Resolution Progressive Compression of Encrypted Images

Remya S and Dilshad Rasheed V A
MES College of Engineering, Kuttippuram,Kerala,India
Email: remyaakhil@yahoo.com, dilshadfaruk@gmail.com

***Abstract*—The image compression algorithms are used to reduce the memory space or transmission time. This image compression algorithms can be combined with cryptography to keep the security of the data. Once the data are decrypted, all secrets will be leaked. Hence compression is performed after encryption of the image if there is a need to transmit the redundant data over an insecure and bandwidth constrained channel. The reverse system is also used now a days and it ensures more security. In both cases there is no compromise in compression efficiency. For compression and encryption several techniques are used. Some of these techniques are applicable to grayscale images, some others to color images and others do both. To encrypt the compressed data and for transformation function many techniques are used in several areas. For this transform based coding is used. Resolution Progressive Compression (RPC) is an efficient method for compressing encrypted gray scale images and is based on DWT. In this method at the encoder side a down sampled version of the cipher text is created and an intraframe prediction is performed and it is sent to the decoder. This is a low resolution image and the decoder decodes and decrypts this image and get a high resolution version. This predicted image together with the encryption key is known as Side Information (SI). This SI is used as the input for the next resolution level. The decoder is Slepian Wolf decoder and works by avoiding the Markovian property. Thus the complexity of coding and decoding can be reduced. This resolution progressive compression performs best result for grayscale and color images.**

***Index Terms*—slepian wolf coding, RPC**

I INTRODUCTION

Images are arranged in pixels and image compression programs are generally used for compressing images, which is different from compressing the data. In most of the applications the user needs security. Therefore needs an encryption before compression. This authenticity is provided by a cryptographic system by using transform based coding. Transform based coding is most popular in now a days. The pixels in an image are highly correlated to each other. Therefore the pixels can be predicted from their neighboring pixels. The transform coding transforms the image from spatial domain to frequency domain. In transform coding the pixel values are transformed from spatial to frequency domain. For this firstly the images are subdivided in to blocks. For each block the transform coefficients are calculated. The resulting coefficients are then quantized and the output of the quantize is used by symbol encoding techniques to produce the output bit stream which represents the encoded image. In image decompression model the reverse process takes place. For this two systems are used [1]

Cryptosystem

Reverse cryptosystem.

In a cryptosystem, the data are to be first compressed and then encrypted as shown in Fig. 1. But in some cases the reverse ordering is used. This system offers more security and there is no compromise in compression efficiency. These systems are known as reversed cryptosystem and is shown in Fig. 2.

For these systems several techniques are used. Some of these techniques are applicable to gray scale images, some others to color images and some others do both. In a cryptosystem there are two distinct entities such as the content owner and the network operator. These entities do not trust each other. But they can communicate each other. The content owner protect the privacy of the content using encryption. The network operator reduces the network traffic to maximize the network utilization for gaining the maximum profit. Thus compression is performed by the network operator. The owner do not share the cryptographic key that was used to encrypt the data, to the network provider. The network operator compresses the data after it has been encoded.

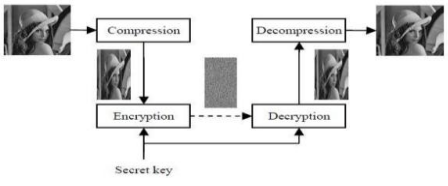

Figure 1. Cryptosystem

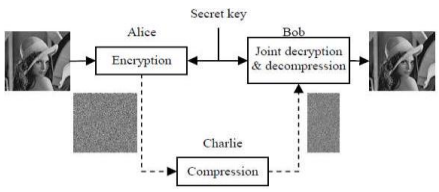

Figure 2. Reverse cryptosystem

Manuscript received Feb 12, 2013; revised June 1, 2013

doi: 10.12720/ijsps.1.1.7-10

This section gives an idea about the basic techniques used in image processing. In the following sections, section II explains the transform coding and section III explains compression of the proposed scheme, section IV explains related works and the conclusion is in section V.

II TRANSFORM BASED TECHNIQUES

The main concept of transform based coding is shown in Fig. 3.

