Performance Evaluation of Discrete Wavelet Transform for compression of encrypted color images

Hina Shakir, S Talha Ahsan, Haroon Rasheed

Abstract— With the invasion of multimedia content over public networks and its subsequent confidentiality aspect, images are often required to be secured via encryption. The encrypted images can later be subjected to compression to utilize the available bandwidth efficiently. This research paper presents the performance evaluation of discrete wavelet transform when used for compression of encrypted color images. The test images are first encrypted with stream cipher RC4 and then compressed using wavelets including db1, db2, sym1, sym2, coif1, coif2 and bior1.5 with various compression rates. These encoded images are transmitted. On the receiving end; they are first decompressed and then decrypted. It is found that the wavelets coded encrypted images perform well for bit rates of 2 bits per pixel and above, with Peak Signal to Noise Ratio (PSNR) greater than 39 dB and Mean Square Error less than 6.9. The PSNR of encrypted images is compared with the PSNR of unencrypted images subjected to the same wavelets based compression and decompression process. The PSNR of unencrypted images is found to be typically 40 to 45 dB and at maximum 270 dB larger than that of encrypted images. The results of this study will be useful in compression of encrypted color images.

Index Terms— Image compression, wavelet, image encryption, stream cipher, PSNR, DWT, MSE

1 INTRODUCTION

Information including images often experiences security threats on public networks from unauthorized users. One method to obscure images for security purposes is to apply encryption on them [1]. These encrypted images are often required to be compressed before transmission by the end user in order to efficiently utilize the channel bandwidth and to improve transmission data rates. Johnson et al. [2] showed that significant compression of the data can be achieved after encryption when based on the theory of source coding with side information. This research paper presents the performance evaluation of discrete wavelet transform (DWT) based lossy compression, of fully encrypted color images.

Stream cipher RC4 which is a fast encryption algorithm with reasonable security [3] is employed to encrypt the images. The efficiency of DWT based compression for encrypted images has been assessed in terms of Peak Signal Noise to Ratio (PSNR) and Mean Square Error (MSE). For comparison purpose, DWT based compression is also applied on unencrypted images. The framework for this testing of different wavelets is shown in Fig. 1.

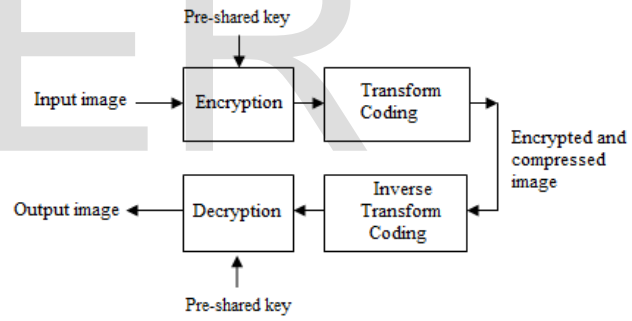

Fig. 1. Framework for testing of wavelets

Previous research work carried out in the area of lossy compression of encrypted images has demonstrated performance of various compression techniques on encrypted gray-scale images [4] - [8]. However, DWT coding has only been used by [9] and [10] where Al-Maadeed et al. in [9] used DWT for the compression of chaos based encrypted gray scale images which were readily coded in the gif and jpg image formats. A. Gurijala et al. in [10] applied wavelets via JPEG2000 standard on pre/post filtered Lena gray scale image. Research study in [9] and [10] motivated us to test DWT coding on color images without any prior coding unlike the previous studies done in this area. Hence, the authors hereby propose DWT coding on RC4 based encrypted color images and evaluate the efficiency of the framework for wavelets including db1, db2, sym1, sym2, coif1, coif2 and bior1.5.

1). Engr. Hina Shakir, Electrical Engineering Department, Bahria University, Karachi , Pakistan, +9221-99240002, (e-mail: hina.shakir@bimcs.edu.pk)

2) Dr. S. Talha Ahsan, Electrical Engineering Department, Usman Institute of Technology, Karachi, Pakistan, (9221) 34978274-5 , (e-mail: stahsan@uit.edu)

3). Dr. Haroon Rasheed, Electrical Engineering Department, Bahria University, Karachi, Pakistan, +9221-99240002-4., (e-mail: haroon.rasheed@bimcs.edu.pk).

2 BACKGROUND

This section briefly discusses the encryption technique, wavelet transform and wavelet based compression employed for the research work.

