Improved Color Plane Permutation *for Satellite Imagery Encryption*

Assist. Lecturer Fadhil Hannoon Abbood
College of education- Al-Mustansriyh University- Iraq- Baghdad
Fadhil_alsaadi@yahoo.com

Abstract

The standards Image coding permitted the wide-ranging spread use for applications of multimedia. Nowadays, digital documents might make discrete over the World Wide Web to a many number of customers in a cost efficient way. So the real need for more security and services to keep the provision of digital multimedia work both profitable for the document owner and reliable for the customer. Privacy and Authentication services for multimedia data streaming are crucial in today data dissemination through internet. This paper focuses on Image security and integrating encryption with multimedia (Satellite Imagery) compression method. However, Image encryption algorithms combining with JPEG encoding are proposed. the approach for integrating encryption with image compression system are proposed, Improved Color Plane Permutation. The proposed method is improved by selective encryption, were a portion of the coefficients from either the final results or intermediate steps of a compression method are enciphered with a cryptographic cipher.

The securities of the proposed approach are analyzed Experimental results and compared with the results that obtained from traditional algorithm such as (Chaotic). The proposed system is more secure, of low cost, supports direct bit-rate control and is more robust to transmission errors. These properties make it suitable for multimedia applications with real – time operation and image transmission over a network.

Keywords:- *DCT, Selective Encryption,, Color plane permutation*

م.م فاضل حنون عبود

الجامعة المستنصرية– كلية التربية – قسم علوم الحاسبات

المستخلص:

سَمحتْ معايير تشفير الصورة بالانتشارِ الواسع لاستخدام التطبيقاتِ المتعددة الأوساطِ . ففي الوقت الحاضر، الوثائق الرقمية يُمْكِنُ أَنْ تُوزّعَ عن طريق الشبكة العالميةِ للمعلومات إلى عدد

كبير مِنْ الناسِ بكلّفَ تصنيعها. ومن هنا برزت الحاجة الملحَّة للشركات ذات الاختصاص لاستمرار توزيعَ الوسائط المتعددة وان تعمل بشكل مربح لمالكِها وتوفر الضمان للزبونِ. حيث ان العالم هذه الايام بحاجة إلى إن تكون بياناتِ الوسائط المتعددة سريةً وشرعية لنشرها خلال شبكةِ الإنترنت. إن هذا العمل المقترح يركز على أمنية الوسائط المتعددة والذي يكمل نظام التشفير مع نظام ضغط الوسائط المتعددة(صور الاقمار الصناعية). لذلك فقد تم اقتراح خوارزمية تشفير تعمل في البداية على ازالة الضوضاء وتهيأة الصورة لعملية التشفير ومن ثم تغيير النظام اللوني للصورة قبل الشروع بعملية التشفير المقترحة(تحويلات لون المستوي المعدلة).

إن الطريقة المقترحة تعتمد على مبدأ التشفير الانتقائي من خلال الاعتماد على جزء من المعاملات إما يؤخذ من النتائج النهائية أو من الخطوات الوسطية لنظام الضغط ويشفر مع شفرة التشفير. إن أمنية الطريقة المقترحة قد تم تحليلها ومقارنتها بنتائج تم استخلاصها من طريقة تشفير تقليدية. وأظهرت النتائج التطبيقية إن النظام المقترح هواكثر امنا، قليل الكلفة، ويوفر كذلك حصانة ضد أخطاء الإرسال. إن هذه الميزات تجعل أنظمة الأوساط المتعددة ملائمة مع أنظمة الوقت الحقيقي وإرسال الصورة عبر شبكة الانترنيت.

1. Introduction

Nowadays, multimedia content (image, audio and video) presents an huge importance giving the fact of the rapid growth of high technologies. The rate of exchanges these types of information is growing and the need to protect it is more and more essential. However increasing Number of multimedia processing tools, Digital documents and providing global access to the Internet has created an ideal form of distribution can not be controlled from the [1].To protect data, various encryption schemes has been proposed for image encryption, [2,3,4] however in these schemes (total encryption schemes) all data has to be encrypted which will generally take some time, complicated calculations and high memory occupation, which makes these schemes hard to use in real time applications.

