WAVELET DOMAIN IMAGE ENCRYPTION BY SUBBAND SELECTION AND DATA BIT SLELECTION

[*]Young-Ho Seo, [*]Dong-Wook Kim, [**]Ji-Sang Yoo, [***]Sujit Dey, [***]Abhishek Agrawal
[*]Dept. of electronic Materials Eng., Kwangwoon University
[**]Dept of Electronic Eng., Kwangwoon University
447-1 Wolgye-Dong Nowon-Gu
Seoul, 139-701 South Korea
[***]Dept of Electric and Computer Eng., University of California at San Diego
9500 Gilman Dr.
La Jolla, CA 92093

ABSTRACT

Widespread popularity of wireless data communication devices, coupled with the availability of higher bandwidths, has led to an increased user demand for content-rich media such as images and videos. Since such content often tends to be either private, sensitive, or paid for, there exists a requirement for securing such communication. However, solutions that rely only on traditional compute-intensive security mechanisms are unsuitable for resource-constrained wireless devices.

In this paper, we propose a selective partial image encryption scheme, which enables a trade-off between the effectiveness of the encryption method and the cost of using the method. The encryption scheme is invoked during the image compression process, with the encryption being performed between the quantizer and the entropy coder stages. Three data selection schemes have been used as part of the partial encryption scheme: subband selection, data bit selection, and random selection of pixel data.

The experimental results for over 500 test images reveals that the fraction of data to be encrypted with our scheme is between 1/4,096 and 1/256 and the PSNRs are between about 9.5dB to 7.5dB. Since the encryption cost is very low and the effectiveness is good, the proposed scheme can potentially be used to provide secure communications in a variety of wired/wireless scenarios.

I. INTRODUCTION

Recent trend in wired/wireless communication has been to include multimedia content such as video, image, voice, music, text, etc. Especially, image and video contents are preferred because of the very information-implicative property. However, they require a large communication channel capacity due to their data-intensive nature. Thus, for last few decades, most research and development has focused on reducing the amount of data needed for images and videos.

The most famous and widely used ones are MPEG series[1]. Recently, wavelet-based image processing techniques[2] have been widely researched as a replacement for the image compression of MPEG still image. The techniques are known to overcome the blocking effect in MPEGs and provide a better image quality than JPEG for the same compression ratio.

Widespread use of image and/or video contents in wired and wireless communication imposes an additional cost on providing such content. In general, as a large number of images tend to contain private/sensitive information or can be contents for which the users have paid for, ensuring secure communication of such data is necessary. The solution to this problem involves content-encryption[3]. In this area also, the research on MPEG series has led the way and much work has been done[4]~[6]. But for wavelet-based image processing, most of the methods for MPEGs cannot be applied because of the difference in the processing scheme. Lots of recent research[7]~[12] has focused on image encryption techniques for wavelet-based image processing. Because this paper focuses on the wavelet-based image processing, only the research in this area is reviewed.

Most of the research work for image encryption insists that image compression and encryption should be combined or performed simultaneously. Also, because of processing time and power, only part of the image data should be encrypted. In [7], two partial encryption schemes for different techniques have been proposed. For quadtree[14] encryption, the quadtree structure including block and number of bits to represent a leaf were encrypted, while for SPHIT coding scheme, two highest iteration results were encrypted. The encryption rates for quadtree scheme and SPHIT scheme were about 13~27% and 2%, respectively. In [8] and [9], a special wavelet transform, non-stationary multi-resolution analysis (NSMRA) was assumed and the used filters[8] or tree structure[9]was encrypted. Some of the researches have targeted on the results from arithmetic coding which is one of the entropy coding methods. [10] used the method to encrypt the probability models and [13] improved it. [11] also assumed a zero-tree quantization (EZW) method. It proposed a method to ATM-packetize and encrypt the resulting data from EZW. The amount of encryption in this work is the same amount of data after compression. The work in [12] didn't assume any transformation. It encrypted the row image data itself. Instead, it encrypted a certain bit-plane(s) so that the minimum amount of encryption was 1/8 of the original image data.

