A Scalable Image Coding Based on Content Adaptive Interpolation for Pixel Encrypted Images

CH. NAVEEN CHANDRA¹, N. RAJ KUMAR², E. VENKAT REDDY³

¹PG Scholar, Bharat Institute of Engineering & Technology, Hyderabad, Telangana, India, E-mail: cherupally naveen@gmail.com.
²Associate Professor, Bharat Institute of Engineering & Technology, Hyderabad, Telangana, India, E-mail: rajkumar@biet.ac.in.
³Associate Professor, Bharat Institute of Engineering & Technology, Hyderabad, Telangana, India, E-mail: evreddy@biet.ac.in.

Abstract: Compression of encrypted data draws much attention in recent years due to the security concerns in a service-oriented environment such as cloud computing. The traditional way of securely and efficiently transmitting redundant data is to first compress the data to reduce the redundancy then encrypt the compressed data. At the receiver side, decryption is performed prior to decompression. The main problem associated with the previous approach is it encrypts the image based on permutation. However, when using the permutation-based encryption, only the pixel positions are permuted, but the pixel values are not masked in the encryption phase, which means that the histogram of the encrypted image will remain the same as the original image, revealing some significant information. As well as it also utilizing a huge public orthonormal matrix this in turn increases the computational complexity. In this paper, a scalable lossy compression scheme for images is proposed having their pixel value encrypted with a standard stream cipher. At the receiver side, a decoder performs a content-adaptive interpolation prediction based on the decrypted partial information, and the received bit plane information serves as the side information to facilitate accurate image reconstruction.

Keywords: Image Compression; Image Encryption; Lossy Compression; Image Reconstruction; Scalable Coding.

I. INTRODUCTION

Compression of encrypted image has attracted in the recent years with great research interest. To reduce redundancy first compress the image then encryption is applied to the compressed image is the traditional method of securely transmitting the image[1]. The decryption operation as well as the decompression operation may be performed at the receiver side to obtain the reconstructed image. In case of some applications, some data needs to transmit from sender to receiver and keeps the information confidential to a network operator. So sender should encrypt the original image and the network provider may compress the encrypted image without any knowledge regarding the original data. Decompression as well as decryption may be performed to reconstruct the original image. Compressive sensing is an emerging area, which gained a lot of interest due to its ability to reconstruct the sparse signal from relatively smaller sample set[2]. This may provide a new method of signal compression whose particular application is the irretrievable compression of encrypted data. Compression as well as the encryption is necessary while an image is transmitting over insecure bandwidth limited channel.

Comprehensible structure of the image may be converted to incomprehensible structure by an encryption technique, which makes the encrypted image difficult to perform compression by using any simple classical compression algorithm. But the network operator is forced to compress the encrypted image due to the limitation of bandwidth. For such scenarios to compress the data, proposed methods are based on distributed source encoding (DSC) [3]. Since the encryption key is known at the decoder, DSC exploits the correlation between the encryption key and encrypted data. In this case, correlation such as statistics of the information source affected the compression efficiency. Correlation can be modeled by a binary symmetric correlation; while [4] the binary image is assumed to be sparse. To improve the compression efficiency, higher memory models [5] were used to model correlation. Since good compression does not achieve by extending these to gray scale images and hence [6] propose to apply encryption on the prediction errors follow a Laplacian density function to achieve good compression along with good security. Good compression can be obtained, since the prediction errors follow a Laplacian density function.

In this paper, we propose a scalable lossy compression scheme for images having their pixel value encrypted with a standard stream cipher. At the receiver side, a decoder performs a content-adaptive interpolation prediction based on the decrypted partial information, and the received bit plane information serves as the side information to facilitate accurate image reconstruction. The experimental results show that our proposed scheme achieves much better performance than the existing lossy compression scheme for pixel-value encrypted image and achieves similar performance as the...
state-of-the-art lossy compression for permutation-based encrypted images. The rest of this paper is organized as follows: section II gives the details about the earlier approaches proposed by various researchers on compression and encryption. The complete details about the proposed approach are given in section III. Section IV illustrates the performance evaluation of proposed approach and finally the conclusions are given in section V.