Total encryption schemes are not necessary when we talking about most multimedia content.Given to the fact that the content is already voluminous and not all the content represent a significant importance we choose to encrypt only significant parts of the data and leave the rest to enhance time encryption and reduce memory occupation and make the encryption scheme suitable in practical application given to the fact that selective crypto-systems presents a simple architecture.

So the proposed method is providing method of image encryption. This algorithm is mainly based on encrypting DCT coefficients so as not cause any changes in compression ratio. Therefore, the proposed method combines encryption process with JPEG encoding that permute DCT blocks.

2. DCT(Discrete Cosine Transform)

The standard JPEG calls for applying the DCT to data units (Blocks) of 8×8 pixels not to the entire image because of :

1.When Applying DCT on all image pixels (n×n) lead to produces better compression with many arithmetic operations, therefore. Applying DCT to all data units can be reduces the overall compression ratio but is faster.

2.Many experience displays that, in a continuous-tone image, correlations between pixels are short range.

Evry pixel in an image has a value (color or gray) that's close to those of

its near neighbors, but has nothing to do with the values of far neighbors

[5].

The DCT can be done by the following [10]:

$$G_{ij} = \frac{1}{4} C_i C_j \sum_{x=0}^{7} \sum_{y=0}^{7} p_{xy} \cos\left(\frac{(2x+1)i\pi}{16}\right) \cos\left(\frac{(2y+1)j\pi}{16}\right) \quad \text{...........} \ (1)$$

$$\text{where} \quad C_f = \begin{cases} \frac{1}{\sqrt{2}}, & f=0, \\ 1, & f>0, \end{cases} \quad \text{and } 0 \le \mathrm{i}\ , \mathrm{j} \le 7. \ \text{........}(2)$$

where C_f is C_i, C_j and P_{xy} are the values of image component $i,j = 0,1,...,7$, $x,y = 0,1,\ldots,7$.

The JPEG decoder works by computing the inverse DCT (IDCT), using the following equation (2.4):

$$p_{xy} = \frac{1}{4} \sum_{i=0}^{7} \sum_{j=0}^{7} C_i C_j G_{ij} \cos\left(\frac{(2x+1)i\pi}{16}\right) \cos\left(\frac{(2y+1)j\pi}{16}\right), \quad \text{..........}(3)$$

$$\text{where} \quad C_f = \begin{cases} \frac{1}{\sqrt{2}}, & f=0; \\ 1, & f>0. \end{cases} \quad \text{.............}(4)$$

3. Color plane permutation

Blocks position of DCT under the control has been confuse of the key. So, the method of confusion founded by Space Filling Curve (SFC) pseudo-random used in order to decrease the compression ratio changing. Since the DCT coefficients are encoded depending of the previous adjacent ones in JPEG, and SFC method can be keeping the correlation between blocks in some extent.

Figure (2) show confusion method.

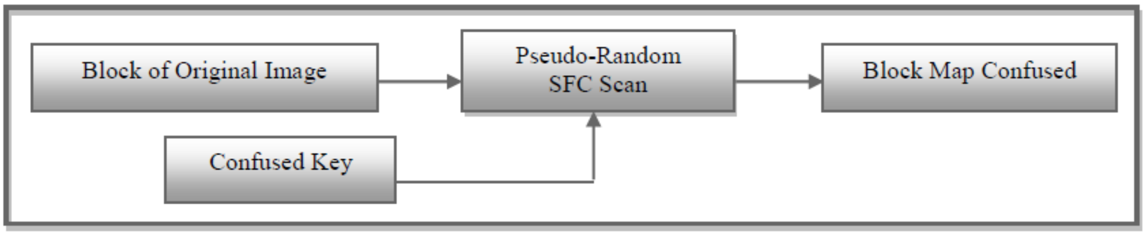
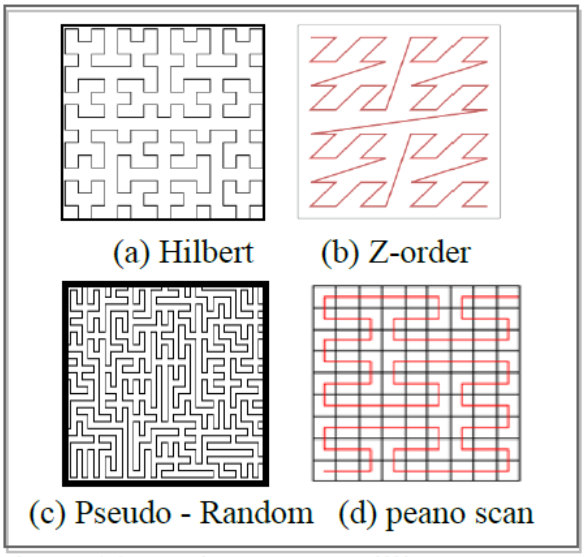


