J. Vis. Commun. Image R. 31 (2015) 64–74

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

Reversible data hiding based on local histogram shifting with multilayer embedding ☆

Zhibin Pan, Sen Hu *, Xiaoxiao Ma *, Lingfei Wang

School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, PR China

ARTICLE INFO

Article history:
Received 26 May 2014
Accepted 13 May 2015
Available online 6 June 2015

Keywords:
Reversible data hiding
Histogram shifting
Localization
Multilayer embedding
Reference point
High embedding capacity
Low distortion
Continuous histogram

ABSTRACT

In this paper, we present a new reversible data hiding method based on histogram shifting using localization. Our proposed method selects peak point as the reference point, then uses the two neighboring points of the peak point to achieve secret data embedding based on histogram shifting and the peak point keeps unchanged. In the extraction end, we no longer need the key information about the peak point, we can directly find the peak point from the histogram to extract the secret data. We also exploit the localization to make the histogram of embedded cover image become almost the same as the histogram of the original cover image. The embedding capacity is also increased rapidly by the localization with multilayer embedding. Experimental results show that our proposed method is effective and superior.

1. Introduction

With the rapid development of the Internet, it is very convenient for people to get information from the Internet. Digital medias such as videos, images, audios are transmitted over the Internet. At the same time, security issues such as interception, interpolation have occurred frequently. Keeping the information transmitted over the Internet safe has become very important.

Data hiding develops very fast and applies to many fields, such as military, communications, medical applications and so on. Some of the applications demand the complete recovery of the cover image after the extraction of secret data, especially in military and medical applications. In order to losslessly recover the cover image, reversible data hiding is proposed. Reversible data hiding is an effective method to embed secret data into cover image, and the cover image can be recovered without distortion after the extraction of the embedded secret data. It can avoid attracting attacker's attention to the embedded cover image, the quality of the embedded cover image must be close to the original cover image because of the low distortion. In recent years, many reversible data hiding methods have been proposed. Luo [1] utilized the interpolation-error to embed secret data by expanding it additively or leaving it unchanged. Sachnev [2] used a sorting technique to record the prediction errors based on magnitude of its local variance, and employed prediction errors to embed data into an image without using a location map in most cases. Coltuc [3] proposed an improved data hiding for prediction-based reversible watermarking which aimed at reducing the embedding distortion of prediction error expansion reversible watermarking. Coltuc [4] proposed a low-distortion transform for prediction-error expansion reversible watermarking. Coatrieux [5] proposed a new reversible watermarking scheme. The Coatrieux's method inserted data in textured areas and made use of a classification process for identifying parts of the image that can be watermarked with the most suited reversible modulation. Tian [6] expanded the difference of two adjacent pixels to embed secret bits. Tian's method was extended by Alattar [7] through generalizing difference expansion from pixel pair to pixel block of arbitrary size. Wang [8] proposed a novel reversible watermarking method based on integer transform by taking pixel block of arbitrary size as embedding unit. Peng [9] proposed adaptive reversible data hiding scheme based on integer transform. In [9], Peng adaptively selected the parameter in integer transform according to block type determined by the threshold and embedded secret bits into block by integer transform with low distortion and high capacity.

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

* Corresponding authors.

E-mail addresses: zbpan@mail.xjtu.edu.cn (Z. Pan), husen.xjtu@gmail.com (S. Hu), xiao.77@stu.xjtu.edu.cn (X. Ma).

http://dx.doi.org/10.1016/j.jvcir.2015.05.005
1047-3203/

In [10], Ni proposed a novel data hiding method based on histogram modification. Ni used pairs of peak point and zero point to embed secret bits with low distortion. Tai [11] improved Ni's method by using the pixel differences histogram of cover image, then used the histogram shifting method to embed secret bits. Chang [12] proposed reversible data hiding scheme using complementary embedding strategy. Chang embedded one secret bit into one pixel horizontally and vertically by decreasing odd-valued pixels and increasing even-valued pixels by one. A reversible image hiding scheme using predictive coding and histogram shifting was proposed by Tsai [13]. Tsai explored the similarity of neighboring pixels by calculating the difference between neighboring pixels, then embedded secret bits by difference histogram modification. Lee [14] proposed the reversible data hiding based on histogram modification of prediction-error. Zhao [15] proposed reversible data hiding based on the histogram of pixel differences with multilevel modification. Zhang proposed novel data hiding methods in encrypted images in [16,17]. Zhang encrypted cover image and divided the encrypted cover image into non-overlapping blocks, and then embedded one secret bit into each block. Hong [18] improved the extraction method of Zhang's method in [16]. Wu [19] and Li [20] proposed the data hiding methods based on the combination of prediction-error and histogram shifting. Wu [19] used the down-sampled image to estimate the pixel values to get the prediction errors, then exploited the histogram shifting method to the histogram of prediction errors. Li [20] divided the image into non-overlapping blocks and then sorted the pixel of each block in an ascending order. Li used the second largest pixel and the second smallest pixel to predict the maximum pixel and the minimum pixel to get the prediction errors, then exploited the histogram shifting method to the histogram of prediction errors.

In this paper, we extend data hiding based on histogram shifting. We no longer need the key information (pairs of peak point and zero point). We do not use the peak point to embed secret bits, but select the peak point as reference point. The points adjacent to peak point are used to embed secret bits. We also adopt the localization to make the histogram of embedded cover image continuous so that the embedded cover image will not attract the attacker's attention. The capacity is increased rapidly because of the localization with multilayer embedding.