This paper focuses its goal on the reduction in computational cost for image encryption, especially for use in wireless communication. The encryption process in this paper is also performed during the image compression process, which is based on wavelet transform. The data to be encrypted is the one resulting from quantization for which this paper uses a common linear quantizer. The encryption scheme in this paper includes several methods which have the property of trade-off between computational effects and computational cost (amount of encryption is between 1/4,096 and 1/256 of the original image data). Thus, the scheme to be proposed can be used as the network-aware adaptive scheme as well as the cost-effective image encryption scheme. As the encryption algorithm, we assume one of the secret-key block cipher algorithms, such as DES, 3DES, AES, etc.

II. PROPERTIES OF DWT AND THE RESUTING DATA

Before the contents of the proposed scheme are explained, we point out some of the properties to be used in our image encryption. Typical image compression procedure based on wavelet transform can be depicted as shown in Fig. 1, that is, DWT(Discrete Wavelet Transform), quantization, and entropy coding for compression and the reverse process for image reconstruction. We used the (9,7) Daubechies' bi-orthogonal filters for DWT. A fixed linear quantizer was used and only Huffman coding was included for entropy coding. We assumed 4-level 2-dimensional DWT(2DDWT) in DWT process and the result is shown in Fig. 2. In the figure, XY*i* is used as the subband notation, where X and Y are L or H which represents the filtered result from low pass filter or high pass filter, respectively, and *i* represent the current DWT level. Also, we assumed an image consists of 512×512 pixels and gray-level of each pixel is expressed by 8 bits. Here in this paper, only gray-level information is considered because of its importance in human eyes.

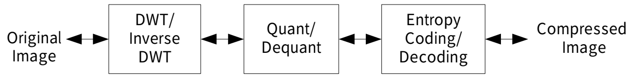


Fig. 1. Image compression and reconstruction procedure

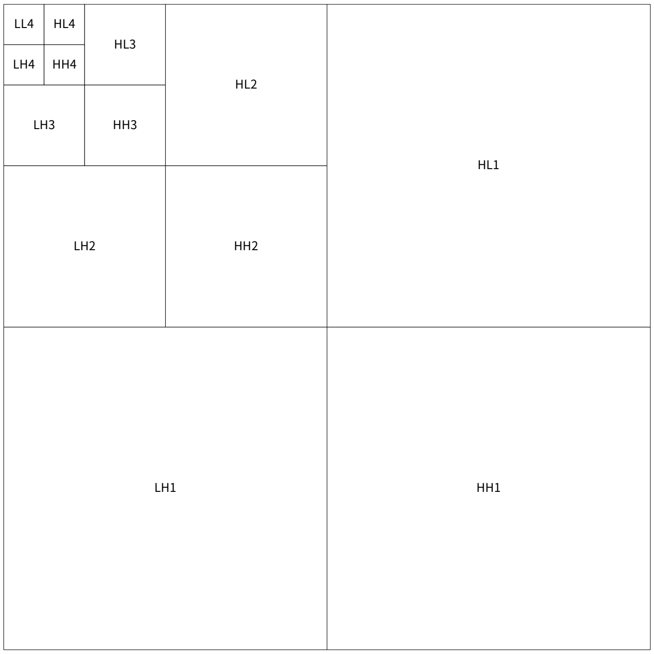


Fig. 2. Decomposed result from 4-level 2DDWT

Without losing generality, the resulting wavelet coefficient (WC) in LL4(the lowest subband) takes a value between 0 and 255 and the WC in other subband takes a value between –255 and 255. In the quantization, usually LL4 is not quantized because it includes the information too important to lose. But other subbands are quantized to be symbols(quntization indices, QXs) which are dependent of bit assignment for a particular subband. Those QXs no longer have quantitative information for the corresponding WCs. The entropy coding cannot disturb any information because it is lossless coding.

