طريقة جديدة في التشفير الجزئي باستخدام تحويل الموجة الصغيرة الثنائية الابعاد

ميساء عبد علي خضر
قسم علوم الحاسبات،
الجامعة التكنولوجية،
العراق،بغداد

الخلاصة:
ان انتشار الشبكات المحلية والدولية واستخداماتها الواسعة جعل من السرية من المتطلبات المهمة ، حيث نقل الصورة عبر الشبكات والمحافظة عليها من الاختراق جعل التشفير من المتطلبات الضرورية في بناء اي شبكة اتصالات.
هذا البحث يقترح طريقة جديدة تعمل على اعتماد التشفير الجزئي ودمج تقنية ضغط الصورة حيث تتم على مرحلتين ، الاولى هو تحويل الصورة المراد ارسالها الى صورة مضغوطة بطريقة الـ 2D Wavelet Transform والوصول بها الى المستوى الثالث LL3 اي اقل حجم ممكن ثم تنفذ عليها عملية التشفير من خلال الاعتماد على توليد صورة ثنائية الابعاد ذات عشوائية عالية واعتماد كمفتاح للصورة المضغوطة .
وكانت النتائج الطريقة المقترحة مشجعة وساعدت على حل مشكلة تناقل الصورة عبر الشبكات بشكل اكثر امنية .

New Approach to Partial Cryptography Using 2D Wavelet Transform

By
Maisa'a Abid Ali Khodher
Computer Science Department,
University of Technology,
Baghdad, Iraq.

Abstract:

Computer security has to re-invent itself. New technologies and new applications bring new threats. Especially with the increasing growth of data a communication cryptography and data security are an essential requirements for communication privacy.

This paper present a new approach that combines between two technical partial cryptography and 2D wavelet transform. The process consists of two stages: First stage is to compress the image to reach LL2 and LL3. Second stage is to pass the resulting image after compression process to encryption process that uses image that has strong randomness used as a key.

The result of this approach is good and helps in solving the problem of keeping image privacy.

Key word: Image Compression, Wavelet, Random Key Generated, Partial Cryptography.

1-Introduction:

The basic design of BMP file format makes it a good general purpose format that can be used for color or black and white image storage. BMP is organized into four sections as illustrated in Figure (1) [1].

The standard structural files are used in the files as pictures for the approved use of the transfer of information networks in the local and the global task. These file are adopted in this work. The files are generally compressed, especially for both BMP and JPG. There is no damage in reconstructed public image and to accelerate and speed up the encoding picture and call for the partial encryption of the image only to maintain the structural parts of the picture and the rest of the image. The research proposes partial encryption of the image compressed using the 2D wavelet transform image of BMP.
This paper uses two types for digital images format BMP and JPG [1].

File Header
Information Header
Palette
Bitmap Data

Figure (1): BMP sections

2- Image Compression:

Image compression involves reducing the typically massive amount of data needed to represent an image. This is done by eliminating data that are visually unnecessary and by taking advantage of the redundancy that is inherent in most images. Image compression is used in computer vision system, it is included as an image processing topic because much of the work being done in the field of computer vision as this paper does uses compression process on the images that are to be examined by people [2].

Image compression has been pushed to the forefront of the image processing field. This is largely a result of the rapid growth in computer power, the corresponding growth in the multimedia market, and the advent of the World Wide Web, which makes the internet easily accessible for everyone. Compression algorithm development starts with applications to two-dimensional (2D) [2].

3- partial cryptography:

The private key is a public-key cryptosystem whose security is based on the intractability of factorizing large integers, such as RSA. While substantial work has been done in the area of partial key exposure. The aim has been to investigate the implications of inadvertent partial exposure of the private key. Instead of the potential advantages of deliberately revealing portions of the private key, significant segments of the key are made publicly available, greatly reducing the amount of data which must be securely hidden. This allows us to use biometric readings to protect the secret portion of the private key. Iris is used for recognition with error-

correcting codes for this purpose. An implementation of this system is proposed for RSA, considering the potential risks and advantages of such a scheme [4].

3.1*Cryptography*: Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.
Cryptography is not the only means of providing information security, but rather one of a set of techniques [4].

