Signal Processing: Image Communication 44 (2016) 84–91

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

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

High capacity reversible data hiding scheme for encrypted images

Thai-Son Nguyen [a], Chin-Chen Chang [b,*], Wen-Chi Chang [b]

[a] *School of Engineering and Technology, Tra Vinh University, Tra Vinh Province, Vietnam*
[b] *Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan, ROC*

ARTICLE INFO

Article history:
Received 13 April 2015
Received in revised form
30 March 2016
Accepted 30 March 2016
Available online 1 April 2016

Keywords:
Data hiding
High capacity
Image encryption
Privacy protection
Reversibility

ABSTRACT

Reversible data hiding is a technique that allows embedding additional data into encrypted images without knowing the content of the original image. The additional embedded data can be extracted exactly and the encrypted image can be reconstructed precisely to its original version. In this paper, a novel, reversible data hiding technique is proposed for encrypted images. In the proposed scheme, half of the pixels are used to classify the rest of the pixels into smooth and complex regions to provide room for embedding additional data. The proposed scheme can achieve complete reversibility, i.e., the data extraction and image reconstruction are error-free. Our experimental results indicated that the proposed scheme significantly outperforms existing schemes in terms of embedding capacity and the visual quality of the marked decrypted image.

1. Introduction

Reversible data hiding (RDH) is a technique that allows the original image to be reconstructed losslessly after the embedded data are extracted. With this property, RDH plays an essential role and is used extensively in many applications, i.e., military imagery, medical imagery, and law forensics. As a consequence, this topic has attracted the attention of many researchers. The RDH technique can be classified into three basic categories, i.e., difference expansion (DE) [1–3] , histogram shifting (HS) [4,5], and schemes based on lossless compression [6,7]. In the DE-based schemes, the difference value between two neighboring pixels is expanded to generate a new least significant bit (LSB) plane for hiding secret bits. In the HS-based schemes, the peak point and the zero point are determined in the histogram of the original cover image, and, then, the pixels are shifted from the peak point to the zero point to embed secret bits. The third category is based on the redundancy in the digital image to implement lossless compression. By doing so, a spare space is generated to contain the additional data. Some recent RDH schemes have combined the features of categories two and three, e.g., prediction error [8–11] to obtain higher performance in terms of visual quality and embedding capacity.

With the development of cloud computing, protecting privacy has become increasingly important, so the ability to hide information into the encrypted data is useful in this scenario. However, most existing studies of RDH are only appropriate for unencrypted images. Therefore, some recent studies have attempted to apply RDH for encrypted images [12–18]. In [12], the original image was first encrypted by a well-known encryption algorithm, such as advanced encryption standard (AES). Then, each encrypted block is used to hide only one additional bit using a simple substitution technique. In the decryption phase, to obtain the marked decrypted image, an analysis of local standard deviation is used to erase the embedded data. However, this scheme provides low embedding capacity, and the image that is decrypted from the marked encrypted version is distorted significantly. In [13], Zhang partitioned the encrypted image into blocks. Then, by flipping the three LSBs of the half number of pixels in each encrypted block, an additional bit is hidden, so that the decrypted image has good image quality. In Zhang's scheme, data extraction and image reconstruction are performed by identifying the parts that have been modified in each block with the aid of spatial correlation in the natural image. However, in [13], the number of incorrect extracted bits increased and the probability of reconstructing the original image precisely was decreased considerably when larger quantities of additional data are embedded. To further improve the performance of Zhang's scheme [13], Hong et al. [14] introduced a scheme to exploit the spatial correlation fully using a different estimation function and side-match algorithm to decrease the error rate of the extracted bits. In [12,13], the additional data only can be extracted from the decrypted version of the image. In other words, the receiver must have both the data hiding key and the encryption key to extract the embedded data. To separate the extraction of data from the decryption of the image, Zhang [15] first compressed the encrypted LSBs of the image

* Corresponding author.
E-mail addresses: thaison@tvu.edu.vn (T.-S. Nguyen), ccc@cs.ccu.edu.tw, alan3c@gmail.com (C.-C. Chang).

