Compression of Quasi-Group Encrypted Grayscale Images

G.Mohana Priya, P.Vasanthi Kumari

Abstract- When data is transmitted over insecure bandwidth-limited channels, data compression and encryption is always necessary. Slepian-Wolf coding can be applied to the lossless compression of encrypted sources. But for the images, image compression techniques present in the literature that make use of Markov properties in the Slepian-Wolf decoder do not offer significant result. This paper proposes compression of encrypted grayscale image.An encryption algorithm called Quasi-group is used to encrypt thegrayscale image so as to protect the image during transmission. The encrypted image is compressed progressively in resolution by Resolution Progressive Compression (RPC) technique. The experimental result shows that the proposed approach provides significant security and high PSNR value.

Index Terms- Slepian-Wolf coding, RPC, Quasi-group, bandwidth-limited channel, PSNR

I. Introduction

Information explosion combined with the extensive development in software and hardware technology are changing industries, educational institutions, organizations, etc., towards ‘paperless’ environment. This transformation has a strong influence on the quantity of information digitized, thus raising the requirement for competent storage techniques. In association compact storage necessity, security is also regarded as an essential factor during image transmission and storage. Presently, digitized information generally comprises of compound images, which are a mixture of different data types like text, graphics, images, etc. traditional image compression techniques do not create quality compression and thus lot of research has been done in the area of image compression[1].

When data is broadcasted over insecure bandwidth-limited channels, data compression and encryption becomes very necessary. An encryption algorithm transforms the information from comprehensible to incomprehensible structure, thus causing the encrypted data hard to compress by means of any of the classical compression algorithms, which depends on intelligence embedded in the data [2].

Image compression schemes can be broadly classified into two types: Lossless compression and Lossy compression. Inlossless compression, the image after compression and decompression is identical to the original image and every bit of information is preserved during the decompression process. The reconstructed image after compression is an exact replica of the original one.Lossless compression scheme is preferred in the case of medical image compression. In lossy compression, the reconstructed image contains degradations with respect to the original image. Here prefect reconstruction of the image is sacrificed by the elimination of some amount of redundancies in the image to achieve a higher compression ratio. In lossy compression, a higher compression ratio can be achieved when compared to lossless compression [3].

II. LITERATURE SUPPORT

In order to compress the encrypted data stream, researchers have proposed several techniques based on Distributed Source Coding (DSC). DSC utilizes the correlation between the encryption key and the encrypted data, since the encryption key will be known at the decoder. The compression competence of DSC is based on this correlation, such as in this case the statistics of the information source (image) [4].

Kumar and Makur [5] proposed to apply encryption on the prediction error instead of the image. As the prediction errors utilize a Laplacian density function, significant compression can be attained. But, when the information owner applies encryption on the spatial domain of images, DSC based techniques cannot attain significant compression due to the uneven statistical distribution of pixels of the image.

An encrypted image is compressed progressively in resolution by Resolution Progressive Compression technique. The encoder initiates by transferring a downsampled version of the cipher text. At the decoder, the equivalent low resolution image is decoded from which a higher resolution image is obtained by intraframe prediction. The symmetric cryptographic technique called Quasi-group has good data scrambling property is used to encrypt the grayscale images[7] [8].

Slepian-Wolf codes are observed to produce fair results for binary images. But, certain drawbacks are associated with this approach. (i)Markov decoding in a Slepian-Wolf decoder is costly, particularly when handling with sources of nonbinary alphabets.(ii) Bit-plane based markov decoding indeed minimizes the complexity, however the source dependency that initially defined in the symbol domain is generally not fully utilized when translated to bit-planes. (iii) As image and video data are known to be extremely non-stationary, a global markov model cannot illustrate its local statistics accurately. Yang et al., [10] integrated Slepian-Wolf coding and trellis coded vector quantization for lossy compression of encrypted Gaussian sources.

Lossy image coding by Partitioned Iterated Function Systems (PIFS) commonly known as fractal image compression. In this approach, an image is encoded as a group of contractive transformations which denote the image compactly and generate an approximation to the original image. Fractal image compression has high compression ratio and resolution independence [12]. A novel secure image-coding is presented for still images based on encrypting certain parameters in the contractive fractal transformation. Thus the end user gets only a partially readable image of poor quality. The clear image can be obtained upon request. In this scenario, the distributor will provide the client with a simple key to retrieve the clear image from the low quality image. This approach is highly secure and moreover, it offers relatively high compression.

