١١٠٠١ ١ ١١٠٠٠١١ ١	١١١٠١١٠ ١ ١٠١١٠٠١ ١ ٠٠١٠٠١١ ١	١٠٠١١١٠ ١ ١١١١٠٠١ ١ ٠١١٠٠١١ ١	١٠٠١١١٠ ١ ١١١١٠٠١ ١ ٠١١٠٠١١ ١
Pix4	R G B	١١٠٠١١٠ ١ ٠٠١١٠٠١ ١ ٠١٠٠٠١١ ١	٠٠١٠١١٠ ١ ١٠١١٠٠١ ١ ١١٠٠٠١١ ١	١١١٠١١٠ ١ ١٠١١٠٠١ ١ ٠٠١٠٠١١ ١	٠٠٠١١١٠ ١ ٠١١١٠٠١ ١ ١٠١٠٠١١ ١	١١١٠١١٠ ١ ٠٠٠٠١٠١ ١ ٠١١٠٠١١ ١

IV. Discussion

The strength of the CTR method in ciphering is depends on the power of the ciphering key, and to explain that; we will summarize some points;

first, the length of the key will be same as the size of the bits of each color. That will mean the length will be eight numbers ranging in [1,2,3,3,4,5,6,7,8]. Each one of them have the same position of the original bit. When the user chooses the ciphering key as the form [12345678], then it will be in the same ordering of the original bits of the image's pixels. That's means there is no change in the positions of bits for the ciphering image and the original image. In addition, the deciphering key must be the same to ciphering key. **Second,** depend on the columnar transportation of the positions of the ciphering key, we will get powerful ciphering key. **Third,** due to the importance of the last positions of the binary form of each color, we must take into account changing the positions of these 4 highest weights when trying to choose a ciphering key. **Four,** the eight digits for each ciphering key mean there are many transportations between the positions. It may get a ciphering key with one transport such as (21345678), the decipher keys (reverse keys) for the cipher keys above will be the same. Table (4) below show that the positions of the first and the second bits are changed. Changing between four bits means two positions changed such as (21435678). The changing to six and eight bits also possible such as (21436578), (21436587). There are thirty-two possible ciphering keys. **Finally,** the power of ciphering depends on substitution the maximum transportations, in this case the CTR method will be very effective in ciphering and this relating with the nature of the original image data. For example, the key (37821546) is a powerful ciphering key and the reverse key of it is (54176823). The powerful ciphering key for certain source image may be unreliable for another source image.

Table (4): Bit changing to create ciphering keys.

Bits changes	**Ciphering key**	**Deciphering key**
One bit change	2 1 3 4 5 6 7 8	2 1 3 4 5 6 7 8
Two bits changes	2 1 4 3 5 6 7 8	2 1 4 3 5 6 7 8
Six bit changes	2 1 4 3 6 5 7 8	2 1 4 3 6 5 7 8
Eight bit changes	2 1 4 3 6 5 8 7	2 1 4 3 6 5 8 7
More bit changes (**Strong Key**)	3 7 8 2 1 5 4 6	5 4 1 7 6 8 2 3

V. Conclusion:

Columnar Transportation and bits reversing (CTR) method has been proposed in this paper. The method simulate analyzing and ciphering the entire image. This achieved by re-ordering the data of image matrix and choose an effective key as one of available ciphering/deciphering keys. Eight different colored images have been collected and used in the experimental results. The results showed high performance in the encryption for the selected images. Furthermore, the CTR was reliable in analyzing and encrypting variety of image features. Moreover, it was an easier to manage use of available keys in order to investigate the desired cipher sample of any color image. To extend this work, we suggest combining the proposed CTR with another method for more security performance and use large dataset to show more stability.

VI. References:

[1] A. Ammar, A. S. S. El-Kabbany, M.I. Youssef and A. Emam, "A Novel Secure Image Ciphering Technique Based On Chaos", 4th WSEAS Int. Conf. on Information Science, Communications and Applications, Miami, Florida, April 21-23, (2004).

[2] Hasan Thabit Rashid and Hind R. M.," New Algorithm for Image Ciphering by Detecting the Edges of Color Image", The Scientific Karbala Journal, Vol: 144, No: 774. (2008).

[3] Hasan Thabit Rashid and Hind R. M.," Ciphering of Stopping and the Attrition Voices Phonemes in Coding Image", 1st Conference for the Secret of the Information and the Ciphering, Islamic University, Najaf, Iraq,Vol: 16, No: 20, April 2008.

[4] El-Zoghdy SF, Nada YA, Abdo AA, "How Good Is The DES Algorithm In Image Ciphering", International Journal of Advanced Networking and Applications. 2(5):796-803,(2011).

[5] Kester, Quist-Aphetsi. "Image Encryption based on the RGB PIXEL Transposition and Shuffling." International Journal of Computer Network and Information Security 5, no. 7, p.43, (2013).

[6] Bhairvee Singh, Parma Nand, India, "Image Encryption and Decryption Using Helical and Session Based Transposition with Key Wrapping ", INTERNATIONAL GLOBAL JOURNAL FOR ENGINEERING RESEARCH, NOV, VOL. 10, NO. 2, (2014).

[7] Acharya, Bibhudendra, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda. "Image encryption using advanced hill cipher algorithm." International Journal of Recent Trends in Engineering 1, no. 1 (2009).

[8] J.M. Rodriguesa, W. Puecha and A.G. Borsb,"A Selective Encryption for Heterogenous Color JPEG Images Based on VLC and AES Stream Cipher", CGIV'06: 3rd European Conference on Colour in Graphics, Imaging and Vision, Jun, Vol. 2006. No. 1, pp.34-39, (2006).

[9] The Data set of Toyama_database-MICT Image Quality Evaluation Database (2008).

Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.1 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

تشفير الصور باستخدام تقنية النقل العمودية وعكس البتات

محمد حسن عبدالأمير
قسم الحاسبات /كلية التربية للبنات /جامعة الكوفة

المستخلص :

أصبح الأمن جانبا هاما جدا أثناء نقل البيانات والتخزين ويستخدم التشفير للحفاظ على الأمن. تقنية النقل العمودية هي واحدة من الطرق الأكثر شيوعا التي تستخدم في تشفير الصور. في هذه البحث، نحن نقترح تقنية التشفير على أساس النقل العمودي وعكس البتات تسمى طريقة سي ار تي . وتستخدم الصور الملونة المختلفة في التجارب. وأظهرت النتائج التجريبية أن الطريقة المقترحة هي آمنة وفعالة كطريقة تشفير للصورة الملونة.