 CMC, vol.56, no.1, pp.107-121, 2018

A New Encryption-Then-Compression Scheme on Gray Images Using the Markov Random Field

Chuntao Wang[1, 2], Yang Feng[1], Tianzheng Li[1], Hao Xie[1] and Goo-Rak Kwon[3]

Abstract: Compressing encrypted images remains a challenge. As illustrated in our previous work on compression of encrypted binary images, it is preferable to exploit statistical characteristics at the receiver. Through this line, we characterize statistical correlations between adjacent bitplanes of a gray image with the Markov random field (MRF), represent it with a factor graph, and integrate the constructed MRF factor graph in that for binary image reconstruction, which gives rise to a joint factor graph for gray images reconstruction (JFGIR). By exploiting the JFGIR at the receiver to facilitate the reconstruction of the original bitplanes and deriving theoretically the sum-product algorithm (SPA) adapted to the JFGIR, a novel MRF-based encryption-then-compression (ETC) scheme is thus proposed. After preferable universal parameters of the MRF between adjacent bitplanes are sought via a numerical manner, extensive experimental simulations are then carried out to show that the proposed scheme successfully compresses the first 3 and 4 most significant bitplanes (MSBs) for most test gray images and the others with a large portion of smooth area, respectively. Thus, the proposed scheme achieves significant improvement against the state-of-the-art leveraging the 2-D Markov source model at the receiver and is comparable or somewhat inferior to that using the resolution-progressive strategy in recovery.

Keywords: Encryption-then-compression, compressing encrypted image, Markov random field, compression efficiency, factor graph.

1 Introduction

Compressing encrypted signals is such a kind of technology that addresses the encryption-then-compression (ETC) problem in the service-oriented scenarios like distributed processing, cloud computing, etc. [Johnson, Ishwar and Prabhakaran (2004); Erkin, Piva, Katzenbeisser et al. (2007)]. In these scenarios, the content owner merely encrypts its signal and then sends it to the network or cloud service provider for the sake of limited computational resources. The service provider then compresses, without access to the encryption key, encrypted signals for saving bandwidth and storage space. The

[1] South China Agricultural University, Guangzhou 510642, China.

[2] Shenzhen Key Laboratory of Media Security, Shenzhen University, Shenzhen 518060, China

[3] Chosun University, Gwangju 501-759, Republic of Korea.

* Corresponding Author: Chuntao Wang. Email: wangct@scau.edu.cn.

receiver finally performs the successive decompression and decryption to reconstruct the original signal.

As the encryption prior to the compression masks the original signal, one may intuitively believe that it would be intractable to compress the encrypted signal. By taking the encryption key as the side information of the encrypted signal and further formulating the ETC problem as the distributed coding with side information at the decoder, however, Johnson et al. [Johnson, Ishwar, Prabhakaran et al. (2004)] demonstrated via the information theory that the ETC system would neither sacrifice the compression efficiency nor degrade the security, as achieved in the conventional compression-then-encryption (CTE) scenario that compresses the original signal before encryption. According to [Johnson, Ishwar, Prabhakaran et al. (2004)], by taking the syndrome of a channel code as the compressed sequence, channel codes like the low-density parity-check (LDPC) code can be exploited to compress the encrypted signal, and the DISCUS-style Slepian-Wolf decoder [Pradhan and Ramchandran (2003)] can then be used to recover the original signal. To illustrate this, Johnson et al. [Johnson, Ishwar, Prabhakaran et al. (2004)] also proposed 2 practical ETC schemes, which well demonstrates the feasibility and effectiveness of the ETC system.

From then on, a lot of ETC schemes [Schonberg, Draper and Ramchandran (2005, 2006); Schonberg, Draper, Yeo et al. (2008); Lazzeretti and Barni (2008); Kumar and Makur (2008); Zhou, An, Zhai et al. (2014); Liu, Zeng, Dong et al. (2010); Wang, Xiao, Peng et al. (2018)] have been developed. These schemes compress the cipher-stream-encrypted signal by generating the syndrome of LDPC code, and perfectly reconstruct the original signal via the joint LDPC decoding and decryption. Brief introduction to them are presented in the next section.

In contrast to these lossless compression schemes, a number of lossy compression approaches [Kumar and Makur (2009); Zhang (2011); Song, Lin and Shen (2013); Zhang (2015); Zhang, Ren, Feng et al. (2011); Zhang, Feng, Ren et al. (2012); Zhang, Sun, Shen et al. (2013); Zhang, Ren, Shen et al. (2014); Wang and Ni (2015); Wang, Ni and Huang (2015); Kumar and Vaish (2017); Wang, Ni, Zhang et al. (2018); Kang, Peng, Xu et al. (2013); Hu, Li and Yang (2014); Zhou, Liu, An et al. (2014)] have also been developed to improve the compression efficiency at the cost of tolerable quality loss. The approaches of Kumar et al. [Kumar and Makur (2009); Zhang, Ren, Feng et al. (2011); Song, Lin and Shen (2013); Zhang, Wong, Zhang et al. (2015)] use the CS technique [Donoho (2006)] to compress the stream-cipher encrypted data and modified the basis pursuit (BP) algorithm to reconstruct the original signal. In an alternative way, the schemes of Zhang et al. [Zhang (2011); Zhang, Feng, Ren et al. (2012); Zhang, Sun, Shen et al. (2013); Zhang, Ren, Shen et al. (2014); Wang and Ni (2015); Wang, Ni and Huang (2015); Kumar and Vaish (2017); Wang, Ni, Zhang et al. (2018)] condense the stream-ciphered or permutation-ciphered signal mainly using a scalar quantizer, while the methods of [Kang, Peng, Xu et al. (2013); Hu, Li and Yang (2014); Zhou, Liu, An et al. (2014)] compress the encrypted signal via the uniform down-sampling.

