J. Vis. Commun. Image R. 31 (2015) 154–164

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

Effective reversible data hiding in encrypted image with privacy protection for image content ☆

Chuan Qin [a,*], Xinpeng Zhang [b]

[a] Shanghai Key Lab of Modern Optical System, and Engineering Research Center of Optical Instrument and System, Ministry of Education, University of Shanghai for Science and Technology, Shanghai 200093, China
[b] School of Communication and Information Engineering, Shanghai University, Shanghai 200072, China

ARTICLE INFO

Article history:
Received 22 January 2015
Accepted 12 June 2015
Available online 20 June 2015

Keywords:
Reversible data hiding
Privacy protection
Image encryption
Data embedding
Image decryption
Data extraction
Image recovery
Isophote direction

ABSTRACT

In this paper, we propose a novel reversible data hiding scheme in encrypted image. The content owner encrypts the original image with the encryption key to achieve privacy protection for image content, and then, each block of the encrypted image is embedded with one secret bit by the data hider using the data-hiding key. Through the elaborate selection for partial pixels to be flipped, data hiding process only conducts slighter modifications to each block, which leads to significant improvement of visual quality for the decrypted image. The receiver can easily decrypt the marked, encrypted image using the encryption key, and then, through the data-hiding key and an adaptive evaluation function of smoothness characteristic along the isophote direction, secret data can be extracted from the decrypted image, and the original image can further be recovered successfully. Experimental results demonstrate the effectiveness of the proposed scheme.

1. Introduction

Information hiding, also named as data hiding, has been widely studied in academia. This kind of technique can imperceptibly embed secret information into cover data, such as audios, images, and videos [1]. There are two main research directions for data hiding: (1) achieving the various protecting functionalities (copyright identification, tampering recovery, etc.) for cover data through inserting the data, i.e., watermark, in different ways [2]; (2) realizing the covert communication (steganography) for high embedding payload of secret data while keeping satisfactory fidelity of cover data through well-designed encoding methods [3]. Recent years, in the research field of data hiding, many investigations have been conducted to study the problem of complete recovery for the cover data after the hidden data are extracted, which is called as reversible data hiding (RDH) [4–7].

Earlier studies for RDH focused on the two basic mechanisms, i.e., difference expansion (DE) [4] and histogram shifting (HS) [5,6]. In the DE-based RDH scheme proposed by Tian [4], cover image was segmented into a number of non-overlapping, neighboring pixel pairs, and the difference of each pixel pair was calculated and doubled. Then, the doubled difference of each pixel pair was either kept reserved or modified by one to match the parity of each secret bit for hiding. The processed difference was re-assigned to the two pixels in each pair, and the stego pixels carrying secret data were produced. Thus, the maximum hiding payload of this scheme approximated to 0.5 bits per pixel (bpp). On the receiver side, the hidden secret bits can be easily extracted from the least significant bits (LSBs) of the re-calculated differences in stego pixel pairs. The original values of cover pixel pairs can also be recovered through the inverse processing for the differences. However, for some pixels, the underflow and overflow problems may occur due to DE operation, thus, extra information of location map was required to record the information of these inappropriate pixels. In 2006, Ni et al. proposed a RDH scheme by shifting the histogram of cover image [5]. In this scheme, the peak point and the zero point of cover image histogram were first chosen, and then, the histogram bins within the range from the right one of peak point to the left one of zero point were all shifted to the right by one. Thus, one vacant histogram bin right to the peak point was created. During the embedding, the pixel values corresponding to the peak point were either kept unchanged or increased by one according to the secret bits. Obviously, the total hiding payload of secret bits depended on the pixel number of the peak point in the histogram.

☆ This paper has been recommended for acceptance by M.T. Sun.

* Corresponding author at: School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, No. 516 Jungong Road, Shanghai 200093, China. Fax: +86 21 55272982.
E-mail addresses: qin@usst.edu.cn (C. Qin), xzhang@shu.edu.cn (X. Zhang).

http://dx.doi.org/10.1016/j.jvcir.2015.06.009
1047-3203/

The receiver can easily extract the secret bits through the histogram of stego image, and further shifted back the moved bins for image recovery. But, the information of the peak point and zero point should be transmitted to the receiver side as the auxiliary data.

In order to further improve the performances of hiding capacity and stego image quality for the traditional DE-based and HS-based schemes, recently, many researchers have attempted to introduce the prediction mechanism into RDH [8–18]. Instead of directly using original image as cover data, prediction-based schemes utilized the relative data of original image, i.e., prediction error (PE), as the cover data for embedding, and PE can be obtained by the difference between original image and predicted image [8]. PE was modified to carry secret bits and added back to the predicted image to produce the final stego image. Note that, on the receiver side, the same predicted image should be generated and then the modified PE carrying secret bits can also be obtained, which guaranteed the correctness of secret bit extraction and original image recovery. Thus, the two focuses of the prediction-based RDH studies are: (1) how to acquire the appropriate PE from original image through the predictor; (2) how to operate the obtained PE for reversible data embedding.

