Signal Processing: *Image Communication* 39 (2015) 234–248

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

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

Reversible data hiding in encrypted images using cross division and additive homomorphism

Ming Li [a,*], Di Xiao [b], Yushu Zhang [c], Hai Nan [b]

[a] *College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China*
[b] *College of Computer Science, Chongqing University, Chongqing 400044, China*
[c] *School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China*

ARTICLE INFO

Article history:
Received 12 May 2015
Received in revised form
21 August 2015
Accepted 2 October 2015
Available online 13 October 2015

Keywords:
Reversible data hiding
Image encryption
Cross division
Additive homomorphism
Histogram shifting

ABSTRACT

There are three problems in the existing reversible data hiding (RDH) algorithms in encrypted images: one is that some algorithms are not processed in the encrypted domain; another is that the reversibility which implies exact data extraction and perfect image recovery cannot be ensured in some cases; the last is that data expansion occurs when probabilistic public-key cryptosystem is used for image encryption in some homomorphic schemes. In this paper, a complete RDH in encrypted images is proposed. By using the idea of cross division and additive homomorphism, we solve all of the problems. Experimental results verify the superiority of the proposed method, which will have a good potential for practical applications of multimedia privacy protection.

1. Introduction

Reversible data hiding (RDH) is a technology that embeds secret message into a cover image in a reversible manner, that is, the embedded message as well as the cover image should be completely recovered after data extraction [1–3]. The categorical restoration property is important in some special applications such as medical imagery [4], military imagery and law forensics, for the cover image is too precious or too important to be damaged.

A variety of RDH schemes have been proposed so far, and can be classified into four categories: lossless compression based [5,6], difference expansion based [7–9], histogram shifting based [10–14], and integer transform based [15–17] schemes. Among them, histogram shifting based methods can provide better tradeoff between hiding capacity and visual quality, and therefore, have attracted much attention. Ni et al. [10] proposed a scheme of using peak/zero points in the image histogram, in which the message is embedded into the selected histogram bin with the most occurrences (called peak point). The bins between the selected bin and the zero occurrence bin (called zero point) have to be increased or decreased by one unit according to the shifting direction. Knowing the values of peak point and zero point, the embedded data can be extracted and the cover image can be recovered reversibly from the stego image. The histogram shifting techniques have been extended in [11], which used pixel differences to increase the hiding capacity. In [12], the multilevel data hiding method is employed to achieve higher capacity. In [13] and [14], the histogram shifting based RDH algorithm has been further developed by using two-dimensional difference-histogram modification and dynamic histogram shifting.

Encryption is a well known effective and popular method for protecting the confidentiality of the image [18–20], which aims to make the image not intelligible to any unauthorized entity who might intercept them.

[*] Corresponding author. Tel.: +86 18338989857.
E-mail address: liming@htu.edu.cn (M. Li).

http://dx.doi.org/10.1016/j.image.2015.10.001
0923-5965/© 2015 Elsevier B.V. All rights reserved.

However, if someone hopes to embed some additional message into the encrypted image, for example, a database administrator needs to embed the personal information into the medical images of the patients which have been encrypted for privacy protection, the RDH technique in encrypted image is required.

Since encryption makes the entropy of the image becoming maximal, it is difficult to embed additional data reversibly into encrypted image by using common data hiding algorithms. Some of RDH algorithms in encrypted images concentrate on embedding information into the partial unencrypted data of the images [21,22], but these schemes cannot be considered as real RDH algorithms in encrypted images for the essential embedding processing is not in the encrypted domain. The idea of pre-processing of the image before encryption is also proposed [23,24], in which the information redundancy of the natural image is utilized for vacating room for data embedding.

