Effectiveness of Ciphering Approximate Sub-band of Wavelet Transformed Image

By

Abeer M. Yousif

College of Science, Al-Nahrain University

Abstract

Image encryption plays a more and more important role in today's multimedia world. Image/video encryption algorithms working in wavelet domain attract some attention due to the prevalence of wavelet compression. In this paper, two partial stream encryption methods, based on transposition or substitution, have been studied to assess their effectiveness in concealing the perceptual content of images. To achieve the above goal, the wavelet domain, specifically the approximation coefficients, has been adopted as plaintext media. The set of conducted tests indicated that the use of substitution is more effective than transposition, and the encryption of Y-component alone is more powerful than encrypting RGB bands. The increase in wavelet passes reduces the image concealment capabilities. The ciphering of two most significant bits of approximate Y-subband reduces the image cipher space to %6.25 while the concealment level remains acceptable.

Keywords: Selective encryption of images, Partial encryption, Multimedia encryption, Stream cipher, Wavelet coding.

الخلاصة

يلعب موضوع تشفير الصور دوراً مهماً في عالم الاوساط المتعددة الحالية. لقد حازت خوازميات تشفير الصورة والفيديو، التي تعمل في المجال المويجي على اهتماماً متميزاً بسبب انتشار طرق الضغط الصور المعتمدة على التحويل المويجي. في هذا البحث تمت دراسة فاعلية طريقتين من التشفير التدفقي الجزئي للصور (احداهما استندت على طريقة التعويض والثانية على طريقة الاستبدال) في اخفاء محتوى معالم الصورة. ولتحقيق التشفير الجزئي، تم التعامل مع جزء من المجال المويجي، وتحديداً معاملات التقريب، على انه النص الخاضع للتشفير. لقد اشرت مجموعة التجارب التي جرى تنفيذها بان طريقة التعويض التدفقي هي اكثر فاعلية من طريقة الاستبدال، وان نتائج تشفير مركبة الشدة (Y) هي اكثر تأثيراً من نتائج تشفير مركبات اللون الاساسية (الاحمر، والاخضر والازرق). ان زيادة عدد مرات مرور التحويل المويجي على الصورة سيؤدي الى تناقص فاعلية اخفاء معالم الصورة.

1. Introduction

Encryption schemes for multimedia data need to be specifically designed to protect multimedia content and fulfill the security requirements for a particular multimedia application [1]. There are two levels of security for digital image encryption: low level and high-level security encryption. In low-level security encryption, the encrypted image has degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. In the high-level security case, the content is completely scrambled and the image just looks like random noise. In this case, the image is not understandable to the viewers at all. A major recent trend is to minimize the computational requirements for secure multimedia distribution by "selective encryption" where only parts of the data are encrypted. Selective encryption aims at avoiding 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 bit stream to obtain a fast method [2]. The following issues have to be taken into consideration when advanced encryption algorithms are specially designed for sensitive digital images and videos, for their special features are very different from texts [3]:

1. Tradeoff between bulky data and slow speed: Digital images and videos are generally bulky data of large sizes, even if they are efficiently compressed. Since the encryption speed of some traditional ciphers is not sufficiently fast, especially for software implementations, it is difficult to achieve fast and secure real-time encryption simultaneously for large-sized bulky data.
2. Tradeoff between encryption and compression: If encryption is applied before compression, the randomness of ciphertexts will dramatically reduces the compression efficiency. Thus, one has to apply encryption after compress-ion, but the special and various image/video structures make it difficult to embed an encryption algorithm into the integrated system. For example, some popular compression standards (such as MPEG-x) are antagonistic to selective encryption. That is, there exist notable tradeoffs between the compression and the encryption.
3. Visual degradation (VD); measures the perceptual distortion (preferably configurable) of the ciphered image with respect to the plain image. The Mean Absolute Error (MAE),

Mean Square Error (MSE), and Peak PSNR are widely used as a metrics for this criterion. It is required to be as large as possible.

4. Encryption ratio (ER): This criterion measures the ratio between the size of the encrypted part and the whole data size. It is one of the main expected features of selective encryption.

The organization of this paper is as follows. In section 2, we review the previous research findings. Section 3 introduces the present work. Finally, section 4 shows the experimental results and the conclusions of this study are given in section 5.