For image encryption, this paper chooses the data after quantization because after quantization any information is retained for the further processing. Because of the property of block cipher[3], changing 1 bit in ciphertext can ruin the whole decrypted plaintext.

III. PARTIAL ENCRYPTION FOR IMAGE

The image encryption scheme in this paper is a selective and partial encryption. The most important component of our scheme is how to select the part of image data for encryption. We include three selection schemes which are as follows.

III-1. Subband Selection

Among the subbands in Fig. 2, LL4 includes most of the energy contained by the original image. Thus it retains the most important information for human eyes. Most of the previous works for DWT noticed that with only LL4, a large amount of image information can be extracted. Thus, to hide the image information, the information in this subband must be hidden.

But encrypting only LL4 may reveal higher frequency information such as edge components and it can be used to infer useful information, although the importance of it depends on the application area. Thus, a certain amount of high frequency information is required to be hidden to increase the security. For the higher frequency information, we don't have to include a lot of it because the original image usually contains much redundancy. For example, the information in level 1 is hardly recognizable by human eyes.

Thus, we consider 4 combinations of subbands as follow;

① LL4 : only LL4
② LL4-HH4 : LL4 and HH4
③ Level 4 : all four subbands in level 4
④ Level 4-HH3 : all subbands in level 4 and HH3

III-2. Data Bit Selection

The amount of encryption could be so excessive that the processing cost might be unacceptably high if all the results from quantization are encrypted. The purpose of this paper is to enhance maximal encryption effect with minimal amount of encryption. In this sense, this paper chooses only one bit per QX, which is the MSB.

For LL4 which is usually not quantized, MSB of a certain QX has the following property. If a WC of LL4 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($W(a_i)$) has the property of,

$$W(a_0) > W(a_1) + W(a_2) + \cdots + W(a_{m-1}) \qquad (1)$$

It means that the effect by hiding MSB only is greater than the sum of effects for all the other bits. Also, encryption effect by encrypting additional bits to MSB does not increase as much as the computational cost increases.

But for other subbands, the value of QX is not necessarily related to the magnitude of the corresponding WC, which depends on how to assign the symbols to the quantization bins. Thus MSB of a QX cannot be said that it is the most significant bit. Changing MSB of a QX can be considered as the change of corresponding quantization bin in a random fashion.

III-3. Random Selection of Pixels

The last scheme of selecting data taken in this paper is random selection of pixels to be encrypted. Usual situation for encryption is that all the detailed of the scheme is known to the public and the security is stemmed from the secrecy of the encryption key. But because the target content is image, we add random selection scheme to hide the positions of the QXs to be encrypted. For this, we used a Linear Feedback Shift Register (LFSR) as a random number generator (actually pseudorandom number generator) which is shown in Fig. 3.

When an LFSR with *n* stages is used, the maximum length of the generated sequence is 2^n-1 if the feedback characteristic polynomial is primitive[16]. Also, if the number of stages is large enough with primitive feedback characteristics, the probability for a bit in the output sequence to be '1' or '0' is almost the same as 1/2. LFSR also has the property that different initial value produces different order of sequence. By using *n* bits from the secret key for encryption as the initial value of LFSR, the output sequence cannot be anticipated.

The way for this paper to use this LFSR is as follows. This paper uses the serial output of the LFSR. Each bit of the output sequence is one-to-one matched to each QX in a subband chosen for encryption. If the LFSR bit is '1'('0'), the corresponding QX is included(excluded) in(from) encryption. From this scheme, only 1/2 of QXs in a particular subband are encrypted.

