Partial Encryption in Digital Image Based On Plasma Encoding Techniques

Dr. Hala B. Abdul Wahab [1], Sura A. Sarab [2] , Thair A. Sarab[3]

[1] Department of Computer Science / University of Technology
hala_bahjat @yahoo.com.

[2]Computer Sciences Department/ University of Baghdad
suraaljanaby@yahoo.com

[3] Information Technology Department/ Institute of Technology
thairit@yahoo.com

Abstract: *Many digital services require reliable security in storage and transmission of digital images. Due to the rapid growth of the internet in the digital world today, the security of digital images has become more important and attracted much attention. The prevalence of multimedia technology in our society has promoted digital images to play a more significant role than the traditional texts, which demand serious protection of users' privacy for all applications. Encryption techniques of digital images are very important and should be used to frustrate unauthorized access from opponents. In this paper a new approach is proposed for partial encryption in digital image based on dragging the longest wavelength color in digital image then input the extract color to the plasma encoding algorithm to have partial ciphered image that can be deciphered at the recipient side using the proposed retrieve algorithm. It is possible to apply multilevel for the proposed approach to increase the security level with less time for encryption/decryption. The new approach test appeared that the encryption/decryption processes was very flexible and efficient.*

Keywords: digital image, partial encryption, wavelength, covert image, host image, plasma encoding algorithm

الخلاصة: ان العديد من الخدمات الرقمية تتطلب امنية موثوقة لخزن وارسال الصور الرقمية. وبسبب النمو السريع للانترنيت في العالم الرقمي اليوم فان امنية الصور الرقمية اصبحت اكثر اهمية وتجذب الاهتمام. ان انتشار تقنيات الوسائط المتعدده في مجتمعنا روج الصور رقمية لتلعب دور اكثر اهمية من النصوص الاعتيادية التي تتطلب حماية كبيرة لسرية المستخدم في جميع التطبيقات. تقنيات التشفير للصور الرقمية جدا مهمه ويجب ان تستخدم لاحباط الوصول الغير مخول من قبل الخصوم. في هذا البحث تم اقتراح وسيلة جديده للتشفير الجزئي في الصور الرقمية بالاعتماد على سحب اطول طول موجي للالوان في الصورة الرقمية ومن ثم ادخال اللون المستخرج الى خوارزمية ترميز البلازما للحصول على صورة مشفرة جزئيا من الممكن فك تشفيرها من قبل المستلم باستخدام خوارزمية الاسترجاع المقترحة. ومن الممكن تطبيق مستويات متعدده للطريقة المقترحة لزيادة مستوى الامنية مع وقت اقل للتشفير وفك التشفير. اختبار الطريقة الجديده اظهر ان عمليات التشفير وفك التشفير هي جدا مرنة وفعالة.

1. INTRODUCTION

With advancements in Digital communication technology the information security takes place as an important role. Nowadays, information security is becoming more important in data storage and transmission. An increasing amount of information is being transmitted over the Internet, including not only text but also audio, image, and other multimedia files. The revolution of multimedia has been a driving force behind fast and secured data transmission techniques. Images are widely used in several processes; therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones [1].

Data encryption is widely used to ensure security in open networks such as the internet. Each type of data has its own features; therefore, different techniques should be used to protect confidential image data from unauthorized access. Most of the available encryption algorithms are used for text data. However, due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data [2].

In this research, a new transformation algorithm is proposed for image security using a combination of plasma and fractal image addition encoding techniques. This algorithm will be used as an encryption transform to confuse the relationship between the original images and the generated ones. The generated ciphered images can be retrieving by using the proposed retrieve algorithm. The randomness tests (Frequency, serial, run, poker and autocorrelation) have been used to measure the security level of the images. Experimental results have shown that the proposed method offers a good concealment of the data in the encrypted image, thus reduces the chance of the encrypted image being detected.

2. PARIAL ENCRYPTION (SELECTIVE ENCRYPTION)

Encryption is used to securely transmit data in open networks. Each type of data has its own features; therefore different techniques should be used to protect confidential image data from unauthorized access. Image encryption can be divided into full encryption and partial encryption (also

called selective encryption) schemes according to the percentage of the data that is encrypted [3].

