Partial Encryption of Wavelet Compressed Images

Dr. Ayad A. AbdulSalam
College of Education for Women
University of Baghdad.
Baghdad, Iraq
e-mail: ydsalam@yahoo.com

***Abstract*--This work focuses its goal on the reduction in computational cost for image encryption. Bit selection for partial encryption is applied in this paper to show haw can match applications requirements without the overhead of full encryption. The suggested encryption process can be performed during the image compression process, which is based on wavelet transform. The technique is built to reduce the encryption time and keep the compliant with the wavelet format. Histogram of encrypted image used to determine the quality of partial encryption, without the need to compare with original one.**

Keywords-compression; bit selection; partial encryption; histogram; wavelwt transform.

I. INTRODUCTION

Many digital services, such military imaging systems, satellite imaging, medical imaging (digital radiography), digital broadcasting and scientific visualization, all need data compression in order to cope with high memory requirements. On the other hand, people want to keep the contents of their communications private and require reliable security in storage and transmission of digital images. With the rapid progress of Internet in the digital world today, the security of digital images has become more and more important.

There are many legitimate reasons to protect, sometimes to protect fundamental rights, sometimes because law requires it, sometimes to protect some businesses, etc. The way to get such protection is to encrypt the data and the usual approach is to encrypt everything **[1]**. This approach is good in many cases, but not in all: sometimes (computing) resources are a scarce resource and one has to make concessions: use the available CPU power for a better compression and ignore the encryption problem, or invest more CPU time for better encryption and live with slightly degraded compression quality. In such cases, partial encryption can be a solution for the problem, since it tries to solve both problems at the same time.

II. THE AIM OF USING EXPONENTIAL DISTRIBUTION

Basing on the fact, that the effect of changing only the Most Significant Bit MSB of Quantization index QX is greater than the sum of effects of changing all the other bits, so as the effect of each bit is greater than the effects of bits which are followed. This fact lead us to proposed a selection method based on exponential random distribution to enforce the selection of MSBs more frequently than other bits, to guarantee that the most significantly bits should high probable chosen and least significant bits has a low probability, but not 0%. At the same time, the proposal is based on dynamic selection which adds more complexity to increase difficulties on analysis effort dramatically, and to prevent the fix located chosen.

To implement the exponential random distribution, the probability values for each bit selection are plotted as a pie chart (clockwise, starting at 12:00); the values of selected bits are represented by the size of the pie slices, sum of these slices values are 360 degree, the distribution was based on exponential function:

$$d_n = r.s^n \tag{1}$$

where (r, and s) are distribution parameters. Changing the values of distribution parameters will change the chosen bits probabilities. For example, increasing the value of weight (s) will increase the difference gab between every two adjacent bits probabilities, on the other hand, increasing the value of (r) will increase the first bit probability, so the tradeoff between these two values is very important to reach balanced probabilities, the values of (r) depend on value of (s) as the following:

$$r+ rs+ rs^2+ rs^3+ rs^4+ rs^5+rs^6+ rs^7=360 \tag{2}$$

$$r(1+ s+ s^2+ s^3+ s^4+ s^5+s^6+ s^7)=360 \tag{3}$$

$$r = \frac{360}{1+s+s^2+s^3+s^4+s^5+s^6+s^7} \tag{4}$$

$$r = \frac{360}{\sum_{n=0}^{7} s^n} \tag{5}$$

in this work the value of (r) was taken *5*, and (s) depends on the needed weight, here we chose *1.5* , while n is number of bits per byte (0-7), the calculated values are listed in Table I, the shape of pie wheel distribution is shown in Fig.1.

TABLE I. CHOSEN BITS PROBABILITY

Bit	0 LSB	1	2	3	4	5	6	7 MSB
Percent	2 %	3 %	5 %	7 %	10 %	16 %	23 %	34 %

978-0-7695-4959-0/13 $25.00 © 2013 IEEE
DOI 10.1109/ACSAT.2012.80

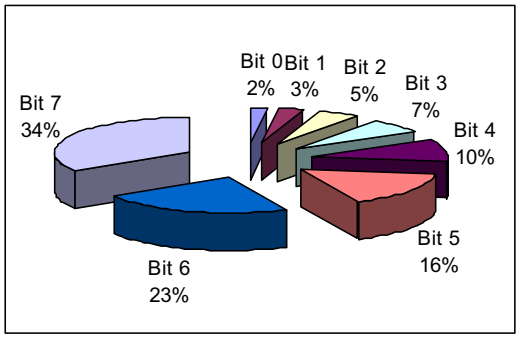

Figure 1. Exponential Distribution.

