International Journal of Digital Crime and Forensics
Volume 11 • Issue 1 • January-March 2019

Reversible Data Hiding with Multiple Data for Multiple Users in an Encrypted Image

Asad Malik, School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China

Hongxia Wang, School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China

Hanzhou Wu, Institute of Automation, Chinese Academy of Sciences (CAS), Beijing, China & State Key Laboratory of Cryptology, Beijing, China

Sani M. Abdullahi, School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China

ABSTRACT

This article presents a new method which embeds multiple data from multiple users in an encrypted image. Here, the data from several users is embedded into an encrypted image. Initially, the image is encrypted by the owner followed by embedding phase, where the encrypted image is divided into four sets. Two of them are used to embed the secret data, while others are remain unaltered. The secret data from multiple users are embedded into Most Significant Bit (MSB) of the encrypted image using their location maps. In the extraction phase, an individual owner can extract the data from the encrypted image using the assigned private key. Subsequently, in the image decryption and recovery phase, images can be recovered using the unaltered neighbor pixels. However, the secret image can be recovered losslessly using the encryption key only. The proposed scheme allows the extraction of the embedded information only for the authorized user out of several users without knowing the cover information. Various simulations have been made related to this, which show the high embedding rate and accuracy.

KEYWORDS

Cloud Computing, Encrypted Image, Image Recovery, Prediction, Reversible Data Hiding

1. INTRODUCTION

Reversible Data Hiding (RDH) is known as lossless and it is a scheme which is the key element in many applications in the field of secret communication, copyright protection and content authentication of digital multimedia (Barni, Bartolini, Cox, Hernandez, & Perez-Gonzalez, 2001; Tian, Zhao, Ni, Qin, & Li 2013). Reversibility of such scheme means losslessly reconstructing the original image as well as recovering the secret embedded information from the cover media.

Primarily reversible data hiding scheme has been proposed by Barton (1997). After that many other RDH schemes have been proposed and those can be find in the open literature. Mainly these schemes are classified into the following three categories such as lossless compression (Fridrich,

DOI: 10.4018/IJDCF.2019010104

Goljan, & Du, 2001; Celik, Sharma, Tekalp, & Saber, 2005), Difference Expansion (DE) (Tian, 2003; Hu, Lee, & Li, 2009) and Histogram Shifting (HS) (Ni, Shi, Ansari, & Su, 2006; Xuan, Yao, Yang, Gao, Chai, Shi, & Ni, 2006). Lossless compression means to compress the original media losslessly and make the space to embed additional information into it, which can be subsequently recovered losslessly after extraction of embedded data. DE-based embedding idea was initially proposed by Tian (2003) having higher hiding capacity but with a disadvantage as it degrades the quality of recovered image to a large extent. Improvement in the hiding capacity and quality of stego-image can be seen in many successive schemes. Later, several improved techniques for DE-based embedding have come into existence. They include prediction, sorting (Kamstra, & Heijmans, 2005; Sachnev, Kim, Nam, Suresh, & Shi, 2009) and location map reduction (Hu, Lee, & Li, 2009). HS-based scheme was initially proposed by Ni (Ni, Shi, Ansari, & Su, 2006) and proposed the algorithm by them is simpler than DE approach and requires less computation than most of other algorithms. Histogram shifting method uses peak and zero (or maximum and minimum) bins in the histogram of the input image pixel values and then, make the room for data hiding by shifting the bin intensities from peak to zero points. And hiding information has been done by modifying the pixels assuming the peak value. Moreover, HS provides a high visual quality and maintains a high Peak Signal-to-Noise Ratio (PSNR). However, the capacity that Ni's algorithm can provide might not be sufficient for most applications, so many scholars have studied and tried to improve Ni's algorithm. Intensities between the maximum points to raise the hiding capacity is used by (Hwang, Kim, & Choi, 2006), but the threshold of embedding capacity is not sufficient for hiding. Chung, Huang, Yang, Hsu, & Chen (2009) come out with a method used in dynamic programming procedure to maximize histogram shifting to improve the hiding capacity. His method increases capacity indeed, but it has two main drawbacks. It is suitable only for specific types of images. Further it needs much execution time which depends on pair of pixels and zero bins in histogram.

However, Reversible Data Hiding in Encrypted Domain (RDH-ED) is also much popular for secret communication and it has a wide application in cloud computing (Shi, Li, Zhang, Wu, & Ma, 2016). In this technique content owner encrypts the cover media before sending the cover information to the cloud. The cloud owner without knowing original content of the cover media can embed the additional information. At the receivers' side, both additional embedded information and original content of cover media are recovered individually. RDH-ED can be classified into two categories (Shi, Li, Zhang, Wu, & Ma, 2016) as follows. First one is Vacating Room Before Encryption (VRBE) (Ma, Zhang, Zhao, Yu, & Li, 2013), where the content owner performs preprocessing before encryption of cover information. The second one is Vacating Room After Encryption (VRAE) (Zhang, 2011), where the data hider performs operations on encrypted cover information. In Zhang (2011), the original image is encrypted by a stream cipher, after data hider divides the encrypted image into blocks where each block is responsible to carry one bit of information. Flipping, three Least Significant Bits (LSB) of half of the pixels into the encrypted image blocks. Further improvement of this approach (Hong, Chen, & Wu, 2012) uses the side-match scheme to decrease the error rate of extracted bits. Zhang (2012) proposed a separable method where, some part of encrypted bits are responsible to carry the parameters and remaining part in compression by LSB using data hiding key to create space in order to accommodate the additional data. The receiver has three options which are, extracting the additional data with the help of data hiding key, recovering similar image by using encryption key and lastly if the receiver wants to recover original information of cover media without any error using both keys. The proposed scheme (Zhang, 2012) guarantees an error free data extraction but it is not suitable for high payload. Further, Qian (Qian, & Zhang, 2016) improved payload capacity and also shows that the secret data can be embedded into the encrypted image by a histogram modification. After that there are some other schemes that achieved more payload capacity and gain better image quality by using image preprocessing (Zhang, Ma, & Yu, 2014). Recently there are some other works done in the field of RDH-ED (Yin, Luo, & Hong, 2014; Qin, & Zhang, 2015; Xu, & Wang, 2016; Huang, Huang, & Shi, 2016; Wu, Shi, Wang, & Zhou, 2017).