The JPEG grayscale image compression is based on a data embedding technique that uses a secret key and secret mapping vector in the frequency domain. An encrypted feature vector obtained from the frequency domain is embedded redundantly and imperceptibly in the marked image. On the receiver side, the feature vector from the received image is obtained again and compared against the obtained watermark to authenticate the reliability and legitimacy [13].

III. METHODOLOGY

The proposed approach compresses the encrypted image progressively in resolution. This paper uses the quasi-group encryption and resolution progressive compression techniques.

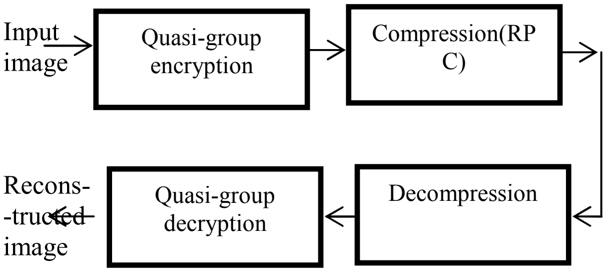

Figure 1: Proposed approach

The encryption technique used in this approach is the quasi-group, which has significant data-scrambling properties and thus it has effectively used in symmetric cryptography. The main aim of the scrambler is to enhance the entropy at the output even in scenario where the input is constant. The massive complexity associated with the assignment of discovering scrambling transformation assures the effectiveness of the encryption process. Quasi-group encryption is a development that has permutation based scrambling at its basis.

Figure 2: Quasi-group Encryptor

If Q is a quasi-group such that $a_1,a_2,a_3,\ldots,a_n$ belong to it, then the encryption operation QE(Quasi-Encryptor) which is defined over the defined elements, maps those elements to another vector $b_1,b_2,b_3,\ldots,b_n$ such that the elements of the resultant vector also belong to the same quasi-group.

The mathematical equation for encryption is defined by,

$$E(a_1, a_2, a_3, \ldots a_n) = b_1, b_2, b_3, \ldots, b_n \qquad (2)$$

where $b_1=a*a_1$,$b_i=b_{i-1}*a_i$, I increments from 2 to the number of elements that have to be encrypted and a is the hidden key.The Multi Level Indexed encryptor is denoted as,

$$QE^{I_r I_s}_{h_1,h_2,\ldots\ldots h_n}(a_1, a_2, a_3, \ldots, a_n) = e_1, e_2, e_3 \ldots e_n \quad (3)$$

where $a_1, a_2, a_3 \ldots, a_n$is the input data and $e_1, e_2, e_2, \ldots e_n$is the output vector $I_r$and $I_s$are called indices that are arrays which have the indices of quasigroups having corresponding order. The vector ($h_1, h_2, \ldots, h_n$) is the hidden key or the secret key.

The decryption process is highly alike the process of encryption. The key point to be considered is the construction of the inverse matrix. The left inverse '\' is used for the quasi-group decryption.The mathematical equation for decryption is defined by,

$$D(a_1, a_2, a_3 \ldots, a_n) = e_1, e_2, e_3, \ldots e_n \qquad (4)$$

where $e_1=a/a_1$ and $e_i=a_{i-1}/a_{i.}$The decryptor for a multilevel indexed based algorithm may be defined as follows,

$$QE^{I_r I_s}_{h_1,h_2,\ldots\ldots h_n}(e_1, e_2, e_3, \ldots, e_n) = a_1, a_2, a_3 \ldots a_n \quad (5)$$

where $e_1, e_2, e_3 \ldots, e_n$ the input data and $a_1, a_2, a_3, \ldots a_n$is the output vector $I_r$and $I_s$are called indices that are arrays which have the indices of quasigroups having corresponding order. The vector ($h_1, h_2, \ldots, h_n$) is the hidden key or the secret key.

3.1 ALGORITHM

3.1.1 Encryption Algorithm:

Input: *Image, Encryption Key*
Output: *Encrypted Image*

1. Get the size of the image and store in *r* and *c* respectively.
2. Convert image matrix into a vector.
3. Obtain all odd position values initially and then even position values.
4. Construct a new image matrix by filling the odd positions values followed by even position values.
5. Convert new image matrix into a vector.
6. Convert the decimal key into binary key data.
7. Binary key datais embedded in the vector.
8. Convert the vector into image matrix of size (r,c).