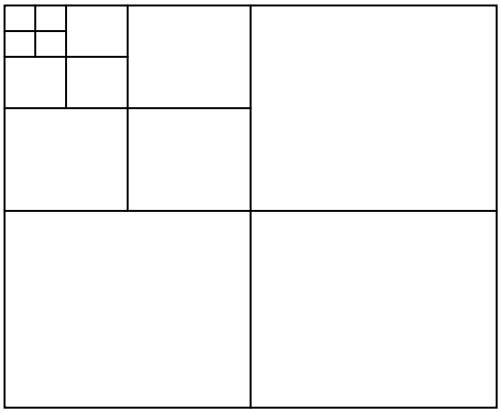

Figure 3. Wavelet subband results for 4-level 2DDWT.

III. DESCRIPTION OF PROPOSED PARTIAL DATA SELECTION

In this section, the proposed selective partial image encryption scheme is illustrated; the encryption scheme is invoked during the image compression process, the encryption being performed between the quantizer and the entropy coder stages [2]. A data bit selection scheme has been used as part of the partial encryption scheme. Most of the image encryption researches insist that image compression and encryption should be combined or performed simultaneously [3]. Also, due to the processing time and computational power requirements, only part of the image data should be encrypted. The proposed scheme can enable a trade-off between the effectiveness of the encryption method and the cost of using the method.

The most typical image compression schemes based on discrete wavelet transform (DWT), is based on utilizing the bi-orthogonal wavelet transform **[4]**. Also some other coding schemes (like, scalar quantization, and entropy coding) are used in the compression stage and the decompression stage for image reconstruction, as depicted in Fig. 2.

Reversible 5/3 bi-orthogonal filter, DWT transform was used in this work. A uniform scalar quantizer was used and only Huffman coding is included for entropy coding. 4-level 2-dimensional DWT was adopted in the current work, and the produced subband will distribute as those shown in Fig.3. In the figure, XY*i* is used as the subband notation, where X

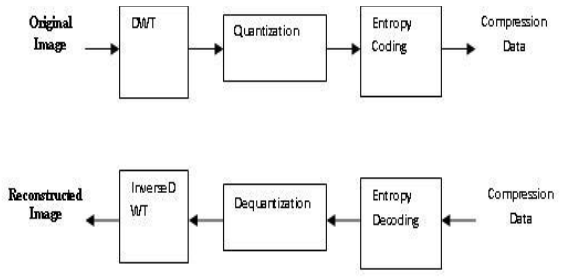

Figure 2. Image compression and reconstruction procedure.

and Y are either L or H, which represents the filters result produced by applying either the low pass filter or the high pass filter in both directions (horizontal and vertical), and *i* represents the current DWT level. Also, we assume an image which consists of Wid×Hgt pixels, and each pixel is expressed by 8 bits for each of its colour components (R, G, B).

Without losing generality, the resulting Wavelet Coefficients (WC) in LL4 (the lowest subband called approximation coefficients) take values between 0 and 255 and the WC in other subband take values between –255 and 255. In the quantization, usually LL4 is not quantized, because it includes very important information that can't be lost **[5]**. But other sub-bands are quantized, later in terms of their quantization indices QXs, the values of the produced quantization indices depend on the bit assignment for the particular subband. In this work the encryption is performed on the image data after quantization, because after quantization all coding processes will be reversible and all the information (i.e., quantization indices) are exactly retained in the decoding stage.

The image encryption scheme in this work is a selective and partial encryption. The most important challenge of our scheme is how to select a part of image data for encryption. We propose the following selection scheme.

IV. RANDOM SELECTION OF WAVELET COEFFICIENT

Selecting data in this work is a random selection of wavelet coefficients to be encrypted. Usual situation for encryption is that all the details of the scheme are known to the public and the security is stemmed from the secrecy of the encryption key. But because the target content is image, the amount of encryption could be so excessive such that the processing cost might be unacceptably high, if all the quantization results are encrypted **[6]**. The purpose of this work is to enhance maximal encryption gain with minimal amount of encryption. In this sense, we add random selection scheme to allocate the positions of the QXs to be encrypted. MSB of a certain QX has the following property:

If a WC consists of m bits $a_0a_1a_2 \cdots a_{m-1}$ (a_0 is MSB, a_{m-1} is LSB), the weight of bits ($W(ai)$) has the property of,

$$W(a_0) > W(a_1) + W(a_2) + .. + W(a_{m-1}) \quad (6)$$

This will match the fact that the effect of changing MSB only is greater than the sum of effects for all the other bits. Also, the effect of encrypting additional bits beside to MSB does not significantly increase the distortion as much as the computational cost increase.

