Signal Processing 123 (2016) 9–21

Contents lists available at ScienceDirect

Signal Processing

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

Separable and error-free reversible data hiding in encrypted images

Dawen Xu [a,*], Rangding Wang [b]

[a] School of Electronics and Information Engineering, Ningbo University of Technology, Ningbo 315016, China
[b] CKC Software Lab, Ningbo University, Ningbo 315211, China

ARTICLE INFO

Article history:
Received 6 July 2015
Received in revised form
23 October 2015
Accepted 16 December 2015
Available online 3 January 2016

Keywords:
Image encryption
Reversible data hiding
Privacy protection
Histogram shifting
Difference expansion

ABSTRACT

Digital image sometimes needs to be stored and processed in an encrypted format to maintain security and privacy, e.g., cloud storage and cloud computing. For the purpose of content notation and/or tampering detection, the cloud servers need to embed some additional information directly in these encrypted images. As an emerging technology, reversible data hiding in the encrypted domain will be useful in cloud computing due to its ability to preserve the confidentiality. In this paper, a novel separable and error-free reversible data hiding scheme in encrypted images is proposed. After analyzing the property of interpolation technology, a stream cipher is utilized to encrypt sample pixels and a specific encryption mode is designed to encrypt interpolation-error of non-sample pixels. Then, the data-hider, who does not know the original image content, may reversibly embed secret data into interpolation-error using a modified version of histogram shifting and difference expansion technique. In order to adapt to different application scenarios, data extraction can be done either in the encrypted domain or in the decrypted domain. In addition, real reversibility is realized, that is, data extraction and image recovery are free of any error. Experimental results demonstrate the feasibility and efficiency of the proposed scheme.

1. Introduction

With the rapid developments occurring in mobile internet and cloud storage, privacy and security of personal data has gained significant attention nowadays. There are no guarantees that stored data will not be accessed by unauthorized entities, such as the cloud provider itself or malicious attackers. Several recent surveys also show that 88% potential cloud consumers are worried about the privacy of their data [1]. Under this specific circumstance, multimedia data are often encrypted to ensure confidentiality in communication and storage processes as well as to protect privacy. In other words, the consumers would like to give the untrusted cloud server only an encrypted version of the data. The cloud service provider (who stores the data) is not authorized to access the original content (i.e., plaintext). However, in many scenarios, the cloud servers or database managers need to embed some additional messages, such as labeling or authentication data, origin information, and owner identity information, directly into an encrypted data for tamper detection or ownership declaration or copyright management purposes. For example, patient's information can be embedded into his/her encrypted medical image to avoid unwanted exposure of confidential information.

The capability of performing data hiding directly in encrypted images would avoid the leakage of image content, which can help address the security and privacy concerns with cloud computing. In [2], a novel technique is

* Corresponding author. Tel.: +86 13736187949; fax: +86 574 87600352.
E-mail address: dawenxu@126.com (D. Xu).

http://dx.doi.org/10.1016/j.sigpro.2015.12.012
0165-1684/

proposed to embed a robust watermark in the compressed and encrypted JPEG2000 images using three different existing watermarking schemes. A Walsh–Hadamard transform based image watermarking algorithm in the encrypted domain using Paillier cryptosystem is presented in [3]. However, due to the constraints of the Paillier cryptosystem, the encryption of an original image results in a high overhead in storage and computation. Karim and Wong [4] proposed a universal reversible data embedding method in the encrypted domain, in which the coding redundancy is exploited by entropy coding the encrypted signal and the resulting codewords are modified for data embedding purposes. More recently, a novel unified data embedding-scrambling technique is proposed to achieve high payload and adaptive scalable quality degradation [5]. Data hiding in the encrypted version of H.264/AVC video stream is proposed in [6], intra-prediction modes, motion vector differences, and residual coefficients are encrypted with stream ciphers. Then, a data-hider may embed additional data in the encrypted domain by using codeword substituting technique. However, within the aforementioned schemes [2–6], the host image/video is permanently distorted caused by data embedding. In general, the cloud service provider has no right to introduce permanent distortion during data embedding in encrypted data. This implies that, for a legal receiver, the original plaintext content should be recovered without any error after image decryption and data extraction. To solve this problem, reversible data hiding (RDH) in encrypted domain is preferred.