Similar to conventional compression approaches, ETC schemes also exploit the redundancy of the original sign al to achieve good compression efficiency. For instance, the ETC methods of Lazzeretti et al. [Lazzeretti and Barni (2008); Kumar and Makur

(2008); Zhou, Au, Zhai et al. (2014)] and [Wang, Ni, Zhang et al. (2018)] leverage the redundancy by generating prediction errors before encryption. The approaches of Liu et al. [Liu, Zeng, Dong et al. (2010); Zhang, Ren, Feng et al. (2011); Zhang, Sun, Shen et al. (2013); Wang and Ni (2015); Wang, Ni and Huang (2015); Kumar and Vaish (2017)] exploit the redundancy by optimizing the compressor with statistical characteristics of the original signal that is intentionally revealed by the content owner. These two categories, however, either remarkably increase the computational burden at the content owner or considerably degrade the security by disclosing statistical distributions to the service provider.

Regarding that the receiver has both the encryption key and feasible computational resources, it is preferable to make full use of statistical correlations of the original signal at the receiver, as analyzed in our recent work [Wang, Ni, Zhang et al. (2018)]. To illustrate this, the work of Wang et al. [Wang, Ni, Zhang et al. (2018)] uses the Markov random field (MRF) to characterize spatial statistical characteristics of a binary image and seamlessly integrates it with the LDPC decoding and decryption via the factor graph. By leveraging the MRF at the receiver side, the work of Wang et al. [Wang, Ni, Zhang et al. (2018)] achieves significant improvement in terms of compression efficiency over the method of Schonberg et al. [Schonberg, Draper and Ramchandran (2008)] using the 2-dimensional (D) Markov source model at the receiver.

In light of this, in this paper we extend our previous work [Wang, Ni, Zhang et al. (2018)] to gray images. Specifically, since each bit-plane of a gray image can be considered as a binary image, we apply the algorithm in Wang et al. [Wang, Ni, Zhang et al. (2018)] on each bit-plane of a gray image to achieve the lossless compression for each bit-plane. By observing that adjacent bit-planes resemble each other, we further exploit the MRF to characterize statistical correlations between adjacent bit-planes and incorporate it in the reconstruction of corresponding bitplanes, aiming to achieve higher compression efficiency for gray images. By representing the MRF between adjacent bitplanes with a factor graph and further incorporating it in the joint factor graph for binary image reconstruction, we construct a joint factor graph for gray image reconstruction (JFGIR) followed by theoretically deriving the sum-product algorithm (SPA) adapted to the JFGIR. Assisted by the stream-cipher-based encryption, LDPC-based compression, and JFGIR-involved reconstruction, this then gives rise to an MRF-based ETC scheme for gray images. Experimental results show that the proposed scheme achieves compression efficiency better than or comparable to the state-of-the-arts exploiting statistical correlations at the receiver.

The contribution of this work is two-fold: i) Exploiting the MRF to characterize statistical correlations between two adjacent bit-planes of a gray image; and ii) Constructing a JFGIR to seamlessly integrate LDPC decoding, decryption, and the MRF within a bit-plane and between adjacent bit-planes, and deriving theoretically the SPA adapted to the constructed JFGIR.

The rest of the paper is organized as follows. Section 2 briefly reviews ETC schemes that perform lossless compression on encrypted images. Section 3 presents the construction of JFGIR and the theoretical derivation of the SPA for the JFGIR. The proposed scheme for

gray images are introduced in Section 4, and experimental results and analysis are given in Section 5. Section 6 finally draws the conclusion.

2 Prior arts

As this paper focuses on the lossless compression of encrypted images, in this section we mainly review ETC schemes for lossless compression of encrypted images. Brief introductions to these ETC schemes are presented below.

Based on Johnson et al.'s work [Johnson, Ishwar, Ramchandran et al. (2004)], Schonberg et al. [Schonberg, Draper and Ramchandran (2005, 2006); Schonberg, Draper, Yeo et al. (2008)] further integrated the Markov model in image reconstruction. These well exploit statistical correlations between adjacent image pixels and thus significantly improve the compression efficiency.

A number of ETC approaches generating prediction errors before encryption have also been proposed in the literature [Lazzeretti and Barni (2008); Kumar and Makur (2008); Zhou, Liu, Au et al. (2014)]. In Lazzeretti et al. [Lazzeretti and Barni (2008)], the authors extended the Johnson et al.'s scheme [Johnson, Ishwar, Ramchandran et al. (2004)] to gray and color images by leveraging the spatial, cross-plane, and cross-band correlations before stream-cipher-based encryption, achieving good compression efficiency. By imposing the LDPC-based compression on encrypted prediction errors rather than directly on image pixels, Kumar and Makur obtained higher compression efficiency [Kumar and Makur (2008)]. Zhou et al. [Zhou, Au, Zhai et al. (2014)] obtained nearly the same compression efficiency as the conventional compression schemes with original, unencrypted images as input through prediction error clustering and random permutation.

In an alternative way, Liu et al. [Liu, Zeng, Au et al. (2010)] compressed the encrypted gray image in a progressive manner and exploited the low-resolution sub-image to learn source statistics for high-resolution ones. Compared to the practical lossless ETC scheme in Johnson et al. [Johnson, Ishwar and Ramchandran (2004)], the work of Liu et al. [Liu, Zeng, Au et al. (2010)] achieves better compression efficiency.

Recently, Wang et al. [Wang, Ni, Zhang et al. (2018)] developed another ETC scheme using the MRF. They deployed the MRF [Li (1995)] to characterize the spatial statistical characteristic of a binary image, represented the MRF with a factor graph [Kschischang, Frey and Loeliger (2001)], sophisticatedly integrated the factor graph for the MRF with those for the decryption and LDPC decoding to construct a joint factor graph for binary image reconstruction, and derived theoretically the SPA for the constructed joint factor graph. This MRF-based scheme achieves significant improvement over the ETC approach using the 2-D Markov source model [Schonberg, Draper and Ramchandran (2006)].

