Journal of Visual Communication and Image Representation 51 (2018) 122–130

Contents lists available at ScienceDirect

Journal of Visual Communication and Image Representation

journal homepage: www.elsevier.com/locate/jvci

A lossy compression scheme for encrypted images exploiting Cauchy distribution and weighted rate distortion optimization☆

Chuntao Wang[a,b,*], Deqing Xiao[a], Hongxing Peng[a], Rongyue Zhang[c]

[a] College of Mathematics and Informatics, South China Agricultural Univ., Guangzhou 510642, China
[b] Shenzhen Key Laboratory of Media Security, Shenzhen University, Shenzhen 518060, China
[c] College of Computer Science, Guangdong Univ. of Tech., Guangzhou 510006, China

ARTICLE INFO

Keywords:
Compression of encrypted signals
Statistical model
Rate-distortion optimization
Lifting wavelet

ABSTRACT

How to improve the compression efficiency of encrypted signals remains a challenging problem. To alleviate this problem, this paper develops a new compression scheme on encrypted gray images by exploiting the Cauchy distribution and the weighted rate-distortion optimization (wRDO). In the scheme, the low-frequency and wavelet subbands generated through lifting wavelet transform are encrypted by stream and permutation ciphers, respectively. They are then compressed in lossless and lossy ways, respectively. Inverse operations are finally conducted at the receiver to reconstruct the original image. The lossy compression is formulated as a problem of wRDO and further solved by incorporating the Cauchy distribution that is demonstrated via extensive simulations to well characterize statistical distributions of wavelet subbands. Experimental results show that the proposed scheme is significantly better than other permutation-based prior arts and achieves comparable or even better performance in comparison to the conventional JPEG algorithm with original unencrypted images as input.

1. Introduction

Along with the coming of big data era, storing and sharing of images, videos, and audios is much easier than before. This, however, leads to the problem of data privacy protection. The conventional way for data privacy protection is to encrypt plain texts via a specific cipher. Nevertheless, such a approach would inevitably limit further processing of encrypted data. To solve the problem, many researchers carry out extensive research on the processing of encrypted signals [1–3].

Encrypted signal compression is one of key problems on encrypted signal processing, which mainly deals with the issue of efficient compression and secure transmission of encrypted signals in the environment like cloud computing, distributed processing, etc. The traditional way to tackle this issue is to perform compression before encryption, then transmit the resultant data via a public channel to the receiver, and finally conduct inverse operations to reconstruct the original signal. In the environment of cloud computing, distributed processing, etc., however, the content owner may merely sends the encrypted signal without any compression to the service provider such as cloud platform, channel operator, etc. This is because the content owner generally neither trusts the service provider nor has sufficient computational complexity and economic interest. Although service providers may have huge storage space or large bandwidth, it is still necessary for them to compress encrypted signals, aiming to save storage or bandwidth to accommodate increasingly huge amount of big data. This then gives rise to a kind of encryption-then-compression (ETC) system, as shown in Fig. 1, which is strongly contrast to the traditional compression-then-encryption (CTE) one.

As the encryption before compression masks statistical characteristics of carrier signals, it makes encrypted signals look completely random. As service providers in the ETC scenario cannot access the encryption key, this leads to serious challenge on the compression of encrypted signals. Intuitively, encrypted signals with complete randomness cannot be compressed, but Johnson et al. [4] proved by means of information theory that the ETC system can achieve the same compression and security performance as the traditional CTE one. In [4], they also presented both lossless and lossy practical compression algorithms for stream-ciphered data sequence converted from a binary image, demonstrating the feasibility of encrypted signal compression. Based on Johnson et al.'s investigation, many researchers conduct researches on the lossless compression of encrypted signals [5–11]. For example, Schonberg et al. [5–7] used the low-density parity-check (LDPC) code to compress the stream-ciphered binary image and employed the LDPC decoder to reconstruct the original image, in which

☆ This paper has been recommended for acceptance by Zicheng Liu.

* Corresponding author at: College of Mathematics and Informatics, South China Agricultural Univ., Guangzhou 510642, China.
E-mail address: wangct@scau.edu.cn (C. Wang).

https://doi.org/10.1016/j.jvcir.2018.01.007
Received 12 February 2017; Received in revised form 3 November 2017; Accepted 14 January 2018

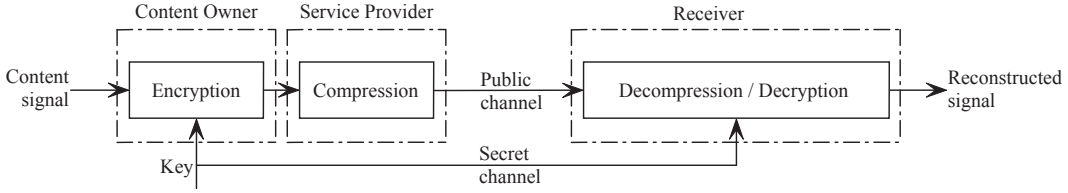

Fig. 1. Illustration of the ETC (encryption-then-compression) system.

the Markov model is integrated in the joint decompression and decryption to significantly improve the compression efficiency. By making full use of statistical correlations between different planes of gray image and that among different color components of color image, Lazzereitt and Barni [8] further enhanced the compression performance on stream-ciphered gray and color images. In contrast to previous approaches, Kumar and Makur [9] first generated prediction errors via a specific predictor and then performed encryption and compression on prediction errors, which well leverages statistical correlations of images and thus significantly improves the compression efficiency. In [10], Liu et al. proposed a novel compression scheme for encrypted gray images using the progressive reconstruction, i.e., the lower resolution version of the original image is exploited to estimate statistics for the higher resolution one, which well improves compression performance. Recently, Zhou et al. [11] designed a new compression scheme using the prediction error clustering and random scrambling, which achieves the performance comparable to the JPEG2000 with the original unencrypted image as input.

