Secure Image Compression Using Auxiliary Information

[1] Mr. S.Vaira Prakash HOD, [2] M.Priyanka,S, [3] S. Rukmani [4] C.Vijayalakshmi,
[1][2][3][4] Department of ECE,
[1][2][3][4] Kalasalingam Institute of Technology.
Krishnankoil, Srivilliputhur

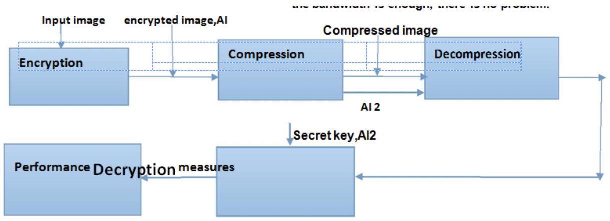
***Abstract*— Secure transmission of data in these days is the need of the hour. Here we have used some techniques to effectively encrypt and compress the multimedia data for transmission. Effective transmission of information is required in many fields like defence,medical field etc. In our proposed scheme the sender uses auxiliary information for compression and image reconstruction. Auxiliary information has two parts one part is useful for image compression and the second part is useful for image reconstruction. At receiver side, the original image content can be reconstructed using the compressed encrypted data and the secret key. Result shows the ratio-distortion performance of the proposed scheme is better than that of previous techniques.**

***Index Terms*—image encryption, image compression, compression ratio-distortion performance**

I. INTRODUCTION

To secure our data at the time of transmission cryptography is the most needed one. It is derived from a Greek word called kryptos which means secrets. It is the art of safe guarding documents and makes sure that only authenticated user are able to recover data.It is a essential facility of converting a plain text into cipher signals again into original form. Encryption plays a main role in this. Here we are using some techniques to reduce the correlation between pixels in the image so as to increase the security. Compressing encrypted multimedia such as images is an emerging technology aimed at reducing the size of cipher-text signals without revealing the plaintext content [1, 2]. In some cases if a sender encrypts the uncompressed plain signals for privacy protection [3],compression work is left to a channel or storage-device provider.After receiving the compressed encrypted data, an authorized user with secret key can reconstruct the plaintext content. For the encrypted multimedia data compression, the cipher signals can be viewed as the source, and the secret key and the estimate of plaintext content as the side information. The goal is to efficiently compress the cipher-texts and to retrieve the plaintexts from compressed data by using secret key. The original binary image may be encrypted by adding a pseudorandom string, and the encrypted data compressed as the syndromes of low-density parity-check (LDPC) chanel codes [1]. Compression of encrypted data by using LDPC codes [5], and lossless compression for encrypted gray and color images using LDPC codes in Various bit-planes [6] can be realized. In [7], encryption is performed on prediction errors rather than the image pixels, and LDPC codes are used. In [8], the encrypted image is decomposed in a progressivemanner.somealgorithmsfor compressing encrypted video are presented. In [9], a lossless compression method for cipher-texts encrypted by AES and cipher-block chaining mode is developed.There are also two types of loss compression methods for encrypted signals: compressive-sensing-based method and quantization-based method. With the first one, the data compressor employs the compressive sensing technique for data reduction. For example, a plaintext image is encrypted by permuting blocks as well as pixels in each block.In [10], after producing the cipher-text images by pixel permutation, the encrypted data are compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. At the receiver side, the discarded rough information of coefficients is retrieved by an iterative procedure with the aid of spatial correlation in natural images so that the principal plaintext content is reconstructed. In [11], the original pixel values are masked by a modulo- 256 addition to avoid leakage of statistical information, leading to better security. The encrypted data are then decomposed into several parts, each being compressed into a bitstream by quantization in Hadamard domain.The more the available bit streams higher will be the resolution of image at the receiver side. This paper proposes a new and efficient way of encrypting images. By employing such techniques we are able to provide a high secure data. In encryption process we are encrypting first the original images. Then it is compressed by the channel provider. At receiver side a secret key is used to retrieve the original image.