Figure (2) Color Plane Confusion Method

3.1 Alternative Space Filling Curve Techniques

A space filling curve is a continuous map of a one-dimensional interval into a two-dimensional area (plane-filling) or a three-dimensional volume. There are different types of SFCs and each of them exhibits different locality preserving properties (also called clustering properties). Figure (3) shows several types of SFCs [6,7].


(a) Hilbert (b) Z-order

(c) Pseudo - Random (d) peano scan

Figure (3): Various Space-Filling Curves.

Space Filling Curve (SFC) Algorithm

```
Input: Image matrix $I_{N \times N}$
Output: Confused matrix
1. Divide I to a set of blocks $b_i = [b_1, b_2, \dots, b_m]$.
2. Generate position array POS[1…m] with random sequence without
   repeated any number, where m is the number of blocks in image
   and the block size (8×8) pixels.
3. Set $i \leftarrow 1$
   While $(i \leq m)$
   a. Get a block number i from I
      $b_i$ = I(block POS[i])
   b. Insert $b_i$ into new matrix I'
       I' (block i) = $b_i$
   c. i = i + 1
```

4. The proposed approach of Improved Color plane permutation

The proposed method based on the idea of decomposing the image into 8x8 blocks, these blocks are transformed from the spatial domain to frequency domain by the DCT. Then, the DCT coefficients related to the higher frequencies of the image block are encrypted using the Color Plane Permutation..The general block diagram of the proposed method of selective image encryption is shown in Figure 4, which combines encryption process with DCT codec, and is composed of date ncoding, parameter encryption and data decoding The general peopsed approach can be showing below.

