A NEW LOSSY COMPRESSION SCHEME FOR ENCRYPTED GRAY-SCALE IMAGES

Ran Hu, Xiaolong Li and Bin Yang

Institute of Computer Science and Technology, Peking University, Beijing 100871, China

ABSTRACT

Compression of encrypted data has attracted considerable research interests nowadays due to distributed processing and cloud computing. In this work, we propose a novel lossy compression scheme for encrypted gray-scale images. The original image is first divided into non-overlapping blocks. Then, it is encrypted by a modulo-256 addition and block permutation. In compression phase, the spatial correlation and quantization are exploited to reduce the compression ratio. At the decoder side, context-adaptive interpolation with an image-dependent threshold is used to make image reconstruction precise. Experimental results show that the proposed scheme achieves better performance compared to the previous work.

***Index Terms*—** Lossy compression, image encryption, image reconstruction, context-adaptive interpolation.

1. INTRODUCTION

In recent years, compression of encrypted data has attracted considerable research interests due to the security concerns in a service-oriented environment such as distributed processing and cloud computing [1–3]. In such scenarios, not only transmission but also processing is done on the public Internet. That is, contents with redundant data are transmitted over an insecure, bandwidth-constrained communication channel. The traditional way of securely transmitting is to first compress the data and then encrypt the compressed data. But in some application scenarios, this should be done inversely. For example, the content owner and network provider are two separate parties, so the former wants to keep the information confidential to the latter. In this case, the content owner may first perform encryption and then send the encrypted data to the network provider who has no access to the encryption key. At the network node, in order to match the constraint of the transmission channel, the compression of the encrypted data is required. At the receiver side, to reconstruct the original content, the received data is decrypted and decompressed simultaneously using the shared encryption key. Fig. 1 illustrates the compression and decompression of encrypted data.

Lossless compression of encrypted images have been developed in some recent works [4–7]. In [4], Johnson *et al.* showed that the performance of such approach can be as good as the traditional way, i.e., following the distributed source-coding (DSC) theory [8], the same compression efficiency as well as the security requirement can be achieved. More specifically, in this work, the authors utilized the Slepian-Wolf and Wyner-Ziv theorems [9] for lossless compression and lossy compression, respectively. Moreover, the authors also described a system which implements compression of encrypted sparse binary images. In [5], Schonberg exploited the Markovian property between bit planes in the Slepian-Wolf decoder. In [6], by exploiting the spatial correlation between adjacent pixels and that between bit planes, as well as the cross-channel correlation, Lazzeretti and Barni

Corresponding author: Bin Yang, e-mail: yang_bin@pku.edu.cn

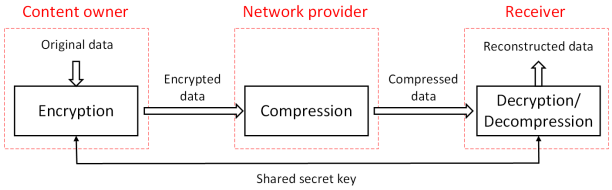

Fig. 1. Sketch of the compression of encrypted data

extended the work of [4] to the cases of gray-scale and color images. In [7], Liu *et al.* proposed resolution progressive compression for lossless image codec. Compared with Schonberg's work [5], Liu *et al.*'s method achieved a superior performance with much better coding efficiency and less computational complexity. It should be mentioned that all these methods [4–7] are based on DSC and they can provide good performance both in compression and security. However, backward communication is often required at the receiver side, and thus the DSC-based methods are not suitable in scenarios without feedback channel.

