LOSSY COMPRESSION OF ENCRYPTED IMAGES USING DISCRETE WAVELET TRANSFORM

Hina Shakir, Dr S. Talha Ahsan
SZABIST
Karachi, Pakistan

Abstract - **With the invasion of Multimedia content over the networks, images are often required to be accessed and used in public channels in a secure manner, in order to avoid third party access to the data. The security of images is best attained by applying encryption to the images. Since enciphered data occupies more memory space and bandwidth on the channel during the exchange, compression techniques are used to address the real time bandwidth utilization issues. This research paper aims to propose and evaluate a new mechanism for both compression and encryption of images. The image details are first enciphered with a stream cipher using a pre shared key between the sender and receiver. The stream cipher chosen for encryption is a variant of the efficient encryption algorithm RC4. The encrypted image is then compressed with the help of a lossy compression technique known as Discrete Wavelet Transform Coding. On the receiving end of the network medium, the encoded image is decompressed and decrypted and the retrieved image is compared with the actual image.**

Keywords: Image Compression, Discrete Wavelet Transform, RC4, Stream Cipher

I. INTRODUCTION

Privacy of information flowing on the public network is being exposed to risks with new and advanced technologies. It is also a concern that the data sizes have increased with inclusion of audio and videos on the websites and in the data traffic as well. The concept of compression can be used then to manage the network bandwidth and improve performance issues. The two issues of bandwidth and security can be addressed by compressing the confidential images as shown in Figure 1.

Initially we discussed and reviewed the available technologies for secrecy and compression of coloured images and focused on the case of private cryptosystems to achieve confidentiality of images. In this work, discrete wavelet transforms have been applied on the enciphered images and their performance for public cryptosystems is evaluated with the help of a simulation on Matlab.

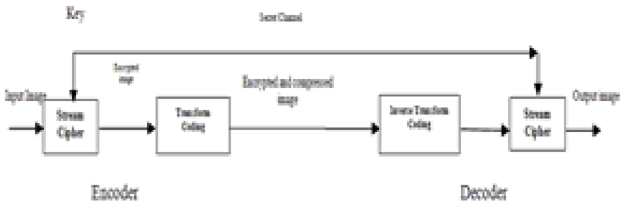

Fig 1: Bandwidth and Security Issues with Media Transfer

Lossy compression of encrypted images is possible with the help of sampling i.e. giving an output image which is easy to be compressed. This is a new approach to work towards images. It was first suggested in research [3] and the technique offers a secure mechanism, making it a potential candidate for exploration. In compressed sensing, no operation is needed for enciphering the data on the sender's side but modifications are made in the decoder at the recipient's end. A method was presented in research [4] to compress linear encrypted images using a similar concept. It was observed that for large compression values the images started showing noise.

Image Encryption techniques include contemporary cryptosystems, which are divided into public and private categories, are discussed .This review of the cryptosystems helped in finalizing the RC4 algorithm for the study. Their purpose, benefits and shortcomings are mentioned. Afterwards, RC4 as an encryption algorithm is explained. Its structure, working and application are included as well. Since RC4 offers reasonable scrambling of data, it is applied on the colour images.

Lossless and lossy are both types of compressions which are defined with an elaborated description of lossy compression. The Transform Coding covers the concept of coding and transformations like the discrete cosine transformation and wavelet transformation. This part explains the reasons that give these transforms an edge over other coding methods. The functional models are explained with the help of charts and figures.

The Discrete wavelet transform and the family of different wavelets are discussed in the next section .The several types of wavelets are listed down with their mathematical models for a better understanding. Their origin, working and benefits in recent times when images with contrast and wide range of frequencies are available on the networks are listed.

Next, the simulation work is provided using Matlab .Colour images after encryption and before encryption are compared. Wavelet transforms are tested on these enciphered images and their performance is measured. PSNR and MSE of decoded images against compression rates are evaluated as performance parameters and then discussed.

In the last section of the paper, the conclusion of this study is given and possible future work for the proposed setup is suggested.

II. EXISTENT

The problem of compressing enciphered information was initially discussed in research [1]. The analysis showed that compressing a secure image without considering some predefined conditions can cause problems in the performance of compression and data security.