II. RELATED WORKS

Compression of encrypted data draws much attention in recent years due to the security concerns in a service-oriented environment such as cloud computing [7,8]. The traditional way of securely and efficiently transmitting redundant data is to first compress the data to reduce the redundancy then encrypt the compressed data. At the receiver side, decryption is performed prior to decompression. However, in some application scenarios (e.g., sensor networking), a sender may first perform encryption with a simple cipher and then send it to a network provider. The network provider always has the interest to reduce the rate. It is desirable to be able to compress the encrypted data without the key to reduce the security concerns. At the receiver side, joint decryption and decompression will be used to reconstruct the original data. It has been proved in [7] that the overall system performance of such approach can be as good as the conventional approach, that is, neither the security nor the compression efficiency will be sacrificed by performing compression in the encrypted domain. Two practical approaches to lossless compression of encrypted binary images and to lossy compression of encrypted Gaussian sequence are also presented in [7].

In the first approach, the original binary image is encrypted by adding a pseudorandom string; the encrypted data are compressed by finding the syndromes with respect to a low-density parity-check (LDPC) code [9]. In the second approach, the original data are encrypted by adding an iid Gaussian sequence, and the encrypted data are quantized and compressed as the syndromes of a trellis code. In [10], compression of encrypted data for both memory less sources and sources with hidden Markov correlation using LDPC codes is also studied. A study [11] introduces a few methods for lossless compression of encrypted grayscale and color images by employing LDPC codes to various bit planes and exploiting the spatial and cross-plane correlation among pixels. In [12], Liu et al. proposed to decompose the encrypted image in a progressive manner, and the most significant bits in the higher levels are compressed using rate-compatible punctured turbo codes. The decoder can observe a low-resolution version of the image, study the local statistics based on it, and use the statistics to estimate the content in the higher levels. Another study [13] presents some algorithms for compressing encrypted data and demonstrates blind compression of encrypted video by developing statistical models for source data and extending these models to video. All of the works mentioned above use the distributed source coding (DSC) technique. However, a frequent backward channel communication is needed for the joint decryption and decoding at the receiver, and thus, large delay maybe of concern. So, DSC-based methods may not be a desirable choice in some practical network transmission scenarios.

III. PROPOSED APPROACH

A. Image Encryption

We assume the images have been encrypted by applying a standard stream cipher to the pixel values in the spatial domain. Even though the pixel value has been encrypted, the resulting encrypted data preserve some of the inherent property of the original image, e.g., the spatial relationship of pixels and the bit plane structure and their relative importance. This leads us to adopt a multi-resolution and bit plane-based scalable approach for the compression. The basic idea is to package and transmit a down sampled version of the encrypted image as the base layer, then selectively transmit additional bit plane information from another down sampled version (with a different spatial offset) of the encrypted image to facilitate the interpolation/Reconstruction of the higher resolution image at the receiver. This process can be recursively applied in a multi-layer structure. This results in an embedded, compressed, and encrypted bit-stream, where the bit-stream can be cut off flexibly to meet a target bit rate constraint without requiring complex communication/negotiation between the encoder and decoder as was the case in some prior work that used DSC, e.g.,[7]. In the following, we describe our proposed scheme in a two-layer scenario. Suppose the size of an original 8-bit gray scale image is N x N. It is encrypted with a standard stream cipher, resulting in an encrypted image E.

B. Image Compression

To compress, we down sample the encrypted image by a factor of two in both dimensions and generate four sub-images, denoted as E_00, E_01, E_10, and E_11. Here, the first digit ‘1′ (or ‘0′) denotes that the horizontal offset for Down sampling is 1 (or 0), the second digit ‘1′ (or ‘0′) denotes that the vertical offset is 1 (or 0). As shown in Fig.1, each icon is a pixel. We use the four icons to distinguish the four sub-images after down sampling. When they are decrypted and decompressed, they are denoted as 00, 01, 10, and 11 sub-images, respectively. The un compressed E_00 sub-image will be transmitted to the decoder. Some of the E_11 sub-image's bit planes will be transmitted, too, according to the target bit rate. The target bit rate (R) per information source bit can be calculated by:

$$R = 0.25 + 0.25 \times N/8, \quad (1)$$

Where N is the number of bit planes of sub-image E_11 to be transmitted. For example, if N = 2, it means two bit planes of sub-image E_11 are transmitted. Let b_0,b_1,b_2,...,b_7 denote the eight bit planes, and b_0,b_8 are transmitted. The compression rate is $0.25 + 0.25 \times 2/8 = 0.3125$. The decoder reconstructs the 00 sub-image by decrypting the E_00 sub-image and also obtains b_7,b_6 of the 11 sub-image by decryption. Here, according to our observation, b_8 can be recovered with little error by decompression, so the b_8 bit plane of sub-image 11
A Scalable Image Coding Based On Content Adaptive Interpolation for Pixel Encrypted Images

is always transmitted only when all of \(b_7, b_6, \ldots, b_1\) bit planes of sub-image 11 are transmitted, that is, only when \(N = 8\). \(N = 8\) means that sub-image 11 is transmitted. For every pixel in the 11 sub-image, there are four neighboring pixels \(t = [t_1, t_2, t_3, t_4]\) in the 00 sub-image. We predict the 11 sub-image using the 00 sub-image with the context-adaptive interpolation (CAI) scheme proposed in [12].

C. Image Retrieval

In this work, we propose to use the received bit plane values of sub-image 11 as the side information to facilitate the estimation of the image edge information in the context adaptive interpolation thus improving the prediction. For the 10 sub-image, there are also four neighboring pixels in the 00 and 11 sub-images as shown in the bottom right of Fig.1. So, when the receiver obtains sub-image 00 and sub-image 11, the 10 sub-image (and 01 sub-image) can be predicted by the conventional CAI (please refer to[6] for a detailed description of the conventional CAI). In the following, we only present the improved CAI prediction of the 11 sub-image with the received bit plane information as the side information. Let \(0\) be a pixel in the 11 sub-images which is to be predicted and \(t = [t_1, t_2, t_3, t_4]\) be the vector of its four neighboring pixels. The preliminary prediction of pixel 0 with CAI [6] is:

\[
pred_0 = \begin{cases} 
\text{mean}(t) & \text{(max}(t) - \text{min}(t) \leq 20) \\
\frac{5t_2 + 2t_3}{3} & \text{medium}(t) \text{ otherwise} \\
\frac{5t_1 + 2t_4}{3} & \text{(max}(t) - \text{min}(t) > 20) \\
\frac{5t_1 - t_2}{2} & \text{(min}(t) - \text{max}(t) > 20) \\
\frac{5t_3 - t_4}{2} & \text{otherwise} 
\end{cases}
\] (2)

In Equation 2, the local region is classified into four types: smooth, horizontally edged, vertically edged, and other median-related edge. With the received bit plane values of sub-image 11, we can match the bit plane values of pred0 with the received bit plane value. If they match with each other, we accept the preliminary prediction value; otherwise, we find a better-matching prediction using the image edge directions other than the four local regions considered in Equation 2.

The decoder will receive \(E_{00}\) sub-image and some bit planes of the \(E_{11}\) sub-image. After decryption, the decoder will get 00 sub-image and some bit planes of the 11 sub-image. We denote the decimal value of the bit planes which are transmitted and decrypted as \(w\). Take \(N = 2\) for example, \(b_7 b_6\) of the 11 sub-image was considered. If \(b_7 b_6 = (10)2, w = 2\). \(w \in [0, 2N - 1] = [0, M - 1]\). Let \(\Delta\) be the step size corresponding to the most significant bit plane of the side information. In this paper, we adopt \(\Delta = 2^7\) when \(N < 8\) in our scheme. Define the matching distance \(d\) as follows:

\[
d = \text{floor}\left(\text{mod}\left(\frac{\text{pred}_0}{2}, M\right)\right) - w, \quad (3)
\]

Where mod( ) is the modulation operation. As \(b_7 b_6\) was known, we calculate the distance \(d\) between \(w\) and the decimal value of the same bit planes of \(\text{pred}_0\). The distance can be used to judge whether the \(\text{pred}_0\) matches well. If the distance is large, such that:

\[
M/4 < |d| < 3 \times M/4, \quad (4)
\]