Lossy compression of encrypted images has also been studied so far [10–13]. In [10], Kumar and Makur introduced a compressive sensing technique and modified a basis pursuit algorithm appropriately to enable joint decryption and decompression. In [11], Zhang proposed a lossy compression and iterative reconstruction for a pseudorandom permuted image. In this method, the original image is encrypted by permutation and thus its histogram is kept after encryption. As a result, there is a leakage of statistical information. In [12, 13], two different methods of scalable coding for encrypted images were proposed in which the compression ratio can be freely chosen by the network provider. Particularly, in [13], after encryption, the image is first divided into sub-images. Then, one sub-image and some bit planes of another sub-image are transmitted. For image reconstruction, the bit planes are used as side information in context-adaptive interpolation (CAI). The CAI technique was first proposed in [7] for lossless compression of encrypted images. The method [13] is computationally efficient and the feedback channel is not required. However, there is a lot of loss in bit-plane transmission and the reconstructed image quality is to some extent low.

In this paper, also based on CAI, we propose a novel lossy compression scheme for encrypted gray-scale images. Instead of bit-plane transmission utilized in [13], the spatial correlation existing in natural images and quantization operation are exploited in our method to perform efficient compression. Experimental results show that, by our method, at decoder side, the reconstructed image quality can be enhanced compared with [13]. Specifically, in our encryption phase, the original image is first divided into non-overlapping 2×2 sized blocks and each block is encrypted by a modulo-256 addition on the original pixel values with pseudorandom numbers. Then the divided blocks are permuted in a pseudorandom way. In compression phase, the encrypted image is decomposed into four downsampled sub-images, and only one sub-image and the difference between this sub-image and another one are transmitted. Moreover, before

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

transmission, quantization operation and arithmetic coding are applied to the difference image to reduce the compression ratio. Finally, at the decoder side, when the received data is decrypted, CAI with an image-dependent threshold is used for image reconstruction.

The rest of this paper is organized as follows. Some related works are first introduced briefly in Section 2. The proposed lossy compression scheme is described in details in Section 3. The experimental results are reported in Section 4. Finally, the conclusion is made in the last section.

2. RELATED WORKS

Some previously proposed lossy compression schemes for encrypted images [11–13] are briefly introduced in this section.

In [11], Zhang proposed a method in which the original image is encrypted by pixel permutation. For compression, excessively rough and fine information of coefficients generated from orthogonal transformation are discarded to reduce the data amount. At the decoder side, the spatial correlation in natural image is exploited for image construction. By iteratively updating the values of transformed coefficients, the image can be recovered. The compression ratio and the reconstructed image quality achieve good performance. The higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image. However, in Zhang's work, the pixel values are not masked since only the pixel positions are shuffled, so the pixel value distribution can be revealed from an encrypted image.

In another work [12], Zhang *et al.* proposed a method in which image encryption is performed based on modulo-256 addition. At the encoder side, the encrypted image is first decomposed into a downsampled sub-image and several data sets. The sub-image and the Hadamard coefficients of each data set are quantized. After quantization, the sub-image and the Hadamard coefficients are transmitted. At the decoder side, the quantized sub-image is served as a low resolution version of the original image. The quantized Hadamard coefficients are used to provide detailed information to get high resolution information with an iteratively updating procedure until the original image is recovered. The computation complexity of this method is low and it is suitable for real-time application.

We now introduce the scalable lossy compression scheme proposed by Kang *et al.* [13]. In this method, the original gray-scale image is first encrypted by a standard stream cipher or a modulo-256 addition, resulting in an encrypted image E. Then E is downsampled by a factor 2 in both horizontal and vertical directions and generate four sub-images denoted as E^{00}, E^{01}, E^{10} and E^{11}. The number 0 and 1 denote the horizontal and vertical offsets of the downsampling. Referring to Fig. 2, each icon represents an encrypted image pixel. Finally, E^{00} and N bit planes of E^{11} are transmitted. The compression ratio is thus $0.25(1 + N/8)$. For the reconstruction phase, E^{00} is first decrypted and then used to predict the original unencrypted version of E^{11} using CAI. Referring to Fig. 2, for an original pixel x of E^{11}, consider its four decrypted neighboring pixels $\{t_1, ..., t_4\}$ belonging to E^{00}. The preliminary prediction of x with CAI is calculated by