It was investigated in research [2] that permutation can be used as a technique to rearrange the information resulting in the encryption of input images and then compression can be applied by removing the repetitive and useless information available after the coding process.

Lossy compression of encrypted images is also possible with the help of sampling i.e. giving an output image which it is easy to be compressed. This is a new approach to work towards images. It was first suggested in research [3] and offers a secure mechanism, making it a potential candidate for exploration. In compressed sensing, no operation is needed for enciphering the data on the sender’s side but modifications are made in the decoder at the recipient’s end. A method was presented in research [4] to compress linear encrypted images using a similar concept. It was observed that for large compression values the images started showing noise.

Instead of encrypting the whole data a better approach is to encipher a portion of the image which will contribute towards the efficiency of the image cryptography. Such a method lets the image contain reasonable information so that lossy compression techniques can easily be implemented. Aparna et al in [5] uses this idea to encrypt the images also discussed by Kuo et al in [6]. In research [5], they use filters for this purpose and work on the phase of the image .Two filters are used, one adds the phases and scrambles the phase band using a filter that sums phases to the existing set .Then on the decoder side there is another filter that reverses the scrambling. They used the JPEG compression technique to encrypt the partial phase encrypted images. The simulation work evaluated the results of compression on the encrypted images partially for various bits per pixel. When 1/4 of the phase coefficients were sparse, the results of compressing the enciphered images were comparable to the input image for compression ratios between 10 and 16. The author concluded that by compressing the image at a higher ratio, the visual details of the image were distorted.

It was noted that most of the work presented discussions about grey scale images and that discrete wavelet transforms have not been used in conjunction with cryptosystems therefore this study may produce some interesting results after investigation.

III. RC4 CIPHER AS OUR CHOSEN CIPHER

RC4 is picked to secure the images for wavelet testing and works on the streams of data rather than working on chunks of bytes. RC4 is a successor of R2 and has shown satisfactory performance for enciphering big files or messages. The code was written keeping in mind the computer architecture and design which makes it an obvious choice [18].

RC4 consists of key initialization, key bytes and enciphering. The initial step is to produce scrambled bytes that work as an input key. The length of these bytes can be anywhere from 5 to 64. The scrambled bytes are later used to produce the key stream. The phase that outputs one byte at a time is vital. The exclusive OR logical operator is applied on the key and the message bytes and the result is to produce the cipher text completing the whole act of cryptosystems.

Wireless LANs use RC4 through which successful attacks have been reported on the confidential data travelling on the network making it a vulnerable cipher but secure web services still use this algorithm to transport secure information to the web users.

IMAGE COMPRESSION TECHNIQUES

Images and videos make up the major part of the traffic on the public data networks. Normalizing the size of information flowing on these networks help in the problem related to poor performance and bandwidth. Image compression is an essential part of the normal image transmission because it offers vast benefits in Information Technology .Various compression standards are already adopted by internet users but a lot is yet to be explored in this field.

An image is compressed by removing unnecessary information which will not alter the visual information of an image perceived by the user. Image compression can be classified into lossy image compression and lossless image compression.

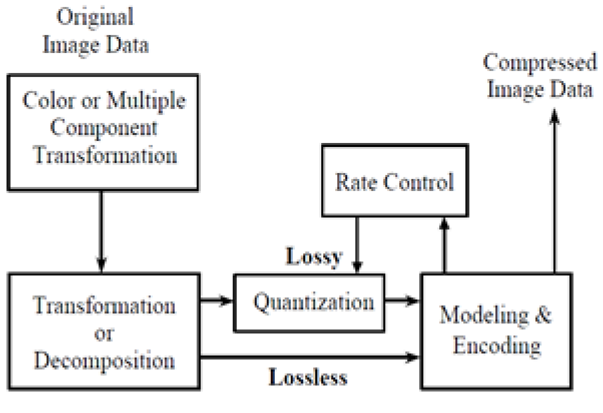

Fig 2: Step by step explanation of Image compression

Lossy predictive coding works directly on the pixels of an image and is a time domain method. Transform coding brings in changes in the transform of an image. This coding works on reversible linear transform like discrete cosine transform and Fourier transform and maps the image into a set of transform coefficients .The coefficients are quantized with little image distortion.

