Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

COMPRESSING ENCRYPTED IMAGES VIA ADAPTIVE SAMPLING

Aida Kurian[1], Sharika TR[2]

[1,2]*Department of Computer Science, IIET, Nellikuzhi*

Abstract- In many applications, image sending should be done very secretly. This secret sending of image can be done by image encryption and compression. Image encryption should be done before compression to provide more security. This paper proposes a method for compressing encrypted images where the image encryption is done by permutation. The compression is done in two layers such as base layer and enhancement layer. In the base layer, downsampling of the image is first done and adaptive arithmetic compression is applied to each patches of the downsampled image. In the enhancement layer, pixels for coding are selected by reconstruction error and greedy strategy. A multiscale technique is applied by the decoder for the reconstruction of compressed image. Our evaluations show that the reconstructed image should possess the quality of original image.

Keywords- Encryption,Compression,Sampling.

I. INTRODUCTION

In the day today life importance of information passing is increased . We access the internet for many purposes such as searching, send and receive email, to share pictures, songs and videos and other applications. Also we are concerned about the security of these informations. If a person wants to transmit an image to another person via an untrusted channel, sender encrypts the image. The compression of encrypted image is done by the untrusted channel. When receiver receives the compressed image, he decrypt and decompress the image. The compression of encrypted images had received much attention in the recent years. Image encryption is not enough for the security, so that compression is applied to the encrypted image.

Many works have been presented based on compressing encrypted images. In [5], LDPC codes are used for the compression of encrypted grayscale/color images. Compression of encrypted images is done by compressive sensing mechanism and the image cab be reconstructed by using a modified basis pursuit algorithm [9]. Zhang designed a system in which compression of encrypted image is achieved via multilayer decomposition [6].

This paper proposes a novel scalable coding scheme for encrypted grayscale images. Encryption is done using permutation. The compression is done in both base layer and enhancement layer. In both layer, compression is done in each bit stream. Compression is done via adaptive arithmetic compression. The encrypted and compressed image is reconstructed with the quality of original image at the decoder side.

II. BACKGROUND

The primary focus of the paper is to design a scalable compression system for encrypted images. There are three components including sender who encrypts the image, untrusted channel which compress the encrypted image and the receiver who decrypt and decompress the image.

2.1. Image Encryption

The sender encrypts the image to be send. The encryption is done using AES algorithm in the CTR mode. The encrypted image is obtained by XORing the original image and the secret key stream.

2.2. Encrypted Image Compression

The compression of encrypted image consists of a base layer and an enhancement layer. For compression in the base layer, downsample the encrypted image. The downsampled image is of size N/4 x N/4. The downsampled image is then partitioned into a series of patches. Each partition is then treated as subimage and compressed individually into bit stream by applying the lossless compression method of [7] which is based on LDPC codes. The operations in the base layer is done parallel for achieving high throughput. The final bit stream in the base layer is obtained by concatenating all bit streams in the base layer. In the enhancement layer, pixels to be coded is selected on the basis of patch reconstruction error and greedy strategy. For patch reconstruction error, we construct a context model and this model is able to drive a greedy strategy for pixel sample selection in the enhancement layer.

The greedy algorithm is as follows:

1. Initialize a vector E where conditional expectations are obtained from the offline training process.
2. Find the index q corresponding to the element E :

   $q = \text{argmax } E_i$
3. Randomly choose s encrypted pixels.
4. Update

   $E_q = E\ (d\ (n_q + 1)|\ h_q)$

   $N_q = n_q + 1$
5. Repeat steps 2-4 until all F * S samples are selected.
6. Reshape the pixel samples and encode it into binary bit stream.

2.3. Image Reconstruction

When the bit stream from the base layer and the enhancement layer arrives, the decoding algorithm is applied. Image decryption is simply done by XORing the image with the corresponding key stream. The image reconstruction is done via SAI interpolation method. At the end NLM based approach is employed to find the missing pixels to estimate the refined version of the image.

III. PROPOSED WORK

Inorder to solve the problems in the base paper, we are using permutation and arithmetic compression to provide more security. The proposed work consists of image encryption, compression, decryption and decompression.