http://dx.doi.org/10.1016/j.image.2016.03.010
0923-5965/

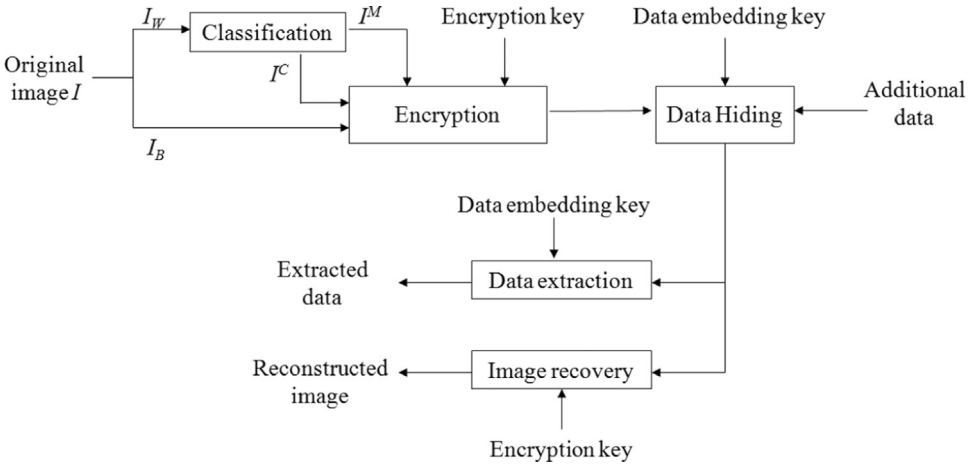

Fig. 1. Framework of the proposed scheme.

by using syndromes of a parity-check matrix. By doing so, his scheme generates space for carrying the additional data. However, side information is required in the receiver side to guarantee the perfect reconstruction of the original image, and this technique is not suitable for high embedding capacity. To obtain better visual quality of the marked decrypted image, Zhang et al. [16] proposed new RDH scheme for encrypted images in which low-density parity-check codes are applied to compress a part of the encrypted data and create space to contain the compressed data and additional data. In addition, their scheme utilized side information to reconstruct the original image perfectly. Concerning error-free reconstruction of images, Ma et al. [17] proposed an RDH scheme for encrypted images by reserving room before encryption by using a conventional RDH scheme [11]. Then, the reserved room was used to carry the additional data. Ma et al.'s scheme obtained error-free functionality in both extracting data and reconstructing the image. To obtain reversibility, Zhang et al. [18] proposed a new RDH scheme for encrypted images. Before encryption of the images, some pixels are predicted, and, then, room is vacated for hiding additional data using histogram shifting of prediction errors. Therefore, Zhang et al.'s scheme can recover the original image free of any errors [18]. In 2015, Cao et al. [21] proposed a new RDH scheme for encrypted images that is based on patch-level sparse representation. In their scheme, a complete dictionary is trained by using the K-means singular value decomposition (K-SVD) [22]. Then, according to the generated dictionary, the sparse coding technique is used to construct a large vacated space for embedding data.

In this paper, a new RDH scheme for encrypted images is introduced, in which half of the pixels are used to classify the rest of the pixels into a smooth region and a complex region to create room before encryption, and the rearranged image is encrypted by the standard encryption technique. Then, the middle bits of the pixels in the smooth region are emptied out, providing room for additional data. In the proposed scheme, bit replacement is used to embed additional data into the encrypted images. In general, the proposed scheme obtains excellent performance in four areas:

- The scheme allows complete reversibility, meaning that no any errors occur in extracting the data or in reconstructing the image.
- For under-embedding rates, the visual quality of the marked decrypted image is better than that provided by existing schemes.
- Greater embedding capacity than some existing schemes is obtained, allowing the proposed scheme to be used when large embedding capacity is required.
- The data extraction and image reconstruction phases are independent, meaning that the proposed scheme is more applicable.

The rest of the paper is organized as follows. Section 2 provides details concerning the proposed scheme, and our experimental results are presented, analyzed, and compared to other schemes in Section 3. Discussion of the proposed scheme and our conclusions are provided in Section 4.

2. Proposed scheme

In this section, we propose a novel RDH scheme to further improve the performance of previous schemes by vacating room before the original image is encrypted. The main idea of the proposed scheme is that the content owner first creates additional room by selecting smooth pixels according to their local complexity and emptying out them with free space for embedding additional data. The proposed scheme can be divided into three primary phases, i.e., image encryption, embedding additional data into the encrypted image, and extracting the additional data and reconstructing the image. Fig. 1 shows the main steps of the proposed scheme.

2.1. Image encryption

Assume that the original image I with the size of $H \times W$ is an 8-bit grayscale image, meaning that $I(i, j) \in [0, 255]$ and $1 \le i \le H$, $1 \le j \le W$. In this section, the content owner first partitions the image I into two sets in a chessboard fashion as shown in Fig. 2(a).

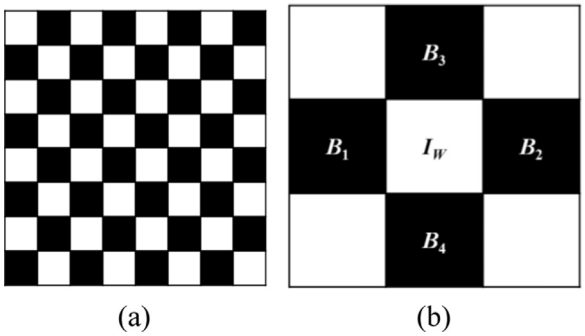

Fig. 2. (a) Pixel partition in chessboard fashion; (b) relationship between the pixel I_W and its four neighboring pixels.