$$\begin{cases} \text{mean}(t_1, ..., t_4) & \text{if } \max(t_1, ..., t_4) - \min(t_1, ..., t_4) \le T \\ (t_1 + t_2)/2 & \text{if } |t_3 - t_4| - |t_1 - t_2| > T \\ (t_3 + t_4)/2 & \text{if } |t_1 - t_2| - |t_3 - t_4| > T \\ \text{median}(t_1, ..., t_4) & \text{otherwise} \end{cases} \tag{1}$$

where the threshold T is taken as a fixed value 20. Then, using the CAI-based preliminary prediction and the transmitted N bit planes of E^{11}, a more concise prediction of x can be derived. When E^{11} is recovered, E^{10} and E^{01} can be predicted also by CAI, and thus the original image is finally reconstructed. This method is computationally efficient and it is proved better than [10, 14].

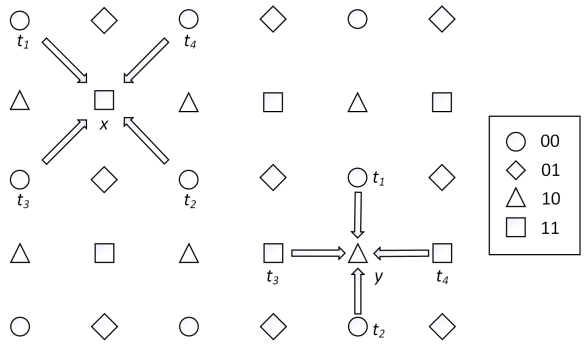

Fig. 2. Sub-images generation and CAI-based prediction of [7, 13].

3. PROPOSED SCHEME

We describe our scheme in details in this section. The same as the other methods, the proposed scheme contains three basic steps: encryption, compression and reconstruction.

3.1. Image Encryption

Consider a gray-scale image I. For encryption, I is first divided into 2×2 sized blocks. Then, each block is encrypted by a modulo-256 addition on the original pixel values with pseudorandom numbers. In particular, the top-left and bottom-right pixels in the same block are encrypted with the same pseudorandom number. That is to say, a block $\{I_{2i,2j}, I_{2i+1,2j}, I_{2i,2j+1}, I_{2i+1,2j+1}\}$ is encrypted as follows to get an interim image F

$$\begin{cases} F_{2i+s,2j+t} = \text{mod}(I_{2i+s,2j+t} + K_{2i+s,2j+t}, 256) \\ F_{2i+1,2j+1} = \text{mod}(I_{2i+1,2j+1} + K_{2i,2j}, 256) \end{cases} \tag{2}$$

where $(s, t) \in \{(0, 0), (0, 1), (1, 0)\}$ and K denotes the pseudorandom numbers matrix. Then, all blocks in F are randomly permuted to get the final encrypted image E. A number of image permutation methods such as [15, 16] can be used here.

Although the encoder or potential attacker knows a little part of difference histogram of original image (e.g., consider the difference of $F_{2i,2j}$ and $F_{2i+1,2j+1}$, see (2)), it is impossible to perform a brute force search to recover the original image. The size of the secret key space is $3M/4$ and the number of possible permutations is $(M/4)!$, where M is the image size. Thus this two-stage encryption can be used in most scenarios without a perfect secrecy requirement.

3.2. Compression of Encrypted Image

The same as [7, 13], in the compression phase, the encrypted image E is first downsampled by a factor 2 and four sub-images E^{00}, E^{01}, E^{10} and E^{11} are generated. Then, compute the difference

$$D_{i,j} = E^{11}_{i,j} - E^{00}_{i,j}. \tag{3}$$

According to our encryption (2), D follows a Laplacin-like distribution and can be compressed remarkably. Finally, transmit E^{00} and the compressed D using arithmetic coding to the decoder. The compression ratio is thus $0.25 + L/(8M)$, where L is the code length of arithmetic coding compression for D.

