International Journal of Image Processing and Vision Science

Volume 1 | Issue 4 Article 7

October 2012

EFFICIENT COMPRESSION AND ENCRYPTION SCHEME FOR SECURE TRANSMISSION OF IMAGES AND ITS RECONSTRUCTION

NEETHU SARA RAJU
ECE Department, ICET, Mulavoor, neetu.s.raju@gmail.com

JOBINS GEORGE
ECE Department, ICET, Mulavoor, jobins.george@gmail.com

EFFICIENT COMPRESSION AND ENCRYPTION SCHEME FOR SECURE TRANSMISSION OF IMAGES AND ITS RECONSTRUCTION

NEETHU SARA RAJU[1] & JOBINS GEORGE[2]

[1,2]ECE Department, ICET, Mulavoor

Abstract:- When it is desired to transmit redundant data over an insecure and bandwidth-constrained channel, it is customary to first compress the data and then encrypt it. In this paper, we investigate the efficiency of reversing the order of these steps, i.e., first encrypting and then compressing, without compromise for compression efficiency or the information-theoretic security. A pseudorandom permutation and a linear encoding scheme is used to encrypt an original image, and the encrypted data are efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. After receiving the compressed data, based on spatial correlation, a receiver can reconstruct the principal content of the original image by iteratively updating the values of coefficients and the linear decoding procedure.

Key Terms–Permutation, Linear encoding, Image compression, Image reconstruction.

I.INTRODUCTION

Consider the problem of transmitting redundant data over an insecure, bandwidth-constrained communication channel. It is desirable to both compress and encrypt the data. The traditional way to do this is to first compress the data to strip it of its redundancy followed by encryption of the compressed bit stream. The source is first compressed to its entropy rate using a standard source coder[3]. Then, the compressed source is encrypted using one of the many widely available encryption technologies. At the receiver, decryption is performed first, followed by decompression. In this paper, we investigate the novelty of reversing the order of these steps, i.e., first encrypting and then compressing the encrypted source. The compressor does not have access to the cryptographic key, so it must be able to compress the encrypted data (also called ciphertext) without any knowledge of the original source[2],[3]. At the receiver, there is a decoder in which both decompression and decryption are performed in a joint step.The compression ratio and the quality of the reconstructed image are dependent on the values of compression parameters. Generally, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image.

Several techniques for compressing and decompressing encrypted data have been developed. In [1], proposes a novel scheme for lossy compression of an encrypted image with flexible compression ratio. A pseudorandom permutation is used to encrypt an original image.It has been shown in [2] that, based on the theory of source coding, the performance of compressing encrypted data may be as good as that of compressing non encrypted data in theory. In [3], the encrypted image is decomposed in a progressive manner, and the most significant bits in high levels are compressed using rate-compatible punctured turbo codes. In [4], a compressive sensing technique is introduced to achieve lossy compression of encrypted image data, and a basis pursuit algorithm is appropriately modified to enable joint decompression and decryption.In [5], Compression of encrypted data is possible by using distributed source coding. Cipher text will be generated by adding a random key to the prediction errors.

In this work, we propose a novel system for lossy compression of encrypted image with flexible compression ratio, which is made up of image encryption, compression, and iterative decompression phases. The network provider may remove the redundant and trivial data from the encrypted image, and a receiver can retrieve the principal content of the original image using an iterative procedure.

II.ENCRYPTION, COMPRESSION AND RECONSTRUCTION

In the proposed scheme, a pseudorandom permutation and linear encoding scheme is used to encrypt an original image. Then, the encrypted data can be compressed by discarding the excessively rough and fine information of coefficients in the transform domain. When having the compressed data, the permutation way and secret key for linear encoding, with the aid of spatial correlation in natural image, the receiver can reconstruct the original image by iteratively updating the values of the coefficients.

A.Image Encryption

During encryption, 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 as N1 and N2 , and the number of all pixels as N=(N1x N2). So,the amount of bits of the original image is 8. N . For image encryption, the data sender pseudorandomly permutes the N pixels[5] and the permutation way is determined by a secret key.

In this scheme only the pixel positions are changed,but the pixel values are not masked. However, the number of possible permutation ways is N!, so that it is practical to perform a brute force search when N is fairly large. That means the attacker cannot recover the original content from the encrypted image with ordinary size and fluctuation.