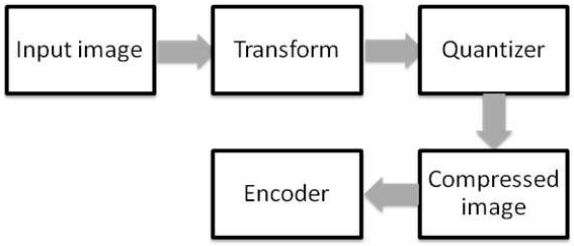

Figure 3. Transform based coding

In transform coding the pixel values are transformed from spatial to frequency domain. For this firstly the images are subdivided in to blocks. For each block the transform coefficients are calculated. The resulting coefficients are then quantized and the output of the quantizer is used by symbol encoding techniques to produce the output bit stream which represents the encoded image. In image decompression model the reverse process takes place.

In transform coding Discrete Wavelet Transform(DWT)[2], [3] decomposes a given image into different levels and these decomposition levels contain a number of sub bands, which consist of coefficients that describe the horizontal and vertical spatial frequency characteristics of the original image. The wavelet transform is computed separately for different segments of the time-domain signal at different frequencies. DWT technique is used to reduce the size of the image with a very small loss in the resolution. In this method the image is divided into blocks of N x N samples and these blocks are transformed independently for calculating the coefficients. For most cases the coefficient is zero. For achieving the compression the coefficients are quantized and by this the non zero values becomes zero. DWT is popular because of their data reduction capability. In DWT the entire image is the input for transformation and the image is compressed as a single data object instead of blocks as in DCT [4]. In DWT the compression error is uniform. DWT provides better image quality but the implementation is more expensive.

III RESOLUTION PROGRESSIVE COMPRESSION

A. Coding and Decoding

The encoder divides the cipher text Y in to four subbands such as 00, 01, 10 and 11. Here the image is an encrypted one and performs down sampling. The 00n represents the subimage in the nth resolution level. And this sub image can be get from

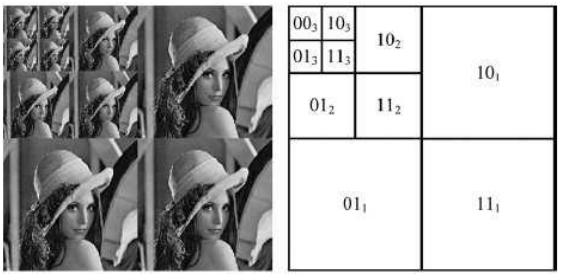

Figure 4. Three level decomposition

00n+1, 01n+1, 10n+1 and 11n+1. This is called down sampling and is shown in Fig4. Here the pixel locations are not shuffled. After the downsampling the low resolution image is obtained. Then each sub image is encoded independently by using the Slepian Wolf coding [5]. The decoding process starts from the 00 subimage of the lowest resolution level. Then the local statistics of the subimage 00 is derived. Based on these local properties other sub images of the same resolution levels are derived by using the interpolation. After the interpolation step SI of the plaintext is obtained and then generate the SI of the cipher text. This is a one-to-one mapping between the SI of the plain text and cipher text. From the SI, the conditional pdf of the original pixel values are calculated with the help of a channel estimation module. Then the SI, estimated PDF and the key is passed to the decoder. The decoder decrypts the 01n, 10n, 11n and then 00n-1 can be synthesized. Repeat the process till the target is obtained. If the SI is a good approximation of the target image the pixels are conditionally independent to each other and there is no need of the Markovian property of Slepian Wolf decoding. The encoder accompanies a feedb ack channel and t h i s channel reports how many bits are transmitted for each subimage. This increase the transmission delay. But this is reasonable.

B. Interpolation

Here for interpolation Context Adaptive Interpolation (CAI) is used for generating side information. For interpolation four horizontal and vertical neighbors or four diagonal neighbors are used for each pixel. If these neighbors are geometrically close to the pixel which is to be interpolated the SI quality will be better. Here a two step interpolation is used.

1. Sub image 11 is interpolated from 00
2. 11 is decoded. Then 00 and 11 is used to interpolate

   01
   and
   10.

The interpolation is shown in Fig 5. The interpolation pattern scales a factor of root 2 and a rotation of Π/4. In the case of pixels on the edge, interpolation along the edge orientation is preferred. A maximum likelihood approach is taken in a statistical model of gray levels to enhance edge detection in the presence of impulsive noise in digital image processing. The median, i.e., the middle value in algebraic rank, of each image

neighborhood, was selected because of its effectiveness for location estimation over a broad range of symmetric noise distributions. The edge detection problem is modeled for both average and median based detectors where the edge is contaminated by various additive noises, and a deterministic analysis is performed to compare the sensitivities of the average and median based methods. The median value technique is shown to have nearly rotationally invariant edge sensitivity when the edge is scanned by the center of the detector. The median value approach is superior for edge detection and sample images and edge maps are provided for a Gaussian noise-corrupted visual scene.

