A Multilevel Reversible Data Hiding Scheme in Encrypted Domain Based on LWE

Yan Ke, Min-qing Zhang, Jia Liu, Ting-ting Su, Xiao-yuan Yang

PII: S1047-3203(18)30099-3
DOI: https://doi.org/10.1016/j.jvcir.2018.05.002
Reference: YJVCI 2182

To appear in: *J. Vis. Commun. Image R.*

Received Date: 28 October 2017
Revised Date: 19 April 2018
Accepted Date: 4 May 2018

Please cite this article as: Y. Ke, M-q. Zhang, J. Liu, T-t. Su, X-y. Yang, A Multilevel Reversible Data Hiding Scheme in Encrypted Domain Based on LWE, *J. Vis. Commun. Image R.* (2018), doi: https://doi.org/10.1016/j.jvcir.2018.05.002

A Multilevel Reversible Data Hiding Scheme in Encrypted Domain Based on LWE

Yan Ke*, Min-qing Zhang, Jia Liu, Ting-ting Su and Xiao-yuan Yang

Key Laboratory of Network and Information Security under Chinese People Armed Police Force (PAP), College of Cryptography Engineering in Engineering University of PAP, Xi'an, China

A B S T R A C T

This paper proposes a multilevel reversible data hiding scheme in encrypted domain by utilizing the controllable redundancy of learning with error public key cryptography. Messages can be embedded into multilevel sub-regions of ciphertext by quantifying the encrypted domain and recoding its redundancy. We recode redundancy based on the characteristics of cipher's distribution. Extraction and decryption processes are separated by dividing the encrypted domain into multilevel sub-regions and introducing different quantification standards. Original plaintext can be losslessly recovered from the marked ciphertext by using the decryption key; with a specific level data-hiding key, only the message hiding in the corresponding level can be extracted, while plaintext and other messages remain secret. We provide theoretical analysis and experimental results on the feasibility, reversibility, and security of the proposed scheme. The capacity and encryption blow up factor are discussed. The experimental results demonstrate the maximum embedding rate can exceed 0.3000 bpb of ciphertext.

Keywords: **Information security; reversible data hiding; multilevel embedding; public key cryptography; learning with Error**

1. Introduction

Reversible data hiding in encrypted domain (RDH-ED) is an information hiding technique that aims to not only accurately embed and extract covert messages, but also restore the original cover losslessly. RDH-ED is useful in applications in which distortion is unacceptable and ciphertext must be managed or identified by embedding private marks or error correction codes without knowing any information about the plaintext. Most importantly, no permanent change is allowed when the original plaintext and covert data are recovered in these applications, such as ciphertext management or retrieval in the cloud environment, imagery annotation for medical or military use. With increasing demand for information security and the development of signal processing techniques in the encrypted domain, RDH-ED has been an issue of great contention in the information security and encrypted signal procssing field [1].

The difficulty of RDH-ED lies in embedding additional data into ciphertext without causing distortion of the decrypted result. We analyze two aspects of this problem. The first is that once data is encrypted, the plaintext features (*e.g.*, image pixels' relativity) that traditional data hiding technologies use are lost. The second is that modern cryptography algorithms require diffusibility, *i.e.*, even one bit change of plaintext would diffuse through the entire encrypted domain. However, data hiding requires the ciphertext to be modified; thus, the more the ciphertext is changed, the greater the distortion of the decrypted results. The utilization of the redundancy in the cover media is the fundamental component of data hiding technique. Thereofore, the existing methods of RDH-ED can mainly be classified into two frameworks: "vacating room before encryption (VRBE)" [2] and "vacating room after encryption (VRAE)" [3]. The room, namely the redundancy, is vacated for embedding in these two frameworks.

The VRBE framework creates embedding redundancy in the plaintext domain, so there is always an extra preprocessing step before encryption. The VRBE schemes are mainly based on three strategies: lossless compression [4], difference expansion (DE) [5], and histogram shifting (HS) [6]. Most RDH methods [7]–[10] are derived from these three strategies. HS based methods have attracted much attention and can be divided into three categories: histogram shifting (HS) [6], difference histogram shifting (DHS) [8] and prediction-error histogram shifting (PEHS) [9]. DHS and PEHS based methods have drawn much more attention because of their large embedding capacities and high reversibilities. In [11], a new framework of RDH-ED was proposed, in which a specific stream encryption algorithm was used to preserve some of the correlation between the neighboring pixels. Different DHS and PEHS based RDH schemes can be performed directly in the encrypted domain. However, the VRBE framework might be impractical because it requires a preprocessing step to be performed before the content encryption.

The first VRAE method was proposed by Zhang for encrypted images [12], and then [13]-[14] enhanced its capacity. Qian, *et al.* proposed a similar method to embed data in an encrypted JPEG bit stream [15]. Liao, *et al.*[16] proposed embedding data in encrypted images based on the absolute mean difference between multiple neighboring pixels. Other VRAE schemes include compression sensing in the encrypted domain [17] and homomorphic public key encryption [18]-[24]. To adapt to practical applications, separable schemes have been proposed [17], [25]-[27], in which the extraction and data decryption processes can be

* Corresponding author.
E-mail address: 15114873390@163.com (Y. Ke), api_zmq@126.com(M.-Q. Zhang); twinly77@gmail.com(J. Liu);suting0518@163.com(T.-T. Su); yxyangyxyang@163.com(X.-Y. Yang)