2. Previous works

Several selective encryption methods have been used in compressed images from early 1990s. In this section, researches related to DWT-based algorithms are presented only. In [4], secret permutations were suggested to shuffle the DWT coefficients in each sub-band of wavelet compressed images. An enhanced version of this scheme suggested encrypting the lowest sub-band with a traditional cipher. In [5], some permutation methods of DWT coefficients were compared, and a novel method was proposed to realize stronger confusion of shuffled coefficients. In [6,7], several perceptual encryption schemes were proposed by selectively encrypting partial DWT coefficients. The bit-shift encryption function used in [7] is not secure enough against known/chosen-plaintext attacks. In [8, 9], the use of selective encryption in JPEG2000 image encryption was discussed. It was pointed out that at least 20% of encrypted data are needed to provide sufficient security. In [10], encryption of sign bits of partial DWT coefficients was suggested. This scheme is not secure due to the aforementioned second defect of selective encryption. In [11], the idea of encrypting wavelet filters was proposed to develop a new encryption system. Later, in [12, 13, 14], this algorithm was studied with wavelet packet decomposition, and it was shown that such an encryption scheme is not secure enough against the cipher text-only attack based on a heuristic cryptanalytic method.

3. The Present Work

The basic idea behind this work is to implement a partial stream cipher methods for images that is integrated into the compression process based on using 9/7 biorthogonal wavelet filter.

As shown in figure (1); the main involved steps are: color transformation, wavelet transformation, quantization and ciphering methods. First the data is decomposed into (RGB) color components, and then transformed to other color domains selectively. These domains are: YUV, YIQ, YCbCr1, and YCbCr2. Color transformation is utilized in image compression schemes, because it is helpful to reduce spectral redundancy and exploits some of characteristics of the human vision system to improve the compression performance. So, the use of YCbCr model (or the equivalent color models) as ciphering domain will be useful to implement both compression and encryption at a time. Second, biorthogonal wavelet transform is applied on each of the three bands. It consists of recursive application of the low-pass/high-pass one dimensional filter bank

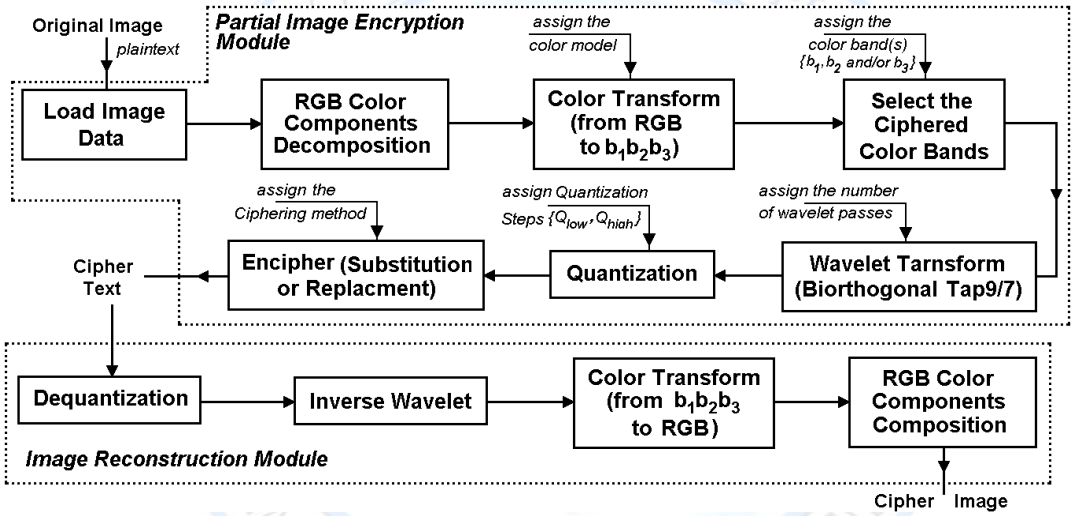


Fig. (1): The proposed partial image compression system based on wavelet transform

Successively along the horizontal and vertical directions of the images. The low pass filter provides the smooth approximation coefficients while the high-pass filter is used to extract the detail coefficients at a given resolution. The transformed image is then fed into quantization process to reduce the number of bits required to represent all possible values of mapping outputs to fewer bits needed to describe approximates. Different quantization step sizes have been applied in experimental tests, to investigate their affection on the perceptual quality. Applying quantization process results in making error (up to permissible level) at the decoding phase; this cause was the reason of impacting encryption algorithm directly after

quantization. Two stream cipher methods are implemented: (Transposition and substitution) and in both schemes a uniform random generator is utilized.