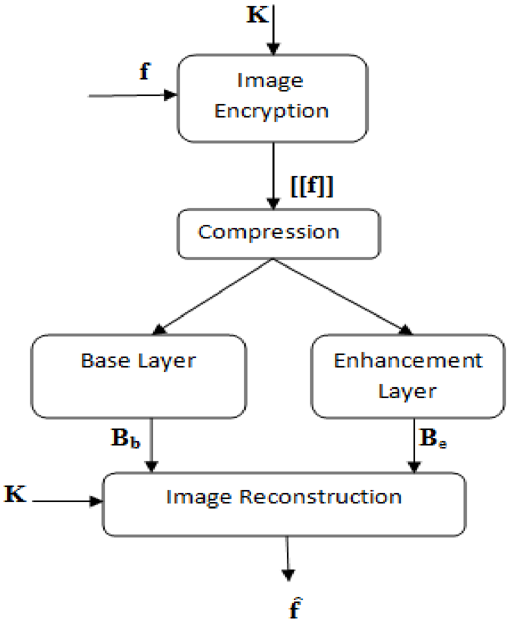

Fig 1: The proposed system

3.1. Image Encryption

The sender encrypts the image to be send. The encryption is carried out by applying permutation on the image. The permutation is obtained by performing two key-driven cyclical shift operations. Both column shift and row shift operations will be carried out.

The permutation algorithm is described as follows:

1. Compute the prediction errors of the whole image.
2. Divide all the prediction errors into L clusters C_k.
3. Reshape the prediction errors into a 2-D block having four columns and C_k / 4 rows.
4. Perform column shift and row shift operations.
5. All the permuted clusters are concatenated and converted into encrypted form.

3.2. Encrypted Image Compression

The compression of encrypted image consists of a base layer and an enhancement layer. For compression in the base layer, downsample the encrypted image. The downsampled image is of size N/4 x N/4. The downsampled image is then partitioned into a series of patches. Each partition is then treated as subimage and compressed individually into bit stream by applying adaptive arithmetic compression. The arithmetic compression is to represent a probability by an interval and this interval is encoded.

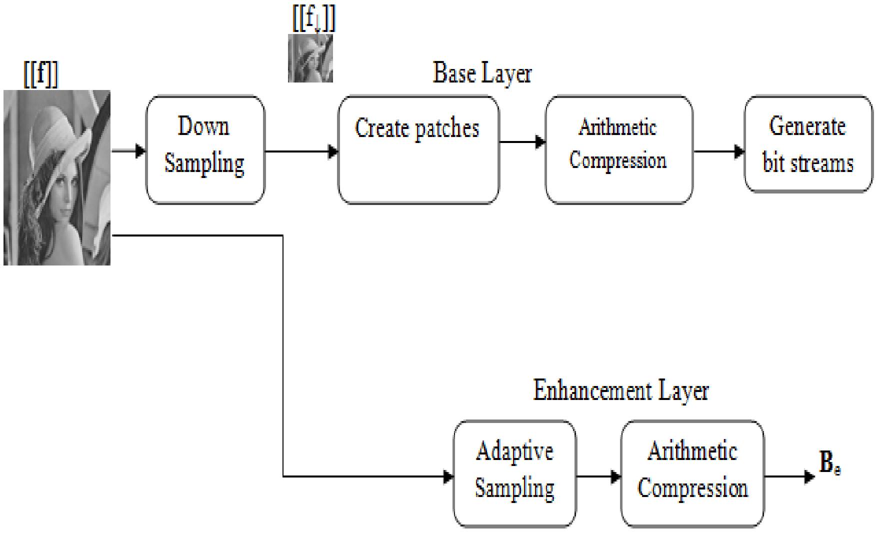

Fig 2 : The proposed compression scheme

Inorder to select pixels for coding in enhancement layer, we should find the patch reconstruction error from the pixel samples. Consider 4M x 4M sized patch Q from the original image and M x M sized patch P from the downsampled image. Then duplicate the pixels of downsampled image. The image patch denoted as R is reconstructed from the available pixels of the duplicated version and additional samples from the patch of original image. These additional samples reduce the reconstruction error. Generate a context model for the reconstruction error and using this model, a greedy strategy can be derived for selecting pixels. For that, first find the reconstruction error difference by,

$$d(n) = e(n-1) - e(n))$$

The patch reconstruction error is given by,

$$\mathrm{e(n)} = e(0) - \sum_{i=1}^{n} \mathrm{d(i)}$$

If the value of d(n) is larger, the additional samples s can reduce the reconstruction error. So we introduce a conditional probability p(d(n)|h). But to prevent the context dilution, the conditional expectation E(d(n)|h) is estimated.