4- Image Cryptography:

The cornerstone of all privacy mechanisms is encryption, which may be viewed as the process of transforming image documents, using a secret key, into ciphered image document. Only individuals who know the key can decrypt the ciphered image document to recreate the original image documents [3].

Cryptography can provide practical solution to the protection of stored image document, in terms of both the nondisclosure of confidential images and the detection of unauthorized modification of image documents.
Image cryptography hasn't been widely studied as normal cryptography or visual cryptography. It was used by Zenon et al. [Zen97], to encode digital media (images and video) to provide confidentiality and intellectual property protection against unauthorized access.

Image cryptography is one of the fields based on both image processing and cryptography. It is concerned with ways to encrypt pictures, i.e. information which can be perceived directly by Human Visual System (HVS). Figure (2) shows the basic concept of image cryptography [3].

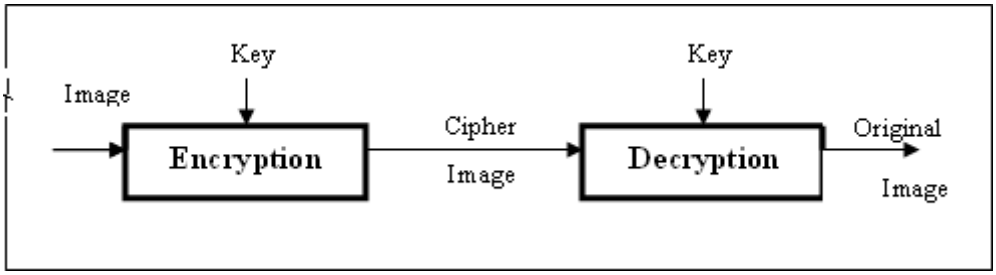


Figure (2): Image cryptography concept.

5- The Random Image Generation:

Random Art is defined as a technique that converts meaningful strings into abstract structured images. Random Art was developed by Andrej Baure, and is based on the idea of genetic art by Micheel Witbrock Mount. Originally , Random Art was conceived for automatic generation of artistic images.

Figure (3) shows an example of generated 2D- randomness digital image according the implementation in [5]. This paper uses the generated image

shown in Figure [3] to represent as a key in this work.

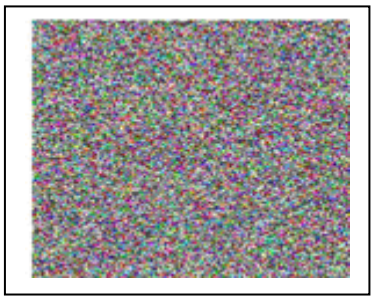


Figure (3): Example of randomness in digital image size 256×256 pixels [5].

6- 2D Wavelet Transform:

Human visual perception is known to do functions at multiple. Wavelet transforms were developed for the analysis of multiscale image structures. Unlike traditional transform domain methods, such as the Fourier transform, wavelet-based methods not only dissect singles into their component frequencies but also enable the analysis of the component frequencies across different scales. As a result these methods are more suitable for such applications as image data compression, noise reduction, and edge detection [6].

6.1 *Wavelet-Based Image Compression*:

There are two types of image compressions: lossless and lossy. With lossless compression, the original image is recovered exactly after decompression. Unfortunately, with images of natural scenes it is rarely possible to obtain error-free compression at a rate beyond 2:1. Much higher compression ratios can be obtained if some error, which is usually difficult to perceive, is allowed between the decompressed image and the original image. This is lossy compression. In many cases, it is not necessary or even desirable that there be error-free reproduction of the original image [7].

6.2 *Lossy Compression*:

The proposed approach in this paper concentrates on the following method of lossy compression: DWT (Discrete Wavelet Transform)[7].

Quantizing refers to a reduction of the precision of the floating point values of the wavelet transform, which are typically either 16 or 32 or 64 bit floating point numbers.

To reach less bits in the compressed transform which is necessary if compression of 8bpp or 12bpp images is to be achieved these transform values must be expressed with less bits for each value. This leads to rounding error. These approximated, quantized, wavelet transforms will produce approximation to the images when an inverse transform is performed. Thus creating the error inherent in lossy compressed see image compressed in Figure (4) and image decompressed in Figure (5) [7].