To enhance the secrecy of permuted data,a linear encoding scheme[7] is used to change the pixel values as well. In this method,the image is first converted into a column vector and then the pixels are grouped into a particular size specified by a key-span.Each of these sets are then multiplied by a lower triangular matrix generated, which serves as the secret key for pixel value encryption.The multiplied values of pixels are then transformed to original image format and then transmitted as the encrypted image.Fig.1illustrates the entire encryption procedure and Fig.2 illustrates linear encoding scheme in detail.

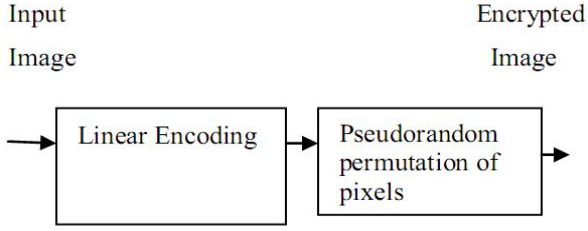

Fig .1. Image Encryption Procedure

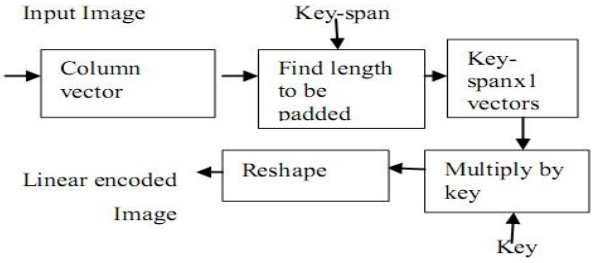

Fig. 2.Linear encoding

B.Compression of encrypted data

The compression technique to be proposed for the encrypted data is presented here. A lossy ompression[1] is chosen for the compression of the 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. 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. Denote the pixels in the first part as p1,p2,p3,…. and the pixels in the second part asq1,q2,q3,… 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.

2) Perform an orthogonal transform in the elastic pixels to calculate the coefficients

$Q_1,Q_2,\ldots\ldots,Q_{(1-\alpha).N}$

$[Q_1,Q_2,\ldots,Q_{(1-\alpha).N}]=[q_1,q_2,\ldots,q_{(1-\alpha).N}].H$

Here, H is a public orthogonal matrix and it can be generated from orthogonalizing a random matrix.

3) For each coefficient, calculate

$$S_k=\mathrm{mod}\left[\ \mathrm{round}\left(\frac{Q_k}{\Delta/M}\right),\ M\right]\quad ,k=1,2,\ldots,(1-\alpha)N$$

where Δ and M are system parameters. The round operation returns the nearest integer and the mod operation gets the remainder. By Qk is converted intan integer Sk within (0,M-1) With a small M , the data amount for representing the elastic pixels is reduced. As Qk can be rewritten in the following manner

$$Q_k = r_k \cdot \Delta + s_k \cdot \Delta + \frac{t_k}{M}$$

Where r_k and S_k are integers and

$$0 \le S_k \le M-1\ ;\ -\frac{\Delta}{2M} \le t_k < \frac{\Delta}{2M}$$

It can be seen that the rough information and the fine information are discarded, while only the information on the medium level remains. Note that the rough information will be retrieved by an iterative image reconstruction procedure, and the loss of the fine information cannot seriously affect the quality of the reconstructed image. 4) Since are within, we can regard them as a set of digits in a notational system with a base . Segment the set of into many pieces with digits and calculate the decimal value of each digit piece. Then, convert each decimal value into bits in a binary notational system, where L2= L1.log2 M

5) Collect the data of rigid pixels, the bits generated from all pieces of , and the values of parameters including N1,N2, α, ∇, M and L1 and to produce the compressed data of encrypted image. Since the data amount of parameters is small, the compression ratio R , a ratio between the amounts of the compressed data and the original image data, is approximately

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

C. Image Reconstruction

The image reconstruction technique that is to be handled at the receiver side is presented here. 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) Initially

decomposition of the compressed data is done and retrieve the rigid data and their positions. Then estimate the elastic pixels using the nearest rigid pixels. 2)Rearrange the estimated values of elastic pixels using the same permutation way and calculate the coefficients.

$$[Q1',Q2'...Q(1-\alpha).N'] = [q1',q2'..q(1-\alpha).N'].H \text{ ; and}$$

$$dk = \text{mod}\,(Qk'/[\Delta/M], M) - Sk$$

3)Then modify the coefficients to the closest values consistent with the corresponding value.