One class of the typical predictors for RDH was based on the causal context of the current pixel for prediction, i.e., the neighboring pixels in the left and upper region of the current pixel [8–12]. This kind of causal-context based predictors for RDH often kept the pixels in the one/two top-most rows and the one/two left-most columns of original image unchanged and conducted the progressive prediction for remaining pixels in the raster-scanning order. The schemes in [10,11] adopted the mean value of causal context as the predicted value for current pixel. The schemes in [8,9] used the predictors of median edge detection (MED) that exploited the value relationship between the three pixels in the causal context. Gradient-adjusted prediction (GAP) used in [12] first estimated the edge characteristics with respect to direction and intensity for current pixel through the seven pixels in its causal context, and then generated the corresponding predicted value according to the estimated edge characteristics. Another class of the typical predictors for RDH was based on image interpolation mechanism [13–17]. This kind of interpolation-based predictors for RDH often indicated a portion of pixels dispersed in original image with different patterns as the reference pixels, which were then used to assist the prediction for remaining pixels by different image interpolation techniques. Hong and Chen presented an adaptive mechanism for reference pixel distribution in [13], which can achieve a satisfactory compromise for prediction accuracy and hiding capacity. In their method, more reference pixels were located in complex region rather than smooth region, and according to the reference pixels, the bi-linear and bi-cubic interpolation techniques were tried to calculate predicted values for remaining pixels. Qin et al. improved the choosing mechanism for reference pixels in [14] and introduced a curvature driven diffusion (CDD)-based inpainting method with a third-order partial differential equation (PDE) for interpolation, which can obtain more accurate predicted results. The schemes in [15,16] borrowed the idea of local edge sensing from image zooming in CFA image processing and adopted local refined reference patterns during prediction. The weight factors and thresholds for interpolation were respectively improved in these two schemes to achieve better performances.

Once the predicted result for original image was obtained, PE can also be calculated easily. The advantages of using PE as cover data were that PE often had more concentrated histogram than original image due to the accuracy of prediction and that more concentrated PE histogram can lead to higher hiding capacity and lower embedding distortions. Similar with the HS-based RDH for the cover data of original image, some reported schemes selected one or two highest bins of the histogram of the obtained PE and conducted HS operations on PE for reversible data embedding [9,13]. Lee et al. expanded the PE within a smaller value range and shifted the remaining larger PE to avoid overlapping [10]. The expanded PE can be used to carry secret bits reversibly. Actually, the shifting operation for the histogram of PE can be considered as a special case of PE expansion. Different with the conventional methods that uniformly embedded one bit into each expanded PE, Li et al. proposed an adaptive embedding strategy that can embed more bits into the smaller PE located in smooth regions, which improved the capacity limit of conventional methods [12].

Due to the popularity of cloud computing in recent years, a large amount of personal data can be stored and processed with various functionalities on Internet to reduce the computation burden on user client [19]. But, in order to protect user privacy, the user data must be encrypted before being processed on Internet. Therefore, the researches on data processing in the encrypted domain are necessary. As for the processing of RDH in encrypted images, here, we give an applicable scenario for instance: in a hospital with cloud server for data storage and management, the doctor (content owner) obviously has the right to know and access the contents of medical image of his/her patient during diagnosis; after the doctor finishes the current diagnosis, he/she will send the medical image to the cloud storage center of the hospital, i.e., medical image database center constructed by the cloud server, for data management and backup. However, in order to protect the privacy of the patient, the doctor should first encrypt the medical image of the patient and then send to the administrator of medical image database center. Although the administrator (data-hider) does not know the contents of the received image, he/she may embed some tagging information, such as the doctor name, ID number, department, and diagnosis date, which can effectively facilitate the image management and can be utilized for future retrieval.

Recently, some works about RDH in encrypted images have been presented [20–26]. Generally speaking, there are three main categories of RDH methods for encrypted images, i.e., the methods by vacating data-hiding room after image encryption [20–23], the methods by reserving data-hiding room before image encryption [24,25], and the method based on the properties of homomorphic encryption [26]. Compared with the latter two categories, the first category of methods that vacate data-hiding room after encryption, are more practically applicable because original image is only required for the encryption with low-complexity stream cipher before data embedding. However, this kind of methods may suffer from the low visual quality of decrypted, marked images and also the errors of extracted bits and recovered images. Other relevant data-hiding schemes in encrypted domain were reported in [27–31]. The schemes [27–29] embedded data into encrypted images, while the schemes [30,31] considered the data embedding for encrypted videos. Additionally, the schemes [27,28,30] are reversible and the schemes [29,31] are irreversible.

In this work, we mainly focus on studying the method of the first category mentioned above and propose a novel RDH scheme in encrypted images, which can provide effective privacy protection for image content. In the proposed scheme, to achieve privacy protection, data hider can only conduct the data embedding process on the encrypted version of original image, thus, he/she cannot access the image content without the warrant of the content owner. The legal receiver can decrypt the marked, encrypted image with the authorized encryption key from the content owner, and further extracts the embedded secret bits from the decrypted, marked image and recovers the original image simultaneously. In order to further improve the performances of the reported schemes that vacate the room of data hiding after image encryption, during data embedding, instead of flipping the LSBs of half pixels in the encrypted image, the proposed scheme only flips the LSBs of fewer