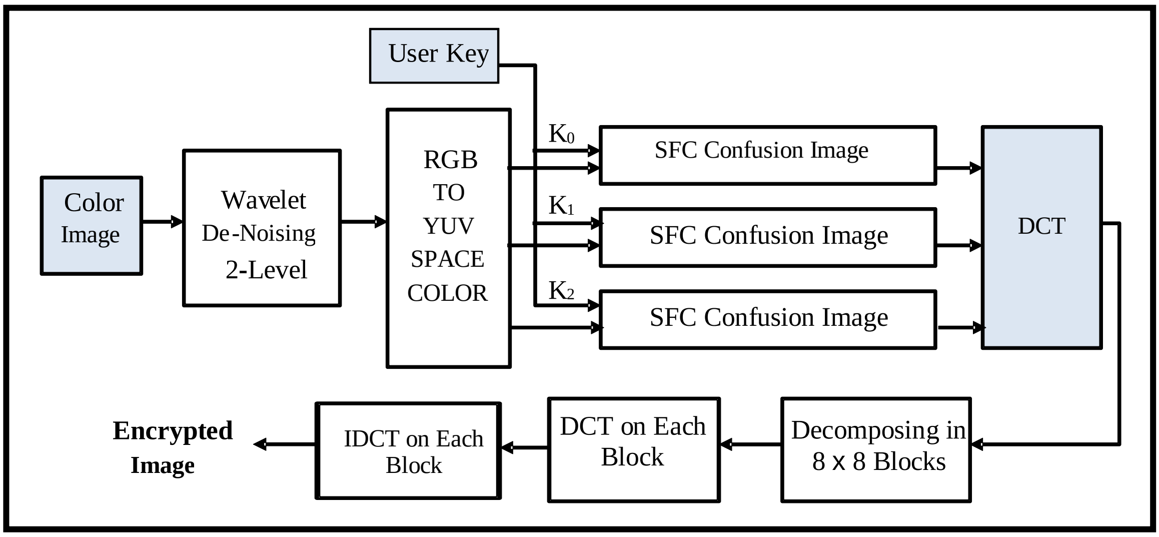


Figure (4): The proposed Improved Color Plane Permutation based on DCT

<u>**Improved Color Plane Permutation Algorithm**</u>

Input: Image matrix $I_N \times_N$

Output: Encrypted Image

1. **Read color image**
   Input the satallite Imagery (color image) (RGB)
2. **Image De-Noising By wavelet**
   De-Noising and enhancement the input image using waveletwith 2-Levels
3. **Convert Image Color Space**
   The satallite Imagery (color image) after complete de-noising process and prepering transformed from RGB into a YUV color space.
4. **Apply SFC Confusion**
   This approach is to effect a Block permutation by changing the position of DCT blocks without changing the Block’s value.

5. Apply DCT
To perform DCT, it must first divide the image to a block (8 × 8 pixels),and then apply DCT equation on each block.

5. **Apply IDCT**

5. **Quality** Measures **and Performance of Decrypted Image**

In this stage PSNR,NAE,AD,NCC, Time measures are used to show the quality of images as shown below.

1) Peak Signal to Noise Ratio (PSNR)

The small value of Peak Signal to Noise Ratio (PSNR) means that image is poor quality. PSNR is defined as follow:

$$PSNR = 10 * \log\left(\frac{(L-1)^2}{MSE}\right) \qquad \text{..........} (5)$$

2) Mean Absolute Error(MAE):

The average absolute error (MAE) value means more of the image quality

is poor. MAE is defined as follows:

$$MAE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} |x(i,j) - y(i,j)| \qquad \text{..........} (6)$$

M, N: size of image

x (i, j): shows samples of original image.

y (i, j) shows samples of image enhancement.

i and j is the number of pixels in rows and columns trends.

3) Average Difference (AD)

It is defined as the average difference between the original and enhanced images. AD is defined as follow:

$$AD = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} [(x(i,j) - y(i,j)] \qquad \text{..........} (7)$$

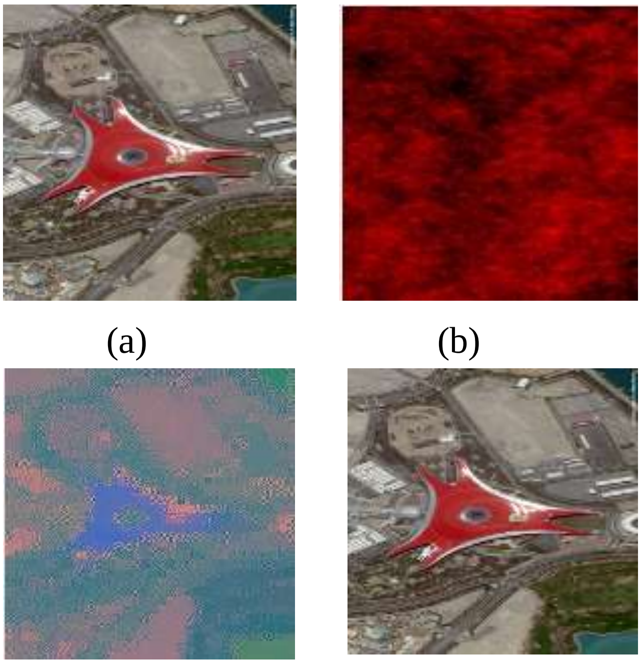
4) Normalized Cross – Correlation (NK)