The remainder of this paper is organized as follows. In Section 2, the Ni's method is briefly reviewed. The proposed method is elaborated in Section 3. Experimental results and performance analysis are presented in Section 4, and Section 5 is our conclusion.

2. Related work

In [10], Ni et al. introduced a reversible data hiding scheme based on histogram shifting using pairs of peak and zero points. Let I be the cover image, P is the value of the peak point and Z is the value of the zero point. The histogram is shifted according to the pair of peak point and zero point. If $P > Z$, the histogram ranged from $Z+1$ to $P-1$ is shifted to left side by 1. Otherwise, the histogram ranged from $P+1$ to $Z-1$ is shifted to right side by 1.

$$I'_{i,j} = \begin{cases} I_{i,j}+1 & \mathit{if}\ P+1 \leqslant I_{i,j} \leqslant Z-1\ \mathit{and}\ P < Z \\ I_{i,j}-1 & \mathit{if}\ Z+1 \leqslant I_{i,j} \leqslant P-1\ \mathit{and}\ P > Z \end{cases} \tag{1}$$

where $I_{i,j}$ is the pixel value at the position (i,j) of the cover image I, $I'_{i,j}$ is the pixel value at the position (i,j) of the embedded cover image I'.

Once a pixel with value P is encountered, if the secret bit S is "1", the pixel value is increased by 1 if $P < Z$; the pixel value is decreased by 1 if $P > Z$. If the secret bit S is "0", the pixel value remains unchanged.

$$I'_{i,j} = \begin{cases} I_{i,j}+1 & \mathit{if}\ I_{i,j} = P\ \mathit{and}\ P < Z, S = 1 \\ I_{i,j}-1 & \mathit{if}\ I_{i,j} = P\ \mathit{and}\ P > Z, S = 1 \\ I_{i,j} & \mathit{if}\ I_{i,j} = P\ \mathit{and}\ P < Z, S = 0 \\ I_{i,j} & \mathit{if}\ I_{i,j} = P\ \mathit{and}\ P > Z, S = 0 \end{cases} \tag{2}$$

The total amount of embedded secret bits in the cover image equals the number of pixels associated with peak point. The number of peak points is very small in most cover images, so the embedded capacity is very low.

In the extraction end, we need to know the key information (the peak point and zero point). We cannot extract the secret bits if we lose the key information. If the attacker intercepts the key information, the secret bits may be extracted by the attacker. The key information reduces the security of the embedded secret bits. Fig. 1 shows the histograms of the original cover image and the histograms of the embedded cover image.

From Fig. 1, we can see that the peak points of the embedded cover image disappeared. Compared with the histogram of original cover image, the histogram of embedded cover image has a big drop in the position of peak point so that it becomes not continuous. The attacker may be attracted by the drop of the histogram of embedded cover image, and this will also reduce the security of the embedded secret bits.

In our proposed method, we have overcome the problems of the histogram-based data hiding method. We do not need the key information any more and the histogram of embedded cover image is continuous, or it is almost the same as the histogram of original cover image. This keeps the embedded secret bits safe. The capacity of proposed method is very high and the distortion is low.

3. Proposed method

In order to extract the secret bits without using the transmitted key information, we select the peak point as the reference point and use the neighboring points of peak point to embed the secret bits. Let I be the cover image, P is the value of the peak point, $P-1$ is the value of left neighboring point of peak point, $P+1$ is the value of right neighboring point of peak point. The histogram ranged from 1 to $P-2$ is shifted to left side by 1, the histogram ranged from $P+2$ to 254 is shifted to right side by 1.

$$I'_{i,j} = \begin{cases} I_{i,j}+1 & \mathit{if}\ P+2 \leqslant I_{i,j} \leqslant 254 \\ I_{i,j}-1 & \mathit{if}\ 1 \leqslant I_{i,j} \leqslant P-2 \end{cases} \tag{3}$$

where $I_{i,j}$ is the pixel value at the position (i,j) of the cover image I, $I'_{i,j}$ is the pixel value at the position (i,j) of the embedded cover image I'.

Once a pixel with value $P-1$ is encountered, if the secret bit S is "1", the pixel value is decreased by 1; if the secret bit S is "0", the pixel value keeps unchanged. A pixel with value $P+1$ is encountered, if the secret bit S is "1", the pixel value is increased by 1; if the secret bit S is "0", the pixel value keeps unchanged.

$$I'_{i,j} = \begin{cases} I_{i,j}+1 & \mathit{if}\ I_{i,j} = P+1\ \mathit{and}\ S = 1 \\ I_{i,j}-1 & \mathit{if}\ I_{i,j} = P-1\ \mathit{and}\ S = 1 \\ I_{i,j} & \mathit{if}\ I_{i,j} = P+1\ \mathit{and}\ S = 0 \\ I_{i,j} & \mathit{if}\ I_{i,j} = P-1\ \mathit{and}\ S = 0 \end{cases} \tag{4}$$

When the embedding process is finished, we obtain an embedded cover image I'. We transmit the embedded cover image I' to the receiver without using any extra information.

At the receiver end, we can extract the secret bits without the key information. We can obtain the peak point from the histogram