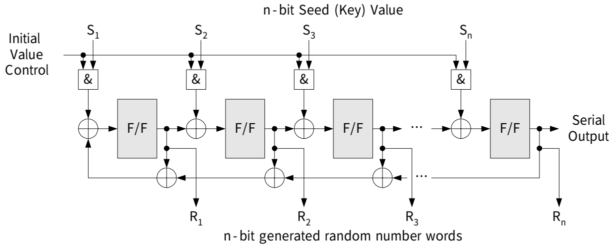


Fig. 3. LFSR for random number generation

III-4. Encryption Procedure

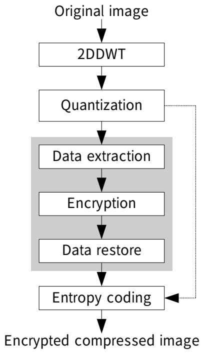


Fig. 4. Encryption procedure

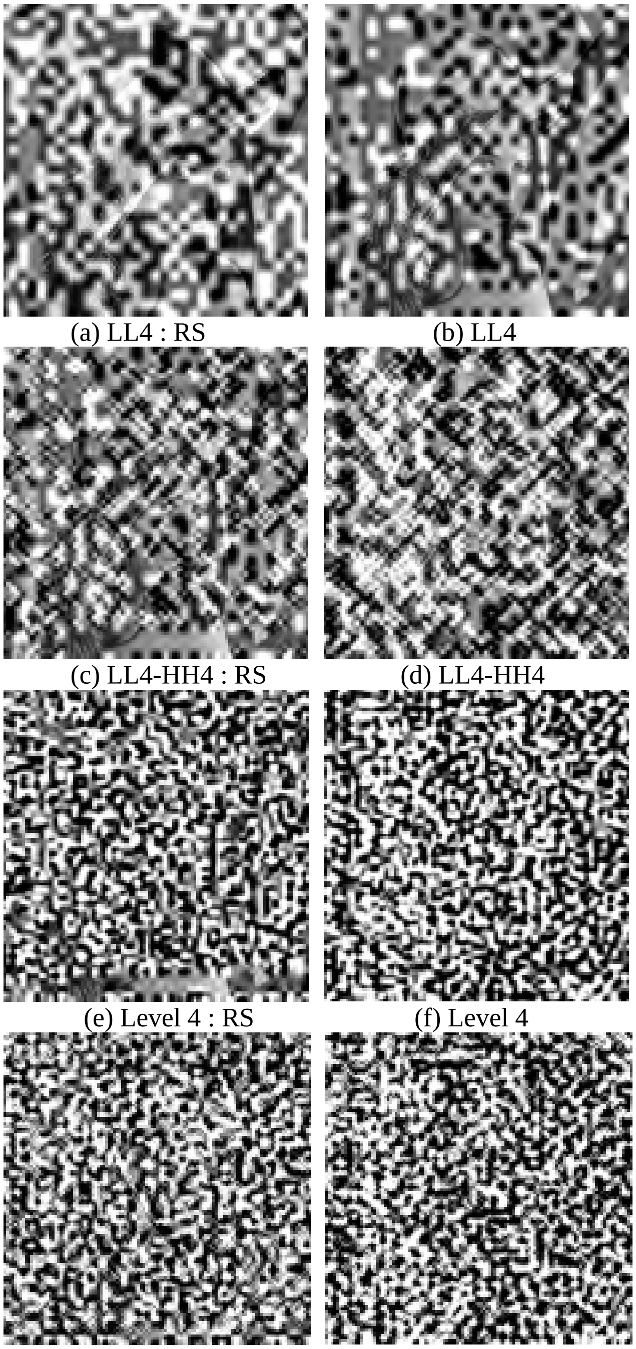
With the selection schemes above, the encryption procedure is shown in Fig. 4. Because a block cipher algorithm was assumed to be used, the data selected by the above selection schemes needs to form encryption blocks. In this paper, 128-bit cipher block is assumed. First, the selected data is extracted from memory. Then, the data forms cipher blocks and the encryption is performed as the unit of block. The resulting encrypted data is restored to the extracted positions.