2.1 Encryption Technique

The chosen RC4 algorithm is a symmetric algorithm that consists of key initialization, key bytes generation and encryption. The input key is passed first through key initialization algorithm and then through pseudo-random key stream generation algorithm to produce stream of key bytes. The exclusive-OR (XOR) logical operation is performed on the resultant key bytes and image data bytes to obtain the encrypted image. The algorithms of key initialization and pseudo-random key stream generation are given in Fig. 2 and Fig. 3 respectively.

```
Initialization:
    For i = 0 to 2^n -1
        S[i] = i
    j = 0
Scrambling:
    For i = 0 to 2^n -1
        j = j + S[i] + K[i mod l ]
        Swap(S[i],S[j])
```

Fig. 1. Key Initialization

```
Initialization:
    i = 0
    j = 0
Genenration Loop:
    i = i +1
    j = j + S[i]
    Swap(S[i] ,S[j])
    Output z = S[ S[i] + S[j] ]
```

Fig. 3. Pseudo-random key stream generation

2.2 Wavelet Function and DWT

The wavelets selected for this research study are db1, db2 from Daubechies family; sym1, sym2 from Symlet family; coif1, coif2 from Coiflet family and bior1.5 from Biorthogonal family of wavelets. A family of wavelets can be represented using translation and dilation on mother wavelet ψ of the wavelet family by following equation [12]:

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right) \quad (1)$$

The mother wavelet ψ is the prototype basis function and has a scaling or dilation factor a, and translation factor b, whose values can be varied to produce other wavelets in the family. Wavelet transformation represents any arbitrary function f(x) into a sum ψa,b of basis functions.

Wavelets can be realized with the help of iteration of digital filters along with rescaling. Filtering operation determines the resolution of the signal or image while down sampling and up sampling of the digital image determines the scaling of the signal. Successive low pass and high pass analysis filters banks are used to compute the DWT of a discrete time-domain signal. At every level, high pass filter produces the detail information and low pass filter produces the approximation details of the image [13]. Therefore the image is decomposed into its detail component and approximation component. The approximation component is further recursively decomposed into detail component and approximation component. This practice enables to adapt relevant image resolution required for a particular application.

Fig. 4 shows two-level wavelet decomposition of an image. At sending end, the first half band filter with impulse response h[n], passes half band of the frequencies with highest frequencies of the image which is then downsampled by a factor of 2. The output is the image detail information d[n]. The second half band filter with impulse response g[n], allows half of the frequency band with low frequencies which is then down sampled by a factor of 2. This process produces coarse approximation component a[n] of image. a[n] is subsequently subjected to successive high pass and low pass filters to produce detail component and approximation component respectively.

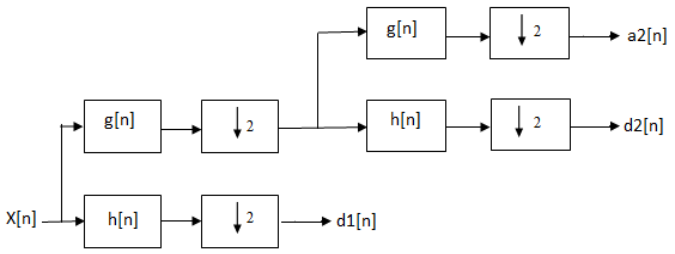

Fig. 2. Two-level wavelet decomposition tree

DWT of a signal ϰ[n] can be mathematically expressed in terms of detail coefficient d[n] and approximation coefficient a[n] with the help of following equations:

$$d[n] = \sum_{k=-\infty}^{\infty} x[k].h[2n-k] \quad (2)$$

$$a[n] = \sum_{k=-\infty}^{\infty} x[k].g[2n-k] \quad (3)$$

By concatenating all the coefficients of d[n] and a[n], DWT of the original image is obtained. The reconstruction of the image using wavelets coefficients is demonstrated in Fig. 5.