For the last few years, RDH is gaining popularity because of its increasing applications in some important and sensitive areas, i.e., military communication, medical diagnosis, and law-enforcement. Up till now, quite interesting researches, e.g., compression based [7,8], histogram modification based [9,10], difference expansion based [11,12], have been carried out in the field of RDH. For more details of these methods and other RDH methods, refer to the latest review of recent research [13]. Although RDH techniques have been studied extensively, these techniques are suitable for unencrypted covers rather than encrypted covers. Nowadays, RDH in encrypted domain has emerged as a new and challenging research field. In [14], Zhang divided the encrypted image into blocks, and each block carries one bit by flipping 3 Least Significant Bits (LSB) of each encrypted pixel in a set. Hong et al. [15] improved Zhang's method by adopting new smooth evaluation function and side-match mechanism to decrease the error rate of extracted bits. In both [14,15], data extraction and image recovery is achieved by using the spatial correlation in the decrypted image. Therefore, the encrypted image containing hidden data should be first decrypted before data extraction, which remains a major limitation to practical application. Similarly, Qian et al. [16] proposed a framework of RDH in an encrypted JPEG bitstream. To separate data extraction from image decryption, the method in [17] compressed the LSB of encrypted pixels to create a space for accommodating the additional data. Recently, Zhang et al. [18] further proposed an improved scheme, in which a part of encrypted data is losslessly compressed using Low Density Parity Check (LDPC) code and used to carry the compressed data as well as the additional data. In summary, the embedding capacity of these methods [14–18] is relatively small and some errors occur during data extraction and/or image recovery. In order to achieve real reversibility, two major methods of reserving room before encryption (RRBE) are proposed [19,20]. Ma et al. [19] provided a RDH idea in encrypted images by reserving room before encryption. This method first empties out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypts the image, so the positions of these LSBs in the encrypted image can be used for data hiding. Although the embedding capacity of this method is greatly improved, an additional RDH has to be implemented by the sender. Zhang et al. [20] proposed a reversibility improved RDH method in encrypted images. Prior to encrypting the image, room for data hiding is vacated by shifting the histogram of estimating errors. More recently, Cao et al. [21] proposed a method for high capacity separable reversible data hiding in encrypted images, which inherits the merits of RRBE based on patch level sparse representation. As can be seen from the foregoing analysis, many exploratory studies are currently ongoing to improve the overall performance. But there is still much room for improvement, especially in capacity and reversibility.

Different from above schemes, in our recent paper [22], a novel scheme of reversible data hiding in encrypted images based on interpolation technique is proposed. Before encryption and data embedding, an interpolation technique is adopted to generate interpolation-error. Sample pixels, which are sampled to form the low-resolution image, are encrypted using a standard stream cipher. The additional data can be embedded in the encrypted image by modifying the histogram of interpolation-error. In contrast to the existing technologies [14–18] discussed above, our scheme in [22] can achieve excellent performance in the following prospects.

- It can achieve complete reversibility, i.e., no errors occur in data extraction and image recovery.
- It can be applied to two different application scenarios by extracting the hidden data either from the encrypted image or from the decrypted image.

The main limitation of this scheme is that it has a relatively low level of security, since only sample pixels are encrypted and interpolation-errors are not encrypted. In this paper, we develop a more secure and reliable framework for reversible data hiding in encrypted domain. Compared with our preliminary paper [22], the new contribution of this paper is the utilization of specific encryption for interpolation-error. In addition, a more flexible embedding mechanism is adopted, which is more suitable for practical issues with different capacity requirements.

The rest of the paper is organized as follows. In Section 2, we describe the proposed scheme, which includes image encryption, data embedding in encrypted image, data extraction and original image recovery. Experimental results and analysis are presented in Section 3. Finally in Section 4, conclusion and future work are drawn.