An Efficient Reversible Data Hiding Scheme for Encrypted Images

Kai Chen, School of Electronics and Information Engineering, Ningbo University of Technology, Ningbo, China
Dawen Xu, School of Electronics and Information Engineering, Ningbo University of Technology, Ningbo, China

ABSTRACT

Reversible data hiding in the encrypted domain is an emerging technology, as it can preserve the confidentiality. In this article, an efficient method of reversible data hiding in encrypted images is proposed. The cover image is first partitioned into non-overlapping blocks. A specific modulo addition operation and block-scrambling operation are applied to obtain the encrypted image. The data-hider, who does not know the original image content, may reversibly embed secret data based on the homomorphic property of the cryptosystem. A scale factor is utilized for selecting embedding zone, which is scalable for different capacity requirements. At the receiving end, the additional data can be extracted if the receiver has the data-hiding key only. If the receiver has the encryption key only, he/she can recover the original image approximately. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error. Experimental results demonstrate the feasibility and efficiency of the proposed scheme.

KEYWORDS

Histogram Shifting, Homomorphic Property, Image Encryption, Privacy Protection, Reversible Data Hiding

1. INTRODUCTION

With the rapid developments occurring in mobile internet and cloud storage, privacy and security of personal data has gained significant attention nowadays. The cloud service provider or malicious attackers may access users’ sensitive information without authorization. A general approach to protect the data confidentiality is to encrypt the data before outsourcing (Xia, X. H. Wang, Sun, & Q. Wang, 2016; Xia et al., 2016). However, in some application scenarios, the cloud service provider or database manager needs to embed some additional messages, e.g., authentication or notation data, directly into an encrypted data for tamper detection or ownership declaration purposes. For example, patient’s information can be embedded into his/her encrypted medical image to avoid unwanted exposure of confidential information.

As a trend, the research on data hiding in the encrypted domain has gained increasing attention, which is primarily driven by the needs from the third-party computing platforms (e.g., cloud computing). Over the past few years, a considerable amount of schemes about data hiding in encrypted images or videos have been reported in the literature (Subramanyam, Emmanuel, & Kankanhalli, 2012; Xu, Wang, & Shi, 2014; Xu & Wang, 2015; Guo, Zheng, & Huang, 2015; Parah, Sheikh, Hafiz, & Bhat, 2014; Xu, Wang, Shi, & 2016; Xu, Wang, & Zhu, 2017). However, within these schemes, the cover medium has been distorted during the data embedding operation and cannot be restored into its original form after data extraction. In some sensitive scenarios, such permanent distortion is strictly forbidden. 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 the encrypted domain is preferred.

RDH is a technique that slightly alters digital media (e.g., images or videos) to embed secret data while the original digital media can be recovered without any error after the hidden messages have been extracted (Shi, Li, Zhang, Wu, & Ma, 2016). This specific data hiding technique has been found to be useful in some important and sensitive areas, i.e., military communication, medical science, law-enforcement, and error concealment (Xu, Wang, Shi, 2014; Xu & Wang, 2016). Three major approaches, i.e., lossless compression (Fridrich, Goljan, Du, & R, 2002), histogram modification (Ni, Shi, Ansari, & Su, 2006; X. L. Li, B. Li, Yang, & Zeng, 2013), difference expansion (Tian, 2003; Li, Yang, & Zeng, 2011), have already been developed for RDH. For more details of these methods and other RDH methods, refer to the latest review of recent research (Shi, Li, Zhang, Wu, & Ma, 2016).

Although RDH techniques have been studied extensively, RDH in the encrypted domain has emerged as a new and challenging research field. In recent years, several RDH methods for encrypted images have been proposed. In general, these methods can be divided into three categories, that is, methods by vacating room after encryption (VRAE) (Zhang, 2011; Hong, Chen, & Wu, 2012; Qin & Zhang, 2015; Zhang, 2012; Qian & Zhang, 2016; Zhou et al., 2016; F.J. Huang, J.W. Huang, & Shi, 2016), methods by reserving room before encryption (RRBE) (Ma et al., 2013; Zhang, Ma, & Yu, 2014; Cao, Du, Wei, Meng, & Guo, 2016; Xu & Wang, 2016), and methods based on homomorphic encryption (Chen, Shiu, & Horng, 2014; Shiu, Chen, & Hong, 2015; Zhang, Long, Wang, & Cheng, 2016; Wu, Cheung, & Huang, 2016; Li, Xiao, Zhang, & Nan, 2015; Xu, Chen, Wang, & Su, 2016). In VRAE framework, the original signal is encrypted directly by the content owner, and the data-hider embeds the additional bits by modifying some bits of the encrypted data. The advantage of this framework is that the operation of end user is simple and efficient. However, as the entropy of an encrypted image has been maximized, the embedding capacity is limited. Moreover, the accuracy of data extraction and the quality of restored image are not satisfactory. RRBE framework creates an embedding room in the plaintext domain, i.e., vacating room before encryption. The advantages of this framework are mainly reflected in two aspects, namely embedding capacity is relatively large and pure reversibility is achieved. But, this framework might be impractical because it requires the content owner to perform an extra preprocessing before content encryption. In general, the content owner expects to send only an encrypted image to the manager without extra information. In addition to VRAE and RRBE, another type of method has recently been proposed by using homomorphic encryption. With the additive homomorphic property of Paillier cryptosystem, Chen et al. (2014) firstly proposed a homomorphic encryption based RDH approach. Shiu et al. (2015) improved Chen et al.'s method (2014) by adopting the concept of difference expansion into homomorphic encryption. Moreover, RDH in the homomorphic encrypted domain has also been investigated in (Zhang, Long, Wang, & Cheng, 2016; Wu, Cheung, & Huang, 2016). However, the used public-key cryptosystems such as Paillier cryptosystem lead to data expansion after image encryption. In (Li, Xiao, Zhang, & Nan, 2015; Xu, Chen, Wang, & Su, 2016), the additive homomorphic property of modulo operation is utilized to realize the RDH in the encrypted domain. The advantage is that encryption does not cause data expansion.

In this paper, we develop a more effective and reliable framework for RDH in the encrypted domain. Compared with our preliminary paper (Xu, Chen, Wang, & Su, 2016), the new contribution of this paper is the utilization of a scale factor for embedding zone selection, which is scalable for different capacity requirements. The scalable feature is much more flexible and convenient for meeting the various requirements of practical applications. In addition, the proposed scheme can also achieve excellent performance in the following four aspects. First of all, room for data hiding does not need to be vacated before encryption, which is more reasonable compared with the methods in (Ma et al., 2013; Zhang, Ma, & Yu, 2014; Cao, Du, Wei, Meng, & Guo, 2016; Xu & Wang, 2016). Secondly, completely reversible can be achieved, which is more reliable than the methods in (Zhang, 2011; Hong, Chen, & Wu, 2012; Qin & Zhang, 2015; Zhang, 2012). Thirdly, the modular addition operation,
On the Reliability of Cryptopometry
[www.igi-global.com/article/on-the-reliability-of-cryptopometry/79139?camid=4v1a](www.igi-global.com/article/on-the-reliability-of-cryptopometry/79139?camid=4v1a)