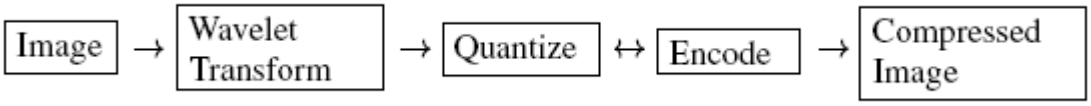


Figure (4) Compressed Image

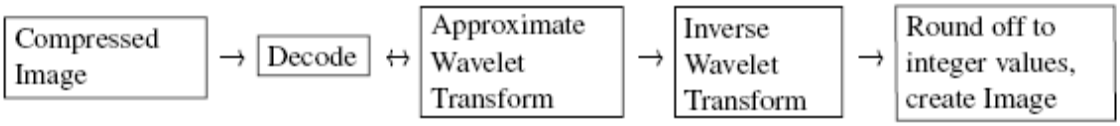


Figure (5) Decompressed Image

6.3 *Wavelet Thresholding:*

The application of wavelet-based methods to image enhancement has been studied extensively. A widely used technique known as wavelet thresholding performs enhancement through the manipulation of wavelet transform coefficients so that object signals are boosted while noise is suppressed. Wavelet transform coefficients are modified using a nonlinear mapping. Hard-thresholding and soft- thresholding functions are representative of such nonlinear mapping functions [6].

$$\begin{aligned} &\text{if } X > T \quad \text{then } X - T \\ &\text{if } X < -T \quad \text{then } X + T \qquad (1) \\ &\text{if } |X| \le T \quad \text{then } 0 \end{aligned}$$

Small coefficients (below thresholding T or above –T) normally corresponding to noise are reduced to a value near zero. Usually, the thresholding operation of Equation (1) is performed in the orthogonal or biothorgonoal wavelet transform domain [6].

6.4 *Example :*

This section illustrates in simple way the steps for wavelet transform at two levels and three levels for simple digital image. Figure (6) shows wavelet transform process.

1	2	5	8	17	24	25	32
3	4	6	7	18	23	26	31
9	10	13	14	19	22	27	30
12	11	15	16	20	21	28	29
33	34	35	36	49	50	54	55
40	39	38	37	51	53	56	61
41	42	43	44	52	57	60	62
48	47	46	45	58	59	63	64

1	2	5	8	17	24	25	32
3	4	6	7	18	23	26	31
9	10	13	14	19	22	27	30
12	11	15	16	20	21	28	29
33	34	35	36	49	50	54	55
40	39	38	37	51	53	56	61
41	42	43	44	52	57	60	62
48	47	46	45	58	59	63	64

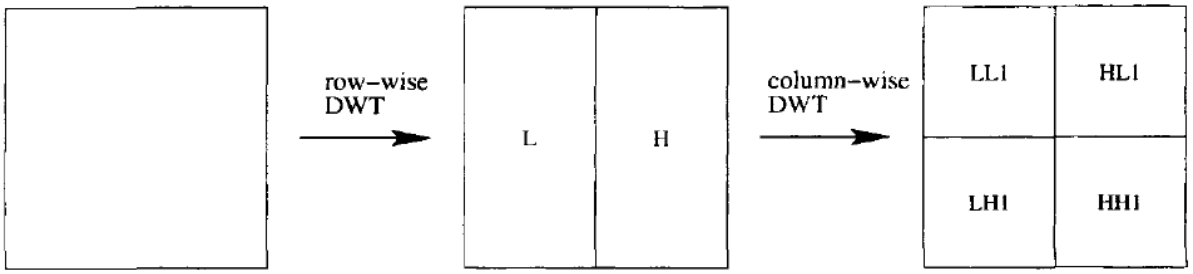
16 Parts of Images (2-level) **32 Parts of Images (3- level)**

Figure (6) Wavelet transform

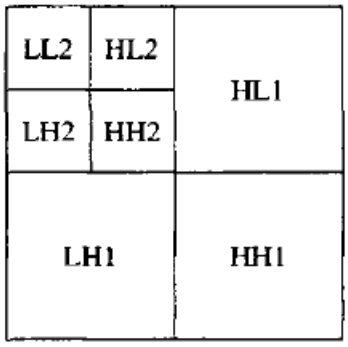
7-The Proposed Algorithm:

The image is compressed by 2D wavelet transform into four parts. In the first level, as shown in Figure (7), the upper part on the left hand is taken and then the image is compressed and the image is reduced and divided into sixteen parts in two levels. Then the upper part on the left is taken and the image is, compressed, as shown in Figure (8-a, b). The compressed image is encrypted with the encryption key and the encryption key is encrypted on the image above to clarify the method of encoding the image. It is clear that the size of the image encoded is as small as possible to be sent through the Internet and your network up without losing the features of the full picture as shown in Figure (9-a).

