Image Encryption and Compression Using Some Auxiliary Information

R. Ramesh
Department of Electronics and Communication Engineering
Narayana Engineering College, Nellore, Andhra Pradesh, India

J.Sunil Kumar
Associate Professor
Department of Electronics and Communication Engineering
Narayana Engineering College, Nellore, Andhra Pradesh, India

Abstract- This paper proposes a novel scheme of encryption and compression of images in this we are using some additional information called auxiliary information. The original information sender encrypts the original image before compressing and some auxiliary information also generates, that the auxiliary information will be used for image compression and reconstruction of the image at output side. Then, we are using encryption for the channel provider cannot access the original information at the time of compression. The compression of the encrypted images by using quantization method with optimal parameters that are derived from auxiliary information and compression- ratio distortion criteria, and transmitted compression data. The transmitted data consists of quantization data, quantization parameters, and another part of auxiliary information and encrypted sub-images. At receiver side, the compressed image to be decompressed and decryption will be performed by using encrypted and compressed data and the secrete key. Experimental result shows that performance of the ratio- distortion is better than previous technique.

Index terms – Ratio - performance, Image encryption, Compression.

I. INTRODUCTION

Compressing and encrypting both are emerging technologies, compressing aimed to reduce the amount of data in cipher-text (encrypted image) signals without degrading plaintext (original image) signal. The owner of the content encrypts the original uncompressed image due to better security, after completion of encryption the compressing process is performed at channel provider, the channel provider access only limited amount of data but encryption key is not received, so that accessing information at compression is difficult. Authorized person only access original information who having secret key can only reconstruct the plaintext content. These process having better security for our information. In general compressing encrypted process, the content owner first encrypts the images and then transmits to the channel provider for compression. In this process compression does not compromise security of systems. For the compression of encrypted multimedia, the cipher-text signals are to be both source as well as secret key. The aim is to compress efficiently the cipher-texts and to retrieve the good quality plaintexts data from decompressed process by exploiting the side information. According to Slepian-Wolf coding, number of practical schemes using have been proposed. For example, the encryption of original binary image is to be adding a pseudorandom string, and compressed the encrypted data using Low-Density Parity-Check (LDPC) channel codes. Encrypted data compression for hidden Markov sources and memory less using LDPC codes, and encrypted gray and color images are used lossless compression using LDPC codes in different bit-planes are also to be realized. In this prediction errors are performed in encryption process of the image pixels, and for cipher-texts compression used LPDC codes. Perfectly decoding of plain text content can be using some local Statistics are obtained from a low-resolution version. After the cipher-text images producing by pixel-permutation, compressed the encrypted data by removing the excessively rough and fine information of coefficients.

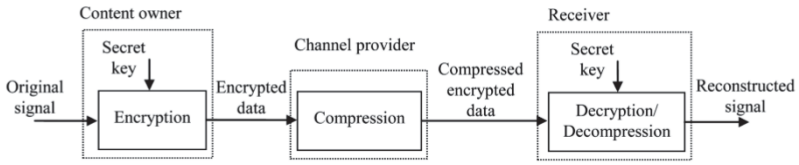


Fig. 1. System of encrypted signals compression.

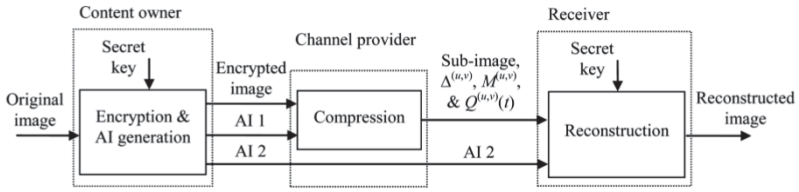


Fig. 2. Sketch of the proposed scheme.

Scalable coding is another method for encrypted images, by using this scalable coding all original pixel values in image are masked by using modulo-256 addition. Use of this process is to avoid statistical information leakage, and better security also provide. At the receiver side more the available bit streams, the higher the resolution of principle plaintext contents can be reconstructed. In this performance of compressing encrypted data may be as good as that compression of non-encrypted data, the practical compression ratio distortion performance is not up to that of the conventional compression methods.