DISCRETE WAVELET TRANSFORM

Discrete wavelet transforms work on the scale and frequency components of the image and can resolve the signal into many levels which show their multiple resolution nature. As of late, only a few image compression standards have included these transforms.

The Wavelet Transforms are different from other transforms because they work in both domains of the signal. It was seen that earlier transforms were not able to analyse specific frequency details in isolation without affecting the rest of the image. However, Wavelets solved this problem by discretely decomposing the signal to many levels. On every level, the signal is passed through a digital filter and sampled up by a factor of 2.

We can express the scenario mathematically as:

$$y[n] = \sum_{k=-\infty}^{\infty} h[k] \cdot x[2n-k] \qquad (1)$$

For reconstructing the signal, the coefficients achieved by the decomposition are passed through high pass and low pass synthesis filter and down sampled by 2.

SIMULATION WORK AND DISCUSSION

Traditional encryption methods remove frequency patterns from the images making the processing of images difficult if it was relying on the perceptual information of the image. The compression show different performance for different images since it is dependent on the frequency details of the image. Lossy compression technique removes information which cannot be retrieved back and this may cause quality of the output image to be low after transformation.

This research study discusses and evaluates the performance of discrete wavelet transform (DWT) as a compression agent on traditional symmetric cipher for color images. Many wavelets transforms which were discussed and tested during this study were: Haar, db2, sym1, sym2, bior1.5, coif1, and coif2. The suggested setup for RC4 secured images and the DWT is given in Figure 3.

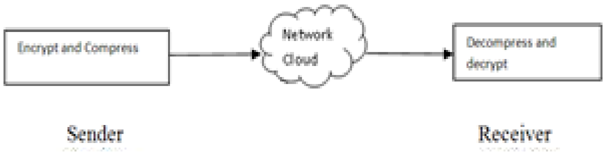

Fig 3: Setup for RC4 and DWT

For simulation purposes the image used is of a Baboon with 256 x 256 x 3 resolution. This study focuses on one image but the results are a representation of other images as well after testing the simulation setup on a variety of other images.

A. *Performance of Proposed Encryption Algorithm*

RC4 has been slightly modified to save processor resources and time. The input key is a 64 bit key and after passing through the two algorithms used by the cipher RC4, the resultant bytes are used as the final key to encipher the image.

The key once received through the above steps is not changed because the simulation uses one image only with known dimensions throughout this whole discussion therefore it is not essential to change the key many times. Finally, the image details are enciphered with the key and the resultant image is scrambled to remove all the information that could show some correlation between the pixels.

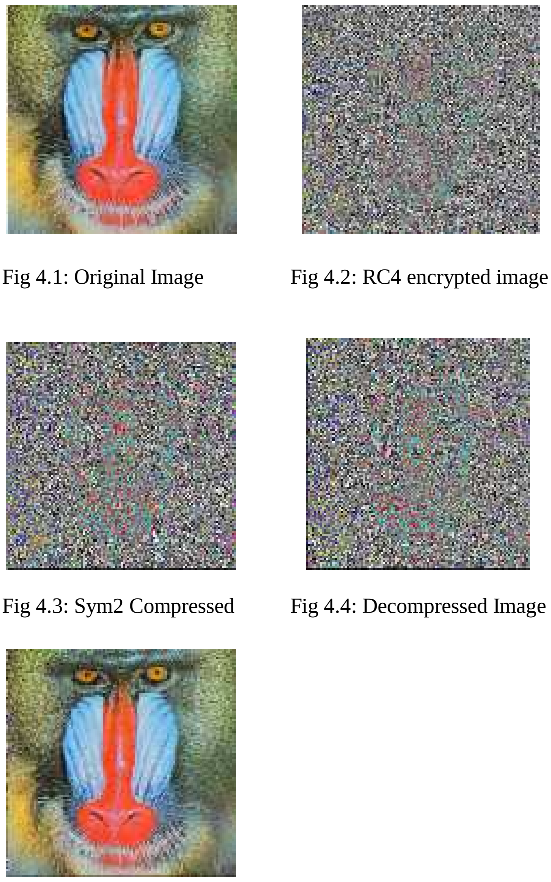

Fig 4.1: Original Image

Fig 4.2: RC4 encrypted image

Fig 4.3: Sym2 Compressed

Fig 4.4: Decompressed Image

Fig 4.5: Output Image

Fig 4: Encoder ((1),(2)&(3)) & Decoder ((4)&(5))