Selective encryption aims to avoid the encryption of all bits of a digital image and yet ensuring a secure encryption. The key point is to encrypt only a small part of the data to obtain a fast method. The variety of applications for secure multimedia requires either full encryption or selective encryption. Selective encryption reduces the computational requirements in networks with diverse client device capabilities. The goal of Selective encryption is to encrypt a well-defined range of parameters or coefficients. Always, when considering image processing applications on such devices we should use minimal resources. However, the classical ciphers are usually too slow to be used for image and video processing in commercial low powered systems. The selective encryption can fulfil the application requirements without the overhead of the full encryption. In this case, only the minimum necessary data are ciphered [4].

Multimedia communications often requires real-time data transmission, so tremendous image; audio and video data need to be transferred securely. Given that all multimedia data are encrypted, this will consume a great deal of overhead, so that multimedia data is difficult to transmit timely and the quality of communication cannot be guaranteed. Under such circumstances, the design of a selective encryption algorithm with less processing time but with relatively high security level is extremely significant [5].

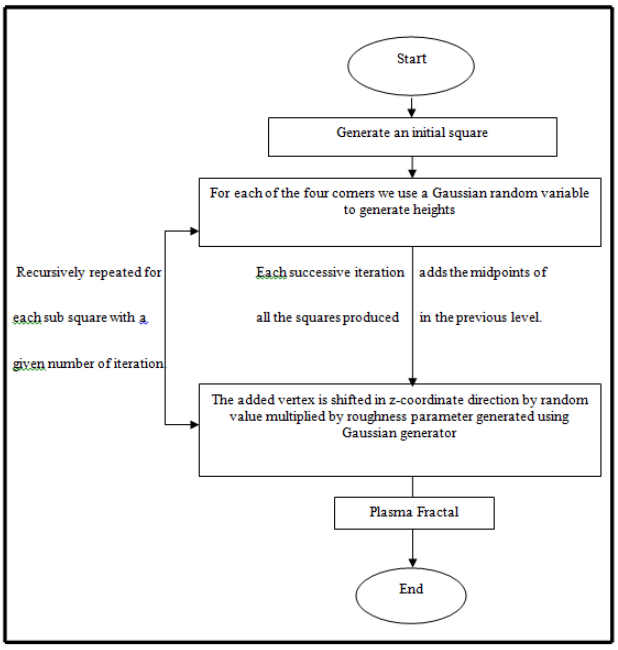

Figure 1: The flow chart of generating the plasma fractal on a rectangular piece [6].

3. PLASMA ENCODING TECHNIQUES

Secure image cryptography was gotten by using plasma coding techniques that combining between plasma algorithm and fractal addition encoding algorithm that are illustrated as the following:

A. Plasma algorithm

Plasma fractals are perhaps the most useful fractals those have a random element in them, which gives them random self- similarity, a scientific name for this type of fractals would be: random midpoint displacement fractals, another popular name for them is fractal clouds. Due to their randomness, plasma fractals closely resemble nature. Because of this, the plasma fractals can be used in many different applications. For example by using standard atlas colors and determining the heights by the values of the points, very realistic landscapes can be obtained. Plasma fractals can be used in many different applications with different roughness range. The formula of the plasma algorithm was as the following: [6].

$$M = ((A + B + C + D)/4 + rnd) \times P \quad (1)$$

Where M is the midpoint, (A, B, C, D) represents the four corner points of the image, rnd represents the displacement in the current iteration that range between [0, 1], and P represent the fractal factor. This formula was executed iteratively, and generates a rectangular terrain.

Figure 1: Illustrates the flowchart of generating the plasma fractal on a rectangular piece of plane that is shown in Figure 2.