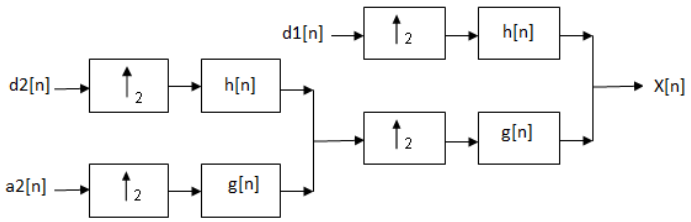

Fig. 3. Two-level wavelet reconstruction tree

While wavelets realize the detail information of the image, the approximation information of the image can be obtained with a scaling function ∅(t) which is a dual of mother wavelet which must satisfy the following equation [14]:

$$\emptyset(t) = \sqrt{2}\sum_{n\in Z} h[n]\emptyset(2t-n) \quad (4)$$

The wavelets can also be represented in terms of sum of translated scaling function ψ(t) [14]:

$$\psi(t) = \sqrt{2}\sum_{n\in Z} g[n]\emptyset(2t-n) \quad (5)$$

2.3 DWT based image compression

Wavelet based compression takes place in three steps. In the first step, the image is decomposed into its wavelet coefficients. These coefficients are quantized and then encoded using an entropy encoding and/or run length encoding scheme as shown in Fig. 6(a) [16].Wavelet based decompression follows the reverse process to obtain the output image and is demonstrated in Fig. 6 (b) [15].

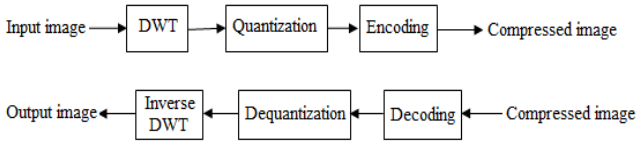

Fig. 6. Wavelet based compression and decompression

After decomposing the image into its wavelet coefficients, soft or hard thresholding can be applied on either of detail and approximation components or only on detail components. Thresholding as a part of quantization enables lossy compression of the image [16]. In hard thresholding, all the wavelet coefficients of image which are equal to or less than the thresholding value λ are set to zero. On the other hand, in soft thresholding, wavelet coefficients less than the thresholding value λ are equated to zero. The thresholded coefficients are then quantized and encoded. For decompression; encoded wavelet coefficients of the image are decoded and processed through inverse wavelet transform at the receiver end to obtain the output image. The two types of thresholding techniques are mathematically expressed by Eq. (7) and Eq. (8) [14].

$$\text{Tsoft}(x) = \begin{cases} 0 & if\ |x| \le \lambda \\ x+\lambda & if\ x > \lambda \\ x+\lambda & if\ x < -\lambda \end{cases} \quad (7)$$

$$\text{Thard}(x) = \begin{cases} 0 & if\ |x| \le \lambda \\ x & if\ |x| > \lambda \end{cases} \quad (8)$$

where λ is the thresholding value which is a positive real number and x is the coefficient value of the image matrix X.

2.4 Experimental setup

The performance of different wavelets on RC4 encrypted color images is evaluated with the help of a Matlab (version 2012) based program that was run on a computer with 64 bit CPU. The experimental setup is outlined in Fig. 7 and has been tested on six 2-D test images which are shown in Table 1.

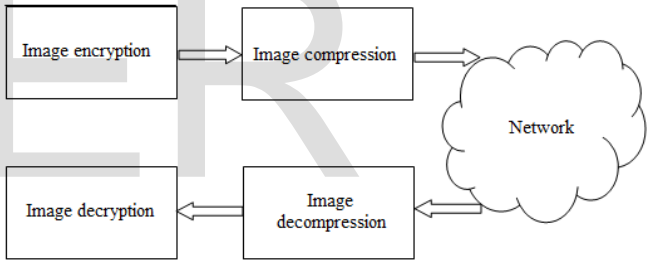

Fig. 7. Experimental setup for testing of wavelets

TABLE 1
TEST IMAGES

The size of test images is 256 × 256 with bit depth equal to 24. A 64 bit key with decimal value of 232 102 6 32 114 56 78

200 is used as the input key for encryption. With the help of key generation algorithms outlined in previous section, a key of length 65536 bytes is generated which ensures sufficient security. The key is stored in a matrix of dimensions 256 × 256 bytes whereas the test images are stored in arrays of dimensions 256 × 256 × 3 bytes. Encrypted images are produced by subsequently XORing the key bytes with the arrays of the test images data using RC4 algorithm.

The encrypted test images are then subjected to 2-D two-level wavelet based compression to achieve compression rates ranging from 0.5 bits per pixel (bpp) to 7.5 bpp (Compression rate in bpp is a measure of calculating the number of bits used to store the information of 1 pixel in the image). Hard threshold along with quantization is implemented within compression process to achieve the desired compression rates. Tested wavelets include db1, db2, bior1.5, sym1, sym2, coif1, and coif2. Same test images are also subjected to only wavelet based compression for a comparative analysis.