3 Design of JFGIR and derivation of SPA

3.1 Characterization of statistical correlations between adjacent bitplanes

Let $I(x,y)$ be an 8-bit image of size $m \times n$. Then its kth $(k = 1,\ldots,8)$ bit-plane, says $B^k(x,y)$, is obtained as:

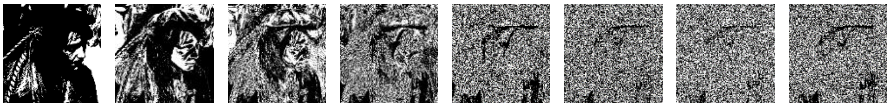

Figure 1: Illustration of 8 bit-planes of Image "Man", where bitplanes from left to right are $B^8(x,y)$, $B^7(x,y)$, ..., and $B^1(x,y)$, respectively

$$B^k(x,y)=\left\lfloor \frac{I(x,y)}{2^{k-1}} \right\rfloor \%2, k=1,\ldots,8, \tag{1}$$

where $\lfloor\cdot\rfloor$ is a floor function. The $B^8(x,y)$ denotes the MSB while the $B^1(x,y)$ stands for the LSB.

Fig. 1 illustrates 8 bit-planes of gray image "Man". It is observed that any two adjacent bit-planes, $B^k(x,y)$ and $B^{k-1}(x,y)$ ($k=8,\ldots,2$), resemble each other. That is, if $B^k(x,y)$ is equal to $b\,(b=0,1)$, then $B^{k-1}(x,y)=b$ may hold with high probability. Therefore, there exists statistical correlations between $B^k(x,y)$ and $B^{k-1}(x,y)$. Similar results can also be found in other gray images.

As the MRF well characterizes the spatial statistical feature of binary images, as demonstrated in Wang et al. [Wang, Ni, Zhang et al. (2018)], we deploy the MRF [Li (1995)] to model statistical correlations between $B^k(x,y)$ and $B^{k-1}(x,y)$. As the MRF within a bitplane has, according to Wang et al. [Wang, Ni, Zhang et al. (2018)], already taken into account spatial statistical correlations between pixels in the neighborhood, we mainly characterize statistical correlations between bits $B^k(x,y)$ and $B^{k-1}(x,y)$ at the same coordination rather than modeling those between $B^k(x,y)$ and $B^{k-1}(\mathcal{N}(x),\mathcal{N}(y))$, where $\mathcal{N}(x)$ denotes a set containing x and its neighborhood. Thus, statistical correlations between bits $B^k(x,y)$ and $B^{k-1}(x,y)$ can be characterized with the MRF as:

$$p\left(\mathrm{F}^{k-1}(x,y)\,|\,\mathrm{F}^k(x,y)\right)=\frac{1}{Z}\exp\left(-\frac{V_c\left(\mathrm{F}^{k-1}(x,y)\,|\,\mathrm{F}^k(x,y)\right)}{T}\right) \tag{2}$$

where $p(\cdot)$ is a probability function, and $\mathrm{F}^k(x,y)$ denotes a random variable for bit $B^k(x,y)$ that takes on values in the state space, $\Phi=\{0,1\}$. The T in Eq. (2) is a temperature constant and Z is a normalizing constant defined as:

$$Z=\sum_{\mathbf{F}^k\in\Omega}\exp\left(-\frac{U\left(\mathbf{F}^k\right)}{T}\right) \tag{3}$$

where $\Omega=\{\mathbf{F}^k=(\mathrm{F}^k(1,1),\ldots,\mathrm{F}^k(x,y),\ldots,\mathrm{F}^k(m,n))\,|\,\mathrm{F}^k(x,y)\in\Phi\}$ is a configuration set including all possible realizations of $\mathbf{F}^k$. The $U(\mathbf{F}^k)$ in Eq. (3) is an energy function defined as:

$$U\left(\mathbf{F}^k\right)=\sum_{c\in C}V_c\left(\mathbf{F}^k\right) \tag{4}$$

where C is a set of cliques formed by the neighborhood system, and $V_c(\cdot)$ is a potential function defined on a given clique $c\,(c\in C)$ (e.g. in our case bits $B^k(x,y)$ and $B^{k-1}(x,y)$ form a clique). Eq. (2) calculates the probability of $\mathrm{F}^{k-1}(x,y)$ given $\mathrm{F}^k(x,y)$, and $p(\mathrm{F}^k(x,y)\,|\,\mathrm{F}^{k-1}(x,y))$ can be computed similarly.

3.2 Design of JFGIR

To seamlessly integrate the MRF between adjacent bit-planes in the bit-plane reconstruction using the factor graph, we further represent the MRF between adjacent bit-planes with a factor graph [Kschischang, Frey and Loeliger (2001)]. By denoting $\mathrm{F}^k(x,y)$ and $\mathrm{F}^{k-1}(x,y)$ with variable nodes (VNs) and characterizing the statistical correlation in Eq. (2) with a factor node (FN), we construct a factor graph for the MRF between adjacent bit-planes, as shown in Fig. 2, where circles and squares stand for VNs and FNs, respectively.

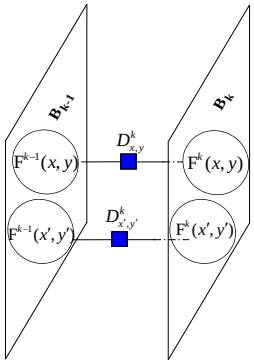

Figure 2: Illustration of the factor graph for the MRF between adjacent bit-planes, where B^k and B^{k-1} denotes 2 adjacent bit-planes and $D^k_{x,y}$ stands for the statistical correlation between $\mathrm{F}^k(x,y)$ and $\mathrm{F}^{k-1}(x,y)$

According to our previous work [Wang, Ni, Zhang et al. (2018)], the factor graph for the reconstruction of each bit-plane can be constructed as Fig. 3, where the bit-plane index, k, is omitted for simplicity. As shown in Fig. 3, the factor graphs in boxes with solid lines, dot lines, and dot-and-dash lines are those for the MRF within a bit-plane, decryption, and LDPC-based decompression, respectively. $\mathrm{S}_j\,(j=1,\ldots,q)$ are LDPC syndrome bits, which are taken as the encrypted and decompressed bit sequence, $\mathrm{Y}_i\,(i=1,\ldots,mn)$ is the decompressed but encrypted sequence, K_i is the encryption key sequence, $\mathrm{F}_i\ (i=(y-1)n+x)$ is a 1-D bit sequence converted from a given bit-plane, and $\mathrm{F}_{x,y}$ denotes bits of a 2-D bit-plane. $\mathrm{M}_{x,y}/\mathrm{N}_{x,y}$, $\mathrm{P}_{x,y}$, t_i, and g_j represent the

constraints imposed by the MRF within a bit-plane, image source prior, decryption, and LDPC code, respectively.