Encoder and decoder of the suggested framework are outlined in Fig 4. It is also noted that our encryption module eliminated visually perceivable details from the image in Figure 4.2.

B. Compression Performance of Wavelets

The encrypted image is compressed on the encoder side with sym2 wavelet at 1 bpp and 8% compression ratio in Figure 4.3.

The enciphered image is subjected to DWT coding with several hard threshold values for compression rates between 0.5 to 7.5 bpp .These compression ratios are lower than the usual performance of the wavelets as wavelets are found to perform better for unencrypted images. The Discrete wavelets used in this experiment are Haar, db2, sym1, sym2, bior1.5, coif1, and coif2.

At the recipient side, the coded image is decoded and decrypted while the quality of output image is measured by computing the Peak Signal to Noise ratio and Mean Squared Error of the output image.

MSE is defined as:

$$MSE= \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}\left[I\,(x,y) - I\,'\,(x,y)\right]^2 \qquad (2)$$

M and N are the dimensions of the image and I(x,y) and I'(x,y) are the image information of the original image and the output image for pixel (x,y).

PSNR is given by:

$$PSNR = 10 * \log10\,(255*255 / \mathrm{sqrt}\,(MSE)) \qquad (3)$$

The PSNR values of the decoded images for chosen wavelets are plotted against various compression rates in Figure 5. It is evident from the plotted chart that for a higher compression ratio, the wavelets performance decreases.

For compression rates of 4 bpp and onwards the wavelets of coif1, coif 2 and sym2 perform comparatively better than the remaining wavelets. This comparison also indicates that these wavelets do not perform well for higher compression ratios when applied on traditional cryptosystems. The relationship of PSNR with compression rates is linearly increasing for low values of bpp but become constant for higher values of bpp.

The same observation can be made when MSE for the decoded images is plotted for various compression rates in Figure 6. The results only confirm what PSNR calculations exhibited showing an error in the images for higher compression. The error in the decoded images decreases with increasing higher compression rates.