4. Experimental Results

In this work, many test sets have been conducted to assess the present selective encryption. In each set of tests, the effectiveness of one of the following parameters has been investigated:

1. Number of wavelet passes.
2. Number of ciphered sub-bands.
3. Type of color models.
4. Ciphering methods.
5. Quantization over approximate and detail coefficient.
6. Number of ciphered bits.

The standard 'Lena' image was taken as a test image sample. For evaluating the distortion level, the MSE measure has been adopted to evaluate the degree of difference occurred between the original image pixels and their corresponding pixels in ciphered image.

$$\dots (1)\ MSE = \frac{1}{WH}\sum_{y=0}^{H-1}\sum_{x=0}^{W-1}(I_p(x,y)-I_c(x,y))^2$$

Where, W is the image width, H is the image height, $Ip(x,y)$ is the original image, $Ic(x,y)$ is the ciphered image.

One of the remarks appointed about the usage of pixel-to-pixel difference metrics (like MAE, MSE, and PSNR) they don't reflect the actual subjective distortion occurred in ciphered image, specifically they don't show the degree of difference in pixel neighborhood. So, to handle this weakness in the above traditional objective metrics, the distortion level was evaluated by determining the MSE for the gradient of images (i.e. for both original and ciphered) because the gradient reflects the degree of existing correlation between neighbor pixels.

$$MSE_G = \frac{1}{WH}\sum_{y=0}^{H-1}\sum_{x=0}^{W-1}(\nabla I_p(x,y)-\nabla I_c(x,y))^2 \qquad \dots (2)$$

Where ∇ indicates the gradient operator.

To asses the degree of visual concealment due to ciphering part of image data, Concealment ratio parameter was suggested to evaluate the degree of achieved ciphering relative to its value when whole image data is ciphered. The mathematical expression for the adopted concealment ratio parameter (CR) is:

$$CR = \frac{MSE_s}{MSE_w} \quad \ldots (3)$$

Where MSE_s is the value of MSE when ciphering is applied on selected band(s), while MSE_w is the MSE when whole image data is ciphered.

Table 1, lists the values of MSE_G and CR when the RGB bands are ciphered using substitution method, also the table shows the variations in ciphering results when a number of passes are taken. The results in the table indicate the following:

Table 1. The effect of ciphering RGB bands using substitution cipher

Band	Pass One		Pass Two	
	MSE_G	CR (%)	MSE_G	CR (%)
R	1003.9	32.97	300.4	31.34
B	1035.1	34.00	323.8	33.78
G	1027.6	33.75	320.4	33.43
R+G	2022.1	66.41	627.4	65.46
R+B	2044.5	67.15	628.9	65.62
G+B	2075.7	68.18	652.3	68.06
ALL (R+B+G)	3044.7	100.00	958.4	100.00

1. The significance of ciphering any of the three bands is alike. The values of CR is relatively low (not more than 34%) when one band is ciphered, to achieve acceptable concealment the two color bands need to be ciphered.
2. The increase of wavelet passes with ciphering only the approximate sub-bands will cause a decrease in concealment ratio around (32%), which indicates the important of including portion of detail sub-band in ciphering process.

Figures (2) and (3) present different cipher results when different color bands have been ciphered with different wavelet passes. Table 2, presents the ciphered results when YCbCr1 color model is adopted. Although, the determined values of MSEG metric (specified for gradient images) indicate that the encryption of each sub-band cause a significant distortion in image, but the samples of images shown in figure (4) and (5) illustrate that the encryption results due to Y-component is enough to conceal the image details subjectively, while the distortion due to ciphering both Cb and Cr sub-bands is not effective, only color shift is occurred. To clarify this effect table (3) presents the MSE values of the gray part of 'Lena' image and its corresponding ciphered images.