Moreover, we point out that, to further reduce the compression ratio, the difference image D can be quantized before encoding. That is to say, for a given quantization step Q, for each difference value in $[kQ, (k+1)Q-1]$, it will be quantized as $x_k \in [kQ, (k+1)Q-1]$. In this case, the quantization distortion $Dis(x_k)$ can be formulated as

$$Dis(x_k) = \sum_{D_{i,j} \in [kQ,(k+1)Q-1]} (D_{i,j} - x_k)^2. \quad (4)$$

Then, for given Q and k, the quantized element x_k is selected to minimize the distortion (4), i.e., it is defined as

$$x_k = \underset{x \in [kQ,(k+1)Q-1]}{\arg\min} Dis(x). \quad (5)$$

Clearly, there is actually no quantization when $Q = 1$, and the compression ratio decreases when Q increases.

3.3. Image Reconstruction

With the received data, the decoder first converts it into E^{00} and D, and then get E^{11} by taking $E^{11} = E^{00} + D$. Notice that the difference image D obtained by decoder is the quantized version, so E^{11} determined here may not be exactly the same one used by encoder since quantization error occurs. Then, using the shared secret key, after re-permutation and reversing (2), the pixels with indices $(2i, 2j)$ and $(2i+1, 2j+1)$ can be recovered. For the other pixels, i.e., the pixels with indices $(2i, 2j+1)$ and $(2i+1, 2j)$, they will be predicted using CAI. For example, referring to Fig. 2, the pixel y can be obtained applying CAI to its neighbors $\{t_1, ..., t_4\}$. Here, we mention that, to enhance the prediction performance, instead of a fixed threshold T used in the conventional CAI in (1), we can take an image-dependent threshold. Actually, the threshold can be adaptively determined based on the image complexity. Notice that, since only the sub-image E^{00} can be exactly obtained by the decoder, we then measure the image complexity using this sub-image.

Suppose the decrypted version of E^{00} is G. For each pixel $(i, j) \in G$, we first define the local complexity of this pixel as

$$LC_{i,j} = \left(\frac{1}{8} \sum_{s=-1}^{1} \sum_{t=-1}^{1} (G_{i,j} - G_{i+s,i+t})^2 \right)^{\frac{1}{2}} \quad (6)$$

Then, the image complexity denoted as C is measured as the mean value of $LC_{i,j}$ counting all pixels of G. For example, the complexity is 12 for the image Lena, while 29 for Baboon. Finally, we take empirically the threshold T as $2C$ in the CAI-based prediction (1). Through our experiments, the performance of CAI-based prediction can be enhanced using this adaptively determined threshold.

Before closing this section, to better illustrate our method, we show in Fig. 3 the images during the compression and decompression procedures. The left, center and right figures of Fig. 3 show the original image Lena, the encrypted image and the reconstructed image, respectively. Here, in compression phase, the quantization step Q is taken as 2, and the compression ratio is 0.38. For image quality, the PSNR of reconstructed image versus the original one is 37.78 dB. It can be observed that the reconstructed image is very similar to the original one and the difference is visually imperceptible.

4. EXPERIMENTAL RESULTS

For the first experiment, eight standard 512×512 sized gray-scale images including Airplane, Baboon, Elaine, Boat, House, Lake, Lena and Peppers are used here. All these images are downloaded from USC-SIPI database[1]. In compression phase, the chosen quantization step Q is ranging from 1 to 8. Fig. 4 shows the comparison results between our method and Kang *et al.*'s [13] for the eight standard images. In each figure, x and y-axes mean the compression ratio and the PSNR of reconstructed image versus the original one, respectively. From these figures, one can see that our method achieves a better performance than Kang *et al.*'s since, for a given compression ratio, our method can provide always a larger PSNR. Moreover, for our method with increasing Q, the compression ratio decreases significantly while the corresponding PSNR decreases slowly. As a result, our superiority with respect to Kang *et al.*'s method is significant for the case of low compression ratio.