3 Results And Discussion

3.1 Performance of encryption algorithm RC4

The test images after RC4 encryption exhibit unavailability of perceptual and statistical information of pixels and ensure image confidentiality. Complete process of encoding the Mandrill test image at sending end and decoding the image at receiving end is illustrated in Fig. 8 for sym2 wavelet. The original image is shown in Fig. 8 (a) and the encrypted image is shown in Fig. 8 (b).

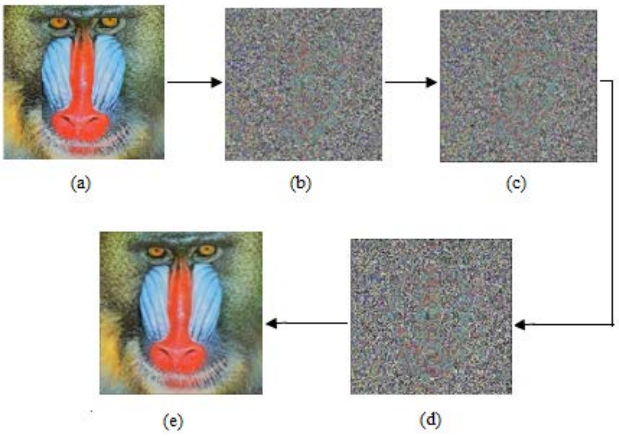

Fig. 4. Performance of sym2 wavelet on encrypted image at 1 bpp

3.2 Performance of wavelets for encrypted images

The encrypted images are compressed in the encoder at various compression rates and transmitted through wireless medium as shown in Fig. 8(c). At receiving end, the images are decompressed at the same rates as given in Fig. 8 (d) and then decrypted to retrieve the original images as given in Fig. 8(e).

The quality of the output color images are measured by computing Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) of the output image. MSE is defined as:

$$\mathrm{MSE} = \frac{\sum_{x,y=1}^{M,N} [I(x,y) - I'(x,y)]^2}{3 \times M \times N} \quad (9)$$

where M and N are the dimensions of the image and I(x,y) and I′(x,y) are the image information of original image and the output image for pixel (x,y) respectively. The PSNR is given by:

$$\mathrm{PSNR(dB)} = 10 \times \log\left[\frac{255^2}{\mathrm{MSE}}\right] \quad (10)$$

The PSNR values of test images for chosen wavelets are plotted against various compression rates and are shown in Fig. 9(a), 9(b), 9(c), 9(d),9(e) and 9(f) respectively. It is evident from the plotted charts that PSNR of the decrypted images is approximately 40 dB and greater, for compression rates larger than 2 bpp. Since PSNR of 40 dB and higher is considered to produce image that is visually acceptable [17] with the noise in the image not being detectable by naked eye, these wavelets show good performance on encrypted images for high compression rates i.e. low compression ratios. After an initial rapid increase, the PSNR increases linearly between 2 bpp and 5.5 bpp but slows down for higher values of bpp as shown for test images in Fig. 9(a), 9(b), 9(c),9(d),9(e) and 9(f).

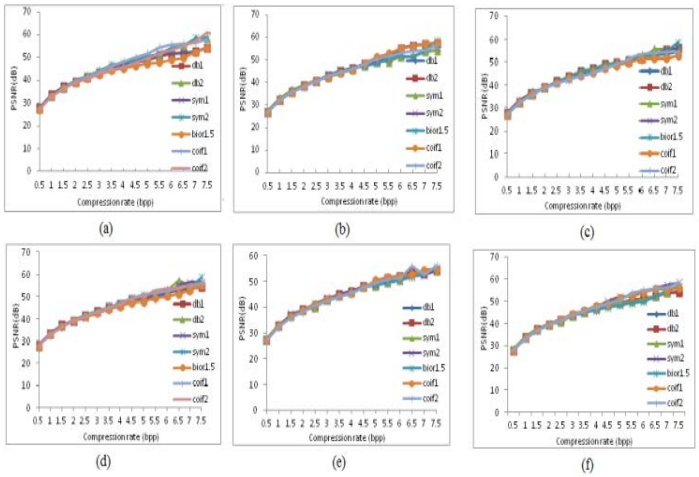

Fig. 5. PSNR of wavelet coded encrypted images

For compression rates of 4 bpp onwards, the performance of wavelets slightly varies from each other. For example at 5.5 bpp, coif2 performs better than the remaining wavelets for Lena image, coif1 shows better results for House image and sym2 exhibits higher PSNR than others in case of Beans image.