NK is defined as follow:

$$NK = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} [x(i,j) - y(i,j)]}{\sum_{i=1}^{M} \sum_{j=1}^{N} [x(i,j) - y(i,j)]^2} \qquad \text{..........} (8)$$

7. Results

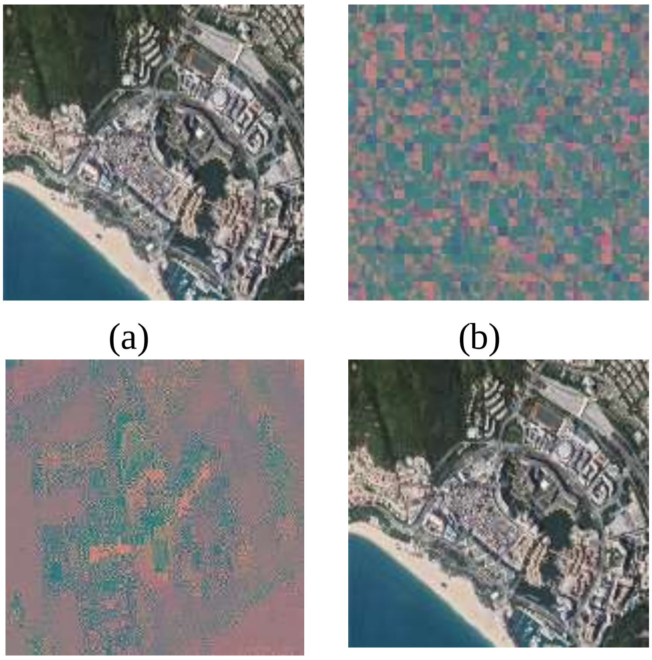
After applying these encryption methods with it's steps on various images size 256 x 256 . The results of images (satellite image) are shown in figure (5)-(7). Where, image (a) is original image, (b) encrypted image Improved Color Plan Permutation (c) encrypted image using chaotic algorithmand (d) is decrypted image. the encrypted images are understood. Encrypted images of Improved Color Plan Permutation are compare withe the encrypted images of traditional algorithm (chaotic) using some of quality measurs showing in the table (3)-(5).



(a) (b)

(c) (d)

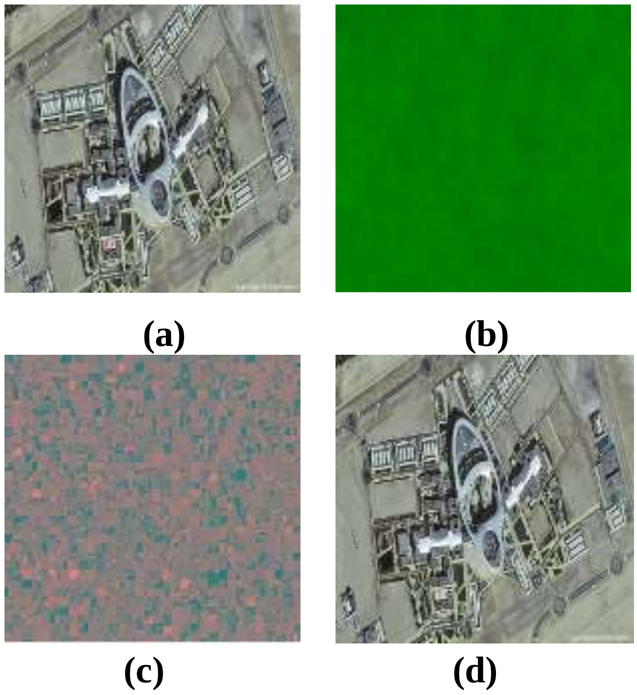
Figure(5): (a) original image ,(b) encrypted images of Color Plan Permutation(c) encrypted images using chaotic algorithm and(d) decrypted image



(a) (b)

(c) (d)

Figure(6): (a) original image ,(b) encrypted images of Color Plan Permutation(c) encrypted images using chaotic algorithm and(d) decrypted image



(a) (b)