3.1.2 Decryption Algorithm:

Input: *Encrypted Image,, Decryption Key*
Output: *Decrypted Image*

1. Convert the encrypted image matrix into a vector.
2. Convert the decimal key into binary key.
3. The binary key *data1* is initially used for decryption and stored as a vector.
4. Thevector is converted to image matrix of size (r,c).
5. Image matrix is divided into two vectors.
6. *// if 'n' is number of pixels in image, then 'n/2' is the size of the vectors.*
7. The new image matrix is created by filling the, odd position pixels and even position pixels values from two vectors.
8. The resulted image is the decrypted imageof size (r,c).

The encrypted image is compressed using resolution progressive compression. The encoder gets the ciphertext Y and decomposes it into four subimages, namely, the 00,01,10 and 11 subimages. Each subimage is a downsampled –by-two version of the encrypted image. The name of a subimage denotes the horizontal and vertical offsets of the downsampling. The 00 subimage is further downsampled to create multiple resolution levels. We use 00_n to represent the 00 subimage in the n-th resolution level. The 00_n subimage can be losslessly synthesized from the 00_{n+1}, 01_{n+1}, 10_{n+1} and 11_{n+1}subimages. Decoding initiates from the 00 subimage of the lowest resolution N level. Then, other subimages of the identical resolution level are interpolated from 00_N subimage. Context adaptive interpolation technique is used to obtain the subimages of same resolution level.

IV. EXPERIMENTAL RESULTS

The performance of the proposed approach is evaluated based on MSE and PSNR. For this experimental observation, standard images like lena, cameraman and Barbarais taken. The software package (MATLAB) is used as the engine for image processing experiments.Mean Square error(MSE) is the error between the original and reconstructed image. A very small value of MSE means lower error. The formula for MSE (6) is,

$$MSE = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}[f(i,j) - f'(i,j)]^2 \qquad (6)$$

where M and N are number of rows and columns, f(i,j) is the original image and f'(i,j) is the reconstructed image.The image quality is measured objectively by using Peak Signal to Noise Ratio (PSNR). The common use of the PSNR is to measure the quality of reconstructed images. PSNR is usually expressed in decibels, which is a logarithmic scale. The formula for PSNR (7) is,

$$PSNR = 20 * \log_{10}\frac{255}{\sqrt{MSE}} \qquad (7)$$

where MSE is the Mean Square Error.The basic metric, Compression Ratio (CR) is used to evaluate the performance of compression algorithm. The formula for compression ratio (8) is,

$$CR = \frac{Uncompressed\ image}{Compressed\ image} \qquad (8)$$

Table I shows the MSE and PSNR value for the images. Encrypted image is compressed using Resolution Progressive Compression.

.

Table I : MSE and PSNR value for proposed method

Images	MSE	PSNR(db)
Lena	0.9118	48.5316
Cameraman	2.3445	44.4303
Barbara	2.7744	44.7044
Goldhill	2.6222	43.9431

Table II shows the storage space used after and before compression.Figure 3 shows the comparison of storage space before and after compression.

Table II: Memory space used before and after compression

Standard Images	Before Compression (KiloBytes)	After Compression (KiloBytes)
Lena	65	8.35
Cameraman	64	7.34
Barbara	70.5	8.03
Goldhill	62	7.77

Figure 3 shows the comparison of storage space before and after compression.