To exploit these differences of changing WC effectiveness, seven bits from random generator are used as a random number sequence (actually pseudorandom number sequence), to assign the area in pie wheel which point to a specific bit of the encrypted coefficient, taken into consideration the generator highest probability is for the MSB (as 34%), while for the 7th bit it is 23%, 6th bit is 16%, 10%, 7%, 5%, 3%, and 2% for LSB.

Most of researches and literatures considered the Peak Signal to Noise Ratio (PSNR) as the main measure to determine the coding effects whether the coding scheme is for lossy compression or for encryption **[4,7]**; but we can notice that for encryption considerations PSNR cannot be a good measure to estimate the encryption effects, this could be proved in simplified way by subtracting a fix value from each pixel of Lena image (such as 50), and then calculate the PSNR value as a distortion measure between the original image and the result image after subtraction, it will be found that its value is 7.44 dB, which indicates a high distortion, but in fact the details of the image is still clearly visible with some colour differences, as shown in Figure (4). Other example, changing of colour regions by mapping, making PSNR indicate a high distortion, while the details of mapped areas will not disappear by changing colours.

The most important image attributes that should be successfully removed during image compression is the spatial correlation. Due to this attribute some well known simple encryption methods (like substitution) fails to encrypt images. So, the measures used to evaluate the performance of any visual encryption method should be based on the existing spatial correlation in the original image and its version after encryption.

Figure 4. Lena with pixels difference value of 50.

To determine the spatial correlation, different types of measures were mentioned in the literatures, the most important one is the co-occurrence matrix **[8,9]**. But in this research work, the degree of spatial correlation is determined by using the features of the histogram of the difference values between the adjacent pixels, because the difference between neighbour pixels reflect the simplest (primitive) kind of spatial correlation that may exist, and the disappearance of such feature will insure the disappearance of other (higher) spatial correlations that may exist.

The difference values (Δ) of any image pixel could be determined by subtracting the pixel value from its previous pixel,

$$\Delta_{i,j}=W_{(i,j)}-W_{(i-1,j)} \quad (7)$$

$$\Delta_{i,j}=W_{(i,j)}-W_{(i,j-1)} \quad (8)$$

Once the histogram of Δ-values is determined, it will be concentrated around the 0-value because most of the image pixels have close similarity in their values.

Now, we have to test 512x512 pixels image to be given in 24bit/pixel (bpp) precision. We consider the 8bpp data in the binary representation for each colour component. The selective encryption approach is to encrypt a subset of the compressed data only, and we construct a difference matrix by subtracting each pixel value with the previous one, and then calculate the frequency of occurrence of each possible value of $\Delta_{i,j}$, the values will be from –255 to 255. Before the encryption, it is easy to see that most of the differences are small, and more frequently occurred values are 0 and other low values; only a few are outside the range [-30,+30], because most of the adjacent pixels are similar in their color. From the histogram in Fig.5, it is obvious that the percentage of values out of [-30,+30] is only 19.8%.

The selection of bits discussed in this section depends on pie wheel distribution. Each possible subset of bits may be chosen for selective encryption, however, the minimal percentage of data to be encrypted is 12.5 % of the compressed data, increasing in steps of 12.5 % for each encrypted additional bit. The encrypted bits are transmitted together with the remaining bits in plain text. And the reconstructed Lena image after selectively encrypting 1, 2,… 8 bit(s). Whereas in the case of encrypting one bit only some structural information will remain, while encrypting

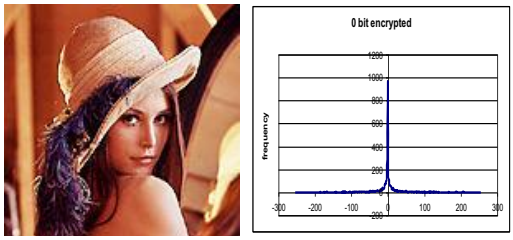

Figure 5. Histogram of difference matrix without encryption.

three bits leaves no useful information in the reconstructed image. It is important to notify the selective encryption should randomly select the bits of the coefficients but with the condition that the most probable selected bit is the MSB.