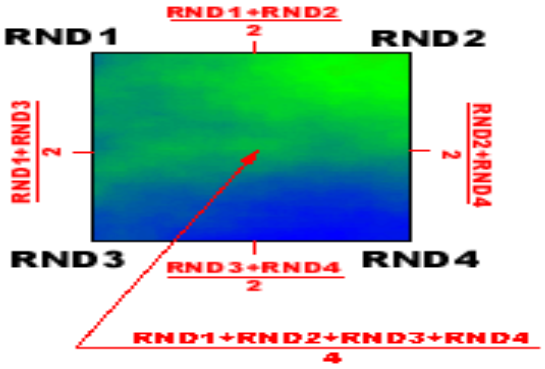

Figure 2: Create a plasma fractal on a rectangular piece of plane steps [6].

B. Fractal image addition encoding algorithm

The meaning of the fractal is broken or irregular fragments. Mandelbrot has analysed the fractal geometry of the nature. The natural objects such as trees, leaves, mountain ranges, coast lines. The fractal geometries have two unique properties known as space filling and self similarity which have generated many opportunities in various branches of engineering and sciences [7].

Fractal is the continuous accurately of small segment (specific shape call recursively and all these shapes are more accurately with simply overwrite pixel have already been plotted) [8].

The fractal image addition method and the binary encoding method are assembled to form a hybrid method for encryption a digital covert image. For this hybrid method, a host image is used to create an overt image with information of the covert image. First, the fractal image addition method

is used to add some fractal images and the covert image to form an image mixing matrix are transferred into the binary data. Finally, binary data are encoded into the host image to create an overt image. The overt image and the host image look almost the same for eyes. The most important feature is that the reconstructed covert image is identical to the original covert image and there is no distortion in the decoding work [9].

Assume that C is an (M×N) 256-gray level covert image for encoding. Assume that F1, F2 … and Fn are (M×N) 256-gray level fractal images, and assume that D is an M×N matrix mixed by adding C, F1, F2 and Fn. First input specified parameters into specified commercial fractal image software to generate the fractal images F1, F2… and Fn. Next, add all the gray values of images C, F1, F2… and Fn at the sponding position to form the value of the matrix D at the corresponding position, i.e [9].

$$D(u,v) = C(u,v) + \sum_{i=0}^{n} F_i(u,v) \dots\dots\dots\dots\dots\dots\dots\dots \quad 2$$

Where $1 \le U \le M$ and $1 \le V \le N$

Figure 3 is an illustration to explain the adding processes for 4×3 images. Figure3 (a) is a covert matrix C; Figure3 (b)-(d) are three fractal images F1, F2 and F3; Figure3 (e) is an image - mixing D derived by adding C, F1, F2 and F3. [9]

a

$$C=\begin{pmatrix} 2 & 4 & 6 & 8 \\ 10 & 12 & 1 & 3 \\ 5 & 7 & 9 & 11 \end{pmatrix}$$

b

$$F1=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}$$

c

$$F2=\begin{pmatrix} 9 & 2 & 22 & 27 \\ 23 & 33 & 17 & 10 \\ 5 & 34 & 12 & 14 \end{pmatrix}$$

d

$$F3=\begin{pmatrix} 3 & 1 & 8 & 9 \\ 10 & 11 & 7 & 4 \\ 2 & 12 & 5 & 6 \end{pmatrix}$$

e

$$D=\begin{pmatrix} 15 & 9 & 39 & 48 \\ 48 & 62 & 32 & 25 \\ 21 & 63 & 37 & 43 \end{pmatrix}$$

Figure 3: Illustration for fractal-image mixing method. (a) covert matrix C; (b) first fractal image F1; (c) second fractal image F2; (d) third fractal image F3; (e) image mixing matrix.

4. THE PROPOSED APPROACH

The final image is established by using plasma fractal algorithm and fractal image addition encoding algorithm, this techniques gives opportunity to change the shape in an easy way to get different new patterns and then different pictures in any time with random colour (value) in each small area in the picture when compare this technique with the normal colour image we see in each small area the pixels have the nearest values.

The plasma fractal approach is giving a random point for each pixel in the image and this achieved after dividing the rectangular image into many squares begging from the midpoint of the image as it was mentioned previously in (3.1). This work proposed a fixed value for (plasma fractal factor = 2000 and rnd = 0.5) because the image cannot be retrieve without there are a fixed starting point for dealing with it.

