Signal Processing 133 (2017) 135–143

Contents lists available at ScienceDirect

Signal Processing

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

A separable reversible data hiding scheme for encrypted JPEG bitstreams

Jen-Chun Chang, Yi-Zhi Lu, Hsin-Lung Wu*

Department of Computer Science and Information Engineering, National Taipei University, New Taipei City, Taiwan

ARTICLE INFO

Keywords:
MSC: Encrypted image
Reversible data hiding
JPEG
Separability

ABSTRACT

In this paper, we construct a separable reversible data hiding scheme for encrypted JPEG bitstreams. Our proposed scheme is constructed via a reserving-room-before-encryption manner, that is, the original JPEG bitstream is modified with small distortion so that the content owner can reserve enough space for future data embedding and then the modified JPEG bitstream is encrypted. To do that, our key observation is that the least significant bits of the two-bit appended values in the JPEG bitstream is a biased bitstream. Thus we design a new lossless compression algorithm for biased bitstreams with better compression ratio than the binary arithmetic coding method to fulfill the above task for pre-reserving space. With this room-reserving technique, the encrypted JPEG bitstream can be generated and the data embedding in this encrypted bitstream can be done easily by the data hider. Finally, the receiver is able to extract the embedded data and recovers the original JPEG bitstream independently.

1. Introduction

Reversible data hiding is a technique which can embed a secret data string into an image such that, from the watermarked image, one can losslessly recover the original image after the whole embedded secret string is extracted. This important technique has found many applications in the area of medical image processing, military imagery, and law forensics where it is required to reconstruct the original image without any distortion. Many reversible data hiding schemes have been proposed in recent years. One of the popular methods is difference-expansion (DE) method developed by Tian [23] in which the difference between two neighboring pixels is expanded in order to embed a message bit. In order to increase the embedding capacity, many improved DE-based reversible data hiding schemes are proposed such as [7,5] in recent years. Another popular approach is histogram-modification (HM) method in which the histogram of pixel values of the host image is utilized by using the uneven distribution of the pixel values in an image. In [27], Vleeschouwer et al. realized a reversible data hiding scheme by rotating the histogram of the input image according to a particular circular mapping. In [16], Ni et al. proposed a typical HM method which utilizes the zero and peak points of the histogram of the host image and shifts the pixel values to embed data bits into the host image. Recently some techniques are developed to improve embedding capacity such as techniques based on prediction-error expansion (PEE) [24,20,13,9,17,3,14] and the technique based on the optimal value transfer matrix [31].

In general, these mentioned reversible data hiding techniques are designed for embedding data bits into those images which are open to the data hiders. However, in some applications, the image owner does not allow the data hider to know the sensitive content of the original image. Let us consider the following application scenario. A processing service provider can help an image owner to losslessly embed some additional message such as image authentication or image notation. However, the image owner distrusts the processing service provider and asks that the processing service provider should not access the content of the original image directly. One of popular and effective ways for the image owner is to encrypt the image before sending the service provider. Thus, in order to resolve the above situation, the service provider should develop a reversible data hiding scheme for encrypted images.

In recent years, some schemes attempting to obtain reversible data hiding in encrypted images are proposed [29,4,30,15,28,2,32,11,1,18]. In general, these schemes can be divided into three categories of reversible data hiding methods for encrypted images, that is, methods by vacating room after encrypting images (VRAE) [29,4,30,11,18], methods by reserving room before encrypting images (RRBE) [15,32,1], and methods based on homomorphic encryption [2]. These methods are reversible data hiding schemes for encrypted *uncompressed* images and they cannot be directly applied to compressed images such as JPEG images. Since JPEG is a commonly used method of lossy compression for digital images, we study the reversible data hiding for encrypted JPEG bitstreams in this paper. More recently, Qian et al. [19] proposed the first reversible data hiding scheme for encrypted JPEG bitstreams. Their scheme uses an error-correcting

* Corresponding author.
E-mail address: hsinlung@mail.ntpu.edu.tw (H.-L. Wu).

http://dx.doi.org/10.1016/j.sigpro.2016.11.003
Received 15 July 2016; Received in revised form 19 October 2016; Accepted 2 November 2016
Available online 06 November 2016
0165-1684/

code to encode the secret message such that the secret data can be extracted by utilizing a block-artifact technique after decrypting the marked encrypted JPEG bitstream. However the data extraction depends on the encryption in their scheme. Thus their scheme is not a separable scheme.

In this paper, we propose a novel separable reversible data hiding scheme for encrypted JPEG bitstreams. Our scheme is designed via a reserving-room-before-encryption manner previously used in [15]. In our scheme, a part of the original JPEG bitstream is compressed first in order to reserving space for embedding the secret message before encryption. As the scheme proposed by Ma et al. [15], the data extraction and decryption in our proposed scheme can be done independently. So the separable scheme for encrypted JPEG bitstreams is obtained. Moreover, the experimental result shows that the marked decrypted JPEG bitstreams constructed by our proposed scheme have good performance on image quality and embedding capacity.

The rest of this paper is organized as follows. In Section 2, we review some recent works on reversible data hiding in encrypted domains. In Section 3, we propose a lossless compression for biased bitstreams. Then, in Section 4, we propose our separable reversible data hiding scheme for encrypted JPEG bitstreams. Experimental results are given in Section 5. Finally, the conclusion is given in Section 6.