We consider that \(\text{pred}_0\) does not match well. Then, other two prediction values \(\text{pred}_1\) and \(\text{pred}_2\), which correspond to other image edge directions, will compete with the preliminary prediction value \(\text{pred}_0\) for the best match with the side information:

\[
\text{pred}_1 = \frac{\text{sum}(t) - \text{min}(t)}{3}, \quad (5)
\]

\[
\text{pred}_2 = \frac{\text{sum}(t) - \text{min}(t)}{3}, \quad (6)
\]

Where \(\text{sum}(\cdot)\) denotes the summation operation, and \(\text{max}(\cdot)\) and \(\text{min}(\cdot)\) denote taking maximum and minimum operation, respectively. We find the best match by seeking the minimum value of \(\min(|d|, M - |d|)\) among the three prediction values \(\text{pred}_0, \text{pred}_1, \text{pred}_2\) and obtain the final best matching prediction \(\text{pred}\). Finally, with the side information, the corresponding prediction value \(r\) can be further refined to be:

\[
r = \begin{cases} 
\text{floor}\left(\frac{\text{pred}_0}{\Delta}\right) \times \Delta + w & \text{if } |d| < \frac{M}{2} \\
\text{floor}\left(\frac{\text{pred}_1}{\Delta}\right) \times \Delta + w & \text{if } |d| > \frac{M}{2} \\
\text{floor}\left(\frac{\text{pred}_2}{\Delta}\right) \times \Delta + w & \text{otherwise}
\end{cases}
\] (7)

Where \(\text{floor}\left(\text{pred}/\Delta\right) \times \Delta\) is the value of the \(b8\) of the prediction in the pixel; \(w \times \Delta/M\) is the value of the bit planes transmitted in the pixel.

IV. RESULTS

In this section, we will examine the performance of our proposed method and also compare it with the existing state-of-the-art works. The proposed compression scheme is applied on a variety of images with different sizes. We will show the test results for four selected standard images which have varying texture contents.

![Fig.1. Original image.](Image)
The above fig.1 shows the original image of Lena with a size of 512x512.

The above fig.2 shows the encrypted image of Lena. The above image has been encrypted by applying a standard stream cipher to the pixel values in the spatial domain. For the above image the process of encryption was performed at N bit plane=2,3,4,5,6.

The above fig.3 shows the down sample of the encrypted image by a factor of two dimensions and generates four sub-images, denoted as E00, E01, E10, and E11. Here, the first digit ‘1’ (or ‘0’) denotes that the vertical offset for down sampling is 1 (or 0).

The above fig.4 shows the down sample E00 of the decoded image after processing the encrypted image through a system. This version of downsample was independent and was decoded in an independent manner.

The above fig.5 shows the down sample E11 of the decoded image after processing the encrypted image through a system. This sub image was decoded based on the number of bitplanes transmitted. This is the recovered E11 at N bit plane =2.

The above fig.6 shows the decoder will receive E00 sub-image and some bit planes of the E11 sub-image. Here target bit rate can be calculated in this bit planes equal to 2.

- N=2
- bit rate = 0.3125
- MSE = 2.1561
- PSNR = 42

The above fig.7 shows the decrypted image.
A Scalable Image Coding Based On Content Adaptive Interpolation for Pixel Encrypted Images

The above fig. 7 shows the decrypted image this is almost similar to the original image.

V. CONCLUSIONS

Compression of encrypted data draws much attention in recent years due to the security concerns in a service-oriented environment such as cloud computing. We propose a scalable lossy compression scheme for images having their pixel value encrypted with a standard stream cipher. The encrypted data are simply compressed by transmitting a uniformly sub sampled portion of the encrypted data and some biplanes of another uniformly sub sampled portion of the encrypted data. At the receiver side, a decoder performs content-adaptive interpolation based on the decrypted partial information, where the received bit plane information serves as the side information that reflects the image edge information, making the image reconstruction more precise. When more bit planes are transmitted, higher quality of the decompressed image can be achieved. The experimental results show that our proposed scheme achieves much better performance than the existing lossy compression scheme for pixel-value encrypted images and also similar performance as the state-of-the-art lossy compression for pixel permutation-based encrypted images. In addition, our proposed scheme has the following advantages: at the decoder side, no computationally intensive iteration and no additional public orthogonal matrix are needed. It works well for both smooth and texture-rich images.

VI. REFERENCES