The following figure is an example on the plasma fractal algorithm that results in random plasma image.

Figure 4: Example on plasma fractal approach

The fractal image addition encoding approach is taking random points from the original image and put them in a new array that result in a new image, then repeat this process as it required for giving N of images. Finally, add the pixel values for the resulting N images and put them in a new array for giving the final random image.

The following figure is an example on the fractal image addition encoding algorithm that result in three different fractal images. The image (a) is the original image, the image (b) is the first random image, the image (c) is the second random image and the image (d) is the fractal addition encoding image that include the summation of the pixels value for the previous three images (a, b, c).

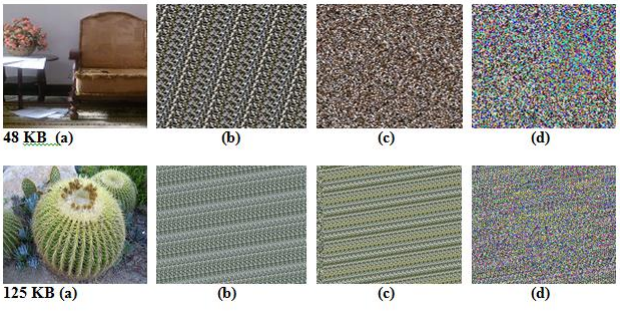

Figure 5: Example on fractal image addition encoding approach

The proposed algorithm include three stages; the first stage is for dragging the longest wavelength color from the image, this color is the blue (the blue color was became independent image including the blue color only, while the other colors of the origin image will have zeros value in the new image). The second stage; the blue color will be collected the similar

colors to the nearest possible color and compresses the rest. Then input the resulting blue image to the plasma encoding algorithm for completely ciphering by implement the fractal addition encoding algorithm on it and calculating the rise in the middle and add a small value of error (randomness), depending on the size of the rectangle then multiply it by the plasma fractal factor.

Although, it can be have the randomness level as it required by changing the randomness values. Finally, return the ciphered blue color to the origin image with the rest colors (red, green), and by this the ciphered image was completed.

In the following figure, it can be illustrated four images, the first one (a) is an original image, the second image (b) is the image of the blue color only, the third image (c) is the extracting for the blue color, the fourth image (d) is the plasma encoding image, and the fifth image (e) is the merge of the ciphered blue color with the rest origin colors (red, green) that can be retrieved without distortion by using the decryption algorithm and this illustrated in the image (f).

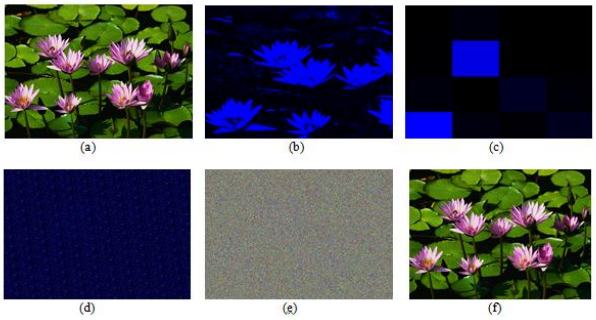

Figure 6: Example for plasma image generation

A. The proposed algorithm

Input: the four corner points, random value, size of mesh control points (N×M) and the size of the image that want to generate.
Output: Plasma encoding image.

Process:
Step-1:- convert image into binary array.
Step-2:- dragging the blue color from the array.
Step-3:- put the pure blue values into a new matrix.
Step-4:- extracting the blue color.
Step-5:- convert the blue image result from step4 into plasma image.
Step-6:- applying the fractal addition encoding algorithm on the resulting image from step5.
Repeated this steps as required from security level.
Step-7:- rearrange the plasma image in its position with the rest colors in the original image.
Step-8:- Show the ciphered image.
Step-9:- reconstructed the original image from the ciphered image.
Step-10:- end.