By merging the same VNs of Figs. 2 and 3, we can build the JFGIR for the reconstruction of two adjacent bit-planes, $B^k(x,y)$ and $B^{k-1}(x,y)$ $(k=8,\ldots,2)$. As illustrated in Fig. 1, the randomness of $B^k(x,y)$ (i.e. entropy) is less than that of $B^{k-1}(x,y)$. Thus, $B^k(x,y)$ would achieve higher lossless compression efficiency than $B^{k-1}(x,y)$ and provide more statistical information for $B^{k-1}(x,y)$, and vice versa. Therefore, it is preferable to first reconstruct $B^k(x,y)$ and then exploit its statistical correlation to recover $B^{k-1}(x,y)$.

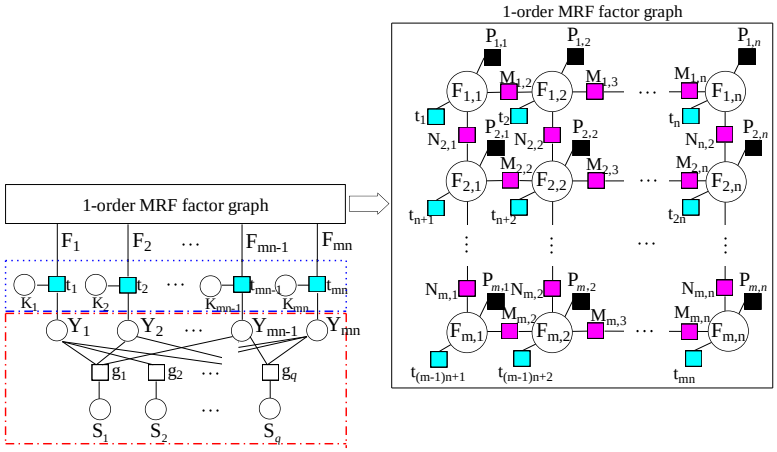

Figure 3: Illustration of the factor graph for reconstruction of each bit-plane B_k of size $m \times n$

3.3 Derivation of SPA adapted to JFGIR

By taking the probability distribution of each bit in a bit-plane as a marginal function in the MRF, each bit-plane can thus be effectively recovered by running the SPA on the constructed JFGIR. By using the $\log(p(0)/p(1))$ as the message passed between VNs and FNs, where $p(0)$ and $p(1)$ denote the probabilities of bits 0 and 1, respectively, we then derive the SPA adapted to the JFGIR as follows.

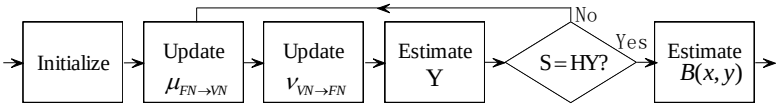

Figure 4: Flowchart of the SPA on the JFGIR

Fig. 4 plots the flowchart of the SPA, where $\nu_{VN\to FN}$ and $\mu_{FN\to VN}$ denote a message updated from a VN to an FN and that from an FN to a VN, respectively. The initialization

step initializes all $v_{VN\to FN}$ s according to the received syndrome S_p $(p=1,\ldots,q)$, the secret key $\mathrm{K}_i(i=1,\ldots,mn)$, and the source prior $\mathrm{P}_{x,y}$ $(x\in[1,n],\ y\in[1,\mathrm{m}])$. Via $v_{VN\to FN}$ s, messages $\mu_{FN\to VN}$ are updated via the product operation of the SPA, which are then used to yield messages $v_{VN\to FN}$ s by means of the sum operation of the SPA. To check whether convergence is met or not, the decompressed but encrypted sequence Y_i is estimated using $v_{VN\to FN}$ s and $\mathrm{S}'=\mathrm{HY}$ is calculated accordingly. If S' is equal to S, then convergence is met and the original bitplane $B(x,y)$ can be perfectly recovered; otherwise, continue to execute these update and estimation steps until convergence is achieved or the predefined maximum iteration number is reached. Due to space limitation, details of these steps for the JFGIR within a bitplane is omitted here and recommended to refer to our previous work [Wang, Ni, Zhang et al. (2018)], while the involved details for the JFGIR between adjacent bitplanes are presented below, where the superscript k indicating the bit-plane index is re-inserted here to make symbols clear.

1) Initialization. As $B^k(x,y)$ has been reconstructed in recovering $B^{k-1}(x,y)$, message $\nu_{\mathrm{F}^k_{x,y}\to\mathrm{D}^k_{x,y}}$ $(k=8,\ldots,2)$ (see also Fig. 2) is initialed as:

$$\nu_{\mathrm{F}^k_{x,y}\to\mathrm{D}^k_{x,y}}=\begin{cases}-\infty & \textit{if } \mathrm{F}^k_{x,y}=0\\ +\infty & \textit{otherwise}\end{cases} \tag{5}$$