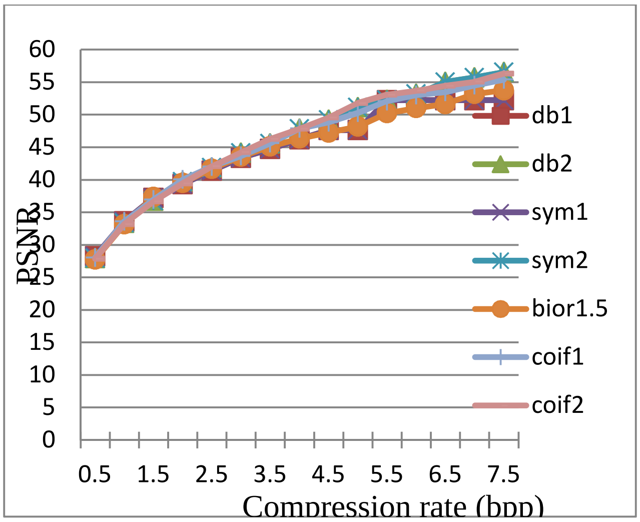

Fig 5: PSNR of wavelet decoded images

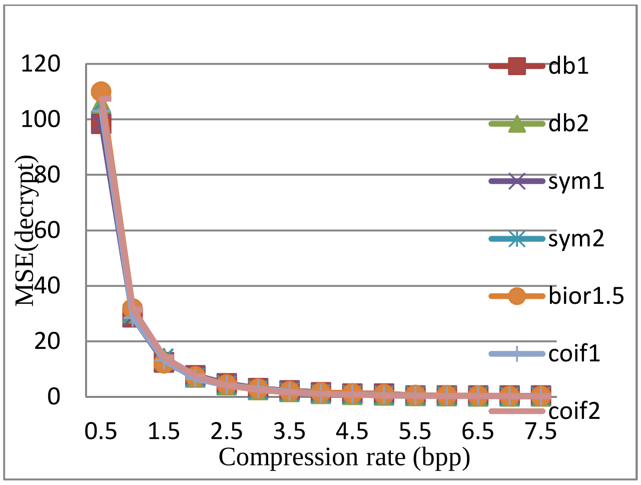

Fig 6: MSE of decoded images

The original image and the output image after decoding for each chosen wavelets are shown in Figure 7 at a compression rate of 0.6bpp. Most of the information in the image seem to remain intact and is visible to the user.

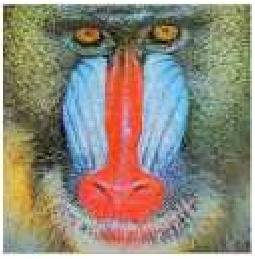

Fig 7.1: Actual Image
Haar

Fig 7.2: Output Image

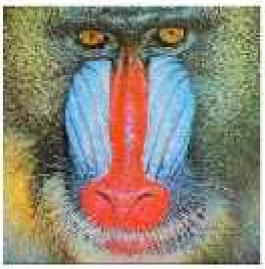

Fig 7.3: Actual Image
Db2

Fig 7.4: Output Image

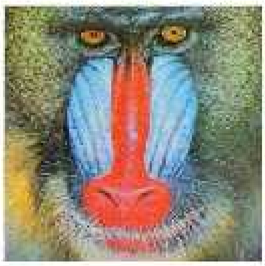

Fig 7.5: Actual Image
Sym1

Fig 7.6: Output Image

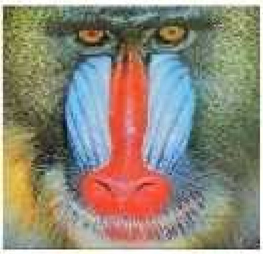
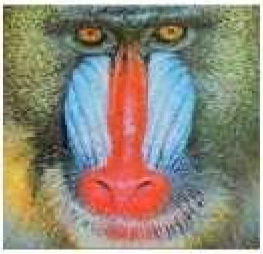

Fig 7.7: Actual Image
Sym2

Fig 7.8: Output Image

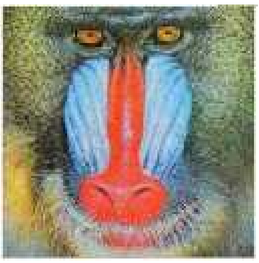

Fig 7.9: Actual Image
Coif1

Fig 7.10: Output Image

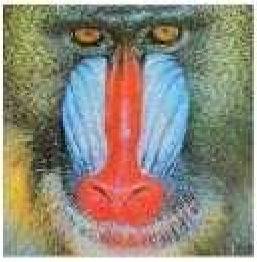

Fig 7.11: Actual Image
Coif2

Fig 7.12: Output Image

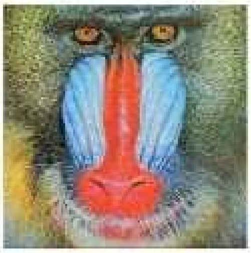

Fig 7.13: Actual Image
Bior1.5

Fig 7.14: Output Image

Fig 7: Comparison of different wavelets used in proposed cod

CONCLUSION AND FUTURE WORK

C. Conclusion

It was found that applying the Haar, db2, sym1, sym2, bior1.5, coif1 and coif2 wavelets on the traditionally enciphered images showed considerable compression but the performance of these wavelets is better when applied directly on the unencrypted color images .The PSNR and MSE values of output images for different compression rates are calculated to support the research study and it is seen that enciphered images lose the spectral information which is to needed by wavelets for compression purpose. This causes producing low compression ratios. The same analysis of PSNR and MSE parameters for output images w.r.t input images reveal that good visual quality of the output images can be obtained at averages compression ratios. It was also concluded that out of all the wavelets used for the simulation work coif1, coif 2 and sym2 performed comparatively better than the rest of the wavelets at higher compression rates hence this family of wavelets can further be investigated.