To estimate the conditional expectation, an off-line learning approach is employed with a set of training images. For each training image f_u , $Q_{u,t}$'s can be readily extracted and hence we get the corresponding $P_{u,t}$ and $R_{u,t}$. Where u is the index of training images and t is the patch index. For each $R_{u,t}$ increment the pixel samples in vacant locations and get the reconstructed patch. Then calculate the $d_{u,t}(n)$.

$$\mathrm{d_{u,t}} = (\mathrm{d_{u,t}}(1), \mathrm{d_{u,t}}(2), \dots, \mathrm{d_{u,t}}(\mathrm{S}))$$

where $\mathrm{S} = \frac{15\mathrm{M}^2}{\mathrm{s}}$
Then the conditional expectation is calculated by

$$\mathrm{E(d(n)|h = h_0)} = \frac{\sum_{\mathrm{(u,t)\varepsilon\Omega}} \mathrm{d_{u,t}\,(n)}}{\Omega}$$

Where $\Omega = \{(u,t)|h_{u,t} = h_0\}$

Using this patch reconstruction error, we select the samples to be coded in the enhancement layer. For that greedy algorithm which consists of F stages is used. We had already discussed the greedy algorithm.

3.3. Image Reconstruction

Using the bit streams from the base layer and enhancement layer and the secret key stream, the receiver can re-estimate the original image f. The decoding algorithm is applied to the bit streams of base layer to get the encrypted downsampled image $[[f_\downarrow]]$. For decompression we use adaptive arithmetic decompression. The encrypted image can be decrypted into $f_\downarrow$ by simply XORing with the corresponding key stream. Similarly, the bit streams from enhancement layer can be converted to $[[f_e]]$ and it can be decrypted into f_e.

With $f_\downarrow$ and f_e the original image can be reconstructed. Using the samples from these an image f_0 is constructed. Then f_0 is downsampled twice to form f_1 and f_2. First convert the f_2 using SAI interpolation method. With this missing pixels of f_1 is estimated. It is given as,

$$f_1(i) = \sum_{j \in W_i} w(i,j) f_1 \ (j)$$

Then an iterative non local mean (NLM) based approach is employed to get the final estimate. The interpolation method and NLM approach is employed twice to get the original image.

IV. CONCLUSION

The goal of this research is to securely transmit images to another persons via an untrusted channel. In this paper, an efficient image compression system is designed. The encryption is done using random permutation. The compression is done in base layer and enhancement layer using arithmetic compression. In base layer, a series of patches of downsampled image is compressed and the enhancement layer selects the additional pixel samples to be compressed. Then the image is reconstructed by the interpolation method. The evaluations shows that the reconstructed image will have the quality of original image.

.

REFERENCES

[1] D. Schonberg, S. Draper, and K. Ramchandran, “On compression of encrypted images,” in Proc. IEEE Int. Conf. Image Process., Oct. 2006,pp. 269–272.

[2] 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.

[3] R. Lazzeretti and M. Barni, “Lossless compression of encrypted grey-level and color images,” in Proc. 16th Eur. Signal Process. Conf. (EUSIPCO), Lausanne, Switzerland, 2008, pp. 1–5.

[4] X. Zhang, G. Feng, Y. Ren, and Z. Qian, “Scalable coding of encrypted images,” vol. 21, no. 6, pp. 3108–3114, Jun. 2012.

[5] R. Lazzeretti and M. Barni, “Lossless compression of encrypted grey-level and color images,” in Proc. 16th Eur. Signal Process. Conf. (EUSIPCO), Lausanne, Switzerland, 2008, pp. 1–5.

[6] X. Zhang, G. Sun, L. Shen, and C. Qin, “Compression of encrypted images with multi layer decomposition,” Multimedia Tools Appl., vol. 72, no. 1, pp. 489–502, Feb. 2013.

[7] X. Zhang, Y. Ren, G. Feng, and Z. Qian, “Compressing encrypted image using compressive sensing,” in Proc. 7th IEEE Int. Conf. IIH-MSP, Oct. 2011, pp. 222-2225.

[8] H. Lipmaa, P. Rogaway, and D. Wagner. CTR Mode Encryption.[Online]. Available:http://csrc.nist.gov/encryption/modes/workshop1/papers/lipmaa-ctr.pdf, accessed Sept. 2000.
[9] A. A. Kumar and A. Makur, "Lossy compression of encrypted image by compressive sensing technique," in Proc. IEEE Region 10th Conf., Jan. 2009, pp. 1–6.

.