IV. EXPERIMENRAL RESULTS

The encryption methods explained so far have been implemented with C/C++ language(but they are not optimized) and have been applied to more than 500 images. In this chapter, we characterize the proposed methods with the average values for the whole applied images.

In Fig. 5, the results for an example image(Lena) from the proposed encryption schemes are shown. The left figures((a), (c), (e), (g)) are the results including random selection(RS) by LFSR, while the right ones((b), (d), (f), (h)) without random selection. The PSNRs(Peak Signal-to-Noise Ratios) in the order from (a) to (h) are 9.39dB, 9.52dB, 9.18dB, 9.26dB, 10.52dB, 11.18dB, 9.53dB , and 9.67dB. As can be seen from the figures and PSNR values, PSNR cannot be the absolute value to estimate the encryption effect. With the same subband selection, left one including only LL4 show a little more information but the difference is negligible. Also, The amount of encrypted data increases as more subbands are selected, but the PSNR values do not encrypted 1/2 of the right one, but PSNR difference is necessarily decrease. As can see from the figure, the cases of LL4 reveal a certain amount of edge components in both with and without random selection. But from the LL4-HH4 cases, the original image is almost not recognizable. In a very acute application, LL4 cases cannot be used. But we include them in our image encryption menu because they also can be used depending on the application area.

Table 1 shows some statistical results from the experiments. Here, we assumed a pixel in the original image consists of 8 bits and only gray-level component is



(a) LL4 : RS (b) LL4

(c) LL4-HH4 : RS (d) LL4-HH4

(e) Level 4 : RS (f) Level 4

(g) Level 4-HH3 : RS (h) Level 4-HH3

Fig. 5. Lena example of proposed schemes

Table 1. Encryption statistics from experiments

Item case	Encryption ratio	Encrypted # blocks	CPU (ms)	PSNR (dB)
LL4 : RS	1:4096	4	10.76	9.244
LL4	1:2048	8	21.79	7.996
LL4-HH4 : RS	1:2048	8	22.45	8.673
LL4-HH4	1:1024	16	44.59	7.760
Level 4 : RS	1:1024	16	45.09	7.933
Level 4	1:512	40	93.64	7.669
Level 4-HH3 : RS	1:512	40	105.21	7.785
Level 4-HH3	1:256	64	201.43	7.624

considered.

The second column shows the ratio of the amount of encrypted data to the amount of original image data and its conversion to the number of encryption blocks is shown in the third column. As can see in the table, the encryption ratios lie between about 0.024%(1/4,096 for LL4 with random selection) and about 0.4%(1/256 for Level 4-HH3 without random selection), which are much lower than the previous works.

The last column shows the average PSNR values for the over 500 test images. As expected, the PSNR values have a tendency of decreasing as the amount of encryption increases. Even for the LL4 encryption with random selection, the PSNR value is low enough to hide the enough image information.

The third column shows the computation time to perform each encryption, which has been estimated with the time measurement function in C. Note that the implementation in C was not optimized. Theoretically, encryption time is proportional to the number of the blocks to be encrypted, but the values in Table 1 are a little deviated even though the increasing trend follows theory. This is because our image encryption scheme consists of other transactions in addition to the encryption itself, and they are LFSR execution, data extraction to form encryption blocks, and restoration of the encrypted data to the original position.

Fig. 6 shows the CPU times for those transactions separately for each encryption scheme. The CPU time to execute LFSR was negligible. The biggest CPU time is spent by data restoration. The sum of the CPU times for data extraction and data restoration was about three times bigger than the encryption time. This situation can be similar to the other works if they use block cipher algorithm. So the total CPU time was up to 5 times of the encryption time. The total encryption time including all the transactions for the worst case(Level 4-HH3 without random selection) was about 2% of the time to execute the image compression.