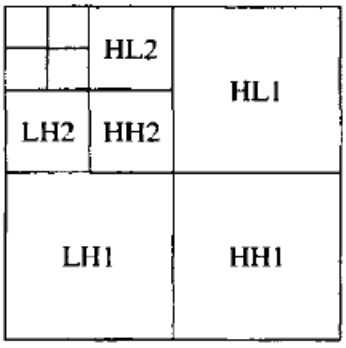
When the picture becomes similar to the image it is divided into 32 parts in three levels and the compressed part is encrypted with the encryption key as in Figure (9-b) which shows that the size of the sent image is as small as possible without loss of image. The transmitted image can be recovery the key after the return of the compression as a picture, upon receipt of image.



First Level Decomposition



Two Level Decomposition



Three Level Decomposition

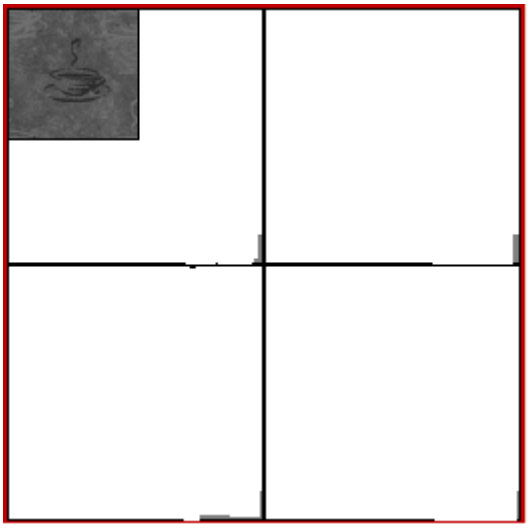


Image compression in four parts (level one)

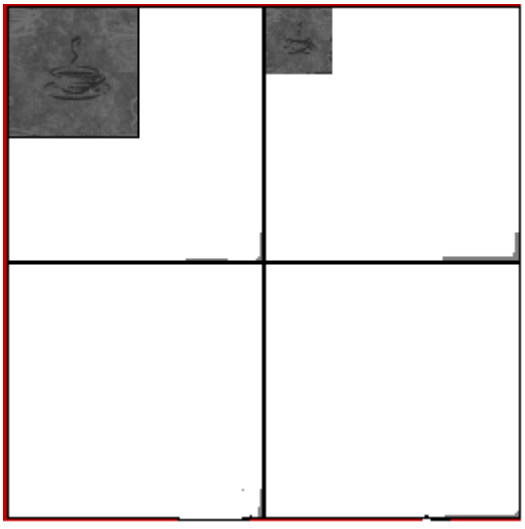


Image compression in sixteen parts (level two)

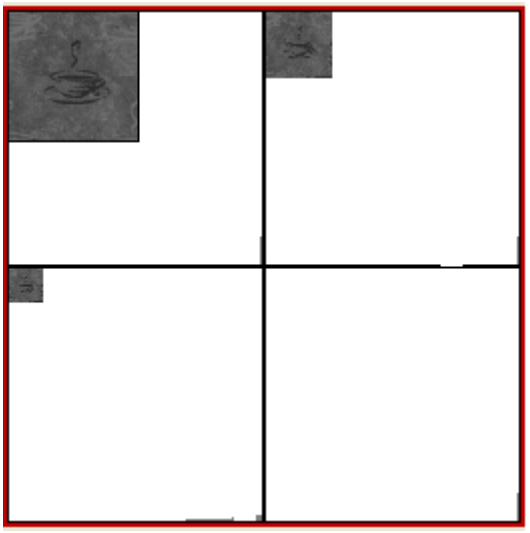


Image compression in thirty two parts (level three)

7.1 Compressed Image Encryption Algorithm:

Input: Compression picture (A), key (generated image).
Output: Cipher image

Process

Step 1: Initial

A= Load Compressed picture.
K= Key (generated Image)