D. Future Work

Other wavelets from the wavelets family which have not been tested in this study may be taken up for compression of enciphered images in future. Since RC4 is a cipher with average security, strong ciphers like AES may be used along with the wavelets and the performance of such a framework may be evaluated for further elaboration. The results may prove to be useful for practical implementation and applications development.

REFERENCES

[1] Borie J., Puech w., as M, "Crypto-Compression System for Secure TraDumnsfer of Medical Images ",2nd International Conference on Advances in Medical Signal and Information Processing (MEDSIP 2004), September 2004.

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

[3] Xinpeng Zhang, “Lossy Compression and Iterative Reconstruction for Encrypted Image”, in IEEE Transactions of Information Forensics and Security, Vol. 6, NO. 1; March 2011, pp 53-58

[4] Y. Rachlin and D. Baron, “The secrecy of compressive sensing measurements”, Proc. 46th Allerton conference on commun., control, and computing, Monticello, IL; Sep. 2008

[5] A Anil Kumar and Anamitra Makur, “Lossy Compression of Encrypted Image by Compressive Sensing Technique”, IEEE Region10 Conference ;2009

[6] Aparna Gurijala, Syed A. Khayam, Hayder Radha, and J. R. Deller, 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.

[7] C. J. Kuo, J. R. Deller, and A. K. Jain, “Pre/post-filter for performance improvement of transform coding,”Signal Processing: Image Communication Journal, vol. 8, no. 3, pp. 229-239; April 1996

[8] Daniel Schonberg, Stark Draper, Kannan Ramchandran, “On compression of encrypted images”,ICIP 2006;2006

[9] D. Dia, M. Zeghid, M. Atri, B. Bouallegue, M. Machhout and R. Tourki, “DWT-AES Processor for a Reconfigurable Secure Image Coding” in International Journal of Computer Theory and Engineering, Vol. 1, No.2,1793-8201; June 2009

[10] Eric Wharton, Karen Panetta, and Sos Agaian , ‘Simultaneous Encryption/Compression of Images Using Alpha Rooting’in Proceeding DCC '08 Proceedings of the Data Compression Conference IEEE Computer Society Washington, DC, USA ;2008

[11] 10.E. J. Wharton, K. A. Panetta, S. S. Agaian, “Scalable Encryption Using AlphaRooting,” in SPIE Defense and Security Symposium 2008, Orlando, FL,March; 2008

[12] S. Aghagolzadeh and O.K. Ersoy, “Transform image enhancement”, Optical Engineering, 31(3), 614-626;1992

[13] 12.R. Kogan, S. Agaian, and Karen A. Panetta, “Visualization Using Rational Morphology and Zonal Magnitude Reduction”, in Proc. SPIE Symp. Electronic Imaging Science & Technology, 3387, 301-312;1998

[14] 13.R. Kogan, S. S. Agaian, and K. Panetta, “Visualization using rational morphology and zonal magnitude-reduction,” in Proc. SPIE, 3304, 153–163; 1998

[15] Michael Gschwandtner, Andreas Uhl, and Peter Wild, “Compression of Encrypted Visual Data”in Communications and Multimedia Security; 2006: pp141-150

[16] V.Radha, *Member, IAENG*, D.Maheswari,San Francisco, USA “Secured Compound Image Compression Using Encryption Techniques”in Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011; October 19-21, 2011

[17] Somaya Al-Maadeed and Afnan Al-Ali, ‘A new chaos-based Image-Encryption and compression algorithm’ in Journal of Electrical and computer Engineering;2012

[18] A. Boukhriss, O. Jemai and C. Ben Amar , ‘Images Encrypt-Compression by Wavelets Networks’, 4rd International Conference on Natural Computation – IEEE, ICNC'08; Jinan-China; August 2008

[19] Matt J.B. Robshaw, Stream Ciphers, RSA Labs technical report TR-701, Version 2.0; July 25, 1995

[20] Rafael C. González , Richard Eugene Woods, ‘Digital Image Processing’, Prentice Hall; 2008