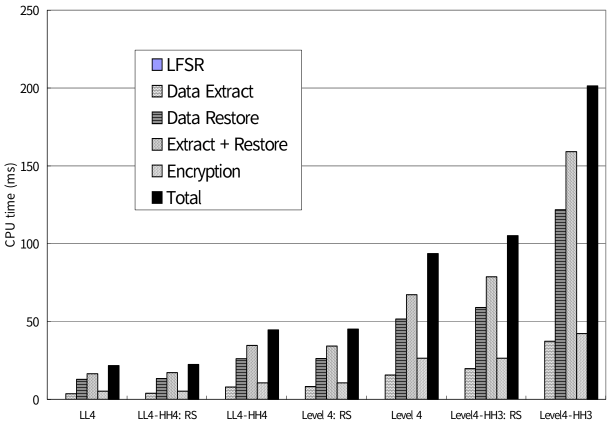


Fig. 6. Separate CPU times for encryption transactions

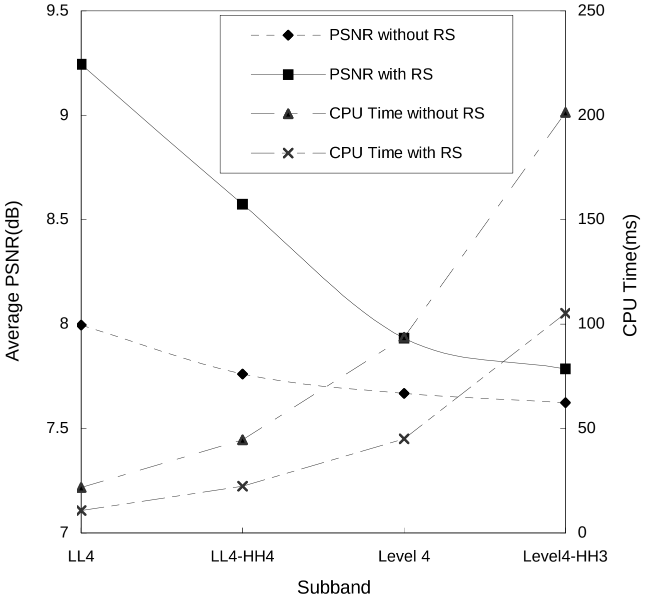


Fig. 7. Tread-off between the effect of encryption and encryption cost

In Fig. 7, the relationship between the PSNR values as the effect of encryption(although it is not the absolute estimation quantity) and execution time as the encryption cost is shown. As can see from the figure, the effect and the cost of our encryption schemes have a property of trade- off. That is, as the amount of data to be encrypted increases, the encryption cost increases and the encryption effect also increases. Between the schemes with and without random selection also, the execution time and quality have the relationship of trade-off. Because the random selection is performed for the additional security to the encryption itself, it can be chosen in compensation of additional execution cost. One more thing peculiar in Fig. 7 is that at the LL4 side, the difference in PSNR(encryption effect) is dominant, but at the Level 4-HH3 side, execution time difference is distinct between the schemes with and without random selection. This means that a particular scheme can be chosen for low execution time or encryption effect in the corresponding dominancy to fit the particular application.

V. CONCLUSION AND DISCUSSION

This paper proposed a set of encryption schemes for images, which encrypt the selective and partial data for each image during the wavelet-base image compression procedure. The data to be encrypted is extracted after quantization for which we used fixed linear quantizer. Three data selection schemes were involved for selective partial encryption: subband selection, data bit selection, and random selection of the quantization indices.

The experimental results showed that the encryption cost was about 2% of the image compression cost in the worst case(all the subbands in level 4 and HH3). Also the amount of data to be encrypted was between 1/4,096 and 1/256 of the original image data. This value is so small that the proposed schemes can be used in the wireless environments, especially in the area requiring the low-cost image encryption, such as wireless hand-held devices.

The proposed set of encryption schemes(8 schemes including with and without random selection) have the property of trade-off between the encryption effect and its cost. That is, as the amount of encryption data increases(as the encryption cost increases), the more image information is hidden(the effect of encryption increases). This property makes it possible to apply the encryption scheme adaptively according to the network condition and/or the computational capability of the communication device.