This paper proposes a novel scheme of encrypting and compressing of images by using some extra information called auxiliary information. In encryption stage, the original images before compressed images are encrypted by the content owner, and at the time of encryption some auxiliary information is also produced. This auxiliary information used for when the channel bandwidth is not enough. In compression stage, the encrypted data is the input of compression and in this compression various DCT sub-bands are used, these are compressed effectively by using a quantization mechanism without degrading the original information, and an optimization method with ratio-distortion criteria is employed to select the quantization parameters according to the auxiliary information. At a receiver side, by using secret key the original plaintext content can be re constructed. The result of the experiment shows the ratio-distortion performance of the proposed scheme is significantly better than that of existing techniques.

II. PROPOSED SYSTEM

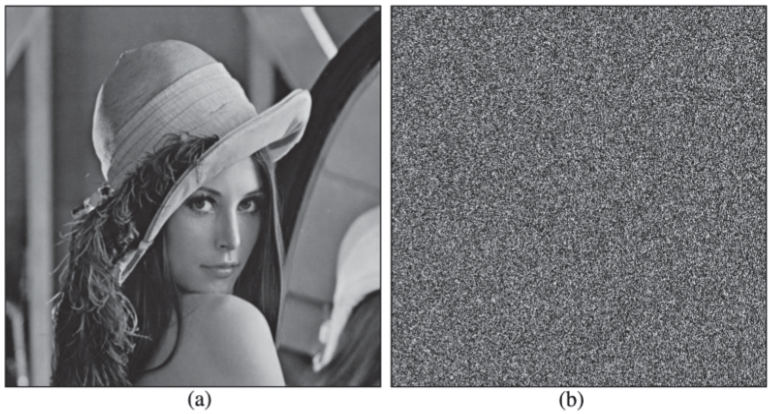
In the proposed scheme, the owner of the content firstly masks all pixel values in original image before compressing image to get an encrypted image and the encrypted image is send to the channel provider. If the bandwidth is sufficient then the channel provider transmits the encrypted data. Otherwise, the channel provider sends a message "insufficient-bandwidth" to the owner of the content, and then the auxiliary information generated by the content owner according to the original and encrypted information and provides it to the channel provider. Basically the auxiliary information (AI) is having two parts that will be used for compression of the data and image reconstruction. Then, the compression of the image because of the original content is secured in the channel who cannot access the original content. The coefficients in encrypted domain by a quantization method with using the first part of auxiliary information (AI 1), and compression data is transmitted, that the transmitted data include an quantization data ,the quantization parameters, encrypted sub-image, and the second part of auxiliary information(AI2), through a channel. At receiver side, an authorized user can reconstruct the principal content of original image by retrieving the coefficient values. By involving the auxiliary information in to encrypted image compression, the performance of the ratio-distortion is improved and the computational complexity is reduced. A sketch of the proposed scheme is presented in Fig. 2.

A. Image Encryption and Generation of Auxiliary Information-

In this stage, the owner of the content first encrypts the original image by adding some pseudo random numbers into the pixels. The original image is before compression the pixel values to be with in [0,255]. The number of and columns in image are N1, N2, and total number of pixels are multiplication of both rows and columns, that is N(N=N1*N2). The original image bit amount is 8*N. The owner of the content generates pseudo-randomly N integers and distributed uniformly within [0,255], and by using modulo 256 addition and produce an encrypted image.

$$c(i,j)=\mathrm{mod}[p(i,j)+k(i,j),256],1=i=N1,1=j=N2 \quad (1)$$

Here, p(i,j) is the pixel position gray value or (i,j), k(i,j) is the numbers of pseudo-random are derived from the secret key, and c(i,j) is the encrypted image. The values of c(i,j) are uniformly distributed within the range of [0,256]. Fig. shows a Lena's original image and its encrypted version. Unknown persons without the knowledge of secret key cannot see the image content.



(a) (b)

Fig. 3. (a) Original image Lena and (b) its encrypted version.

(a) (b)

Fig. 4. (a) Downsampling Lena and (b) its interpolated version.

If bandwidth is sufficient, no need to other operation. Otherwise, if receives a message like "bandwidth-insufficiency" from the channel provider, the content owner must produce the auxiliary information and provides it to the channel provider for convenience of data compression and image reconstruction at receiver side.

