J. Vis. Commun. Image R. 25 (2014) 1164–1170

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

Encrypted signal-based reversible data hiding with public key cryptosystem

Yu-Chi Chen [a,*], Chih-Wei Shiu [b], Gwoboa Horng [b]

[a] Institute of Information Science, Academia Sinica, 128 Academia Road, Section 2, Nankang, Taipei 115, Taiwan
[b] Department of Computer Science and Engineering, National Chung Hsing University, 250 Kuo Kuang Rd., Taichung 402, Taiwan

ARTICLE INFO

Article history:
Received 26 December 2013
Accepted 1 April 2014
Available online 13 April 2014

Keywords:
Steganography
Data hiding
Reversible data hiding
Encrypted signal
Public key cryptosystem
Paillier encryption
Security
Secret message recovery

ABSTRACT

Encrypted image-based reversible data hiding (EIRDH) is a well-known method allowing that (1) the image provider gives the data hider an encrypted image, (2) the data hider embeds the secret message into it to generate the encrypted image with the embedded secret message to the receiver, and (3) finally the receiver can extract the message and recover the original image without encryption. In the literature, the data hider and image provider must be specific parties who know the shared key with the receiver in traditional encrypted image-based reversible data hiding. In this paper, we propose an encrypted signal-based reversible data hiding (ESRDH) with public key cryptosystem, not only for images. The proposed scheme is secure based on Paillier homomorphic encryption. Finally, the experimental results show that the proposed scheme has much payload and high signal quality.

1. Introduction

Steganography is an area of information security [1]. The goal of steganography is to hide a secret message from attackers. For example, in the first work [2], the secret message is embedded into an article. If a reader does not know the hiding method, he or she will consider that it is a normal article without any knowledge of the secret. Only the specific party has the ability to get or extract the secret. Therefore this kind of methods is referred to as a steganography scheme. However, with the development of computer and information technology, lots of digital multimedia are widely used to make human life more colorful, such as images and videos. Digital multimedia can be transformed into digital signals. In particular, signals (not only focuses on images, audio, and videos) are very common to be used in steganography.

Most of steganography studies addresses data hiding [3–6] where the secret message can be embedded into an image by a data hider, and the human vision cannot observe the image with the embedded secret message. The message can only be obtained by the receiver who knows the extraction algorithm. Formally, we always consider the following scenario for using image-based data hiding. The sender generates a ciphertext by encrypting an important message. An attacker is able to infer that this ciphertext may include the important message since it is confidential, and then he can block the ciphertext transference. However, if the sender embeds the message into an image, the attacker will regard it as a normal image. This is, data hiding becomes a significant area to deal with the above issue. In image-based data hiding, we always refer the image with the embedded message to the stego-image and the original one to the cover image. However, there are two types of data hiding schemes: (1) non-reversible data hiding and (2) reversible data hiding (RDH). The difference between these two types is that the cover-image must be recovered and reconstructed after extracting the secret message in reversible data hiding. RDH is important when the cover-image is meaningful such as military and medical images.

1.1. Related work

The kernel methods of RDH are basically classified into two types, difference expansion (proposed by Tian [7]) and histogram shifting (proposed by Ni et al. [8]). After Ni et al. and Tian et al. proposed the RDH schemes, many works presented improvements [9–20]. The first encrypted image-based reversible data hiding (EIRDH) was introduced by Puech et al. [21], and recently an efficient EIRDH was considered by Zhang [22]. An important scenario of EIRDH is that the data hider and image provider are not the same party, and the data hider cannot know the cover-image.

* Corresponding author.
E-mail addresses: wycchen@ieee.org (Y.-C. Chen), chihwei.shiu@gmail.com (C.-W. Shiu), gbhorng@cs.nchu.edu.tw (G. Horng).