For a comparative analysis, the PSNR of unencrypted images is also calculated for various wavelets with compression rates ranging between 0.5 bpp to 7.5 bpp and is plotted in Fig. 10 for the test images. Comparison of the plotted charts for wavelet coded images encrypted images with wavelet coded unencrypted images demonstrates that PSNR of unencrypted images is far greater than PSNR of encrypted images for all compression rates and for every wavelet. In fact PSNR of 320 dB for some test images show lossless compression. In particular, db1 and sym1 outperformed other wavelets when applied on unencrypted images.

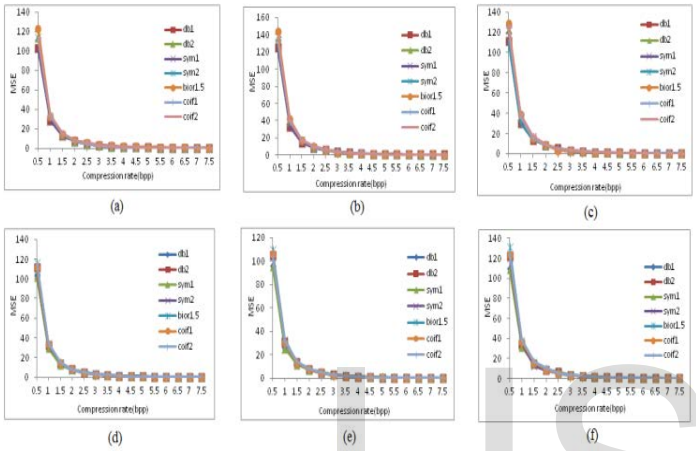

Fig. 6. PSNR of wavelet coded unencrypted images

Comparison of the plotted charts for wavelet coded images encrypted images with wavelet coded unencrypted images demonstrates that PSNR of unencrypted images is far greater than PSNR of encrypted images for all compression rates and for every wavelet. In particular, db1 and sym1 outperformed other wavelets when applied on unencrypted images.

The analysis using PSNR is substantiated with MSE of wavelet coded encrypted images plotted for various compression rates. The plotted charts for Mandrill, Peppers, Lena, Beans, House and Tree test images in Fig. 11(a), 11(b), 11(c) ,11(d),11(e),11(f) respectively show error in the images for lower compression rates; however the errors are almost negligible for compression rates higher than 2 bpp.

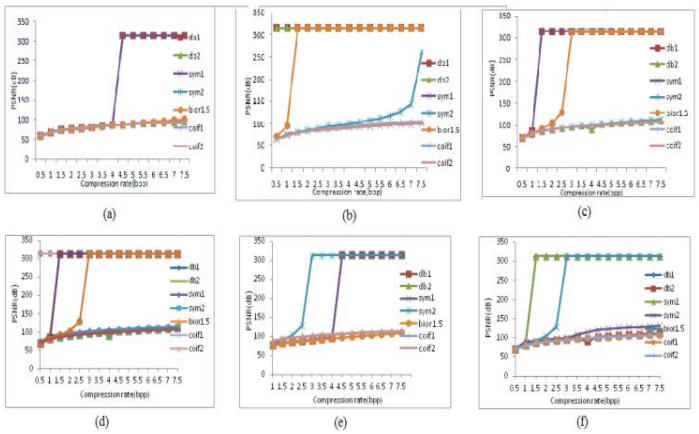

Fig. 11. MSE of wavelet coded encrypted images

Visual output of applying coif1 wavelet on both unencrypted and encrypted Mandrill image is shown in Fig. 12. Fig. 12(a), (a), (c), (e), (g), (i), (k) are the output images coded at 1 bpp without encryption whereas Fig. (b), (d), (f), (h), (j), (l) show the same images coded at 1 bpp with encryption.

Fig. 7. Comparison of coif1-coded output images at 1 bpp

Therefore wavelets' performance on encrypted images is

found to be satisfactory for compression rates higher than 2 bpp as PSNR > 39 dB but their overall performance in terms of PSNR is not as well as it is for the unencrypted color images for due to data scrambling in case of encryption.

