Signal Processing: *Image Communication* 39 (2015) 226–233

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

journal homepage: www.elsevier.com/locate/image

Encrypted image-based reversible data hiding with public key cryptography from difference expansion

Chih-Wei Shiu [a], Yu-Chi Chen [b,*], Wien Hong [c]

[a] *Department of Art Design and Creative Industry, Nanfang College of Sun Yat-Sen University, Guangzhou, China*
[b] *Institute of Information Science, Academia Sinica, Taipei, Taiwan*
[c] *Department of Electronic Communication and Software Engineering, Nanfang College of Sun Yat-Sen University, Guangzhou, China*

ARTICLE INFO

Article history:
Received 17 February 2015
Received in revised form
19 July 2015
Accepted 25 September 2015
Available online 9 October 2015

Keywords:
Data hiding
Reversible data hiding
Difference expansion
Encrypted image
Public key cryptography

ABSTRACT

Encrypted image-based reversible data hiding (EIRDH) is a well-known notion of information hiding. In EIRDH, there are three entities, image provider (also called “context owner”), data hider, and receiver, where particularly they have to hold a shared key. The image provider sends the data hider the encrypted image by encrypting a chosen cover-image. Then, the hider generates the message-embedded encrypted image to the receiver by embedding the secret message. The receiver can simultaneously recover the original cover-image and extract the correct secret message. However, the data hider and image provider must be designated parties; this is, encrypted image-based reversible data hiding with public key cryptography (EIRDH-P) is a natural issue to eliminate the above limitation. In this paper, we construct the new EIRDH-P scheme from difference expansion (DE). We also analyze our scheme with respect to computation and communication. Finally, the experimental results show the effectiveness of this scheme. As pure image-based reversible data hiding from DE, the proposed EIRDH-P from DE also enjoys the advantages of DE.

1. Introduction

In cryptography, for protecting the confidentiality of a private message, the sender first encrypts the message to generate a ciphertext to the receiver. If there is an attacker who locates in the communication channel, he can directly think that ciphertext may contain important information. The ciphertext will be disable, since the attacker block the transference. The above is a security problem in real-life applications, so data hiding is presented to address it.

Data hiding becomes an interesting notion in information security, since its purpose is to prevent the attackers to detect a secret message [1–4]. Typically, the data hider embeds the message into a chosen image (referred to as a *cover-image*) to return the *stego-image*. Such attackers are not able to detect the image with the embedded message via the human vision. Only the receiver knows the extraction algorithm to extract the message in clear. In general image-based data hiding, there are two basic types of schemes: non-reversible data hiding and reversible data hiding. The difference between them is that the cover-image can be recovered by the receiver after extracting the secret message in reversible data hiding (RDH). Due to the advantage above, RDH plays an important role if the cover-image is meaningful and significant such as military and medical images.

1.1. Related work

Reversible data hiding schemes can be categorized into two major methods, difference expansion (proposed by Tian [5]) and histogram shifting (proposed by Ni et al. [6]).

[*] Corresponding author.
E-mail address: wycchen@ieee.org (Y.-C. Chen).

http://dx.doi.org/10.1016/j.image.2015.09.014
0923-5965/© 2015 Elsevier B.V. All rights reserved.

Lots of RDH schemes follow these two concepts to improve payload and image quality [7–16]. Recently, encrypted image-based reversible data hiding (EIRDH) is first introduced by Zhang [17], which maps to the following scenario. The image provider would like to keep privacy of the cover-image, but still requires the data hider to embed the secret message. Therefore, the data hider embeds the message into the encrypted image which is generated by the image provider from the cover-image. Finally, the receiver can recover the original cover-image and extract the secret message correctly.

The EIRDH scheme of Zhang [17] depends on XOR operations, divides an encrypted image into many blocks, and handles each block one by one for hiding. However, this scheme does not work in the case that the block size is small (the false positive rate becomes higher). In order to remedy the above weakness, the scheme Hong et al. [18] provides an adaptive way to choose the block size. Since that, EIRDH has grabbed research attention, and some schemes have been presented [19–21] to give good payload and image quality.