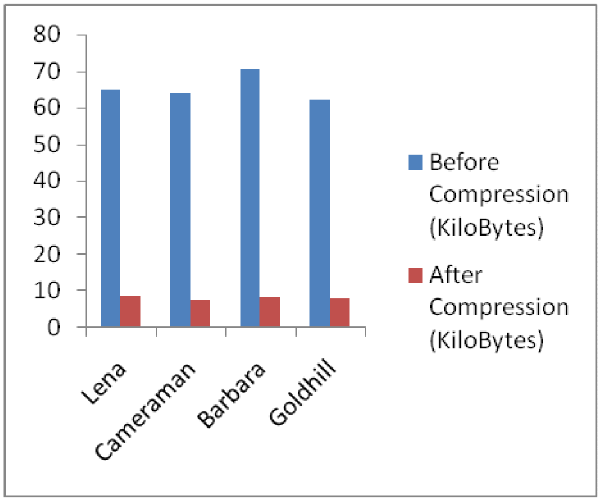

Figure 3: Comparison of original and compressed image

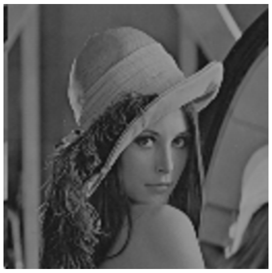

Figure 4: Original image

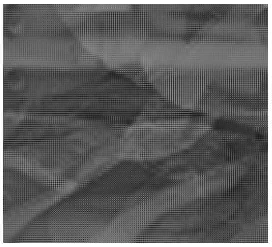

Figure 5: Encrypted image

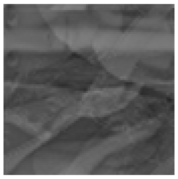

Figure 6: Compressed image

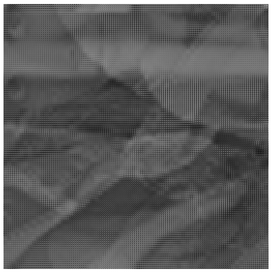

Figure 7: Reconstructed image

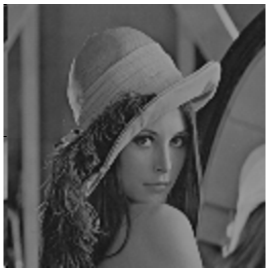

Figure 8: Decrypted image

V. CONCLUSION

This paper proposes a compression of encrypted grayscale images. The grayscale image is encrypted by using Quasi-group algorithm. It enhances the security of image during transmission. The encrypted grayscale image is compressed by Resolution Progressive Compression. The performance of the proposed approach is evaluated based on the PSNR and MSE. It is observed from the experimental results that PSNR approach is high when compared with traditional value.

REFERENCES

[1] Maheswari, D.; Radha, V.; "Secure layer based compound image compression using XML compression", IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Page(s): 1 – 5, 2010.

[2] Kumar, A.A. Makur, A., "Lossy Compression of Encrypted Image by Compressive Sensing Technique", IEEE Region 10 Conference, TENCON, 2009.

[3] S.Jayakumar, S.Esakirajan, T.Veerakumar, "Digital Image Processing", Tata Mc Grawhill publications.

[4] Z. Xiong, A. D. Liveris and S. Cheng, "Distributed source coding for sensor networks", IEEE Signal Processing Magazine, Vol. 21, pp. 80-94,. 2004.

[5] A. A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images", Proc. IEEE 10th workshop on multimedia and signal processing, Cairns, Australia, pp. 760-764, Oct. 2008.

[6] J. D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," IEEE Trans. Inf. Theory, vol. IT-19, pp. 471–480, Jul. 1973.

[7] W.Liu, W.Zeng, L.Dong and Q.Yao, "Efficient Compression of Encrypted Grayscale Images", IEEE Transactions on Image Processing, Vol 19, No 4, April 2010.

[8] Maruti Venkat Kartik Satti, "Quasi Group based Crypto-System", A Thesis, 2007.

[9] 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.

[10] Y. Yang, V. Stankovic, and Z. Xiong, "Image encryption and data hiding: Duality and code designs," in Proc. Inf. TheoryWorkshop, Lake Tahoe, CA, Sep. 2007, pp. 295–300.

[11] D. Schonberg, "Practical Distributed Source Coding and its Application to the Compression of Encrypted Data," Ph.D. dissertation, Univ. California, Berkeley, 2007.

[12] El-Khamy, S.E. Abdou and H.E.-D.M.; "A novel secure image coding scheme using fractal transformation", Proceedings of the Fifteenth National Radio Science Conference, NRSC, 1998.

[13] Mursi, M.F.M.; Assassa, G.M.R.; Aboalsamh, H.A.; Alghathbar, K.; "A Secure Semi-Fragile JPEG Image Authentication Scheme Based on Discrete Cosine Transform", International Conference on Computing, Engineering and Information, 2009.

[14] Kościenly, C. 2002. Generating quasi groups for cryptographic applications. Int. J. Appl. Math. Comput. Sci., vol.12, No.4, 559–569.

[15] V. Dimitrova, J. Markovski, On Quasigroup Sequence Random Generator. Proceedings of the 1st Balkan Conference in Informatics, Y. Manolopoulos and E. Spirakis, Eds., 21-23 November, 2004, Thessaloniki, Greece, pp. 393 – 401.

AUTHORS

First Author – G.Mohana Priya, Email: mohanamecse@gmail.com
Second Author – P.VasanthiKumari, Email: vasanthipvk@gmail.com