We assume both and are multiples of 8. The content owner generates a down sampling sub-image with a size of N1/8*N2/8, and the fig shows the sub-image of Lena and the interpolation image is compressing. Hear the owner of the content original image and interpolated images number of 8x8 sized blocks, and after that 2D discrete cosine transform is perform in each block.

$$\begin{bmatrix} P(8i+1,8j+1) & \cdots & P(8i+1,8j+8) \\ \vdots & \ddots & \vdots \\ P(8i+8,8j+1) & \cdots & P(8i+8,8j+8) \end{bmatrix}$$
$$= \mathrm{DCT}\left\{ \begin{bmatrix} p(8i+1,8j+1) & \cdots & p(8i+1,8j+8) \\ \vdots & \ddots & \vdots \\ p(8i+8,8j+1) & \cdots & p(8i+8,8j+8) \end{bmatrix} \right\},$$
$$0 \le i \le N_1/8-1, \quad 0 \le j \le N_2/8-1$$

and

$$\begin{bmatrix} G(8i+1,8j+1) & \cdots & G(8i+1,8j+8) \\ \vdots & \ddots & \vdots \\ G(8i+8,8j+1) & \cdots & G(8i+8,8j+8) \end{bmatrix}$$
$$= \mathrm{DCT}\left\{ \begin{bmatrix} g(8i+1,8j+1) & \cdots & g(8i+1,8j+8) \\ \vdots & \ddots & \vdots \\ g(8i+8,8j+1) & \cdots & g(8i+8,8j+8) \end{bmatrix} \right\},$$
$$0 \le i \le N_1/8-1, \quad 0 \le j \le N_2/8-1$$

Here DCT means the discrete cosine transform of 2D. The viewing the coefficients are 64 sub-bands, the owner of the content calculates the square roots of the average interpolation distortion in each sub-band, shown in fig at the bellow of page. That is measure the differences between the interpolated and original images in the sub-bands. Fig gives the values of the Lena image. In normal, the lower sub-bands correspond to the larger. Then, the

$$\sigma^{(u,v)} = \sqrt{\frac{\sum_{i=0}^{N_1/8-1} \sum_{j=0}^{N_2/8-1} [P(8i+u,8j+v) - G(8i+u,8j+v)]^2}{N_1 N_2/64}}, \quad 1 \le u,v \le 8$$

80.4	43.1	40.1	20.9	14.6	9.7	6.7	5.1
38.9	26.2	24.9	17.3	10.7	7.8	5.8	4.4
21.2	21.5	18.9	13.2	9.2	7.0	4.8	3.9
11.6	11.6	11.1	9.3	7.3	5.4	4.3	3.4
6.9	6.8	6.7	6.6	5.4	4.3	3.5	3.1
4.6	4.6	4.6	4.4	3.9	3.4	3.1	2.9
3.5	3.4	3.3	3.3	3.2	2.9	2.7	2.6
3.0	2.9	2.8	2.7	2.7	2.7	2.5	2.4

Fig. 5. Values of $\sigma^{(u,v)}$ for Lena.

In this owner regards values of auxiliary information. The owner of the content calculates a binary map

$$s(i,j) = \left\lfloor \frac{p(i,j)+k(i,j)}{256} \right\rfloor \oplus \left\lfloor \frac{g(i,j)+k(i,j)}{256} \right\rfloor$$

Since the g(i,j) of interpolated version is similar to p(i,j) original image, most of s(i,j) are 0 and rest, s(i,j) of small proportion , are 1.

B. Compression of Encrypted Images-

After completion of encryption, the channel band width is sufficient then compression is needless, so the channel provider transmits the information directly. In this stage, allows only a particular, who having secreted key can only decrypts the original information without any loss. If channel resources limited, then the channel provider send a message is "un sufficient bandwidth". Then the content owner generates some auxiliary information and sends it to the channel provider. After receiving encrypted information the channel provider encrypts the original content using some additional compression techniques.