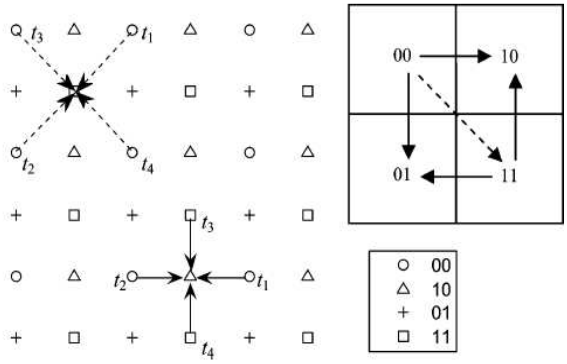

Figure 5. Interpolation

Usually Median Edge Detector and Gradient Adaptive Predictor [4] are used. But the use raster scan order and therefore cannot be used in this scheme and instead Context adaptive Interpolator is used. This two step interpolation provides isomorphism. Isomorphism is a mapping between objects that shows a relationship between two properties or operations. Here only horizontal – vertical interpolator is considered for simplicity.

Let *S* be the pixel to be interpolated. t represents the vector of the neighboring pixel. t[t1,t2,t3,t4] Local statistics of each pixel is considered and divide the local region in to four types such as smooth, horizontally edged, vertically edged and others. For smooth edges median filter is used. Edge filter is used for horizontally and vertically edged regions.

Median filter is used for others.

$$S= \{\text{mean (t)}, (\max(t)-\min(t) <= 20) \; (t1+t2)/2, (|t3-t4|-|t\ I-t2|>20)\ (t3+t4)/2, (|tl-t2|-|t3-t4|>20)\ \text{Median (4), otherwise}\}$$

The second and third condition is adapted from Gradient Adaptive Predictor with an ad hoc threshold.

Another possibility is diagonally edged pixels. But in that case it is not possible to say which side of the edge s lies. In this case also median filter is used.

There is a chance for error propagation due to prediction. By using SW coding the chance for decoding error in high resolution level is minimal even if error occurs in lower resolution level. In this case SI becomes worse and the conditional entropy is increased. But it converges and the error probability vanishes.

C. Features of RPC

- Efficiently exploiting Source dependency in an encrypted image.
- Here the markovian property of SWC coding is avoided and by this the compression performance is better and complexity is reduced.
- Reverse cryptosystem is used in this scheme. Thus the method is more secure.

This section gives the basic idea, coding method and features of the RPC scheme

IV Related Work

Here certain performance measures are used to compare these techniques. Compression ratio(CR) is considered as one of the performance measure. If n1 and n2 denote the number of information carrying units in original and compressed image respectively, then the compression ratio CR can be defined as CR = n1/n2

Based on the compression ratio the relative data redundancy
RD of the original image can be
defined. RD = 1-1/CR

Three possibilities are arised:
1) If n1 = n2, then CR = 1 and hence RD = 0 which implies that original image do not contain any redundancy between the pixels.
2) If n1>>n1, then CR<0 and hence RD>1 which implies considerable amount of redundancy in the original image and
3) If n1<<n2, then CR >$0 and hence RD >1 which indicates that the compressed image contains more data than original image.

Mean S q u a r e d Error (MSE) is considered as another performance measure and is defined as the square of differences in the pixel values between the corresponding pixels of the two images. For DCT based image compression, as the window size increases MSE increases proportionally. But in the case of DWT based image compression MSE first decreases with increase in window size and then starts to increase slowly with finally attaining a constant value.

The comparison is shown in Table I. From these it can be clear that highest PSNR and lowest MSE values provide best features. The comparison with other DWT based methods [6] - [12] are shown in Table1.

TABLE I. Comparison Between Different DWT Methods

PERFORMANCE MEASURE	EZW	SPIHT	SPECK	EBCOT	WDR	ASWDR	RPC
PSNR	31.21	39	32.34	39.26	36.45	36.67	39.46
MSE	155.6583	147.7427	155.6279	146.1438	141.1524	134.1721	128.6754
Edge Correlation	0.549	0.78	0.963	0.966	0.971	0.976	0.98

The method tested in MATLAB with different images and performs well for grayscale and color images both theoretically and experimentally. The PSNR and MSE values show that it is the best method for compression.

and results such as compression performance and entropy are shown in Fig. 6 and Fig. 7.

