A Novel scheme for lossy compression of an encrypted image with flexible compression ratio and reconstruction by iterative interpolation

Miss Christina Bage
Electronics & Telecommunication Department
KCCEMSR
Thane, India
bage.chris@gmail.com

Mr.Ujwal harode
Electronics Department
Pillai Institute of Information technology
Panvel, India
ujwal.harode@gmail.com

Abstract— **The presence of computer networks has prompted new problems with security and privacy. The rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted over the internet. The security of digital images involves several different aspects, including copyright protection, authentication, confidentiality and access control. Content confidentiality and access control are addressed by encryption, through which only authorized parties holding decryption keys can access content in clear text. The objective of image compression is to reduce irrelevance and redundancy of the image data in order to be able to store or transmit data in an efficient form.**

Keywords— Image compression, image encryption, Pseudorandom permutations, orthogonal transform, iterative reconstruction.

I. Introduction

Data compression and encryption is always a necessity when transmitting data on an insecure bandwidth limited channels. Conventionally the task of compression and encryption was achieved first by compression and then by applying encryption on the compressed data stream. At the receiver side, the decryption and decompression operations are orderly performed to recover the original data. However, in some applications, a sender needs to transmit some data to a receiver and hopes to keep the information data confidential that is secure to a network operator who provides the channel resource for the transmission of that particular data. That means the sender should encrypt the original data and the network provider may tend to compress the encrypted data without any knowledge of the cryptographic key and the original data. At receiver side, a decoder integrating decompression and decryption functions will be used to reconstruct the original data.

This work proposes a strategy for lossy compression of an encrypted image with flexible compression ratio. The method used here for encryption is pseudorandom permutation which will encrypt the original image, and the encrypted data will be efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. At the receiver side the encrypted as well as compressed data, with the aid of spatial correlation in natural image, the receiver will reconstruct the principal content of the original image by iteratively updating the values of coefficients. This way by updating the coefficients value the compression ratio will be high which will lead to a smoother original image thus the better quality of the reconstructed image. This ratio gives an indication of how much compression is achieved for a particular image. The compression ratio typically affects the picture quality. The tradeoffs between compression ratio and picture quality is an important one to consider when compressing images.

.

II. SYSTEM MECHANISM

In this scheme, a pseudorandom permutation is used to encrypt an original image. Then, the encrypted data will be efficiently compressed by discarding the excessively rough and fine information of coefficients in the transform domain and the receiver will reconstruct the principal content of the original image by iteratively updating the values of the coefficients.

A. Encryption of an image

Encryption masks digital content so that it appears completely random, and thus renders traditional compression algorithms ineffective. Best practices therefore dictate that content must be compressed before it is encrypted. Unfortunately best practices in compression and security cannot be assumed. Encryption coding has been done in may applications[3]. This motivates the search for novel compression routines that operate on uncompressed, encrypted data.

Assume the original image is in uncompressed format and each pixel with a gray value falling into [0, 255] is represented by 8 bits. Denote the numbers of the rows and the columns in the original image asN1 andN2 , and the number of all pixels asN (N=N1*N2). Then, the amount of bits of the original image is 8N.

Encrypted data = permuted pixel-sequence

Original data =

1	2	3	4	5	6	7	8	9	10
13	14	12	68	59	100	111	42	39	36

Permutation order 8, 7, 3, 1, 6, 2, 9, 4, 10, 5

Encrypted data =

1	2	3	4	5	6	7	8	9	10
42	111	12	13	100	14	39	68	36	59

B. Compression on encrypted image

In the compression procedure, a majority of pixels are converted to a series of coefficients using an orthogonal transform, and then the excessively rough and fine information in the coefficients is removed, leading to a reduced data amount. The detailed procedure is as follows:

1) When having the permuted pixel sequence, the network provider divides it into two parts: the first part made up of (α-N) pixels and the second one containing the rest of the (1-α)N pixels.

2) Denote the pixels in the first part asp1,p2,p3…pαN and the pixels in the second part asq1,q2,q3….q(1-α)N.The value of α is within (0,1) Here, the data in the first part will be reserved while the data redundancy in the second part will be reduced. We call the pixels in the first part rigid pixels and the pixels in the second part elastic pixels.

3) Perform an orthogonal transform in the elastic pixels to calculate the Q1, Q2……… Q (1 - α). N

[Q1, Q2… Q (1 - α) N] = [q1, q2……….q (1 - α). N]. H

Here,

H is a public orthogonal matrix with a size of

(1 - α) N x (1 - α).N and it can be generated from orthogonal zing a random matrix.