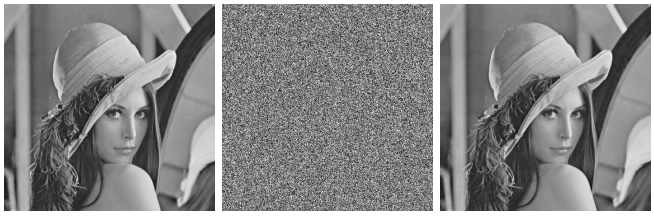

Fig. 3. The left, center and right figures show the original image of Lena, the encrypted image and the reconstructed image with a PSNR of 37.78 dB, respectively.

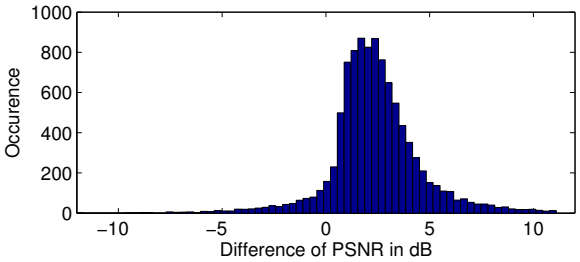

Fig. 5. Distribution of PSNR difference between our scheme and the method of Kang *et al.* [13] on the database of BossBase v1.01.

For the second experiment, we conduct the comparison on a large database of BossBase v1.01[2] [17] containing 10,000 gray-scale images. The images in BossBase are never-compressed images coming from several digital cameras. All these images are created from full-resolution color images in RAW format (CR2 or DNG). The images are then resized such that the smaller side is 512 pixels long, then they are cropped to 512×512 pixels, and finally converted to gray-scale. In this experiment, Kang *et al.*'s compression ratio is fixed as 0.375, and our compression ratio is taken as a value equal to or smaller than 0.375 by using a suitable quantization step Q. The probability distribution of PSNR difference between the proposed method and Kang *et al.*'s is shown in Fig. 5, demonstrating the superiority of our method on a large database. Specifically, the PSNR increase is 2.40 dB in average for the 10,000 images.

5. CONCLUSION AND RELATION TO PRIOR ART

In this paper, we proposed a new lossy compression scheme for encrypted gray-scale images. The main features of our method are described as follows. First, in compression phase, the spatial correlation and quantization operation are exploited to make the compression efficient without much information loss. Second, at the receiver