http://dx.doi.org/10.1016/j.jvcir.2014.04.003
1047-3203/

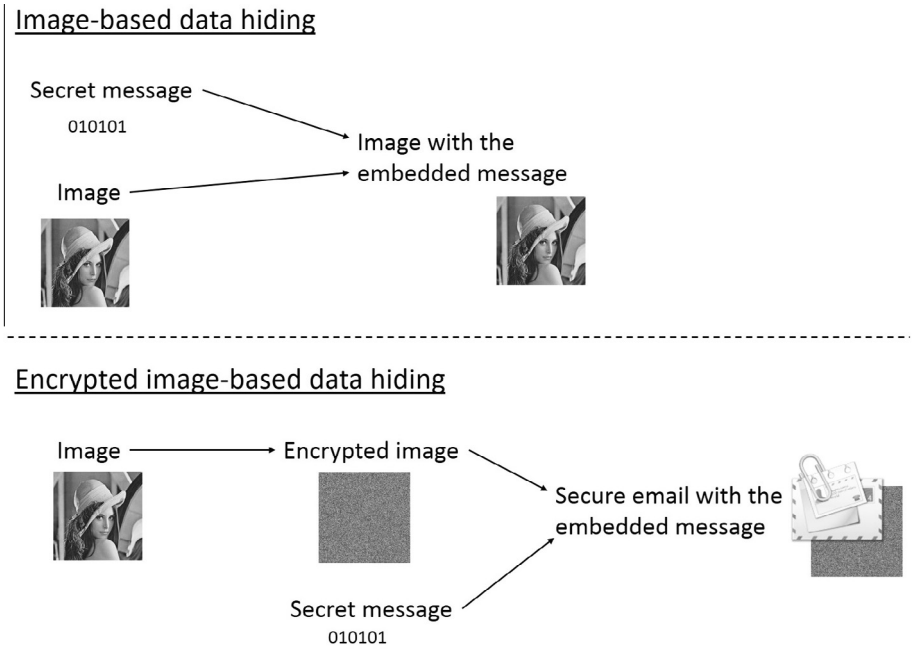

Fig. 1. System comparison with RDH and EIRDH.

In real-life, the data hider does not have the contract to access images from the image provider, but the receiver is able to know the images. Therefore we look EIRDH and traditional RDH as totally different systems (see Fig. 1 for more details).

In Zhang's scheme [22], the image provider first generates an encrypted image from a chosen cover-image, and then the data hider embeds the secret message into the encrypted image. Therefore the encrypted image with the embedded message is a noise-like encrypted image. Eventually, the receiver can decrypt it to recover the original cover-image and extract the secret message (see Fig. 2). The core of this scheme is to utilize the XOR operations, separate an encrypted image into blocks, and finally deal with each block one by one. In fact, it is not reliable if the block size is small, which implies that the false positive rate becomes higher. Nevertheless, Hong et al. [23] proposed an improvement which adaptively chooses the block size to overcome the weakness of Zhang's scheme. Since that, there are some schemes have been presented [24–26].

1.2. Contributions

The major contributions of this paper are summarized as follows.

1. In this paper, we address the issue that anyone can be a data hider such as the e-mail system. We introduce a new notion of encrypted signal-based reversible data hiding (ESRDH), where the receiver sets his public/secret key pair.[1] The signal provider generates the encrypted signal, and then the hider is able to perform the hiding method to further generate the encrypted signal with the embedded message by using the receiver's public key. Differing from the previous EIRDH schemes, this paper is the first to consider the above issue of ESRDH with public key cryptosystem.
2. According to the properties of Paillier homomorphic encryption [27], an encrypted signal-based RDH scheme is proposed. We use images as a case of signals to construct this scheme in Section 3. The security of the proposed scheme is under that of Paillier encryption. Moreover, we also give the experimental results to show that our scheme has more payload and higher signal quality than other EIRDH schemes [22,23,25] if we use some test images instead of signals. Due to using public key cryptosystem, for signal with more bits than 8 (a pixel), our scheme is worth more than using images.

The rest of the paper is organized as follows. In Section 2, we briefly describe preliminaries including Paillier homomorphic encryption and the model of EIRDH. In Sections 3 and 4, we propose a new ESRDH scheme based on Paillier encryption, and give the experimental results. Finally, conclusions are given in Section 5.

2. Preliminaries

In this section, we will present the system model of encrypted image-based reversible data hiding, and then review Paillier homomorphic encryption in details.

2.1. System model of encrypted image-based reversible data hiding

There are three entities, image provider $\mathcal{P}$, data hider $\mathcal{H}$, and receiver $\mathcal{R}$, in an EIRDH scheme. A valid EIDRH scheme is composed of the following algorithms:

1. I-Enc: This algorithm, run by $\mathcal{P}$, takes a cover-image *CI* and a key as input, and then returns an encrypted image *EI*.
2. M-Enc: This algorithm, run by $\mathcal{H}$, takes a message and a key as input, and then returns a secret message *SM*.
3. Embedding: This algorithm, run by $\mathcal{H}$, takes *SM* and *EI* as input, and then returns an encrypted image with the embedded message, *EIM*.

[1] Public key encryption is used to construct the email system, since the e-mail address can map to a public key and the account password can be transformed to the private key. The above notion implies that anyone can have the receivers email address (public key), but only the receiver can log in this account (private key).