4 Conclusion

It is found that applying db1, db2, bior1.5, sym1, sym2, coif1 and coif2 wavelets on fully encrypted color images showed considerable compression for low compression ratios, as evident from the resulting high PSNR (greater than 39 dB) and low MSE (less than 6.9) values, for the compression rates of 2 bpp and above. The PSNR of unencrypted images is also calculated for the said wavelets to perform a comparative analysis with the encrypted images. The performance of these wavelets viz-a-viz PSNR of image is found to be much better when applied directly on the unencrypted color images, as the PSNR was typically 40 to 45 dB and at maximum 270 dB larger than that of encrypted images. These results imply that encrypted images lose the spectral information which is needed by wavelets for compression purpose. However, wavelet based compression on encrypted color images still produces images of good visual quality when used with compression rates of 2 bpp and above, as observed in the experimental findings.

References

[1] C. Chang, M. Hwang, and T. Chen, "A New Encryption Algorithm for Image Cryptosystem," The Journal of Systems and Software, vol. 58, pp. 83–91, 2001.

[2] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg and K. Ramchandran ,"On compressing encrypted data," IEEE Trans. Signal Processing; vol. 52, pp. 2992–3006 , Oct. 2004.

[3] A. M. Ramchandran, A. R. Shehata, "Evaluation of the RC4 algorithm as a solution for converged networks", Journal of Electrical Engineering, Vol 60, pp.155-160, 2009.

[4] X. Zhang, "Lossy Compression and Iterative Reconstruction for Encrypted Image", IEEE Transactions of Information Forensics and Security, Vol. 6, NO. 1; pp. 53-58, March 2011.

[5] A. A. Kumar and A. Makur, "Lossy Compression of Encrypted Image by Compressive Sensing Technique", IEEE Region10 Conference, pp.1-6, 2009.

[6] D. Schonberg, S. Draper, K. Ramchandran, "On compression of encrypted images", *Proc. 2006 IEEE Intl. Conf. on Image Processing (ICIP '06)*, Piscataway, NJ: IEEE Press, pp. 269-272, 2006.

[7] M. Gschwandtner, A. Uhl, P. Wild, "Compression of Encrypted Visual Data", Communications and Multimedia Security, pp. 141-150, 2006.

[8] X. Kang, X. Xu, A. Peng and W. Zeng, "Scalable Lossy Compression for Pixel-Value Encrypted Images", Data Compression Conference, pp. 400-400, 2012.

[9] S. Al-Maadeed and A. Al-Ali, "A new chaos-based Image-Encryption and compression algorithm", Journal of Electrical and Computer Engineering, Volume 2012, January 2012

[10] A. Gurijala, S. A. Khayam, H. Radha, and J. R. Séller, Jr., "On Encryption -Compression Tradeoff of Pre/Post-Filtered Images," in Proc. SPIE Mathematics of Data / Image Coding, Compression, and Encryption VIII, with Applications, Vol. 5915, pp. 1-10, September 2005.

[11] A. Mousa , A. Hamad ,"Evaluation of the RC4 Algorithm for Data Encryption", International Journal of Computer Science and Applications Vol.3, No.2, pp. 44 - 56 , June 2006.

[12] M. Vetterli and C. Herley, "Wavelets and filter banks: Theory and design", IEEE Trans. Signal Processing, vol. 40, no. 9, pp. 2207 -2232, 1992.

[13] D. Sripath, "Efficient Implementations of Discrete Wavelet Transforms using FPGAs", MSc Thesis, Florida State University College of Engineering, 2003, http://etd.lib.fsu.edu/ETD-db/ETDbrowse/browse?first_letter=S

[14] M. S. Song, "Wavelet Image Compression", Proceedings of the 2005 Symposium on Great Plains Operator Theory, AMS Contemporary Mathematics book series, 2005.

[15] M. Nasri, A. Helali, H. Sghaier and H. Maaref, 'Adaptive image compression technique for wireless sensor networks', Computers & Electrical Engineering, Vol. 37, pp. 798–810, 2011.

[16] S. Chang, B. Yu, and M. Vetterli, "Adaptive wavelet thresholding for image denoising and compression", IEEE Trans. Image Processing, vol. 9, pp. 1532 -1546, 2000.

[17] J. M. Guo, and Y. F. Liu, "Joint Compression/Watermarking Scheme Using Majority-Parity Guidance and Halftoning based Block Truncation Coding", IEEE Trans. On Image Processing, Vol. 19, No.8, August 2010.