Actually, the compression will be performed in 64 DCT sub-bands with different quantization parameters. The channel provider firstly implements 2D DCT in the encrypted image with a block-by- block manner,

$$\begin{bmatrix} C(8i+1,8j+1) & \cdots & C(8i+1,8j+8) \\ \vdots & \ddots & \vdots \\ C(8i+8,8j+1) & \cdots & C(8i+8,8j+8) \end{bmatrix} = \mathrm{DCT}\left\{ \begin{bmatrix} c(8i+1,8j+1) & \cdots & c(8i+1,8j+8) \\ \vdots & \ddots & \vdots \\ c(8i+8,8j+1) & \cdots & c(8i+8,8j+8) \end{bmatrix} \right\}, \quad 0 \le i \le N_1/8-1, \quad 0 \le j \le N_2/8-1$$

Then reorganizes the coefficients in each sub-band in a vector, which is indicated as

$$[C^{(u,v)}(1), C^{(u,v)}(2), \ldots, C^{(u,v)}(N_1N_2/64)]^T \quad , (1\le u,v\le 8).$$

After that, perform orthogonal transform for the vectors to calculate

$$\begin{bmatrix} D^{(u,v)}(1) \\ D^{(u,v)}(2) \\ \vdots \\ D^{(u,v)}(N_1N_2/64) \end{bmatrix} = \mathbf{A} \cdot \begin{bmatrix} C^{(u,v)}(1) \\ C^{(u,v)}(2) \\ \vdots \\ C^{(u,v)}(N_1N_2/64) \end{bmatrix}, \quad 1 \le u, v \le 8$$

At last channel provider collects all down sampling sub images of the encrypted version,

$$c_D(i,j) = c(8i, 8j), \quad 1 \le i \le \frac{N_1}{8}, 1 \le j \le \frac{N_2}{8}$$

The compression ratio between original and compression data, is

$$R = \frac{\frac{N}{8} + \frac{N}{64} \cdot \sum_{u,v} \log_2 M^{(u,v)} + L_S}{8N} = \frac{1}{64} + \frac{1}{512} \cdot \sum_{u,v} \log_2 M^{(u,v)} + \frac{L_S}{8N}$$

Where Ls is the second part of auxiliary information length.

C. Image Reconstruction-

After completion of compression, we want to retrieve the data at receiver side. By using this method a specific user only reconstruct the original image due to the secrete key. The decomposing of original information is involve several steps are shown below.

1. To get the original data by decomposing the compressing encrypted sub images

$$[Q^{(u,v)}(1), Q^{(u,v)}(2), \ldots, Q^{(u,v)}(N_1N_2/64)]^T,$$

2. Decrypt the sub-image to get the original sub-image, and get the interpolated image using the bilinear interpolation method. Also retrieve the second part of auxiliary information.

3. Calculate,

$$s'(i,j) = s(i,j) \oplus \left\lfloor \frac{g(i,j) + k(i,j)}{256} \right\rfloor$$

Where k(i,j) are pseudo-random numbers, derived from secrete key.

$$s'(i,j) = \left\lfloor \frac{p(i,j) + k(i,j)}{256} \right\rfloor$$

Thus, encryption equation implies the following relation between c(i,j),p(i,j) and k(i,j).

$$c(i,j) = \begin{cases} p(i,j) + k(i,j), & \text{if } s'(i,j) = 0 \\ p(i,j) + k(i,j) - 256, & \text{if } s'(i,j) = 1 \end{cases}$$

Indicating,

$$\bar{k}(i,j) = \begin{cases} k(i,j), & \text{if } s'(i,j) = 0 \\ k(i,j) - 256, & \text{if } s'(i,j) = 1 \end{cases}$$

We have that,

$$c(i,j) = p(i,j) + \bar{k}(i,j)$$

So, that receiver can obtain estimated of encrypted image,

$$c(i,j) = p(i,j) + \bar{k}(i,j)$$

4. In this stage, the receiver will modify the estimated encrypted image. After 2D DCT in a block by block manner

$$\begin{bmatrix} \tilde{C}(8i+1,8j+1) & \cdots & \tilde{C}(8i+1,8j+8) \\ \vdots & \ddots & \vdots \\ \tilde{C}(8i+8,8j+1) & \cdots & \tilde{C}(8i+8,8j+8) \end{bmatrix}$$
$$= \text{DCT} \left\{ \begin{bmatrix} \tilde{c}(8i+1,8j+1) & \cdots & \tilde{c}(8i+1,8j+8) \\ \vdots & \ddots & \vdots \\ \tilde{c}(8i+8,8j+1) & \cdots & \tilde{c}(8i+8,8j+8) \end{bmatrix} \right\},$$
$$0 \le i \le N_1/8 - 1, \quad 0 \le j \le N_2/8 - 1$$