2. Previous works on reversible data hiding in encrypted domains

2.1. Non-compressed domain

In [29], Zhang presented a scheme which partitions the encrypted image into blocks first and then flips the last three least significant bits of the half of pixels in each block according to the embedded bit. The data extraction and image restoration are carried out by determining which part of the block has been flipped. Zhang showed that the scheme can be realized by estimating the spatial correlation in decrypted image. Hong et al. [4] decreased the error rate of the decoding algorithm of Zhang's scheme by using a new estimation equation and a side match technique. To improve the performance of [29,4], Liao and Shu proposed a data hiding scheme by evaluating the complexity of image blocks which considers multiple neighboring pixels according to the locations of different pixels [11]. In [28], Wu and Sun proposed a scheme based on prediction error and showed that the decoding algorithm can be realized by estimating the prediction errors in decrypted image. Note that the schemes mentioned above heavily depend on spatial correlation of the original image to extract embedded data bits. This requires that the marked encrypted images should be decrypted first before extracting data bits. However, if the embedded data is used for image authentication, this will result in a problem. In some situation, the image owner may ask the processing service provider to retrieve the authentication data without giving the encryption key. In this case, the processing service provider is not able to fulfill the task. Thus, it is natural to separate the data extraction from image decryption. In [30], Zhang used the idea of compressing encrypted images [6,12] to design the first separable reversible data hiding scheme for encrypted images. His method, using a random parity check matrix, compresses the encrypted least significant bits to vacate space for accommodating additional data. In [28], Wu and Sun also proposed a separable data hiding scheme for encrypted images by adopting prediction errors. In [18], Qin and Zhang proposed a reversible data hiding scheme which improves the performances of the mentioned schemes. Their scheme flips the least significant bits of partial pixels by the elaborate selection and obtains a significant improvement for the image quality of marked decrypted image. In addition, the authors used a new adaptive judging function based on the distribution characteristic of image local contents to implement the data extraction and image recovery.

Unlike the approach that vacates room of data embedding after image encryption (VRAE-approach), in [15], Ma et al. suggested another approach that reserves room of data embedding before image encryption (RRBE-approach). In [15], Ma et al. proposed a separable scheme which empties out space by embedding least significant bits of some chosen pixels into other pixels with a known reversible data hiding scheme and then encrypts this space-prereserved image. As a result, in this encrypted space-prereserved image, the least significant bits of those chosen pixels can be used for data embedding by the data hider. In [32], Zhang et al. considered the two highest bins of the histogram of prediction errors of randomly selected pixels. Prediction errors in these two highest bins are not encrypted and then the corresponding pixel values of these locations is not encrypted. Now, by using the histogram-shifting technique, one can embed data bits into these prediction errors of the first two highest frequencies. In [1], Cao et al. proposed a patch-based data hiding scheme for encrypted images. Their scheme uses the sparse coding technique to losslessly compress each image patch in order to reserve large room for embedding data.

In [2], based on public key cryptosystem and homomorphic encryption, Chen et al. constructed a reversible data hiding scheme for encrypted images. In their scheme, each 8-bit pixel value is separated into two groups, that is, seven most significant bits and the least significant bit. Then these two groups are encrypted respectively. Next, the scheme losslessly embeds one bit by modifying two least-significant bits of each encrypted pixel pair according to properties of homomorphism. In the receiver's side, the embedded bit can be easily extracted and the original image can be recovered by detecting the relationship of two decrypted least significant bits in each pixel pair.

2.2. The JPEG compressed domain

In [19], Qian et al. proposed the first reversible data hiding scheme for encrypted JPEG bitstreams. In their scheme, the encrypted JPEG bitstream is obtained by encrypting the quantization table and appended bits of the original JPEG bitstream. To embed a secret message into the encrypted JPEG bitstream, the message is encoded by an error-correcting code first. Then, the i-th encoded message bit is embedded into the i-th usable block by performing XOR operations on the last bit of each appended bit with the i-th encoded message bit. To extract the secret message, the marked encrypted JPEG bitstream should be decrypted first. To extract the embedded message bit in the usable block, Qian et al. defined a blocking artifact function (BAF) which evaluates the usable block by correlating its neighboring unusable blocks and used it to predict the corresponding embedded bit. The authors showed that the predicted bit is equal to the real embedded bit with high probability and then one obtains an approximated binary string which is closed to the encoded message in the sense of Hamming distance. Finally the message is decoded from the approximated binary string by using the error-correcting procedure and the original JPEG bitstream is also recovered.

3. An efficient lossless compression for biased bitstreams

A biased bitstream is defined as follows.

Definition 1. For $p \in [0, 1/2]$, we say a bitstream $s \in \{0, 1\}^n$ is p-biased if the fraction of ones is either smaller than p or greater than $1 - p$.

In this section, we propose an efficient algorithm which losslessly compresses a p-biased bitstream s where p is a positive constant less than $1/2$. There are many known lossless compression algorithms for bitstreams such as the well-known binary arithmetic coding [8] which is the most popular compression algorithm for bitstreams. In order to gain more space for embedding data bits, we propose a lossless compression algorithm which has better performance on compressed