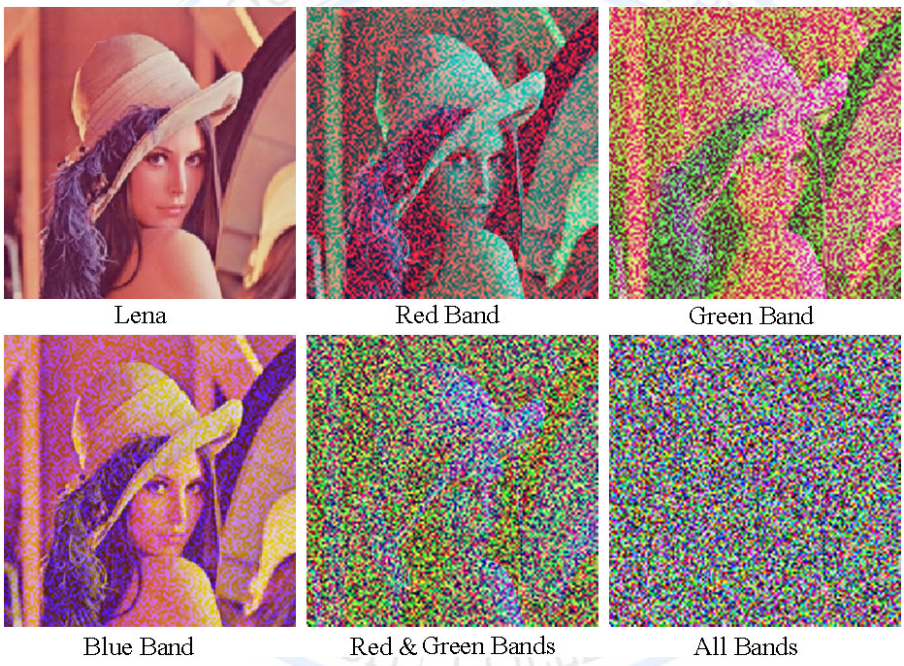


Fig.(2) The effect of ciphering RGB bands using substitution cipher for one pass

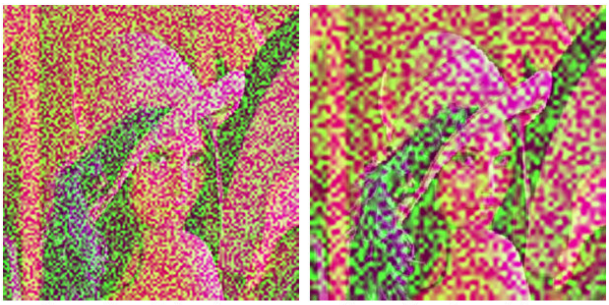


Fig. (3) The effect of ciphering RGB bands using substitution cipher for two passes

A comparison between results of table (1) and those of table (2) indicate that the effect of increasing wavelet passes is similar to the noticed of RGB case. Also, the usage of YCbCr1 is better for ciphering purpose. The same tests have been conducted on other color models (i.e. YUV, YIQ, and YCbCr2); it is found that the same ciphering effects like YCbCr1 are met.

In all above mentioned test results, the used ciphered method was based on making XOR between the quantized values of selected wavelet sub-band coefficients with a stream of numbers generalized using a random generator.

Table 2. The effect of ciphering YCbCR1 bands using substitution cipher

Band	Pass One		Pass Two	
	MSE_G/ MSE	CR_G(%)/ CR(%)	MSE_G/ MSE	CR_G(%)/ CR(%)
Y	2687.75/ 6108.20	50.91/ 57.20	868.306/ 6453.68	48.56/ 57.57
Cb	2052.19/ 3202.23	38.87/ 29.98	684.153/ 3407.06	38.27/ 30.39
Cr	1944.55/ 4286.91	36.84/ 40.14	613.459/ 4562.63	34.31/ 40.70
Y+Cb	4024.95/ 7822.39	76.24/ 73.25	1342.2/ 9481.79	75.07/ 84.58
Y+Cr	4006.02/ 9152.89	75.89/ 85.71	1309.88/ 9420.76	73.26/ 84.04
Cb+Cr	4006.94/ 7379.85	75.90/ 69.10	1308.46/ 7750.78	73.18/ 69.14
(Y+Cb+CR)	5279.02/ 10678.63	100.00/ 100.00	1787.93/ 11209.63	100.00/ 100.00