And reorganizing the DCT coerricients in 64 sub-bands as 64 vectors, calculate

$$\begin{bmatrix} \tilde{D}^{(u,v)}(1) \\ \tilde{D}^{(u,v)}(2) \\ \vdots \\ \tilde{D}^{(u,v)}(N_1N_2/64) \end{bmatrix} = \mathbf{A} \cdot \begin{bmatrix} \tilde{C}^{(u,v)}(1) \\ \tilde{C}^{(u,v)}(2) \\ \vdots \\ \tilde{C}^{(u,v)}(N_1N_2/64) \end{bmatrix},$$
$$1 \le u, v \le 8$$

And

$$\hat{D}^{(u,v)}(t) = \text{round}\left[\frac{\tilde{D}^{(u,v)}(t) - Q^{(u,v)}(t) \cdot \Delta^{(u,v)}}{\Delta^{(u,v)} \cdot M^{(u,v)}}\right] \cdot \Delta^{(u,v)} \cdot M^{(u,v)} + Q^{(u,v)}(t) \cdot \Delta^{(u,v)}$$
$$1 \le u, v \le 8, \quad 1 \le t \le N_1N_2/64$$

$$\text{mod}\left\{\text{round}\left[\frac{\hat{D}^{(u,v)}(t)}{\Delta^{(u,v)}}\right], M^{(u,v)}\right\} = Q^{(u,v)}(t)$$

Then, perform the inverse orthogonal transform

$$\begin{bmatrix} \hat{C}^{(u,v)}(1) \\ \hat{C}^{(u,v)}(2) \\ \vdots \\ \hat{C}^{(u,v)}(N_1N_2/64) \end{bmatrix} = \mathbf{A}^{-1} \cdot \begin{bmatrix} \hat{D}^{(u,v)}(1) \\ \hat{D}^{(u,v)}(2) \\ \vdots \\ \hat{D}^{(u,v)}(N_1N_2/64) \end{bmatrix}$$

and the inverse 2D DCT

$$\begin{bmatrix} \hat{c}(8i+1, 8j+1) & \cdots & \hat{c}(8i+1, 8j+8) \\ \vdots & \ddots & \vdots \\ \hat{c}(8i+8, 8j+1) & \cdots & \hat{c}(8i+8, 8j+8) \end{bmatrix}$$

5. Final stage is reconstruct the original image,

$$\hat{p}(i,j) = \hat{c}(i,j) - \bar{k}(i,j)$$

III. Optimizing Compression Parameters

The channel provider always hopes to achieve a good ratio distortion performance, in other words, to lower the distortion in the reconstructed image with a certain compression ratio or to minimize the amount of compressed data with certain distortion level. This section will present method for optimizing the values of and according to the auxiliary information.

TABLE I
Values of $\Delta_0(1, M)$ and $f_0(1, M)$ with Different M

M	1	2	3	4	5	6	7	8	9	10	…
$\Delta_0(1, M)$	–	2.80	2.33	1.70	1.42	1.18	1.07	0.92	0.83	0.75	…
$f_0(1, M)$	1.00	1.14	0.54	0.31	0.21	0.15	0.11	0.09	0.07	0.06	…
Convex hull	×	–	–	×	×	×	×	×	×	×	…