5. EXPERIMENTAL RESULTS

In the following some examples of images that show the results of implementing the proposed plasma encoding algorithms on different level of security. So, the image (a) is the original image, the image (b) is after implement level1 of security, the image (c) is after implement level2 of security, the image (d) is after implement level3 of security. Finally, the image (e) is the result image after return the ciphered color with the rest colors (red, green).

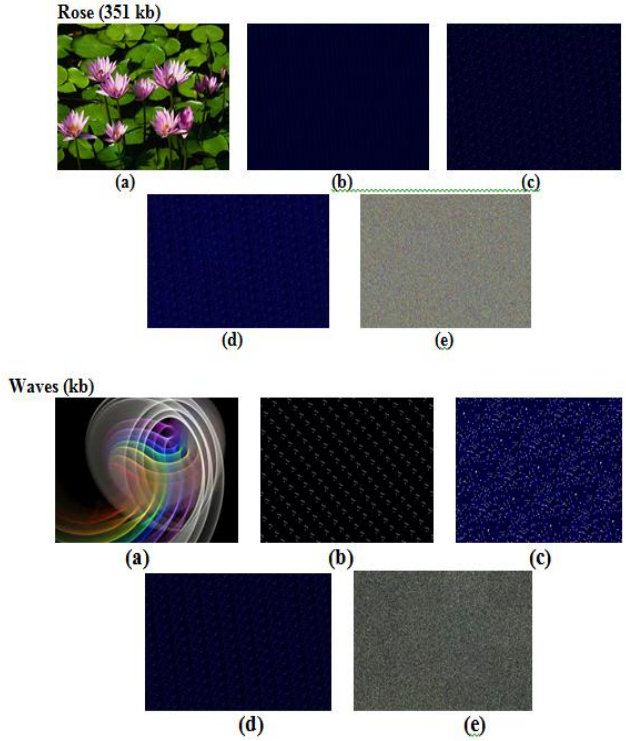

Figure7: Example on the three level security for the ciphered image.

6. TEST THE EXPERIMENTAL RESULTS

This section performing the most popular test for image cryptography and discuss the results as the following:

A. Tests the Randomness to the ciphered image

Let $S = S_0, S_1, S_2, \ldots, S_{n-1}$ be a binary sequence of length n. This subsection presents five statistical tests that are commonly used for determining whether the binary sequence s possesses some specific characteristics that a truly random sequence would be likely to exhibit. It is emphasized again that the outcome of each test is not definite, but rather probabilistic [10].

Different security levels of ciphered image are used in these tests and the results for the tests proved that the ciphered image has a random property and can be used as a secure image in a cryptography field, where the ciphered image was successes in passing all five tests and with a reasonable values for each test, so the ciphered image has a random, different , and effective values as it is illustrated in Table (1) that show the results of randomness test for three different level of the 2D image (rose).

Table 1: Randomness Test to a ciphered image in different level of randomness**.**

Test		Level 1		Level 2	Level 3	Pass Value
Frequency test		3.12		1.531	1.890	<= 3.84
Serial test		4.92		2.523	2.356	<= 5.991
Poker test		12.34		4.824	2.843	<= 43.77
Run test	T0	7.998		3.749	2.781	<= 9.488
	T1	8.423		8.187	6.562	<= 9.488
Auto correlation test		Shift1	3.372	2.103	1.845	<=3.48
		Shift2	2.114	0.856	0.126	
		Shift3	3.474	3.121	1.137	
		Shift4	2.604	1.030	0.018	
		Shift5	3.110	2.663	1.903	
		Shift6	1.396	0.842	0.604	
		Shift7	1.583	1.077	0.209	
		Shift8	1.798	1.608	0.538	
		Shift9	2.928	0.170	0.105	
		Shift10	1.380	0.407	0.318	

B. Objective fidelity criteria

The objective fidelity criteria provide equations that can be used to measure the amount of error in the reconstructed (deciphered) images or to measure the amount of error between pure image and ciphered image. Commonly used objective measures are the Mean-Square- error (**MSE)** and the Peak Signal-to-Noise Ratio (**PSNR**). If MSE tends to zero, then PSNR tends to infinity. Excellent values of PSNR range from (30 to 50 dB) [11].