.

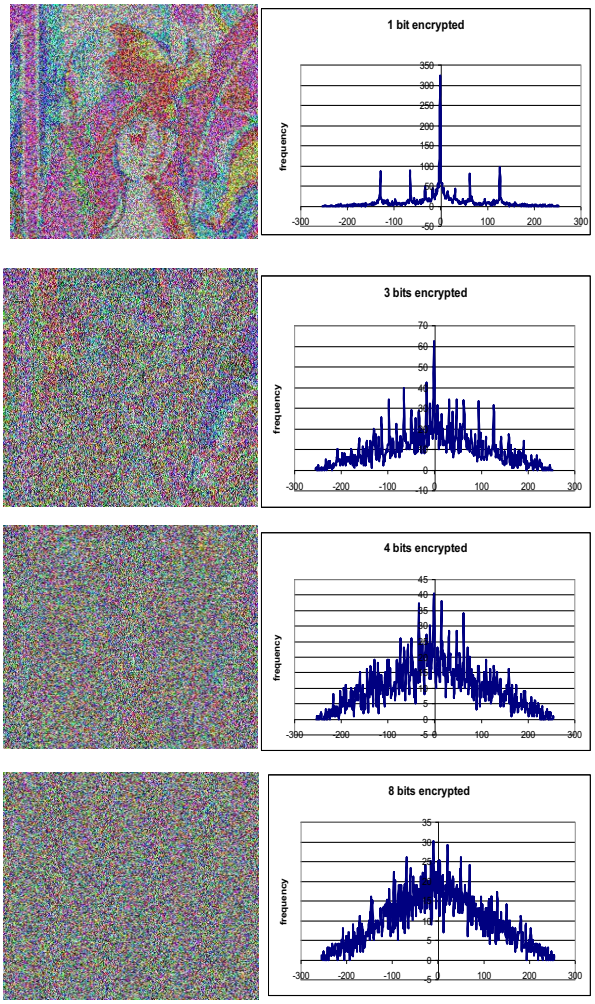

Figure 6. Histogram of difference matrix with x-bits encryption.

By comparison the histogram of difference matrix illustrated with each image, we can notify that in one bit encryption histogram the percentage of values out of [-30,+30] is 55.9%, while in image without encryption was 19.8%. the percentage of value of encryption two bits is 70.1%, three bits is 75.6%, 76.4%, 77.3%, 78.8%, 79.1%, and 79.4% for eight bits encrypted. That is obvious that the amount of encrypted data increases as more WCs are selected, and the difference between adjacent WCs is rapidly increased

REFERENCES

[1] Andreas Pommer and Andreas Uhl. “Application scenarios for selective encryption of visual data”. In Proceeding of Multimedia and security Workshop of 10th ACM International Conference on Multimedia, 2002.

[2] Andreas Pommer and Andreas Uhl. “Selective Encryption of Wavelet-Packet Encoded Image Data,” to appear in ACM Multimedia Systems Journal, Special Issue on Multimedia Security in 2003.

[3] Andreas Pommer “Selective Encryption of Visual Data”, doctorate dissertation submitted to University of Salzburg, college of Engineering, 2003.

[4] Marc Van Droogenbroeck " Partial Encryption of Images for real-time applications". In proceeding of the 3rd IEEE Benelux signal processing symposium (SPS 2003), Leuven, Belgium, 2003.

[5] Philip P. Dang and Paul M Chan “Image encryption for Secure Internet Multimedia Applications” IEEE Trans. Consuming Electronics, vol. 103, 2000.

[6] Xiling Liu, “Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions”, proceeding of International Conference on Computer Communications and Networks, Las Vegas, September 20-23, 2003.

[7] Young-Ho Seo, Dong-Wook Kim, Ji-Sang Yoo, Sujit Dey, and Abhishek Agrawal, “Wavelet Domain Image Encryption by Subband Selection and Databit Selection”, research introduced to Department of Electric and Computer Engineering, University of California, San Diego, USA, 2003.

[8] Mizuki Oka, and Tomoyuki Koiso, “Extracting Features Using the Eigen Co-occurrence Matrix Algorithm”, University of Colorado, Science and Technology Magazine, September 2006.

[9] Nidhi Taneja, “CHAOS Based Partial Encrytion Of SPIHT Compressed Image”, International Journal of Wavelets, Multiresolution and Information Processing, Volume 09, Issue 02, March 2011.