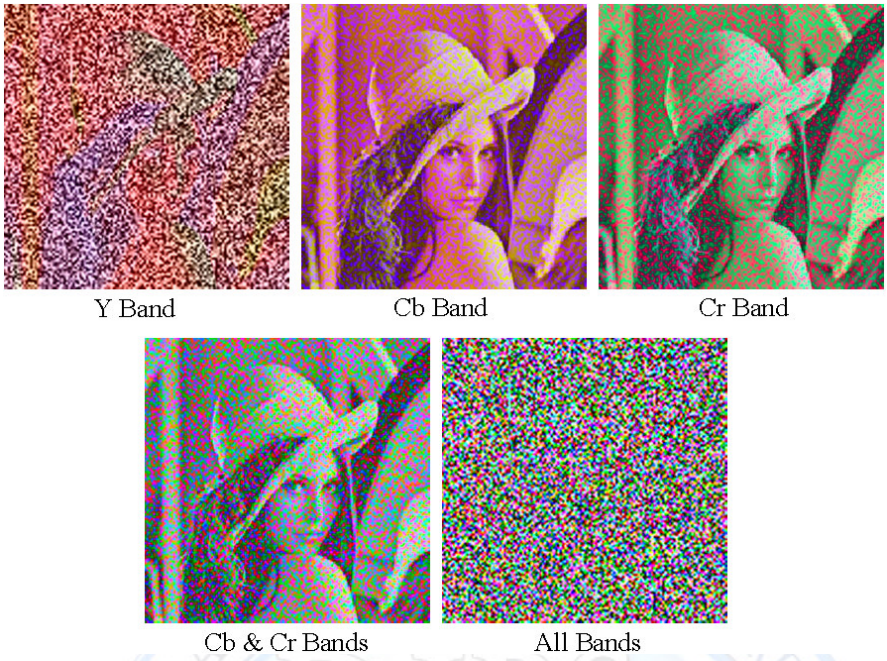


Fig. (4) The effect of ciphering YCbCr1 bands using substitution cipher for one pass

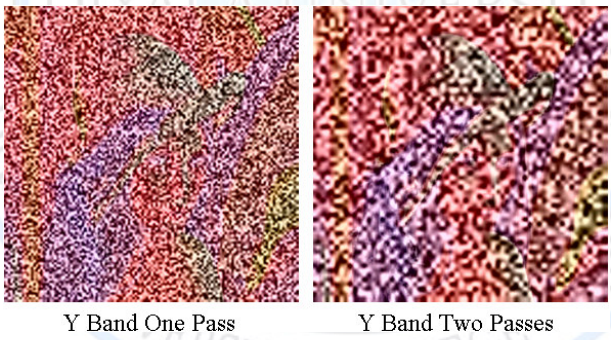


Fig. (5) The effect of ciphering YCbCr1 bands using substitution cipher for two passes

Table 3. The MSE values of the gray part when substitution cipher is applied on YCbCr1 bands for one pass

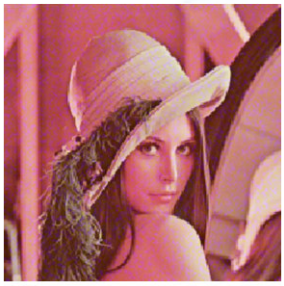
Band	MSE
Y	6040.21
Cb	574.45
Cr	247.07

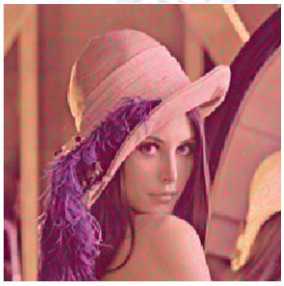
Table (4) presents the ciphering results when transposition method was applied to cipher the approximate sub-band coefficients. The results indicate that the concealment ratio due to substitution using random generator is much better than the case of using transposition. The attained MSE is one third that obtained by the first method. This relative degree in effectiveness is due to weakness in preserving the statistical characteristics of plaintext of transposition method. So, when the dynamic range of the plaintext is narrow, the corresponding range of the ciphered sub-band is preserved. Figure (6) presents a sample of ciphered image using transposition method.