2) Message update for $\mu_{\mathrm{D}^k_{x,y}\to\mathrm{F}^{k-1}_{x,y}}$. It is derived via the SPA and the MRF as:

$$\mu_{\mathrm{D}^k_{x,y}\to\mathrm{F}^{k-1}_{x,y}}=\log\frac{\exp\left(\nu_{\mathrm{F}^k_{x,y}\to\mathrm{D}^k_{x,y}}-\dfrac{V_c(\mathrm{F}^{k-1}_{x,y}=0\,|\,\mathrm{F}^k_{x,y}=0)}{T}\right)+\exp\left(-\dfrac{V_c(\mathrm{F}^{k-1}_{x,y}=0\,|\,\mathrm{F}^k_{x,y}=1)}{T}\right)}{\exp\left(\nu_{\mathrm{F}^k_{x,y}\to\mathrm{D}^k_{x,y}}-\dfrac{V_c(\mathrm{F}^{k-1}_{x,y}=1\,|\,\mathrm{F}^k_{x,y}=0)}{T}\right)+\exp\left(-\dfrac{V_c(\mathrm{F}^{k-1}_{x,y}=1\,|\,\mathrm{F}^k_{x,y}=1)}{T}\right)} \tag{6}$$

The derivation is omitted here for space limitation.

3) Message update for $v_{VN\to FN}$. For bit-plane $B^{k-1}(x,y)$, it is unnecessary to send a message upward to $D^k_{x,y}$ as $B^k(x,y)$ has already been recovered during the reconstruction of $B^{k-1}(x,y)$. It is noted that recovering $B^8(x,y)$ only uses the SPA for a binary image [Wang, Ni, Zhang et al. (2018)] as there does not exist $B^9(x,y)$. The $\nu_{\mathrm{F}^{k-1}_{x,y}\to\mathrm{M}^{k-1}_{x,y}}$ can be calculated as

$$\nu_{\mathrm{F}^{k-1}_{x,y}\to\mathrm{M}^{k-1}_{x,y}}=\sum_{o\in\mathcal{N}\left(\mathrm{F}^{k-1}_{x,y}\right)\backslash\mathrm{M}^{k-1}_{x,y}}\mu_{o\to\mathrm{F}^{k-1}_{x,y}} \tag{7}$$

Messages $\nu_{\mathrm{F}^{k-1}_{x,y}\to\mathrm{M}^{k-1}_{x-1,y}}$, $\nu_{\mathrm{F}^{k-1}_{x,y}\to\mathrm{N}^{k-1}_{x,y}}$, and $\nu_{\mathrm{F}^{k-1}_{x,y}\to\mathrm{N}^{k-1}_{x,y-1}}$ are updated in a way similar to Eq. (7).

4 Proposed scheme

Fig. 5 illustrates the proposed MRF-based ETC scheme for encrypted gray images. Details for these steps are given below.

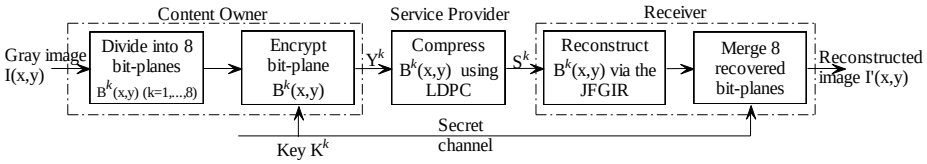

Figure 5: The proposed scheme

1) *Bit-plane division*. This step divides a gray image, $I(x,y)$, of size $m \times n$ into 8 bit-planes $B^k(x,y)\,(k=1,\ldots,8)$ using Eq. (1).

2) *Bit-plane encryption*. First generate a pseudorandom Bernoulli(1/2) bit sequence of length mn, says $\mathrm{K}^k=\{\mathrm{K}_i^k, i=1,\ldots,mn\}$, via the kth secret key $KEY+2^k$, where KEY is a one-time-pad initial secret key. Then encrypt $B^k(x,y)$ with the stream cipher, i.e., $\mathrm{Y}_i^k=B^k(x,y)\oplus\mathrm{K}_i^k, i=(y-1)m+x$.

3) *Bit-plane compression*. According to Johnson et al. [Johnson, Ishwar, Prabhakaran et al. (2004)], the service provider can compress, without access to the encryption key, each encrypted bit-plane using the channel code of LDPC. In particular, Y^k is compressed as $\mathrm{S}^k=\mathrm{H}\mathrm{Y}^k$, where H is a parity-check matrix of size $(1-R)mn\times mn$, where R is the code rate of LDPC.

To compress bitplanes with nearly equiprobable 0 s and 1 s, a doping technology is employed [Wang, Ni, Zhang et al. (2018)]. That is, a number of encrypted but uncompressed bits are sent to the receiver, and these doped bits are then used at the receiver as the "catalyst" to guide the SPA towards convergence. This is essentially equivalent to construct the parity-check matrix in case of doping as follows [Wang, Ni, Zhang et al. (2018)]:

$$\mathrm{H}_{new}=\begin{bmatrix}\mathrm{H}\\ \mathrm{D}\end{bmatrix} \tag{8}$$

where the D of size $dp\_rate\times\left((1-R)\times mn\right)$ contains doped rows, each of which consists of one 1 at a random column and $mn-1$ 0 s. The dp_rate denotes the doping rate, i.e. the ratio between the number of doped bits and the length of $(1-R)\times mn$. Thus, the compression rate in terms of bit per bit (bpb) is computed as:

$$cmp\_rate=\frac{(1-R)mn\times\left(1+dp\_rate\right)}{mn}=\left(1-R\right)\times\left(1+dp\_rate\right) \tag{9}$$

4) *Bit-plane reconstruction*. First reconstruct the MSB, $B^8(x,y)$, using the MRF-based method for a binary image [Wang, Ni, Zhang et al. (2018)] (see also Fig. 3), in which the

secret key $KEY + 2^8$ is used, where KEY is sent through a secret channel from the content owner side. Based on the reconstructed $B^8(x,y)$, we then recover $B^7(x,y)$ by running the SPA on the JFGIR (see also Figs. 2 and 4). After obtaining $B^7(x,y)$, we proceed to recover $B^6(x,y)$, and so on.