Size of H = (1 - α). N x (1 - α). N

$$H=\begin{pmatrix} 0&0&0&0&0&0&1 \\ 0&0&0&0&1&0&0 \\ 1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&1&0&0&0 \\ 0&1&0&0&0&0&0 \end{pmatrix}$$

Then elastic pixels x H =

Q = [14 59 39 36 100 68 13]

4) For each coefficient Q, calculate

$$Sk = mod\left[round\left(\frac{Qk}{\frac{\Delta}{M}}\right), M\right]$$

k = 1, 2 … (1 - α). N

Where Δ and M are system parameters

The round operation returns the nearest integer and the mod operation gets the remainder. Qk is converted into an integer Sk within [0, M -1].

5) Then

$$Qk = rk.\Delta + Sk.\left(\frac{\Delta}{M}\right) + Sk$$

where rk is rough information & tk is fine information.

The rough information rk and the fine information tk are discarded. While only the information Sk on the medium level remains. The rough information rk will be retrieved by an iterative image reconstruction procedure, and the loss of the fine information tk cannot seriously affect the quality of the reconstructed image, where

0 ≤ Sk ≤ M – 1

e.g. M = 4, Δ = 50

Q = [14 59 39 36 100 68 13]

$$S1 = mod\left[round\left(\frac{Q1}{\frac{\Delta}{M}}\right), M\right] = mod\left[round\left(\frac{14}{\frac{50}{4}}\right), 4\right]$$

$$= 1$$

$$S3 = mod\left[round\left(\frac{Q3}{\frac{\Delta}{M}}\right), M\right] = mod\left[round\left(\frac{39}{\frac{50}{4}}\right), 4\right]$$

$$= 3$$

Thus

Sk = [1 1 3 3 0 1 1]

6) Segment the set of Sk into many pieces with L1 digits and calculate the decimal value of each digit piece. Then, convert each decimal value into L2 bits in a binary notational system

Where L2 = [L1. Log2 M]

The total length of bits generated from all pieces of Sk is

L = (1 - α). N .Log2 M

Then

L = (1 – 0.3). 10. Log2 4 = 14

Each value of Sk is represented by Log2 M bits

7) Collect the data of rigid pixels, the bits generated from all pieces of Sk, and the values of parameters including N1, N2, α, Δ, M, and L1 to produce the compressed data of encrypted image. Compression ratio R a ratio between the amounts of the compressed data and the original image data, is approximately

$$R = \frac{8 \cdot \alpha \cdot N + \log_2 M \cdot (1-\alpha) \cdot N}{8 \cdot N} = \alpha + \frac{\log_2 M}{8} \cdot (1-\alpha)$$

C. Iterative image reconstruction

With the compressed data and the secret key, a receiver can perform the following steps to reconstruct the principal content of the original image.

1) Decompose the compressed data and obtain the gray values of rigid pixels, the values of all , and the values of parameters. Here, with the knowledge of and , the receiver may calculate , and then get the values of by converting binary blocks with bits into digit pieces in an M-ary notational system.

2) According to the secret key, the receiver can retrieve the positions of rigid pixels. That means the original gray values at the positions, which distribute over the entire image, can be exactly recovered.

3) For the pixels at other positions, i.e., the elastic pixels, their values are firstly estimated as the values of rigid pixels nearest to them. That means, for each elastic pixel, we find the nearest rigid pixel and regard the value of the rigid pixel as the estimated value of the elastic pixel. If there are several nearest rigid pixels with the same distance, regard their average value as the estimated value of the elastic pixel. Because of spatial correlation in the natural image, the estimated values are similar to the corresponding original values. In the following,

the estimation will be iteratively updated by exploiting the information of Sk.