Table 4: The effect of ciphering YCbCR1 bands using transposition cipher

Band	Pass One		Pass Two	
	MSE	CR (%)	MSE	CR (%)
Y	1104.48	88.40	324.011	87.57
Cb	84.9967	6.80	27.2486	7.36
Cr	66.4541	5.32	22.0508	5.96
Y+Cb	1181.39	94.55	348.849	94.28
Y+Cr	1170.38	93.67	344.547	93.12
Cb+Cr	149.301	11.95	47.4232	12.82
All(Y+Cb+CR)	1249.42	100.00	369.996	100.00


Y band


Cb band


Cr band


Cb & Cr bands


All bands

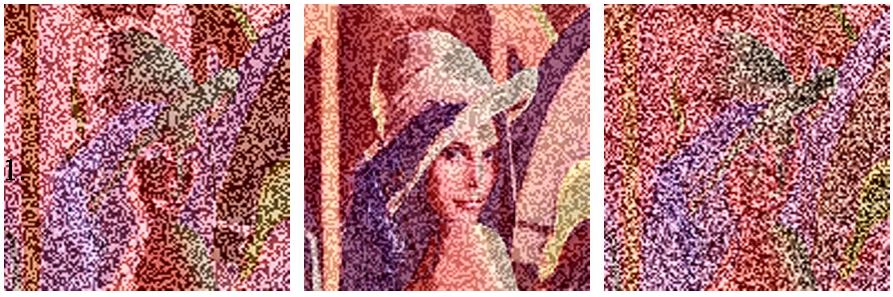
Fig.(6): The effect of ciphering YCbCr1 bands using transposition cipher for two passes

Table (5) presents the MSE values when quantization step is varied, the results indicate that the effects of quantization of detail sub-band is insignificant in comparison with the effect of ciphering the approximate subband. The increase in MSE due to increase in quantization step of detail coefficients is negligible, while the effectiveness of quantizing the approximation coefficients is not systematic but remains high.

Table 5: The effect of quantization steps using substitution cipher of YCbCr1 model

Q_{low}		Q_{high}	
Q_{step}	MSE	Q_{step}	MSE
1	2687.75	1	2687.75
4	4396.48	10	2687.16
6	4136.2	20	2687.78
10	3793.79	30	2687.96
15	3646.4	40	2684

To investigate the degree of visual ciphering of significant bit planes, the seventh and/or sixth bit plane were ciphered. Figure (7) shows the ciphering results when the bits of those two significant bit planes were ciphered. Although that the volume of information covered by each bit plane is 0.125 of the whole information of sub-band, the degree of visual concealment is too high, as shown in table (6).



7^{th} Bit Plane 6^{th} Bit Plane 6^{th} & 7^{th} Bit Planes

Fig. (7): The effect of ciphering different Bit Planes of Y-band

Table 7: The effect of ciphering different Bit Planes of Y-band using Substitution ciphers for one pass

Bit Plane	Pass One	
	MSE	CR (%)
All Bit Planes	2687.75	1.00
only 7th Bit	2282.19	0.85
Only 6th Bit	656.493	0.24
Both 7th &6th Bits	2667.09	0.99

5. Conclusions & Suggestions

The results presented in previous sections led to the following remarks:

1. The use of RGB color model domain is not appropriate for image selective encryption because the encryption of one band only causes a visual concealment doesn't exceed %34. Beside to that, the overall attained concealment due to encryption of RGB bands is lower than those obtained by ciphering YCbCr.
2. The concealment due to Y-encryption is more effective than encrypting other chromatic bands; it is even more than encrypting both of them. The attained concealment is around %50 when substitution encryption is applied, and it is around %88 when transposition is applied. Taking into consideration that the overall concealment when applying substitution encryption on Y band is better than the concealment occurred when applying transposition encryption over all bands. Although the MSE values for the case of applying substitution encryption on Cb and/or Cr bands is high but the visual appearance of image detail is not completely concealed. The high values of MSE are due to the color shift that occurred in color bands.
3. The increase of number of passes leads to a decrease in the effectiveness of encryption to LL sub-band only, the transition from one pass to two wavelet passes had cause a decrease in concealment ratio around (%35). This is rational, because the information energy laid in LL sub-band is gradually decreased when the number of wavelet pass is increased.