5) *Gray-image reconstruction*. By merging the 8 recovered bit-planes $B^k(x,y)$ (k=1, …, 8), we thus reconstruct the original gray image $I'(x,y)$.

5 Experimental results and analysis

In this section, we evaluate the proposed scheme. We first set parameters for the MRF and then compare compression efficiency of the proposed scheme with prior arts.

5.1 Experimental setting

To characterize natural images with both smooth and context areas, we deploy the discontinuity-adaptive potential function [AL-Shaykh and Mersereau (1998); Wang, Xiao, Peng et al. (2018)], i.e.

$$V_c(\mathrm{F}_1 \mid \mathrm{F}_2) = V_c(\mathrm{F}_2 \mid \mathrm{F}_1) = \log\left[\delta^2 + \left(\mathrm{F}_1 - \mathrm{F}_2\right)^2\right] + \frac{1}{\delta^2 + \left(\mathrm{F}_1 - \mathrm{F}_2\right)^2} - \log\delta^2 - \frac{1}{\delta^2} \tag{10}$$

where F_1 and F_2 are essentially a pair of elements in a clique of a given random field, and δ is a model parameter to control the sharpness of edges.

According to Eqs. (2)-(4) and (10), the concerned MRF has 3 parameters, i.e. δ, P, and T. As assessed in our previous work [Wang, Ni, Zhang et al. (2018)], the MRF parameters of $\delta = 45$ and $T = 0.00049$ are a preferable setting, and $\mathrm{P} = 0.35$ and $\mathrm{P} = 0.5$ are used for compression of encrypted binary images without and with doping, respectively. As each bit-plane of a gray image can be considered as a binary image, these MRF parameters in Wang et al. [Wang, Ni, Zhang et al. (2018)] are adopted in the reconstruction of each bit-plane.

Considering that the MRF between adjacent bitplanes may be different to that within a bitplane, we further seek a feasible setting for the MRF between adjacent bitplanes. In more detail, parameters δ and P are set as 45 and 0.5, respectively, and parameter T is decreased gradually from 1. Extensive experimental simulation shows that $T = 0.005$ is desirable for the MRF between $B^8(x,y)$ and $B^7(x,y)$ and $T = 0.05$ is feasible for the MRF between adjacent bitplanes from $B^7(x,y)$ to $B^5(x,y)$. The T for the MRF between other adjacent bitplanes, however, are intractable because bitplanes from $B^4(x,y)$ to $B^1(x,y)$ cannot be compressed, as demonstrated below. This universal parameter setting really works for all test gray images as it provides sufficient side information to guide the SPA towards convergence.

In the simulation, we test 10 100×100 gray images with diverse texture characteristics, as illustrated in Fig. 6. Each test gray image is encrypted, compressed, and reconstructed via

the algorithm in Section 4 (see also Fig. 5), and the lossless compression performance are assessed with compression rates in terms of bpb (bit per bit) and bit per pixel (bpp), where the bpb is used for each bitplane while the bpp is for a gray image. In compression stage, LDPC code rates, R, are set to be $[0.03, 0.95]$ with step 0.025, and the achieved minimum compression rate (MinCR) (see Eq. (9)) is taken as the compression rate (CR) for the involved bitplane, where the minimum doping rate dp_rate corresponding to a given R is sought via a binary search.

Each LDPC code is of length 10000, its degree distribution is obtained from the LTHC website [Amraoui and Urbanke (2003)], and the H_{new} in Eq. (8) is constructed via the PEG method [Hu, Eleftherious and Arnold (2005)].

5.2 Experimental results and analysis

Via the mentioned settings, we run the proposed algorithm on 10 test gray images. Table 1 summarizes lossless compression rates for 8 bitplanes of each test image. It is found that the first 3 MSBs of most test images can be successfully compressed while the other 5 bitplanes cannot. This is because bitplanes from $B^5(x, y)$ to $B^1(x, y)$ are nearly random (see also Fig. 1) and thus cannot be well characterized with the MRF, which in turn makes the compression and reconstruction of these bitplanes difficult. Nevertheless, bitplanes $B^5(x, y)$ of images "F16" and "Milkdrop" with a large portion of smooth area are two exceptions, which can be compressed by the proposed scheme.

Table 1: Compression rates (CRs) for 8 bitplanes of each gray image and their summary CRs (SCRs), where CR^k (k=8, ..., 1) denotes the CR for bitplane $B^k(x, y)$ in terms of bpb

Image	CR^8	CR^7	CR^6	CR^5	CR^4	CR^3	CR^2	CR^1	SCR
Barb	0.4113	0.5841	0.8284	1.0	1.0	1.0	1.0	1.0	6.8238
Couple	0.5505	0.6113	0.7947	1.0	1.0	1.0	1.0	1.0	6.9565
Elain	0.4559	0.6233	0.8988	1.0	1.0	1.0	1.0	1.0	6.9780
F16	0.3524	0.5957	0.6899	0.9355	1.0	1.0	1.0	1.0	6.6380
Goldhill	0.3514	0.5813	0.8634	1.0	1.0	1.0	1.0	1.0	6.7961
House	0.4240	0.6678	0.8802	1.0	1.0	1.0	1.0	1.0	6.9720
Man	0.3017	0.6225	0.9154	1.0	1.0	1.0	1.0	1.0	6.8396
Milkdrop	0.2747	0.5058	0.6494	0.7333	1.0	1.0	1.0	1.0	6.1632
Lena	0.3658	0.5614	0.7711	1.0	1.0	1.0	1.0	1.0	6.6983
Peppers	0.3842	0.5962	0.8144	1.0	1.0	1.0	1.0	1.0	6.7948


(a) Barb (b) Couple (c) Elain (d) F16 (e) Goldhill (f) House (g) Man (h) Milkdrop (i) Lena (j) Peppers