Step 2: supply result of image of the colors RGB

For I = 1 to (image compressed -1)/12
For j = 1 to (Key -1)/12

If R1<0 Then R=0
If G1<0 Then G=0
If B1<0 Then B=0

If R2>255 Then R=255 (Key Generated)
If G2>255 Then G=255 (Key Generated)
If B2>255 Then B=255 (Key Generated)

Step3: Add

Add (R1 with R2)
Add (G1 with G2)
Add (B1 with B2)

Step4:

Put the Result of Add encrypted picture in C
End

7.2 Application:

- **Applied Algorithm in picture**

Example one:

 **XOR**  **=** 

Random image generated XOR image 16 parts = cipher image 16 parts

Example two:

 **XOR**  **=** 

Random image generated XOR image 32 parts = cipher image 32 parts

<u>Time Implementation of Image Encryption:</u>

- **There is a difference in the time of partial encryption of the original image and compressed images time is calculated as in Table (1)**

Number	Name of image	Time encryption
1	Original image	6 second
2	Image compression of 16	4 second
3	Image compression of 32	2 second

Table (1) Time of image encrypted

8- <u>Conclusion:</u>

The image to be transmitted is compressed to reduce the size to keep the general structure of the image of BMP, JPG and it is better in image that are to be to sent to be compressed. Partial encryption gives the fastest transmission because where only one part is used in the encryption and sending pictures over the network.

Images are encoded before transmission because encryption of the compressed image is less than the original image and the strength of encryption is also better for the compressed image of the picture for non-appearance of the original features of the image and the resulting image is clearer.

References :

1- Murray L. D., and Vanryper W., " Encyclopedia of Graphic File Formats ",O,' Reilly And Associates, Inc, 1994.

2- Scott E. Umbaugh, "Computer Vision and Image Processing", Prentice. Hall PTR, 1998.

3- Dhamija Rachna, "*Hash Visualization in User Authentication*" in proceedings of the Computer Human Interaction Conference, 2000.

4- Bruce Schneier "Applied Cryptography", john wiley and sons , 2008.

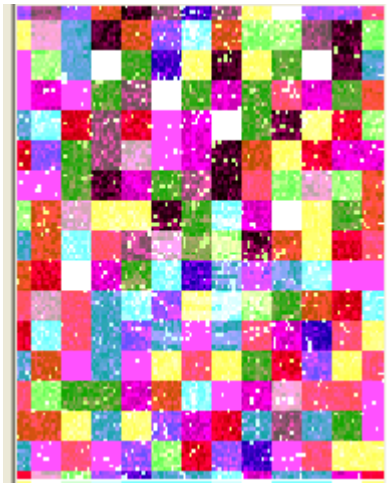
5- Hilal. M. Y. , Monem. R. Hala. (2007), "Using Generated Digital Images to Modify the PGP Cryptography Protocol", International Conference on Security and Managemeny "SAM'07",USA, LasVagae,2007.

6- Qiang wu, Fatima Merchant, Kenneth R. Castleman "Microscope Image Processing", Elsevier Inc , 2008.

7- Rao K. R. and Yip P. C. Ed., "The Transform and Data Compression Handbook", Boca Raton, CRC Press LLC, 2001.

Implementation of system:

Original Image



Cipher Original Image

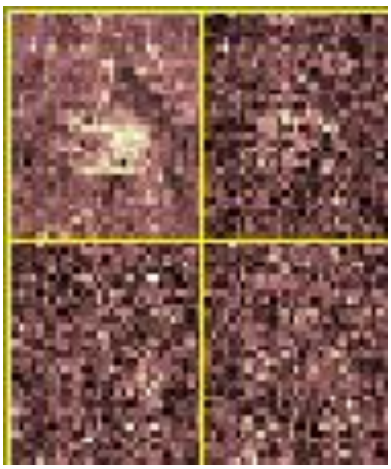


Figure (7) 16 Parts of Image Wavelet Transform

Figure (8-a) Wavelet Transform of Image 16 parts

Figure (8-b) Cipher Wavelet Transform of Image 16 parts

Figure (9-a) Wavelet Transform of Image 32 parts

Figure (9-b) Cipher Wavelet Transform of Image 32 parts