[1] http://sipi.usc.edu/database/database.php?volume=misc

[2] http://www.agents.cz/boss/BOSSFinal/

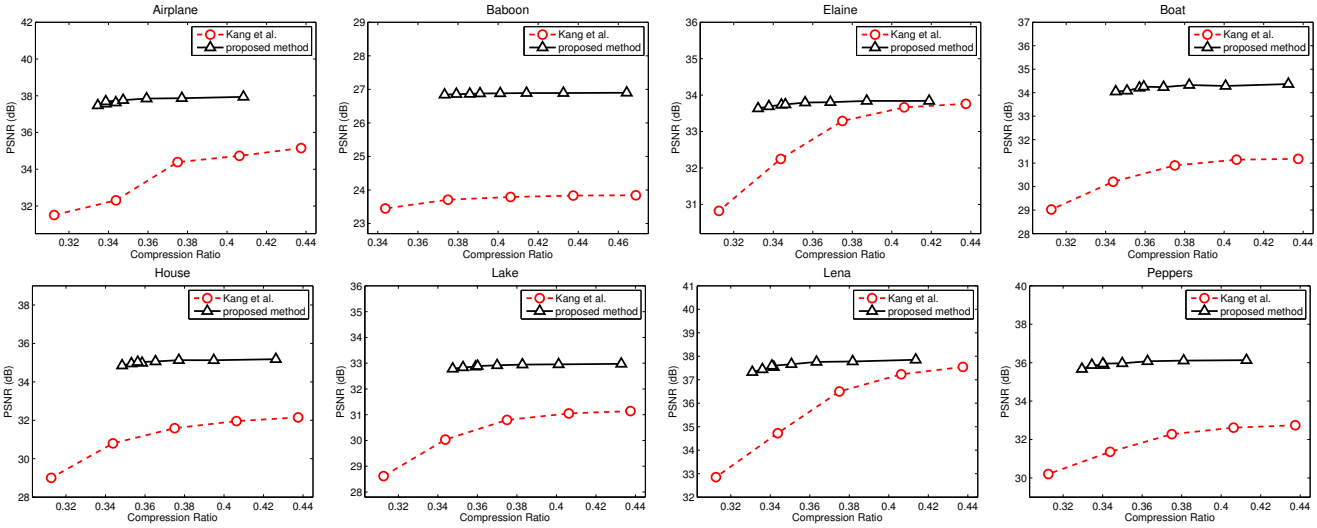

Fig. 4. Performance comparison between the proposed method and Kang *et al.*'s [13] for eight standard test images.

side, CAI with an image-dependent threshold is utilized such that the image reconstruction more precise. The experimental results showed that our scheme is better than the previous work proposed by Kang *et al.* [13].

So far, more and more attention has been paid to signal processing in the encrypted domain (SPED). However, only a few works have been proposed for the lossy compression of encrypted images. As we know, the key issue of SPED is how to integrate the encryption and the desired processing. In this work, a two-stage encryption is employed, and, to our best knowledge, it is the first time to use this type of encryption in SPED. Based on the specific encryption, the spatial correlation of natural images and quantization operation can be exploited to make the compression efficient. Moreover, in our scheme, an improved CAI-based prediction is also proposed and it is proved effective in enhancing the reconstructed image quality.

6. REFERENCES

[1] 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*, vol. 2007, 2008.

[2] R. L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," *IEEE Signal Processing Mag.*, vol. 30, no. 1, pp. 82–105, January 2013.

[3] H. Kiya and M. Fujiyoshi, "Signal and image processing in the encrypted domain," *ECTI Transactions on Computer Engineering, Computer and Information Technology*, vol. 6, no. 1, pp. 11–18, May 2012.

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

[5] D. Schonberg, *Practical distributed source coding and its application to the compression of encrypted data*, Ph.D. thesis, EECS Department, University of California, Berkeley, July 2007.

[6] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey-level and color images," in *Proc. EUSIPCO*, 2008.

[7] 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, April 2010.

[8] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (discus): Design and construction," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 626–643, March 2003.

[9] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, July 1973.

[10] A. Kumar and A. Makur, "Lossy compression of encrypted image by compressive sensing technique," in *Proc. IEEE TENCON*, 2009.

[11] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," *IEEE Trans. Inf. Forens. Security*, vol. 6, no. 1, pp. 53–58, March 2011.

[12] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images," *IEEE Trans. Image Process.*, vol. 21, no. 6, pp. 3108–3114, June 2012.

[13] X. Kang, A. Peng, X. Xu, and X. Cao, "Performing scalable lossy compression on pixel encrypted images," *EURASIP Journal on Image and Video Processing*, vol. 2013, 2013.

[14] D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, "Toward compression of encrypted images and video sequences," *IEEE Trans. Inf. Forens. Security*, vol. 3, no. 4, pp. 749–762, December 2008.

[15] J. Yen and J. Guo, "Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation," *IEE Proceedings-vision, image and signal processing*, vol. 147, no. 2, pp. 167–175, April 2000.

[16] N. Bourbakis and C. Alexopoulos, "Picture data encryption using SCAN patterns," *Pattern Recognition*, vol. 25, no. 6, pp. 567–581, June 1992.

[17] P. Bas, T. Filler, and T. Pevny, "Break our steganographic system - the ins and outs of organizing BOSS," in *Proc. 13th Int. Workshop on Information Hiding*, 2011, vol. 6958 of *Springer LNCS*, pp. 59–70.