4) Rearrange the estimated values of elastic pixels using the same permutation way, and denote them as q’1 q’2 ……….. q’(1 - α). N.Calculate the coefficients

[Q’1 , Q’2 ……… Q’(1 - α). N] = [q’1 q’2 ……….. q’(1 - α). N] . H

And

$$d_k = \bmod\left(\frac{Q'_k}{\frac{\Delta}{M}}, M\right) - s_k,\ k = 1, 2, \ldots, (1-\alpha)\cdot N.$$

Modify the coefficients to the closest values consistent with the corresponding Sk

$$Q''_k = \begin{cases} \left(\left\lfloor \frac{Q'_k}{\Delta} \right\rfloor + 1\right)\cdot\Delta + s_k\cdot\frac{\Delta}{M}, & \text{if } d_k \geq \frac{M}{2} \\ \left\lfloor \frac{Q'_k}{\Delta} \right\rfloor\cdot\Delta + s_k\cdot\frac{\Delta}{M}, & \text{if } \frac{-M}{2} \leq d_k < \frac{M}{2} \\ \left(\left\lfloor \frac{Q'_k}{\Delta} \right\rfloor - 1\right)\cdot\Delta + s_k\cdot\frac{\Delta}{M}, & \text{if } d_k < \frac{-M}{2} \end{cases}$$
$$k = 1, 2, \ldots, (1-\alpha)\cdot N.$$

For example with Q’k=42.6 , Δ = 60 , and M=6 , if Sk=0 ,dk is 4.26 according from above equation, so we should modify the value of Q’k to 60. If ,Sk=3,dk=1.26 and we should modify the value of Q’k to 30. Then, perform an inverse transform:

[q’’1 q’’2 ….q’’(1 - α). N] = [Q’’1 , Q’’2 … Q’’(1 - α). N] . H-1

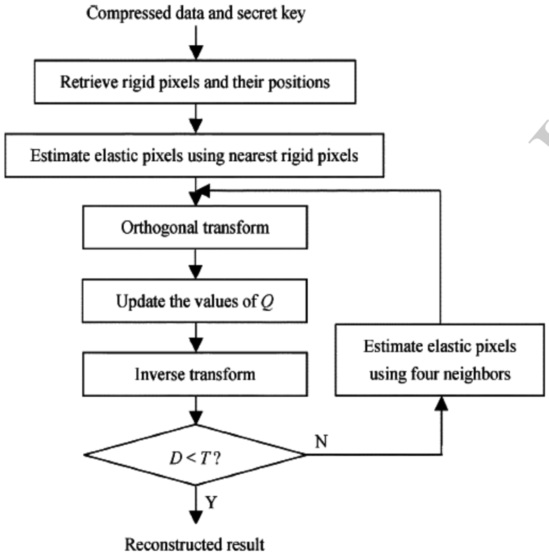

Compressed data and secret key
Retrieve rigid pixels and their positions
Estimate elastic pixels using nearest rigid pixels
Orthogonal transform
Update the values of Q
Inverse transform
Estimate elastic pixels using four neighbors
D < T?
N
Y
Reconstructed result

Fig.1 Image reconstruction procedure.

5) Calculate the average energy of difference between the two versions of elastic pixels

$$D = \frac{1}{(1-\alpha)\cdot N}\cdot\sum_{k=1}^{(1-\alpha)\cdot N}\left(q''_k - q'_k\right)^2$$

If D is not less than a given threshold T, for each elastic pixel, regard the average value of its four neighbour pixels as its new estimated value and go to Step 4. Otherwise, terminate the iteration and output the image made up of the rigid pixels and the final version of elastic pixels as a reconstructed image.

III. *RESULT ANALYSIS*

The test image Lena sized 512× 512 shown in Fig. 2(a) was used as the original in the experiment. After pixel permutation, the encrypted data of the image were produced. For showing their disorder, the encrypted pixel sequence is rearranged as a matrix with size of 512×512 and given in Fig. 2(b). Then, we compressed the encrypted data with ,α=0.15 , , Δ = 60 , and M=6.In this case, the compression ratio R=0.42 . With the compressed data, the receiver can retrieve the original content by using the image reconstruction procedure. Fig. 2(c) shows a medium reconstructed image generated by Steps 1–3, in which all rigid pixels are recovered and the elastic pixels are estimated as the values of their nearest rigid pixels. The value of PSNR in the medium reconstructed image is 27.1 dB, and the quality of the texture/edge area is worse than that of the plain area. When finishing the iterative update in Steps 4 and 5, a final decompressed image shown in Fig. 2(d) was obtained, and PSNR is 39.6dB.It can be seen that the iterative procedure significantly improves the reconstruction quality.