Differing from EIRDH, Chen et al. [22] first introduced a new notion of RDH, called encrypted image-based reversible data hiding with public key cryptography (EIRDH-P, for short). In EIRDH-P, the receiver initially sets his public/secret key pair. The image provider generates the encrypted image by using the public key, and then sends it to the hider. The hider is able to perform the hiding algorithm to generate the encrypted image with the embedded message by using the public key. The receiver finally uses the secret key to decrypt, and further obtain the original cover-image and secret message. Due to the establishment of the shared key of RDH or EIRDH, it no longer depends on a secure channel among all involved parties. We recall the scheme of Chen et al. [22] which uses Paillier encryption [23] to encrypt each pixel. A secret bit will be embedded into a pair of adjacent encrypted pixels. Based on the homomorphic property of Paillier encryption, the receiver compares all pairs of decrypted pixels to obtain the whole secret message, and also recovers the cover-image. However, we state the weakness that each pixel will be transformed to two parts, and then two parts will be encrypted to output two ciphertexts respectively.

1.2. Contributions

Let us summarize the main results of this paper. By using the Paillier homomorphic encryption as the basic primitive, we obtain a new EIRDH-P scheme to overcome a weakness of Chen et al.'s scheme [22] (described it later). The proposed EIRDH-P scheme fully depends on a crucial property of difference expansion [5]. We further present the experimental results for payload and image quality, and then analyze the effectiveness of our scheme by comparisons with literature works [17,18,20–22]. Finally, we give comparisons with Chen et al.'s scheme and our scheme with respect to cost of computation and communication.

Overview of the proposed scheme: We briefly describe the core of the proposed scheme. At a high level, the image provider does some steps as follows:

1. Pre-process the cover-image to generate a new cover-image, referred to as the processed image (with a modified difference expansion method).
2. Send the data hider the encrypted image by encrypting the processed image.

In this scheme, pre-processing is allowed, since the image will be encrypted before sent (e.g. noise-like image). The data hider will generate the encrypted image with embedded message by embedding the secret message into the encrypted image. Finally, the receiver can decrypt the encrypted image with embedded message, and then can recover the cover-image and secret message.

Comparisons with Chen et al.'s scheme: The first EIRDH-P scheme was proposed by Chen et al. [22]. In this scheme, each pixel is divided into two parts: an even integer and a bit, where the summation of them is equal to the pixel value. Both of them are encrypted by using Paillier encryption, respectively. Then, the ciphertext values of the second parts of two adjacent pixels are modified to accommodate an additional bit. However, the scheme always has *overflow*, since the summation of the plaintexts of two encrypted parts (the pixel value) is more than 255 after embedding. In the aspect of images, the inherent overflow is the weakness of Chen et al.'s scheme. One of our results is to overcome this problem. In a practical sense, Chen et al.'s scheme is not useful as long as we care about using images only. Although that scheme provides very nice payload and image quality, we believe that is not an image-based reversible data hiding.

Cryptographic trick for compression: Consider the general situation that a pixel will be encrypted as a ciphertext. However, by using Paillier encryption, the message can be at most 512 bits, and we waste too much space since we use 8 bits a pixel only. To make the total space complexity efficient, a cryptographic trick is workable to put 64 pixels together in a ciphertext. Divide 512 bits into 64 parts where each one contains 8 bits. Let enc be Paillier encryption and the i-th pixel be p_i for all i, $1 \le i \le 64$. Then compute $\mathsf{enc}(p_i)$ as the ciphertext of p_i. Now we hold $\mathsf{enc}(p_1), \ldots, \mathsf{enc}(p_{64})$. To combine them, we compute $\mathsf{enc}(\hat{p}) = \sum_{i=1}^{64} \mathsf{enc}(p_i)^{2^{8(i-1)}}$ by shifting which is the property of plain multiplication in Paillier encryption. Note that the 512 bits $\hat{p} = (p_{64} \| \ldots \| p_1)$, so the compression is achieved. We show the trick to demonstrate how to efficiently use space, while we would not use it to introduce the proposed scheme in the rest of paper.

Organization: In Section 2, some preliminaries are introduced. Then, the proposed EIRDH-P scheme is shown in Section 3, and the experimental results are provided in Section 4. Finally, conclusions of this paper are given in Section 5.