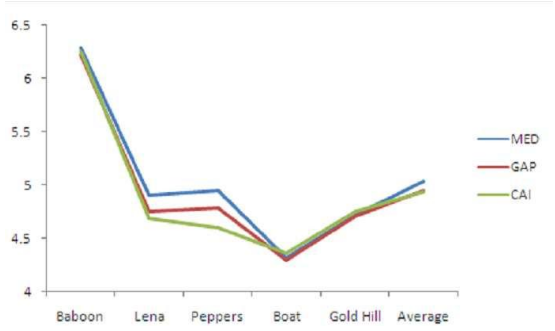

Figure 6. Compression Performance

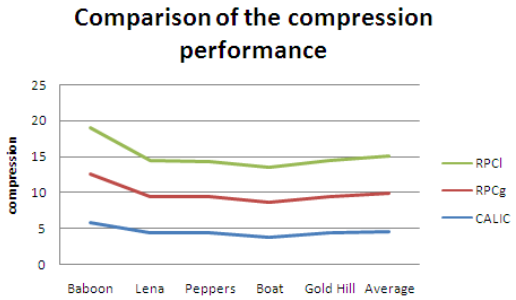

Figure 7. Entropy

V CONCLUSION

Compression of encrypted image is an important issue in image processing. This work focuses on DWT based transform based coding method, RPC.

In DWT based methods Resolution Progressive compression(RPC) scheme proposes to compress the image progressively in resolution so that the decoder can access the image partially. This property offers better results compared to other methods. This method has better coding efficiency and less computational complexity than existing approaches and exploits a 2-D Markov model in Slepian Wolf coding. This method uses reverse cryptosystem and provides a lossless compression.

ACKNOWLEDGMENT

I take this opportunity to convey my deep and sincere thanks to our Principal Dr. V H Abdul Salam and Head of the Department Dr. P P Abdul Haleem. I also extend my deep gratitude to the project coordinators Mr. Lijo V P and Mr. Sobin C C and also to my guide Mrs. Dilshad Rasheed V A for their valuable help and support in presenting the project. I express my sincere gratitude to all the staffs of Computer Science & Engineering Department and my beloved family members who helped me with their timely suggestions and support. I also express my sincere thanks to all my friends who helped me throughout the successful completion of the work. All glory and honor be to the Almighty God, who showered His abundant grace on me to make this project presentation a success

REFERENCES

[1] W. Liu, W. J. Zeng, L. Dong, and Q. M Yao, "Efficient compression of encrypted grayscale images," *IEEE Transactions on Image processing*, vol. 19, no.4, April 2010.

[2] R. Rao Ajit and S. Bopardikar, "Wavelet Transforms-Introduction to theory applications," *Pearson Education Asia*, New Delhi, 2004.

[3] K. P. Soman and K. I. Ramachandran, "Insight into Wavelets from theory to practice," Prentice Hall India, New Delhi, 2002

[4] J. Shukla, M. Alwani, and A. K. Tiwari. *A Survey on Lossless Image Compression Methods*, IEEE 2010

[5] J. Bajcsy and P. Mitran, "Coding for the Slepian-Wolf problem with turbo codes," in *Proc. IEEE Global Telecommun. Conf.*, San Antonio, TX, Nov. 2001, pp. 1400–1404.

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

[7] J. M Shapiro, "Embedded Image coding using zerotrees of wavelets coefficients," *IEEE Transactions on Signal Processing*, vol. 41, no. 12, pp.3445-3462.

[8] A. Said and W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," *IEEE Trans. Circuit and systems for Video Technology*, vol. 6, no. 3, pp. 243-250, June 1996.

[9] A. Islam, Pearlman, "An embedded and efficient low-complexity, hierarchical image coder," *Visual Communication and Image processing 99 proceedings of SPIE*. vol. 3653, pp. 294-305, Jan. 1999.

[10] D. Taubman, "High performance scalable image compression with EBCOT," *IEEE Transactions on. Image Processing*, Mar. 1999.

[11] J. S. Walker, "A lossy image codec based on adaptively scanned wavelet difference reduction," *Optical Engineering*, in press.

[12] S. P. Raja, N. N. Prasanth, S. A. A. Rahuman, S. K. Jinna, and S. P. Princess, "Wavelet based image compression: A comparative study," *International Conference on Advances in Computing, Control, and Telecommunication Technologies*, 2009.