4. The effectiveness of quantization step of the approximate sub-band is high but doesn't show a uniform pattern. The MSE value is kept high but the variation tendency is not clear with variation of quantization step.
5. The encryption of significant bits only will cause good reduction in ciphered part of image information, where the use of one bit only means only 12.5% of the information content will be ciphered, but the attained concealment will kept high (in other words a little reduction in concealment ratio is occurred).
6. The applying of substitution encryption on the most significant two bit planes of the approximate sub-band will causes an acceptable visual concealment with the ciphered volume will not exceed %2 for one wavelet pass.
7. Since the tests results indicated that the concealment is reduced when the number of wavelet passes is increased. But, for compression purposes the increase in wavelet passes is vital, so there is a necessity to study the possibility of applying encryption on certain bit planes of the detail sub bands to by pass the above concealment reduction weakness.
8. Some of the test results show the appearance of high frequency traces, and to remove these traces some of detail coefficients need to be ciphered.

References

[1] Chung-Ping Wu and C.-C. Jay Kuo, "Fast encryption methods for audiovisual data confidentiality", In Multimedia Systems and Applications III, volume 4209 of Proceedings of SPIE, pages 284–295, 2001.

[2] Fonteneau C., Motsch J., Babel M., and D´eforges O., "A hierarchical selective encryption technique in a scalable image codec", International Conference in Communications, Bucharest, Romania 2008.

[3] B. Furht and D. Kirovski, editors, "*Multimedia Security Handbook",* CRC Press, Boca Raton, Florida, 2005.

[4] Takeyuki Uehara, Reihaneh Safavi-Naini, and Philip Ogunbona, "Securing wavelet compression with random permutations", In Proc. IEEE Pacific-Rim Conference on Multimedia (IEEE-PCM'2000), pages 332–335, 2000.

[5] Shiguo Lian and Zhiquan Wang, "Comparison of several wavelet coefficients confusion methods applied in multimedia encryption", In Proc. Int. Conference on Computer Networks and Mobile Computing (ICCNMC'2003), pages 372–376, 2003.

[6] Rapha¨el Grosbois, Pierre Gerbelot, and Touradj Ebrahimi, "Authentication and access control in the JPEG 2000 compressed domain", In Applications of Digital Image Processing XXIV, volume 4472 of Proceedings of SPIE, pages 95–104, 2001.

[7] Hitoshi Kiya, Dhoko Imaizumi, and Osamu Watanabe, "Partial-scrambling of images encoded using JPEG2000 without generating marker codes", In Proc. IEEE Int. Conference on Image Processing (ICIP'2003), volume III, pages 205–208, 2003.

[8] Roland Norcen, Martina Podesser, Andreas Pommer, Hans-Peter Schmidt, and Andreas Uhl, "Confidential storage and transmission of medical image data. Computers in Biology and Medicine", 33(3):277–292, 2003.

[9] Roland Norcen and Andreas Uhl, "Selective encryption of the JPEG2000 bitstream", In Proc. IFIP TC6/TC11 7th Joint Working Conference on Communications and Multimedia Security (CMS'2003), volume 2828 of Lecture Notes in Computer Science, pages 194–204, 2003.

[10] Young-Ho Seo, Dong-Wook Kim, Ji Sang Yoo, Sujit Dey, and Abhishek Agrawal. Wavelet domain image encryption by subband selection and data bit selection. In Proc. World Wireless Congress (WCC'03/ 3GWireless'2003), 2003.

[11] Lutz Vorwerk, Thomas Engel, and Christoph Meinel, "A proposal for a combination of compression and encryption. In Visual Communications and Image Processing 2000, volume 4067 of Proceedings of SPIE, pages 694–702, 2000.

[12] Andreas Pommer and Andreas Uhl, "Wavelet packet methods for multimedia compression and encryption", In Proc. IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM'2001), volume 1, pages 1–4, 2001.

[13] Andreas Pommer, "Selective Encryption of Wavelet-Compressed Visual Data", PhD thesis, Department of Scientific Computing, University of Salzburg, Austria, June 2003.

[14] Andreas Pommer and Andreas Uhl, "Multimedia soft encryption using NSMRA wavelet packet methods: Parallel attacks", In Proc. Int. Workshop on Parallel Numerics (ParNum'2000), pages 179–190, 2000.

[15] Andreas Pommer and Andreas Uhl, "Selective encryption of wavelet-packet encoded image data: Efficiency and security. Multimedia Systems", 9(3):279–287, 2003.