Figure 6: 10 test images of size 100×100

We further evaluate the proposed scheme by comparing it with the state of the arts [Schonberg (2006); Schonberg (2007); Liu, Zeng, Dong et al. (2010)] that also exploit statistical characteristics of natural images at the receiver. The work of Schonberg [Schonberg (2006, 2007)] incorporates the 2-D Markov source model in the reconstruction of binary image and successfully compresses the first 2 encrypted MSBs in a lossless way. Via a resolution-progressive manner, the approach of Liu et al. [Liu, Zeng, Dong et al. (2010)] uses low-resolution sub-images to learn source statistics for high-resolution ones, which can compress the first 4 encrypted MSBs. Regarding that the proposed scheme succeeds to compress the first 3 encrypted MSBs for most test gray images and the first 4 encrypted MSBs for a few test images with a large portion of smooth area (e.g. f16 and milkdrop), it achieves significant improvement in terms of compression efficiency against the method of Schonberg et al. [Schonberg, Draper and Ramchandran (2006); Schonberg (2007)], while it is comparable or somewhat inferior to the approach of Liu et al. [Liu, Zeng, Dong et al. (2010)]. The improvement over the method of Schonberg et al. [Schonberg, Draper and Ramchandran (2006); Schonberg (2007)] comes from the fact that the MRF is better than the 2-D Markov source model in characterizing natural gray images with complex intrinsic structure, while the weakness in comparison to the scheme of Liu et al. [Liu, Zeng, Dong et al. (2010)] attributes to the evidence that the first 4 or 5 encrypted LSBs are difficult to model with the MRF.

Table 2: Compression rates (CRs) and numerical results of $H_1(\mathrm{X})$ and $H_\infty(X)$ for the first 3 MSBs of each test gray image

Image	$B^8(x,y)$			$B^7(x,y)$			$B^6(x,y)$		
	CR^8	$H_1(\mathrm{x})$	$H_\infty(\mathrm{x})$	CR^7	$H_1(\mathrm{x})$	$H_\infty(\mathrm{x})$	CR^6	$H_1(\mathrm{x})$	$H_\infty(\mathrm{x})$
Barb	0.4113	0.9622	0.1599	0.5841	1.0000	0.3417	0.8284	1.0000	0.5730
Couple	0.5505	0.9994	0.2378	0.6113	0.8452	0.3600	0.7947	0.9516	0.5574
Elain	0.4559	0.9847	0.1714	0.6233	0.9999	0.3786	0.8988	0.9999	0.6157
F16	0.3524	0.6645	0.1665	0.5957	0.8278	0.4135	0.6899	0.8640	0.4892
Goldhill	0.3514	0.8664	0.1844	0.5813	0.9313	0.3426	0.8634	0.9889	0.6076
House	0.4240	0.7197	0.2193	0.6678	1.0000	0.4041	0.8802	0.9570	0.6236
Man	0.3017	0.9806	0.2432	0.6225	0.9706	0.4286	0.9154	0.9929	0.6677
Milkdrop	0.2747	0.7063	0.047	0.5058	0.8948	0.1814	0.6494	0.9675	0.3316
Lena	0.3658	0.9999	0.1768	0.5614	0.9878	0.3980	0.7711	1.0000	0.5443
Peppers	0.3842	1.0000	0.1405	0.5962	0.9979	0.3559	0.8144	0.9918	0.5643

In addition, we also examine the bound for compression of encrypted gray images. As compressing encrypted gray images is essentially equivalent to 8-bitplane compression, the bound for compression of encrypted binary images given in Wang et al. [Wang, Ni, Zhang et al. (2018)] can be taken for analysis here. As discussed in Wang et al. [Wang, Ni, Zhang et al. (2018)], the compression bound is equal to the entropy rate of the adopted MRF source, says $H_\infty(X)$, the derivation for which is omitted her for space limitation and recommended to refer to Wang et al. [Wang, Ni, Zhang et al. (2018)]. For convenience, the entropy rate of independent identically distributed (i.i.d.) source,

namely $H_1(\mathrm{X})$, is also compared. Tab. 2 lists compression rates, $H_1(\mathrm{X})$ and $H_\infty(X)$, for the first 3 MSBs of each test gray image, where results for the 4th MSB are not given as the 4th MSB of most test images cannot be compressed. It is observed that compression rates for the first 3 MSBs are far lower than $H_1(\mathrm{X})$ due to the exploitation of the MRF in the reconstruction process, while there still exist sizeable gaps from the bound $H_\infty(X)$ for the proposed scheme to improve.

6 Conclusion

In this paper, we have presented a new ETC scheme for gray images using the MRF. We deployed the MRF to characterize statistical correlations between adjacent bitplanes and within a bitplane, represented them with factor graphs, and further seamlessly integrated the built MRF factor graphs in those for decryption and LDPC decoding, yielding a JFGIR (joint factor graph for gray image reconstruction). The SPA adapted to the JFGIR is then derived theoretically by applying the theory of factor graph. Via the constructed JFGIR and the derived SPA, an MRF-based scheme for compression of encrypted gray images is thus developed, which uses the stream cipher to encrypt each bitplane, employs the LDPC code to compresses each bitplane, and exploits the JFGIR to facilitate inferring the original bitplane. Numerical results show that a universal MRF parameter setting works well for all gray images as the setting provides sufficient side information to guide the SPA towards convergence. Extensive experimental simulation demonstrates that the proposed scheme successfully compresses the first 3 and 4 MSBs for most test gray images and a few test images with a large portion of smooth area, respectively, which achieves significant improvement in terms of compression efficiency over the prior state-of-the-art using the 2-D Markov source model while is comparable or somewhat inferior to that adopting the resolution-progressive strategy.

Acknowledgement: This work is supported in part by the National Natural Science Foundation of China under contracts 61672242 and 61702199, in part by China Spark Program under Grant 2015GA780002, in part by The National Key Research and Development Program of China under Grant 2017YFD0701601, and in part by Natural Science Foundation of Guangdong Province under Grant 2015A030313413.

References

AL-Shaykh, O. K.; Mersereau, R. M. (1998): Lossy compression of noisy images. *IEEE Transactions on Image Processing*, vol. 7, no. 12, pp. 1641-1652.

