Optik 157 (2018) 750–760

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Original research article

# Error-free reversible data hiding with high capacity in encrypted image

Zhenjun Tang[a,b,c,*], Quanfeng Lu[a,b], Huan Lao[a,b], Chunqiang Yu[a,b], Xianquan Zhang[a,b,c]

[a] Guangxi Key Lab of Multi-Source Information Mining & Security, Guangxi Normal University, Guilin 541004, China
[b] Department of Computer Science, Guangxi Normal University, Guilin 541004, China
[c] Guangxi Collaborative Innovation Center of Multi-Source Information Integration and Intelligent Processing, Guangxi Normal University, Guilin 541004, China

ARTICLE INFO

*Article history:*
Received 8 September 2016
Accepted 22 November 2017

*Keywords:*
Reversible data hiding
Image encryption
Encrypted image
Chaotic map
PNG Image

ABSTRACT

Data hiding in encrypted image is a hot topic of data security in recent years. In this paper, we propose a reversible data hiding algorithm with high capacity in encrypted domain by exploiting alpha channel of portable network graphics (PNG) image. Specifically, our algorithm divides secret data into some segments. For each segment, one bit is embedded into the LSB of encrypted pixel and other bits are hidden in the corresponding element of the alpha channel, which is finally encrypted by two chaotic maps. With the use of alpha channel, our algorithm can perfectly recover secret data and reach high embedding capacity and good visual quality. Many experiments with standard benchmark images are carried out to validate efficiency of our algorithm. Comparison shows that our algorithm outperforms Zhang's algorithm (IEEE SPL 18(2011) 255-258).



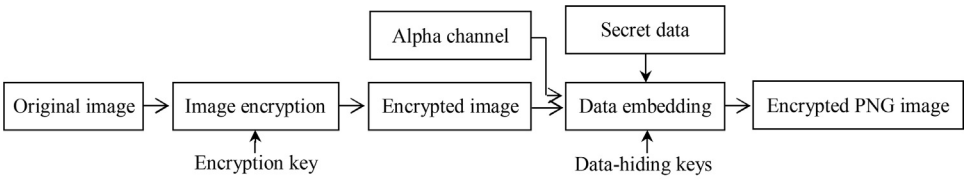
## 1. Introduction

Data security has attracted public attention in the past decade due to the disclosure of global surveillances (e.g., XKeyscore [1] and PRISM [2]). Consequently, efficient techniques for data protection are in demand. One well-known protection technique is encryption [3,4], which converts meaningful data to chaotic data. As attackers cannot observe any useful information from the chaotic data, data protection is thus achieved. Another useful technique for data protection is data hiding [5,6], which embeds secret data into cover data (e.g., image, text, voice and video). Since data embedding will not significantly change perceptual quality of the cover data, stego data is almost the same with the cover data from the viewpoint of human visual/auditory system. Therefore, stego data transmission will not draw attacker's attention, and thus data protection is ensured. In this paper, we study a new reversible data hiding algorithm in encrypted image.

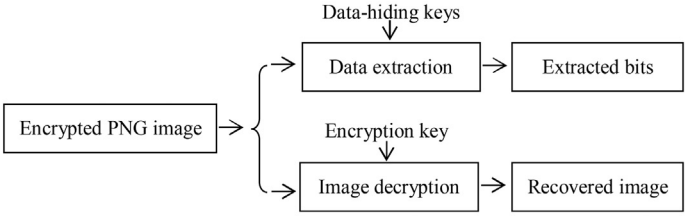
In the past years, researchers have proposed many useful reversible data hiding (RDH) algorithms. For example, Tian [7] exploited redundancy in digital images with difference expansion (DE) to design a reversible data hiding. Ni et al. [8] used histogram shifting to embed secret data. This algorithm can generate stego image with good visual quality in terms of peak signal-to-noise ratio (PSNR). Hu et al. [9] presented a DE based embedding algorithm with integer Haar wavelet transform by using the horizontal and vertical difference images. This method outperforms the original DE based scheme [7]. Tai et al.

* Corresponding author at: Department of Computer Science, Guangxi Normal University, 15 Yucai Road, Guilin 541004, China.
*E-mail addresses:* tangzj230@163.com, zjtang@gxnu.edu.cn (Z. Tang).

https://doi.org/10.1016/j.ijleo.2017.11.154
0030-4026/




(a) Image encryption and data embedding




(b) Data extraction and image decryption

**Fig. 1.** Block diagram of our algorithm.

[10] proposed a histogram modification based RDH method, where a binary tree structure is used to avoid communication of peak point pairs. In another study, Ou et al. [11] exploited correlation of prediction-errors (PE) to calculate a sequence of prediction-error pairs for data embedding. Li et al. [12] applied the strategy of PE expansion to color image and achieved data hiding by using correlation between color channels. Zhang et al. [13] presented a data hiding method for JPEG images with the strategy of exploiting modification direction (EMD) in DCT coefficients. A common feature of the above algorithms [7–13] is that they are all designed for cover images in the plaintext form.

Recently, many researchers have paid more attention to RDH algorithms in encrypted images since the ciphertext/encrypted images are widely generated and stored in cyberspace. A popular RDH algorithm is contributed by Zhang [14]. In this work, Zhang [14] divided encrypted image into blocks, embedded one bit into a block by flipping three LSBs of a half of the block pixels, and extracted secret data by defining a fluctuation function in terms of spatial correlation in natural images. This RDH algorithm reaches good visual quality, but cannot theoretically ensure correction of secret data extraction. It means that the extracted secret data may be not exactly the same with its original one. This is an unforgivable error for many applications and should be fixed in practice. Hong et al. [15] presented an improved version of Zhang's RDH method [14] by exploiting a new fluctuation function of block smoothness measurement. This method can decrease the extraction error rate (EER) of Zhang's method [14]. To reduce EER, Liao and Shu [16] designed a useful metric for measuring block complexity by considering neighbor pixels in terms of the locations. In another work, Qin and Zhang [17] presented an RDH scheme with capability of image content protection. This scheme only alters three LSBs of selected pixels of encrypted image for secret bit embedding. Both the RDH algorithms [16,17] have a smaller EER than Zhang's method [14] and Hong et al.'s method [15].

Although some useful RDH algorithms for encrypted image have been reported, they still have some problems in practice. For example, the above mentioned algorithms [14–17] cannot correctly extract all secret bits from stego image. In addition, their embedding capacity and visual quality are not desirable yet. Aiming at these problems, we propose an error-free RDH algorithm with portable network graphics (PNG) image in encrypted domain. Our algorithm not only perfectly recovers secret message, but also reaches high embedding capacity and good visual quality. Many experiments are conducted to validate our efficiency and the results demonstrate that our algorithm outperforms Zhang's algorithm [14]. The remainder of this paper is organized as follows. Section 2 explains our algorithm and Section 3 discusses experimental results. Conclusions are finally drawn in Section 4.

## 2. Proposed RDH algorithm

Our RDH algorithm includes two parts: Image encryption and data embedding, and data extraction and image decryption, as shown in Fig. 1(a) and (b). Content owner first encypts his/her original image with encryption key and obtains an encrypted image. Data hider creates an alpha channel with the same size of encrypted image, combines the alpha channel and the encrypted image to embed secret data, and finally makes an encrypted PNG image. For the receiver, if he/she has the data-hiding keys, data extraction can be conducted and secret bits are thus extracted. If the receiver knows the encryption key, he/she can recover image by decrypting the encrypted PNG image. In the following sections, we briefly introduce PNG image, and then explain the two parts in detail.