To obtain higher compression efficiency on the condition of feasible reconstruction quality, lossy compression of encrypted signals has also been extensively investigated [12–28]. According to lossy compression methods, they can be roughly classified into three categories, i.e., the compressive sensing (CS) based [12–15], the quantization based [16–25], and the uniformly down-sampling based [26–28] schemes, which are briefly introduced as follows. In [12], Kumar and Makur proposed to use the CS technique [29,30] to compress the encrypted data and modified the basis pursuit (BP) algorithm to reconstruct the original signal. Instead of the conventional CS matrix, Zhang et al. [13] adopted the gradient projection matrix, Song et al. [14] took advantage of the learned image dictionary, and Zhang et al. [15] designed the structurally random matrix. For the second category, Zhang [16] discarded, via a designed scalar quantizer, the rough and fine orthogonally-transformed coefficients of a permuted gray image, and reconstructed them in an iterative way. Subsequently, Zhang et al. [17] proposed to decompose the stream-ciphered image into several parts and quantify each part with a scalar quantizer, which gives rise to a scalable compression algorithm for encrypted images. Later in [18], they developed a lossy compression scheme through multi-layer decomposition, in which quantization steps are optimally determined via the rate distortion theory. In [19], Zhang et al. developed a novel compression scheme exploiting the auxiliary information, in which the auxiliary information of original image is generated before encryption and is further used at both the service-provider and receiver sides to facilitate the compression and reconstruction, respectively. In [20,21], Wang et al. constructed two lossy compression approaches on gray images using the integer lifting wavelet, in which quantization steps for different pyramid levels are obtained through the heuristic strategy and the rate-distortion optimization (RDO), respectively. In [22], Liu et al. applied the game theory to optimally allocate the bit length for each block, determined quantization steps adaptively according to the texture category, and used the image restoration from partial random samples (IRPRS) to generate more exact side information, facilitating the reconstruction of the original image. A prediction error based compression scheme on encrypted images is presented in [23], which encrypts a sub-image and the other ones with pseudo-random numbers and permutation technique, respectively, and compresses them independently via quantization and Huffman coding, respectively. Recently, Kumar and Vaish developed two ETC schemes using the wavelet difference reduction (WDR) and the singular value decomposition (SVD) in [24] and [25], respectively. The scheme in [24] compresses a sub-image of the pseudo-random number encrypted image via quantization and condenses the other sub-images with the WDR. The scheme of [25] encrypts the low frequency wavelet subband and the detailed subbands using the pseudo-random encryption and permutation, respectively, and compresses them via quantization and SVD, respectively. For the third category, Refs. [26–28] mainly deployed the uniformly down-sampling approach to compress the encrypted image, and exploited content adaptive interpolation methods to recover the original image.

From the above literature review, one can observe from the schemes of [7–11,16,18–21] that make full use of statistical properties of carrier signal can well improve compression efficiency and reconstruction quality for encrypted signals. Inspired by this observation, in this paper we propose a new compression scheme on encrypted gray image by leveraging the Cauchy distribution and the weighted RDO (wRDO). First, we decompose the input gray image via the lifting wavelet into a wavelet pyramid. As the lifting wavelet can be implemented in real time, it would merely increase the computational burden of content owner slightly. Second, we encrypt the low-frequency and wavelet subbands with the stream and permutation ciphers, respectively. Next, the encrypted low-frequency and wavelet subbands are compressed at the service provider side in lossless and lossy manners, respectively. In lossy compression, a simple scalar quantizer is used and optimum quantionzation steps are obtained using the Cauchy-distribution-incorporated weighted RDO (wRDO). The Cauchy distribution is adopted because extensive simulations show that, compared to the generalized Gaussian (GGD) and Laplace distributions, the Cauchy distribution can better characterize statistical distributions of wavelet coefficients. Moreover, considering that wavelet subbands at coarser pyramid levels are more important to the reconstruction quality, different weights are assigned to distortions at different pyramid levels, which gives rise to the wRDO. Finally, the receiver performs inverse operations to recover the original image. The contributions of our work are threefold: (i) conducting extensive simulations to show that, among the Laplace, Cauchy, and generalized Gaussian statistical models, the Cauchy one best characterizes wavelet coefficients; (ii) formulating the problem of achieving the minimum distortion under the same compression rate as the wRDO by taking into account different significance of different pyramid levels in image reconstruction; and (iii) applying the Cauchy model in the wRDO to derive theoretically the optimal quantization steps.

Experimental results show that the proposed algorithm can obtain high compression efficiency and good reconstruction quality. Also, it achieves better performance than permutation-based prior arts and obtains comparable or even better performance in comparison to the conventional JPEG algorithm.

The rest of the paper is organized as follows. Section 2 introduces the evaluation on statistical models of Laplace, GGD, and Cauchy distributions. The proposed scheme and the Cauchy-distribution-incorporated wRDO are presented in Sections 3 and 4, respectively. Section 5 gives experimental results and analysis. The conclusion is finally drawn in Section 6.