Reversible Data Hiding for Encrypted Image Based on Interpolation Error Expansion

Fuqiang Di, Engineering University of Chinese PAP, Xi’an, China
Minqing Zhang, Engineering University of PAP, Xi’an, China
Yingnan Zhang, Engineering University of Chinese PAP, Xi’an, China
Jia Liu, Engineering University of PAP, Xi’an, China

ABSTRACT

A novel reversible data hiding algorithm for encrypted image based on interpolation error expansion is proposed. The proposed method is an improved version of Shiu’s. His work does not make full use of the correlation of the neighbor pixels and some additional side information is needed. The proposed method adopts the interpolation prediction method to fully exploit the pixel correlation and employ the Paillier public key encryption method. The algorithm is reversible. In the proposed method, less side information is demanded. The experiment has verified the feasibility and effectiveness of the proposed method, and the better embedding performance can be obtained, compared with some existing RDHEI-P methods. Specifically, the final embedding capacity can be up to 0.74 bpp (bit per pixel), while the peak signal-to-noise ratio (PSNR) for the marked image Lena is 35 dB. This is significantly higher than Shiu’s method which is about 0.5 bpp.

KEYWORDS

Interpolation Error Expansion, Paillier Encryption, Pixel Correlation, Reversible Data Hiding

1. INTRODUCTION

Data hiding technique (Ma, 2016 & Zhang, 2016), which is a rising and effective tool used for multimedia processing and other related fields (Du, 2016; Gopinath, 2013; Liu, 2014; Petrlic, 2013; Radwan, 2009; Thabet, 2014; Zhu, 2013) has attracted more and more attentions. Reversible data hiding (RDH) is a novel technique that allows the original image to be recovered losslessly after the embedded data are extracted. With this property, RDH is widely used in many specific fields including image processing (Liu, 2016; Uchida, 2017; Wang, 2016), web security (Kuniyasu, 2018), etc. With the development of cloud computing and web services, many cover images are transformed into cipher image before uploading, for the purpose of security protection. Reversible data hiding for encrypted image (RDHEI) has become the research hotspot recently, and has many important applications in web security (Di, 2017; Qian, 2016). Specifically, some medical images in the cloud have been encrypted in former, due to the purpose of privacy protecting. Thus, someone in the system need embed some authentication or management message for convenience. However, both the original image and the embedded message need to be recovered.

Existing RDH methods in plain domain such as the difference expansion method (Tian, 2003), histogram shifting method (Dragoi & Coltuc, 2014) and lossless compression method (Jarali & Rao, 2013) are unsuitable for the RDH in the encrypted domain. Zhang (2011) firstly proposes the RDH
method in the encrypted domain using flipping the pixel values. In this method, the additional data is embedded into images which are encrypted with stream cipher. The cover image is recovered by the correlation among the pixels. Hong et al. (Hong, Chen, & Wu, 2012) proposed the improved method of Zhang’s algorithm, but this algorithm did not achieve better performance when the size of the block is small. Many RDHEI methods (Cao, 2016; Ma, 2013; Nyuyen, 2016; Xu, 2016; Zhang, 2014; Zhou, 2016) have improved the embedding performance in recent years.

However, the RDHEI methods based on the symmetric cryptosystem have some problems like the key-management problems. Therefore, the reversible data hiding methods using public-key encryption (RDHEI-P) have advantages in this case. Chen et al. (Chen, Shiu, & Horng, 2014) firstly proposed the RDHEI-P method. In this method, he encrypts the original image based on the public-key. The embedded image is decrypted using private key. The encryption procedure has the homomorphic property. In embedding stage, the second parts of the two neighbor pixels are changed to embed a bit. With the shared key, his scheme does not depend on a safe channel among the image owner, the data-hider and receiver, but it may have the inherent overflow problem since the summation of these two neighbor pixel values can be overflow. Many later RDHEI-P algorithms (Li, 2015; Zhang, 2015) using additive homomorphic algorithms and the methods have low embedding payload, and the image quality of marked image is not good.

Recently, Shiu (2015) proposed a novel RDHEI-P method using difference expansion method (DE). In his method, the preprocessing is needed. The method makes some room based on the difference expansion and hides some additional bits into the cover image, but some additional side information is achieved. According to additive homomorphic property, some additional data is embedded into the decrypted images. But, the method does not make full use of the correlation of the neighbor area and side information is too much which may decrease the embedding payload.

In the proposed method, the prediction of some specific pixels is obtained using the interpolation method. The proposed method can reduce the side information in the embedding phase and the new prediction can better make full use of the correlation among neighbor pixels. The proposed method obtains excellent performance, when compared with some existing methods. Experimental results show that the algorithm can effectively improve embedding performance, when compared with some existing RDHEI methods.

The rest of the article is represented as follows. Some preliminaries are introduced in Section 2. Specifically, the prediction error expansion technique and the Paillier encryption algorithm are introduced. On this basis, the proposed RDHEI-P scheme based on interpolation-error expansion method and public-key encryption is shown in Section 3. Then, in the Section 4, experimental results are given. Finally, Section 5 gives some discussions are provided and the conclusions of our work.

2. SOME PRELIMINARIES

In this part, some preliminaries are introduced to help better depict the proposed method. Firstly, the prediction error expansion which is a popular embedding method is introduced briefly. Secondly, the Paillier encryption method which is a classic public key encryption method is presented.

2.1. Prediction-Error Expansion

PEE (Gui, 2014; Li, 2011; Ou, 2013; Li, 2013; Thodi, 2007) belongs to a simple but effective method for reversible data hiding, and is widely used in many reversible data hiding schemes for encrypted image. It is proposed by Thodi et al. firstly, which is aimed to propose an improve version of the difference expansion method (Alattar, 2004; Dragoi, 2014; Kim, 2008; Lee, 2008). The algorithm will be introduced briefly in the following part.

Denote the pixel as \( I(i, j) \), denote \( \hat{I}(i, j) \) as the predicted pixel value, which is computed from the prediction algorithm, and then compute
Inspired Social Spider Behavior for Secure Wireless Sensor Networks
[www.igi-global.com/article/inspired-social-spider-behavior-secure/73717?camid=4v1a](www.igi-global.com/article/inspired-social-spider-behavior-secure/73717?camid=4v1a)

EMxC3 = e&mLearning Cultivating Connected Communities: Sustainable Workforce Talent Development
[www.igi-global.com/chapter/emxc3--emlearning-cultivating-connected-communities/157983?camid=4v1a](www.igi-global.com/chapter/emxc3--emlearning-cultivating-connected-communities/157983?camid=4v1a)