$$Qk'' = \begin{cases} ([Qk'/\Delta]+1).\Delta+Sk.(\Delta/M); & \text{if } dk \geq M/2 \\ [Qk'/\Delta].\Delta+Sk.(\Delta/M); & \text{if } -M/2 \leq dk < M/2 \\ [Qk'/\Delta]-1].\Delta+Sk.\Delta/M; & \text{if } dk < -M/2 \end{cases}$$

4)Perform the inverse transformation

$$[q1'',q2''..q(1-\alpha).N''] = [Q1'',Q2''...Q(1\alpha).N'']H^{-1}$$

5)Finally calculate the average energy of difference between the two versions of elastic pixels.

$$D = 1/[(1-\alpha).N] \sum_{K=1}^{(1-\alpha).N} (qk'' - qk')^2$$

6)If the calculated value is less than a particular threshold T, then estimate the value of elastic pixel using four neighbouring rigid pixels. This value of T is recommended to be 0.05, to ensure that the last two versions of elastic pixels are close enough and update doesnot improve the reconstructed result further.

7)To retrieve back the original pixel values,linear decoding operation is performed as in Fig.3.Here it uses the same secret key which is used at the encoder end.This secret key is used to find the key-span and then divide each set of multiplied values of pixels to get the original values of pixels.

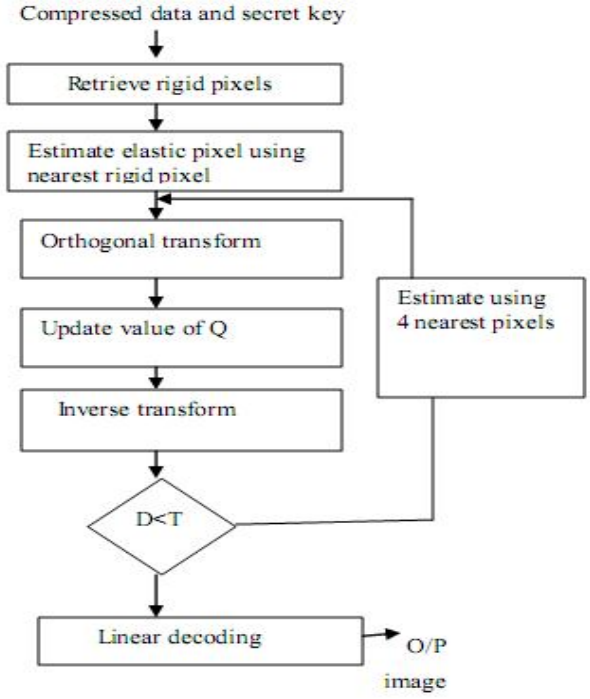

Fig.3.Image Reconstruction procedure

Fig.3 explains the complete reconstruction procedure and in Fig.4 the linear decoding method is illustrated in detail.

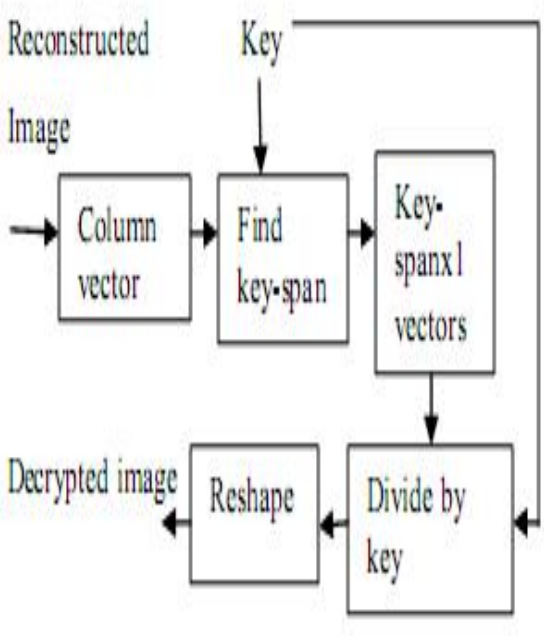

Fig.4.Linear Decoding

As long as we have an approximately estimated version as an initialization, the iterative procedure can produce a satisfactory reconstructed result. While the values of rigid pixels are used to give an initial estimation of elastic pixels, the values of sk provide more detailed information to produce a final reconstructed result with satisfactory quality. By the orthogonal transform, the estimation error of elastic pixels is scattered over all the coefficients. Since the coefficients are generated from all elastic pixels, the errors in a final reconstructed result are distributed over the image with an approximately uniform manner.