Amraoui, A.; Urbanke, R. (2003): Ldpcopt. http://lthcwww.epfl.ch/research/ldpcopt/.

Donoho, D. L. (2006): Compressed sensing. *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289-1306.

Erkin, Z.; Piva, A.; Katzenbeisser, S.; Lagendijk, R. L.; Shokrollahi, J. et al. (2007): Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing. *EURASIP Journal on Information Security*, vol. 2007, no. 1, pp. 1-20.

Pradhan, S. S.; Ramchandran, K. (2003): Distributed source coding using syndromes

(DISCUS): Design and construction. *IEEE Transactions on Information Theory*, vol. 49, no. 3, pp. 626-664.

Hu, R.; Li, X.; Yang, B. (2014): A new lossy compression scheme for encrypted gray-scale images. *IEEE International Conference on Acoustic, Speech and Signal Processing*, pp. 7387-7390.

Hu, X. Y.; Eleftherious, E.; Arnold, D. M. (2005): Regular and irregular progressive edge-growth tanner graphs. *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 386-398.

Johnson, M.; Ishwar, P.; Prabhakaran, V. M.; Schonberg, D.; Ramchandran, K. (2004): On compressing encrypted data. *IEEE Transactions on Signal Processing*, vol. 52, no. 10, pp. 2992-3006.

Kang, X.; Peng, A.; Xu, X.; Cao, X. (2013): Performing scalable lossy compression on pixel encrypted images. *EURASIP Journal on Image and Video Processing*, vol. 2013, no. 1, pp. 1-6.

Kschischang, F. R.; Frey, B. J.; Loeliger, H. A. (2001): Factor graphs and the sum-product algorithms. *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 498-519.

Kumar, A.; Makur, A. (2008): Distributed source coding based encryption and lossless compression of gray scale and color images. *IEEE 10th Workshop on Multimedia Signal Processing*, pp. 760-764.

Kumar, A.; Makur, A. (2009): Lossy compression of encrypted image by compressing sensing technique. *Tencon IEEE Region 10 Conference*, pp. 1-6.

Kumar, M.; Vaish, A. (2017): An efficient encryption-then-compression technique for encrypted images using SVD. *Digital Signal Processing*, vol. 60, pp. 81-80.

Lazzeretti, R.; Barni, M. (2008): Lossless compression of encrypted grey-level and color images. *European Signal Processing Conference*, pp. 1-5.

Li, S. (1995): *Markov Random Field Modeling in Computer Vision*. Springer-Verlag.

Liu, W.; Zeng, W.; Dong, L.; Yao, Q. (2010): Efficient compression of encrypted grayscale images. *IEEE Transactions on Signal Process*, vol. 19, no. 4, pp. 1097-1102.

Schonberg, D. H. (2007): *Practical Distributed Source Coding and its Application to the Compression of Encrypted Data (Ph.D. Thesis).* University of California at Berkeley, USA.

Schonberg, D.; Draper, S. C.; Ramchandran, K. (2005): On blind compression of encrypted correlated data approaching the source entropy rate. *43rd Annual Allerton Conference on Communication, Control, and Computing*, pp. 1-3.

Schonberg, D.; Draper, S. C.; Ramchandran, K. (2006): On compression of encrypted images. *IEEE Conference on Image Process*, pp. 269-272.

Schonberg, D.; Draper, S. C.; Yeo, C.; Ramchandran, K. (2008): Toward compression of encrypted images and video sequences. *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 4, pp. 749-762.

Song, C.; Lin, X.; Shen, X. (2013): Secure and effective image storage for cloud based E-healthcare systems. *IEEE Global Communications Conference*, pp. 653-658.

Wang, C.; Ni, J. (2015): Compressing encrypted images using the lifting scheme. *IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 409-412.

Wang, C.; Ni, J.; Huang, Q. (2015): A new encryption-then-compression algorithm using the rate-distortion optimization. *Signal Processing: Image Communication*, vol. 39 (Part A), pp. 141-150.

Wang, C.; Ni, J.; Zhang, X.; Huang, Q. (2018): Efficient compression of encrypted binary images using the Markov random field. *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1271-1285.

Wang, C.; Xiao, D.; Peng, H.; Zhang, R. (2018): A lossy compression scheme for encrypted images exploiting Cauchy distribution and weighted rate distortion optimization. *Journal of Visual Communication and Image Representation*, vol. 51, no. 2018, pp. 122-130.

Zhang, X. (2011): Lossy compression and iterative reconstruction for encrypted image. *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 53-58.

Zhang, X.; Feng, G.; Ren, Y.; Qian, Z. (2012): Scalable coding of encrypted images. *IEEE Transactions on Image Process*, vol. 21, no. 6, pp. 3108-3114.

Zhang, X.; Ren, Y.; Feng, G.; Qian, Z. (2011): Compressing encrypted image using compressive sensing. *IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 222-225.

Zhang, X.; Ren, Y.; Shen, L.; Qian, Z.; Feng, G. (2014): Compressing encrypted images with auxiliary information. *IEEE Transactions on Multimedia*, vol. 16, no. 5, pp. 1327-1336.

Zhang, X.; Sun, G.; Shen, L.; Qin, C. (2013): Compression of encrypted images with multilayer decomposition. *Multimedia Tools Application*, vol. 78, no. 3, pp. 11-13.

Zhang, Y.; Wong, K. W.; Zhang, L. Y.; Wen, W.; Zhoud, J. et al. (2015): Robust coding of encrypted images via structural matrix. *Signal Processing: Image Communication*, vol. 39 (Part-A), pp. 202-211.

Zhou, J.; Au, O.; Zhai, X. G.; Tang, Y.; Liu, X. (2014): Scalable compression of stream cipher encrypted images through context-adaptive sampling. *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 1, pp. 39-50.

Zhou, J.; Liu, X.; Au, O.; Tang, Y. (2014): Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation. *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 1, pp. 39-50.