BLOCK DIAGRAM



II. PROPOSED SCHEME

In the proposed scheme, the sender uses some ways to encrypt the multimedia signal such as images by suitable encrypting technologies. Here we have used Blowfish algorithm for encryption. Blowfish is a variable length key symmetric block cipher, designed by Bruce schneier and included in a large number of encryption methods. The sender encrypts the input image and transmits the encrypted version to the channel. Upon receiving this data, channel provider transmits this data if the bandwidth is enough to the receiver. Suppose if the bandwidth is not enough, then the sender may receive a message called bandwidth insufficiency. Then sender must generate some auxiliary information for this and provides this to channel. Auxiliary information consists of two parts which is very much useful for image compression and reconstruction.

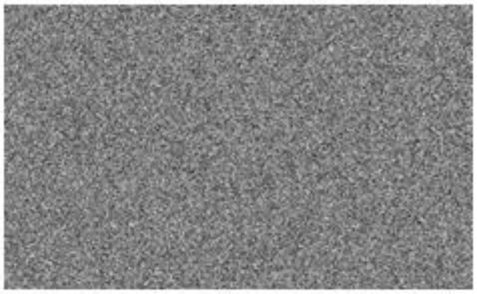
2.1. Image encryption and auxiliary information generation

In this phase, the sender encrypts the original image by using Blowfish algorithm.This algorithm has 16 rounds. First divide input into equal number of pixels. Then perform modulo addition followed by Xor operation. Assume the original image is in uncompressed format and the pixel values are within [0, 255]. Denote the numbers of the rows and the columns in the original image as $N1$ and $N2$, and the number of all pixels as N implying that the bit amount of original image is 8N. Now we are able to get encrypted version of image.It isdenoted by c(i,j).An attacker with out the knowledge of secret key cannot reveal the image content.If suppose the bandwidth is enough, there is no problem.

If the sender receives a band width insufficiency message from the receiver then he must generate auxiliary information. This information is provided to the channel to help in the compression process.Let as assume that N1 and N2 are multiples of 8. The sender then generates a down sampling sub image.The following diagram shows the original and encrypted images.

(a) Original image

(b) Encrypted image



Here we are using the original Lena as a reference. Then, the content owner divides the original and interpolated images into a small number of blocks(64) and performs 2D DCT in each block,where DCT means the 2D discrete cosine transform. With viewing the coefficients as 64 sub-bands, the sender calculates the square roots of the average interpolation distortion in each sub band.It is denoted using Greek letter sigma.These values are regarded as first part of auxiliary information.The following formula is

$/$

$N8\ ^{N}\ 2\ /$

$_{1}\ 1\ \ 8\ 1\quad [P(8i\quad u,8\ \ j\quad v)u,8\qquad j$

$G(8i\qquad\qquad v)]^{2}$ used for

i

$o\ \ j\ \ 0$

calculating the table values.

80.4	43	40.1	20.9	14.6
38.9	26.2	24.9	17.3	10.1
21.	21.5	18.9	13.2	9.2

2				
11.6	6.8	6.7	2.7	7.3

Data amount of encrypted image is same as that of original image. But data amount of auxiliary information is very low.There is less complex involve in generating auxiliary information.Then sender provides two parts of auxiliary information to channel. Here second part is generated by using a binary map. It is denoted by s(i,j). To calculate binary map we have to use modulo addition between pixels in the original and interpolated images. The following formula is used for calculating binary map that s(i,j)=p(i,j)+k(i,j).This formula denotes binary map for original image.

(c) Interpolated image

The above diagram shows interpolated image

2.2 *Compression of encrypted image*

The next important step is compression.If the bandwidth of the channel is enough, there is no further operation is needed.If suppose the bandwidth is not enough, then sender provides some auxiliary information for this purpose.At receiver side, only the authenticated user can recover the original image by using a secret key. We have to generate a number of keys based on our application.The compression procedure is as follows.

1.Implement 2DCT in a block by block manner in encrypted image.Then reorganise the coefficients as a vector $C^{(u,v)}$(n).

2.Then perform orthogonal transform.

3.For each sub band channel provider selects a positive real number and a positive integer.By using this we can form the downsampling sub image.Following is down sampling image,

(d) Sub image

At last find compression ratio R,which is the ratio between compressed data and the original data.