III.EXPERIMENTAL RESULTS AND DISCUSSION

The test image Lena was used for the experiment as the original image.The experiment was conducted with α =0.99,Δ = 80 and M = 4.Fig. 5(a) ,shows the original image and fig.5(b) shows the encrypted image. With the compressed data, the receiver can retrieve the original content by using the image reconstruction procedure.Fig.5(c) shows the medium reconstructed image by completing the reconstruction steps 1, 2 and 3.Fig.5(d) ,shows the complete reconstructed result after completing steps 4 to 7.Here the compression ratio is found to 0.98 and PSNR is found to be 43.7dB. It can be seen that the iterative procedure significantly improves the reconstruction quality.

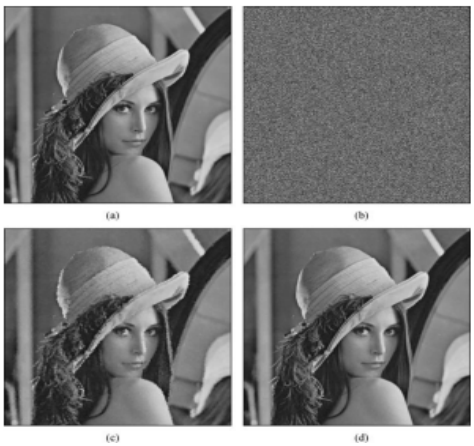

Fig.5 . (a) Original image Lena, (b) its encrypted version, (c) the medium reconstructed image from compressed data with PSNR 39.7dB, and (d) the final reconstructed image with PSNR 43.7dB.

Table 1 shows the values of compression ratio and PSNR for different values of α ,Δ and M,for test image shown in Fig.6

Fig .6.Test Image for calculation of compression ratio and PSNR

		α = 0.15	α = 0.10	α = 0.07
M = 8	Δ = 80	.48 , 36.5	.46 ,36.3	.43 ,36.1
M = 8	Δ = 60	.48 ,39.2	.46 ,38.4	.43 ,40.8
M = 6	Δ = 80	.45 ,34.3	.41 ,33.2	.39 ,32.8
M = 6	Δ = 60	.45 ,36.8	.41 ,35.8	.39 ,34.6
M = 4	Δ = 80	.39 ,33.6	.38 ,31.5	.35 ,31.6
M = 4	Δ = 60	.39 ,35.2	.38 ,34.3	.35 ,33.2

Table 1. Compression ratio R and PSNR (dB) in reconstructed image with different parameters

The quality of reconstructed image varies with different parameters choosen for different images.The compression ratio is determined by α & M , and the smaller α & M correspond to a lower R .

On the other hand, the larger the values of α & M , the iteration numbers are usually smaller and the qualities of reconstructed images are better since more rigid pixels and more detailed can be used to retrieve the values of elastic pixels. The compression ratio is independent of the value of Δ , and, generally speaking, a smaller Δ can result in a better reconstructed image since the receiver can exploit more precise information for image reconstruction. However, more iterations are made for getting a final reconstructed result when using a smaller Δ , and, if the value of Δ is too small, the updating procedure is not convergent

IV.CONCLUSION

In this work, a new method for secure encryption of images is proposed which together with a lossy compression technique and iterative reconstruction method proves to be efficient for image storage and transmission. The encryption is done by a pseudorandom permutation of pixels and a linear encoding scheme that masks the pixel values, which is found to be highly secure. It is then compressed by discarding the excessively rough and fine information of coefficients in the transform domain. In the reconstruction phase, an iterative updating procedure and linear decoding process will retrieve back the original image. The method is found to be highly secure and in general higher the compression ratio and smoother the original image, better will be the quality of reconstructed result. In future, advanced compression technique to improve the PSNR value, can be incorporated with the scheme to improve its efficiency.

REFERENCES

[1]. "Lossy Compression and Iterative Reconstruction for Encrypted Image", IEEE transactions on information forensics and security, vol. 6, no. 1, MARCH 2011.

[2]. "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pt. 2, pp. 2992–3006, Oct. 2004.

[3]. "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[4]. "Lossy compression of encrypted image by compressing sensing technique," in Proc. IEEE Region 10 Conf. (TENCON 2009), 2009, pp. 1–6.

[5]. "Efficient hierarchical chaotic image encryption algorithm and its VLSI realization," Proc. Inst. Elect. Eng., Vis. Image Signal Process., vol. 147, no. 2, pp. 167–175, 2000.

[6]. "Toward compression of encrypted images and video sequences," IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 749–762,2008.

[7]. "Applications of linear algebra to cryptography",. Proc. Inst.Adam Grelck,Math 208,2004