In this section, the similarity between the ciphered image and the reconstructed image was tested, Table (2) shows the results of the deciphered images. The decrypted image proves that the proposed reconstructed algorithm was successes. Notice that, the small results of MSE and the large results of PSNR was indicates that the deciphered images are adequate and efficient.

Table 2:- shows the test results for reconstructed image.

Image Name	*MSE*			*PSNR*		
	R	*G*	*B*	*R*	*G*	*B*
Rose	1.0424	6.0812	2.7019	44.121	32.401	26.281
Waves	4. 6429	1.2923	3.3662	38.583	40.335	35.803

7. DISCUSSION

According the results that obtained from the popular image cryptography tests; the partial encryption time is reduced by encrypting only the part of the image and maintains a high level frequency of image. Partial encryption is a recent approach to reduce the computational requirements for huge volumes of images. Here partial image encryption scheme using plasma algorithm with fractal addition encoding approach. In this method, the approximation matrix (longest wavelength color) is encrypted as it holds most of the image's information.

The ciphering process usually repeated n times, and it is repeated just on the longest wavelength sub band. The implementation of the algorithm achieves high encryption rates; this resulting in an enhancement to the security level of the encrypted image. Another feature of the combination technique is its generality; it can be applied with any other traditional algorithm to enhance its performance. Experimental results have shown that using the combination technique with the other algorithms resulted in a better performance compared to using the other algorithms alone. Although, the method offers a good concealment of the data in the encrypted image, thus reduces the chance of the encrypted image being detected.

CONCLUSION:

This work presents a new method that combines the extracting color techniques and the image cryptography algorithm. The proposed method was encrypted all or partial of image information in order to produce image with high noise only the authorized person can see it. The randomness test of the ciphered image was very efficient, effectiveness and flexible.

REFERENCE

[1] Sapna Sasidharan, Deepu S. Philip, (September 2011), **"A Fast Partial Image Encryption Scheme with Wavelet Transform and RC4"**, International Journal of Advances in Engineering & Technology, India.

[2] Guanrong Chen, Yaobin Mao, Charles K. Chui, (December 2004), **"A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps"**, University of Science and Technology, China.

[3] Ayad A. Salam, (2005), ***"Visual Partial Encryption* Using Wavelet and Clock-Controlled Random Algorithm"**, PhD. Thesis, Ministry of Higher Education and Scientific Research in Computer Sciences.

[4] Lala Krikor, Sami Baba, Thawar Arif, Zyad Shaaban, (2009), ***"Image Encryption Using DCT and Stream Cipher"***, Faculty of Information Technology, Applied Science University, Jordan, EuroJournals Publishing.

[5] Priyanka Agrawal, Manisha Rajpoot, (March 2012), **"Partial Encryption Algorithm for Secure Transmission of Multimedia Messages"**, International Journal of Computer Science and Technology, Dept of CSE, India, Vol. 3.

[6] Harald A., Dr. Mikhail V. Mikhailyuk, (1999), **"Generation and rendering of Virtual Terrain",** Institute of Microprocessor Computer Systems RAS, International Conference Graphic, Moscow, Russia.

[7] Aman A., Raghunandan K., Dhirendra K., Asok D., **"An Application of Fractal Geometry to Design the Microstrip Circuits"**, International Conference on Recent Advances in Microwave Theory and Applications, IEEE, (2008).

[8] Nada Al-ubaidy, **"Cipher By Image Processing",** M.Sc. Thesis of Military College of Engineering, Computer Science Department, (2002).

[9] Kunag Tsan Lin, Sheng Lih Yah, (January 2012), ***"Ecrypting* Image By Assembling The Fractal Image Addition Method And The Binary Encoding Metho*d"***, University of science and Technology, Taiwan, Vol.04, No.01.

[10] Abdulwas M. Alezzani, "**Cryptography Based Cellaur Automata**", PhD. Thesis, Computer & Informatics Information Institute for Postgraduate Studies, (2004).

[11] Scotte E. U., (1998). "**Computer Vision and Image Processing :Practical Approach Using CVIp Tools**", Prentice-Hall ,Inc.