Other schemes that embed data directly into the fully encrypted images are also proposed [25–28]. In [25], the LSBs of the half of the randomly selected pixels in each divided block of the encrypted image are flipped for one bit data embedding. With the help of spatial correlation in decrypted image, the embedded data can be extracted and the image can be recovered simultaneously. Later, Hong et al. [26] improved [25] by using a new block smoothness measurement that considers the pixel correlations in the border of neighboring blocks. Then, Li et al. [27] modified the scheme by eliminating the block mode and using random diffusion and accurate prediction strategy to obtain higher data embedding capacity and lower extracted-bit error rate. Subsequently, by using full embedding strategy, the original scheme was further improved [28]. In [29], the encrypted LSBs of the image are compressed to vacate room for additional data embedding, and the data extraction is separated from image decryption. Nevertheless, the reversibility of all the above methods is affected by the plain image and the embedding rate. If the plain image is too complex or the embedding rate is too high, some extracted-bit errors may occur.

Recently, homomorphic encryption emerged in the research field of RDH in encrypted images [30,31]. Because of the homomorphic property, data embedding in encrypted domain can be achieved easily; however, the used probabilistic public-key cryptosystems such as Paillier [32] and Damgård–Jurik [33] cryptosystems lead to data expansion after image encryption. In [34], by using the same pseudo-random bits to encrypt two neighboring pixels, the exclusive-or values of two neighboring pixels are reserved after image encryption so as to carry the additional data to be embedded. Actually, the homomorphic property is equipped in the scheme, and there is no data expansion after image encryption; however, the performance is not satisfactory compared with other recent works.

In this paper, by using the idea of cross division and additive homomorphism, a novel RDH in encrypted images is proposed. With the help of homomorphic cryptosystem, data hiding in encrypted image is achieved by the proposed difference histogram shifting. The contributions of this paper can be summarized into the following aspects:

(1) Based on cross division, additive homomorphism is used in RDH without causing data expansion.
(2) Data hiding is directly processed in the encrypted domain.
(3) Real reversibility is realized, that is, data extraction and image recovery are free of any error.
(4) The performance of the proposed method is satisfactory.

The rest of the paper is organized as follows. The homomorphic cryptosystem is introduced in Section 2. The proposed scheme is elaborated in Section 3. Experiments with analysis and comparison are given in Section 4. Section 5 concludes this paper.

2. Homomorphic cryptosystem

2.1. Overview

With the rapid development of digital products and communication networks, the demand of privacy of digital data has become stronger during the last few years. For storing and reading data surely there exist several possibilities to guarantee privacy such as data encryption and tamper resistant hardware. The problem becomes more complex when asking for the possibility to publicly compute with private data in such a way that they are still executable while their privacy is ensured. This is where homomorphic cryptosystems can be used since they enable computations with encrypted data.

The most common definition of homomorphic encryption is the following. Let $\mathcal{M}$ (resp., $\mathcal{C}$) denote the set of the plaintexts (resp., ciphertexts). An encryption scheme is said to be homomorphic if for any given encryption key k the encryption function E satisfies

$$\forall m_1, m_2 \in \mathcal{M}, \quad E(m_1 \odot_{\mathcal{M}} m_2) \leftarrow E(m_1) \odot_{\mathcal{C}} E(m_2) \tag{1}$$

for some operators $\odot_{\mathcal{M}}$ in $\mathcal{M}$ and $\odot_{\mathcal{C}}$ in $\mathcal{C}$, where ← means "can be directly computed from," that is, without any intermediate decryption.

If ($\mathcal{M}$, $\odot_{\mathcal{M}}$) and ($\mathcal{C}$, $\odot_{\mathcal{C}}$) are groups, we have a group homomorphism. We say a scheme is additively homomorphic if we consider addition operators, and multiplicatively homomorphic if we consider multiplication operators.

The idea was first suggested by Rivest et al. in 1978, referred to as privacy homomorphisms [35]. For three decades, only a few operations (most noticeably addition and multiplication) are found homomorphic. The most prominent homomorphic encryption schemes, e.g., ElGamal [36], Paillier [32], Damgård–Jurik [33], are homomorphic with respect to a single algebraic operation, i.e., addition or multiplication. The Elgamal encryption is a classical example of multiplicative homomorphism, since, given two cipher texts, it is easy to obtain the encryption of the product of the two corresponding plaintexts. In 2009, a spectacular breakthrough was made by Gentry