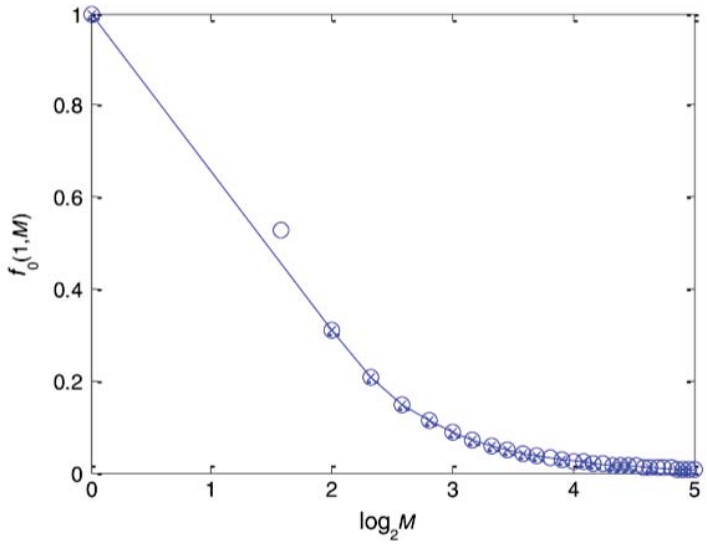


Fig. 6. Points with coordinates $(\log_2 M, f_0(1, M))$ and the convex hull.

56	29	25	13	9	6	1	1
25	17	15	10	6	4	1	1
13	13	12	8	5	1	1	1
7	7	7	5	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1

Fig. 7. Values of $M^{(u,v)}$ when $\lambda = -20$ was used for compressing encrypted Lena.

(a) (b)

Fig.8. (a) Reconstructed Lena with compression ratio 0.172 and PSNR 35.5 dB, and (b) another reconstructed version with compression ratio 0.114 and PSNR 32.8 dB

IV. EXPERIMENTAL RESULT

The Lena image was used as the original in this experiment. During the process of encryption, the auxiliary information also generated. As showed above, the first part of auxiliary information consists of the values of 64 sub-bands given in Fig, and the bit amount of the second parties. In compression phase, when we

chose, meaning that in Fingers were used, the ratio of compression was 0.172. The re constructed result from the compressed encrypted data is shown in Fig. The value of MSE is 18.24, verifying the theoretical value in(47),18.38,and PSNR is 35.5dB. When, the corresponding and are given in Figures. In this case, the ratio of compression is 0.114, and the image is reconstructed with PSNR32. 8dB is shown in Fig. Here, reconstructed MSE image is 34.26, while the theoretical MSE in (47) is 34.27 compares the ratio-distortion performance of several encrypted image compression techniques and unencrypted JPEG compression when Lena was used as the original. We also made a comparison over 100 gray images sized and 100 gray images sized 1920×2560, which contain landscape and people. When compressing the encrypted/unencrypted images with same parameters, we calculated the average values of compression ratios and PSNR in reconstructed images, which are shown in Figs. The ratio-distortion performance of the proposed scheme is lower than that of JPEG compression. On the other hand, the proposed scheme generally out performs the methods in [15] and [16], though the performance of the proposed scheme is slightly better than or very close to that of method in[15] with a high compression ratio. With the methods in [15] and [16], iterative updating procedures are necessary at receiver side to find convergent solutions that are regarded as finally reconstructed results. However, the iterative procedures may be not convergent when the compression ratio is less than 20%.That means the proposed scheme is more suitable for low compression ratio. Furthermore, the computational complexity of the proposed scheme is significantly lower than that of [15] and [16]. There construction procedure of the proposed scheme cost 1.18 seconds for each image in average when PC with 2.40 GHz CPU and 3.00 GB RAM was used, while those in [15] and [16]cost10.24 and 13.65 seconds respectively.

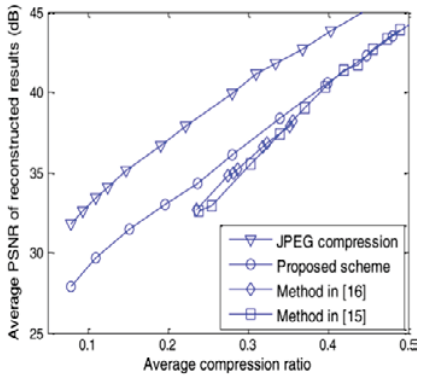


Fig.9. Compression of compression ratio-distortion. Performance over 100 images sized 2520 x 3776

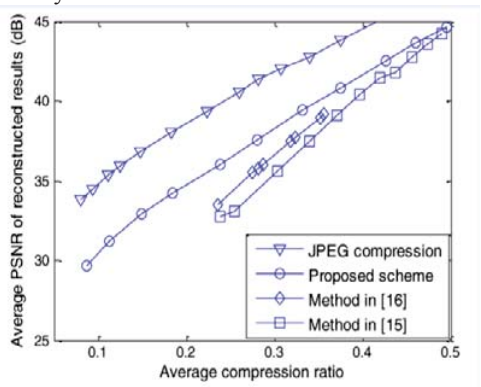


Fig.10. Compression of compression ratio-distortion Performance over 100 images sized 1920 x 2560