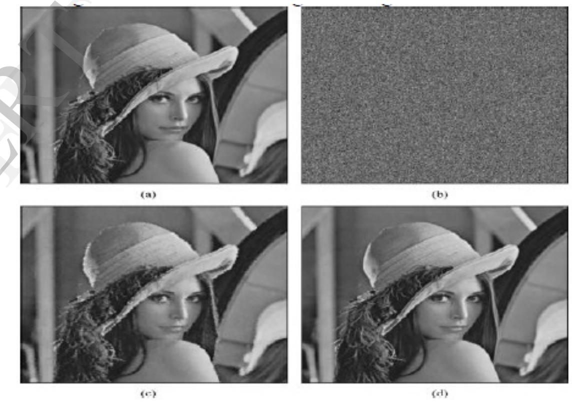


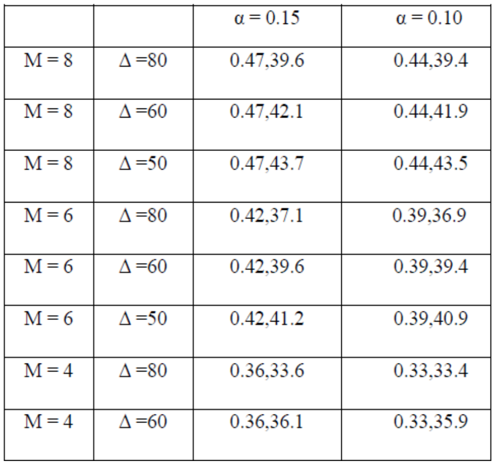
Fig-2 (a) Original image Lena, (b) its encrypted version, (c) the medium reconstructed image from compressed data with less PSNR, and (d) the final reconstructed image with more PSNR

IV. *CONCLUSION*

As Table 1 shows the different values of all the parameters this work proposed a novel idea for compressing and encrypted image and designed a practical scheme made up of image encryption, lossy compression, and iterative reconstruction.

The original image is encrypted by pseudorandom permutation, and then compressed by discarding the excessively rough and fine information of coefficients in the transform domain

Table-1 Compression ratio R and PSNR (dB) in reconstructed image with different parameters for test image Lena



		α = 0.15	α = 0.10
M = 8	Δ =80	0.47,39.6	0.44,39.4
M = 8	Δ =60	0.47,42.1	0.44,41.9
M = 8	Δ =50	0.47,43.7	0.44,43.5
M = 6	Δ =80	0.42,37.1	0.39,36.9
M = 6	Δ =60	0.42,39.6	0.39,39.4
M = 6	Δ =50	0.42,41.2	0.39,40.9
M = 4	Δ =80	0.36,33.6	0.33,33.4
M = 4	Δ =60	0.36,36.1	0.33,35.9

The compression ratio and the quality of reconstructed image vary with different values of compression parameters. In general higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image.

In the encryption phase of the proposed system, only the pixel positions are shuffled and the pixel values are not masked. With the values of elastic pixels, the coefficients can be generated to produce the compressed data.

This work proposed a novel idea for compressing and encrypted image and designed a practical scheme made up of image encryption, lossy compression, and iterative reconstruction. The original image is encrypted by pseudorandom permutation, and then compressed by discarding the excessively rough and fine information of coefficients in the transform domain.

When having the compressed data and the permutation way, an iterative updating procedure is used to retrieve the values of coefficients by exploiting spatial correlation in natural image, leading to a reconstruction of original principal content. The compression ratio and the quality of reconstructed image vary with different values of compression parameters.

In general, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image. In the encryption phase of the proposed system, only the pixel positions are shuffled and the pixel values are not masked. With the values of elastic pixels, the coefficients can be generated to produce the compressed data. On the other hand, the security of encryption used here is weaker than that of standard stream cipher, which can be cooperative with previous lossless compression techniques, since the distribution of pixel-values may be revealed from an encrypted image.

REFERENCES

[1] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pt. 2, pp. 2992–3006, Oct. 2004.

[2] R. G. Gallager, "Low Density Parity Check Codes," Ph.D. dissertation, Mass. Inst. Technol., Cambridge, MA, 1963.

[3] D. Schonberg, S. C. Draper, and K. Ramchandran, "On blind compression of encrypted correlated data approaching the source entropy rate," in *Proc. 43rd Annu. Allerton Conf.*, Allerton, IL, 2005.

[4] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey-level and color images," in *Proc.16th Eur. Signal Processing Conf. (EUSIPCO 2008)*, Lausanne, Switzerland, Aug. 2008 [Online]. Available: http://www.eurasip.org/Proceedings/Eusipco/Eusipco2008/ papers/1569105134.pdf

[5] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[6] 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, Dec. 2008