2.3 Image reconstruction

Steps to recover the original data are

1. Decompose the encrypted image.
2. Then decrypt sub image to get original sub image.For this use bilinear interpolation method.Perform 2DCT in a block by block manner to reorganise sub bands.Perform Inverse Orthogonal and inverse 2DCT transform. Then original image is obtained.

III. OPTIMIZING COMPRESSION *PARAMETERS*

In order to lower the distortion in the reconstructed image,we have to find ways to increase the values of positive real number (*u*,*v*) and positive integer *M*(*u*,*v*).Compression ratio is related to values of (*u*,*v*) and *M*(*u*,*v*) . The larger the value of *M*(*u*,*v*) , lower will be MSE. Hence it is important to select the values to reduce MSE

IV. EXPERIMENTAL RESULTS

Here we have used Lena as original image. When producing a encrypted version, the sender also provides the auxiliary information.The proposed schemeperformsbetterthanmethodsin[10],[11].In[10] and[11]many iterative procedures are needed.But in our proposed scheme no iterative procedure is needed.And also the computational complexity in our scheme is very lower than that of methods in [10]and[11].The reconstruction procedure of the proposed scheme cost 1.18 seconds for each image whilethosein[10]and[11]cost10.24and13.65secondr espectively. Example:Reconstructed image with compressionratio0.172and PSNR 35.5db

V. CONCLUSION

Our work proposes a scheme of compressing encrypted images using auxiliary information. The sender provides encrypted images using blowfish algorithm and auxiliary information to the channel provider.Then at the channel compression can be performed.At the receiver side secret key is used to recover the original data.Here by using auxiliary information along with blowfish algorithm the correlation between pixels is reduced and compression ratio is improved.This scheme is suitable for secure transmission of any kind of data.

REFERENCES

[1] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On Compressing Encrypted Data," *IEEE Trans. Signal Processing*, 52(10), pp. 2992–3006, 2004.

[2] Z. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, "Protection and Retrieval of Encrypted Multimedia Content: When Cryptography Meets Signal Processing," *EURASIP Journal on Information Security*, pp. 1–20, 2007.

[3] N. S. Kulkarni, B. Raman, and I. Gupta, "Multimedia Encryption: A Brief Overview," *Rec. Advan. in Mult. Sig. Process. and Commun.*, SCI 231, pp. 417–449,2009.

[4] D. Schonberg, S. C. Draper, and K. Ramchandran, "On Blind Compression of Encrypted Correlated Data Approaching the Source Entropy Rate," *Proceedings of the 43rd Annual Allerton Conf.*, Allerton, IL, 2005.

[5] R. Lazzeretti, and M. Barni, "Lossless Compression of Encrypted Grey-Level and Color Images," *Proceeding of 16th European Signal Processing Conference (EUSIPCO 2008)*, Lausanne, Switzerland, August, 2008.

[6] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient Compression of Encrypted Grayscale Images," *IEEE Trans. Signal Processing*, 19(4), pp. 1097–1102, 2010.

[7]D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, "Toward Compression of Encrypted Images and Video Sequences," *IEEE Trans. Information Forensics and Security*, 3(4), pp. 749–762, 2008.

[8]D. Klinc, C. Hazayy, A. Jagmohan, H. Krawczyk, and T. Rabinz, "On Compression of Data Encrypted with Block Ciphers," *Proceedings of IEEE Data Compression Conference (DCC '09),PP. 213-222,2009.*

[9] X. Zhang, "Lossy Compression and Iterative Reconstruction for Encrypted Image," *IEEE Trans. on Information Forensics & Security*, 6(1), pp. 53-58, 2011.

[10]X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable Coding of Encrypted Images," *IEEE Trans. on Image Processing*, 21(6), pp. 3108-3114, 2012.

[11] S.-W. Ho, and L. Lai, and A. Grant, "On the Separation of Encryption and Compression in Secure Distributed Source Coding," *Proceedings of IEEE Information Theory Workshop*, pp. 653–657, 2011.