From the experimental results for the computation time, the data extraction time and restoration time was quite large compared to the encryption time. Because the implemented C code was not optimized, the times can be reduced much further by optimizing the code and minor revision of the schemes. In software, all the procedure in each encryption scheme must be executed serially and it is one of the reasons why the execution time is high. But if hardware implementation is considered, the proposed schemes can be more cost-effective. That is, the encryption process can be performed in parallel to the image compression process that the extra cost of execution time for encryption is negligible.

Finally, the proposed methods are performed in the application protocol layer. It means that those methods can be used as the solution of end-to-end security problem for image contents when a communication is performed through a composite network of wired and wireless sections.

ACKNOLEDGEMENT

This work has been partially supported by the grant No. R01-2001-000-00350-0 from the Korean Science & Engineering Foundation.

REFERENCES

[1] http://mpeg.telecomitalialab.com/working_ documents.htm#MPEG-2

[2] R. M. Rao and A. S. Bopardikar, *Wavelet Transforms, Introduction to Theory and Application*, Addison-Wesley, Reading, 1998.

[3] W. Staliings, *Cryptography and Network Security, Principles and Practice*, Prentice-Hall, Upper Saddle River, NJ, 1999.

[4] L. Qiao and K. Nahrstedt, “Comparison of MPEG Encryption Algorithms”, International Journal on Computer and Graphics(Special Issue on Data Security in Image Communication and Networks), Vol. 22, No. 3, pp. 437-444, 1998.

[5] A. M. Alattar, et al., “Improved Selective Encryption Techniques for Secure Transmission of MPEG Video Bit-streams”, ICIP’99, pp. --, 1999.

[6] C. Shi and B. Bhargava, “A Fast MPEG Video Encryption Algorithm”, Proc. Of ACM Multimedia 1998, pp. 81-88, 1998.

[7] H. Chaeng and X. Li, “Partial Encryption of Compressed Images and Videos”, IEEE Trans, on Signal Processing, Vol. 48, No. 8, pp. 2439-2451, Aug. 2000.

[8] A. Pommer and A. uhl, “Wavelet Packet Methods for Multimedia Compression and Encryption”, IEEE Pacific Rim Conf. On Communications, Computers, and Signal Processing, pp. 1-4, 2001.

[9] A. Pommer and A. Uhl, “Selective Encryption of Wavelet Packet Subband Structures for Obscured Transmission of Visual Data”, IEEE Benerux Signal Processing Symposium, pp. 25-28, 2002.

[10] X. Wu and P. W. Moo, “Joint Image/Video Compression and Encryption via High-Order Conditional Entropy Coding of Wavelet Coefficients”, Int’l Conference on Multimedia Computing and Systems, pp. 908-912, 1999.

[11] P. P. Dang and P. M. Chau, “Image Encryption for Secure Internet Multimedia Applications”, IEEE Trans. on Consumer Electronics, Vol. 46, No. 3, pp. 395-403, Aug. 2000.

[12] M. Podesser, H. P. Schmidt, and A. Uhl, “Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments”, Proc. 5th Nordic Signal Processing Symposium, pp. --, 2002.

[13] T. Uehara and R. Safavi-Naini, “Attacking and Mending Arithmetic Coding Entropy Schemes”, Proc. Of Australian Science Conference, pp. 408-419, Jan. 1999.

[14] G. J. Sullivan and R. L. Baker, “Efficient Quadtree coding of images and videos”, IEEE Trans. on Signal Processing, Vol. 3, pp. 327-331, May 1994.

[15] A. Said and W. A. Pearlman, “A New Fast and Efficient Image Codec based on Set partitioning in Hierarchical Trees”, IEEE Trans. on Circuits and Systems on Video Technology, Vol. 6, pp. 243-250, June 1996.

[16] S. W. Golomb. *Shift Register Sequences*, Algean park Press, Laguna Hills, CA, 1982.