V. CONCLUSION

Encryption process we are using modulo-256 addition. This work proposes a scheme of compressing and encrypting images with addition of some auxiliary information. While the owner of the content encrypts the original image and produce some auxiliary information, the channel provider compressing the encrypted image by using quantization method by using some optimal parameters derived from the first part of auxiliary information, and then transmits an the quantized data, encrypted sub-image, the quantization parameters and the part of auxiliary information. At receiver side, the original image content can be regenerated by using the compressed of encrypted data and the secret key. In this scheme, the auxiliary information is need less when channel bandwidth is sufficient.

REFERENCES

[1] X Zang, Y Ren, L Shen, Z. Qian, "Compressing Encrypted Images With Auxilary Information,"IEEE Trans. Multimedia, Vol. 16, No.5, August 2014.
[2] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
[3] 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 J. Inf. Security, pp. 1–20, 2007.
[4] N. S. Kulkarni, B. Raman, and I. Gupta, "Multimedia encryption: A brief overview," Recent Adv. Multimedia Signal Process. Common. Vol. SCI 231, pp. 417–449, 2009.
[5] G. Jakimoski and K. P. Subbalakshmi, "Security of compressing encrypted sources," in Proc. 41st Asilomar Conf. Signals, Systems and Computers (ACSSC 2007), 2007, pp. 901–903.
[6] D.Schonberg, S.C.Draper, andK.Ramchandran,"Onblindcompressionofencryptedcorrelateddataapproachingthesourceentropyrate," inProc.43rd Annu.AllertonConf., Allerton, IL, USA, 2005.

[7] R.LazzerettiandM.Barni,"Losslesscompressionofencryptedgreylevel and color images," in Proc. 16th Eur. Signal Processing Conf. (EUSIPCO 2008), Lausanne, Switzerland, Aug. 2008.
[8] A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," in Proc. IEEE 10th Workshop Multimedia Signal Processing, 2008, pp. 760–764.
[9] W.Liu, W.Zeng,L.Dong, andQ.Yao,"Efficientcompressionofencrypted grayscale images," IEEE Trans. Signal Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
[10] D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, "Toward compression of encrypted images and video sequences," IEEE Trans. Inf.Forensics Security, vol. 3, no. 4, pp. 749–762, 2008.
[11] D. Kline, C. Hazayy, A. Jagmohan, H. Krawczyk and T.Rabinz,"On compression of data encrypted with block ciphers, "in Proc. IEEE Data Compression Conf.(DCC '09), 2009, pp. 213–222.
[12] D. L. Donoho, "Compressed sensing," IEEE Trans. Inf. Theory, vol. 52, no. 4, pp. 1289–1306, 2006.
[13] E. J. Candes and M. B. Wakin, "An introduction to compressive sampling," IEEE Signal Process. Mag., vol. 25, no. 2, pp. 21–30, Mar. 2008.
[14] A. Kumar and A. Makur, "Lossy compression of encrypted image by compressing sensing technique, " in Proc. TENCON2009 IEEE Region 10 Conf., 2009, pp. 1–6.
[15] X. Zhang, Y. Ren, G. Feng, and Z. Qian, "Compressing encrypted image using compressive sensing," in Proc. 7th Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2011), 2011, pp. 222–225.
[16] X. Zhang, "Lossy compression and iterative reconstruction for encryptedimage," IEEE Trans.Inf.Forensics Security, vol.6, no.1,pp. 53–58, 2011.
[17] X.Zhang,G.Feng,Y.Ren,andZ.Qian,"Scalablecodingofencrypted images," IEEE Trans. Image Process., vol. 21, no. 6, pp. 3108–3114, Jun. 2012.
[18] S.-W. Ho, L. Lai, and A. Grant, "On the separation of encryption and compressioninsecuredistributedsourcecoding,"inProc.IEEEInformation Theory Workshop, 2011, pp. 653–657.