(c) (d)

Figure(7): (a) original image ,(b) encrypted images of Improved Color Plan Permutation(c) encrypted images using chaotic algorithm and(d) decrypted image

Image	Improved Color Plan Permutation			
	PSNR	MAE	AD	NK
Image 01	77.072	0.1008	0.0384	0.9803
Image 02	72.447	0.1536	0.0133	0.9589
Image 03	75.370	0.1246	0.0111	0.9660

Table (3) Quality measurs of Improved Color Plan Permutation

Table (4) Quality measurs of Chaotic algorithm

Image	Chaotic algorithm			
	PSNR	NAE	AD	NK
Image 01	45.368	0.1708	0.0445	0.9803
Image 02	52.433	0.1456	0.0200	0.9589
Image 03	54.388	0.1518	0.0844	0.9660

8-1 Encryption Speed Test

Experiments on various satellite imagery (color images) show that the proposed method encryption are of high speed. Here, taking various color images for test, the times required for encryption are shown in Table (5) These speeds mean that the encryption using proposed method is of low cost and the scheme is of high speed. From the comparison it see that the Improved Color Plan Permutation fast than the Chaotic algorithm as seen in table below.

Table (5) show speed test

Image	Speed Test (sec)	
	Improved Color Plan Permutation	Chaotic algorithm
Image 01	81.947	111.351
Image 02	77.672	121.658
Image 03	80.574	115.201

Conclusions

Selective Image Encryption Using DCT with. Improved Color Plan Permutation encryptions method has been presented in this paper. Color Plan Permutation encryptions method can be used to strengthen the security of cryptosystem. The original image is decrypted correctly with no noticed degradation. Theoretical analyses and results show that, the proposed method is of high security.

References

[1] F. Piper and S. Murphy, "**Cryptography: A very short introduction**", Oxford university press, 2002.

[2] M. Kumar and S. Lal, "**A Cryptographic study of some digital signature scheme**", Ph.D. Thesis, Fomerly Agera University, 2003.

[3] D. Arroyo, C.Q. Li, S.J. Li, G. Alvarez, W.A. Halang, **Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm**, Chaos Solitons Fractals 41 (5) (2009) 2613–2616

[4] S. Li, C. Li, G. Chen and Fellow, "**A General Cryptanalysis of permutation only Multimedia Encryption algorithm**", Dan Zhang and Nikolaos G., Bourbakis Fellow, IEEE, AIIS Inc., NY, USA, 2002.

[5] C. Li, S. Li, D. Zhang and G. Chen, "**Cryptanalysis of a Chaotic Neural Network Based Multimedia encryption scheme**", Multimedia Information processing PCM2004 proceedings, part III, volume 3333 of lecture notsin computer science, 2004.

[6] B.Furht,D. Socek and A. M. Eskicioglu, "**Fundamentals of Multimedia Encryption Techniques**", appear in IEEE Trans, Multimedia, 2002

[7] H. Chang and X. Li, "**Partial encryption of compressed images and videos", IEEE Transactions and signal processing**, Vol. 48, No. 8, pp. 2439-2451, Aug. 2000.

[8] C.-P. Wu and C.-C. J. Kuo, "**Efficient Multimedia Encryption via Entropy Codec Design**", Proceedings of SPIE Security and Watermarking of Multimedia Content III, Volume 4314, San Jose, CA, January 2001.

[9] X. Wang, T. Wang, **A novel algorithm for image encryption based on couple chaotic systems**, Int. J. Mod. Phys. B 26 (30) (2012) 1250175–1250183.

[10] M. Van Droogenbroeck and R. Benedett, "**Techniques for a Selective Encryption of Uncompressed and Compressed Images**", Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002, Ghent, Belgium, September 9-11, 2002.

[11] R. C. Gonzalez and R. E. Woods, "**Digital Image Processing**", published by Addison Wesley Longman, Delhi, 2007.

[12] R. Dafner, D. Cohen-Or and YossiMatias, "**Context-based Space Filling Curves",** Volume 19, Number 3, 2000.