Digital Signal Processing ••• (••••) •••–•••

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Mosaic secret-fragment-visible data hiding for secure image transmission based on two-step energy matching

Jiangjin Yin, Bo Ou *, Xuan Liu, Fei Peng

College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Secure image transmission
Secret-fragment-visible data hiding
Energy function
Two-step matching

ABSTRACT

Recently, a new information hiding technology was proposed to hide a secret image into secret-fragment-visible mosaic image for secure image transmission. However, the previous method pays less attention to the block matching in the transform, and may obtain a low quality mosaic transform in some cases. In this paper, we propose to improve the secret-fragment-visible data hiding based the two-step energy function, which returns a weighted value of standard deviation and total variation of block. We match all the blocks according to the energy function and take the zero-mean normalized cross correlation (ZNCC) as the similarity measurement to optimize the matching. The interpolation optimization algorithm is used to stimulate the total ZNCC changes along with the parameter selection, and helps to solve the optimization quickly. Since more block's statistical properties are employed, the image blocks can be matched accurately, and a low distortion is introduced in the transform. Experimental results show that the proposed method can obtain a better visual quality of secret image after extraction and also requires less bits to encode the residuals.

1. Introduction

In the recent years, the image privacy disclosure becomes more serious as there is a lack of protection for the increasing use of multimedia applications. For example, the leakages of celebrity photos from iCloud have made a terrible influence, and arouse the need among the people to protect their own personal privacy information. For protection, encryption and information hiding are the two basic approaches. Image encryption converts the image information into invisible cipher text [1–7], so that the illegal identity can not obtain the message without the correct key. But the drawback is that the encrypted file is a meaningless representation and easily causes the attention of attackers during the transmission. Data hiding is another protection approach which can embed the ownership information into cover media [8–19], so that an unauthorized observer will not be aware of the existence of the hidden messages.

Traditional data hiding methods mainly embed some encrypted data bit stream into a cover medium, where the embedded information is binary representative and meaningless before decoding. Few of them can hide a semantic information such as image into a cover media. Currently, there are two hot topics for the data hiding, i.e., steganography [9], and digital watermarking [18]. Steganography realizes the data transmission by embedding secret information in public digital media files to achieve covert communications. Chan et al. [9] proposed the least significant bit (LSB) substitution to replace the LSBs of a cover pixel with secret bits. Zhang and Wang [14] designed a high quality steganographic technique based on exploiting modification direction, in which each secret digit in a $(2n+1)$-ary notational system is carried by n cover pixels, and at most one pixel is increased or decreased by 1. Digital watermarking is the process of embedding data (called a watermark) into digital multimedia objects. The embedding of the watermark information does not affect the normal use of the digital media objects and can be detected or extracted later to make an assertion about the authenticity and/or originality of the object. To be useful, digital watermarking usually requires a high robustness and anti-attack, but the data embedding capacity is not very large. Zong et al. [18] utilized a histogram-shape-related index to form and select the most suitable pixel groups for watermark embedding and realized a highly robust against geometric attacks. Rasti et al. [19] can realize better robustness for several signal processing attacks, by using singular value decomposition, orthogonal-triangular decomposition, and a chirp Z-transform to embed a watermark on the cover image.

Recently, a new scheme for secret image transmission is proposed to enable an image be hidden in the cover medium. Lai

* Corresponding author.
E-mail addresses: jiangjinyin@hnu.edu.cn (J. Yin), oubo@hnu.edu.cn (B. Ou), xuan_liu@hnu.edu.cn (X. Liu), pengfei@hnu.edu.cn (F. Peng).

https://doi.org/10.1016/j.dsp.2018.06.014
1051-2004/

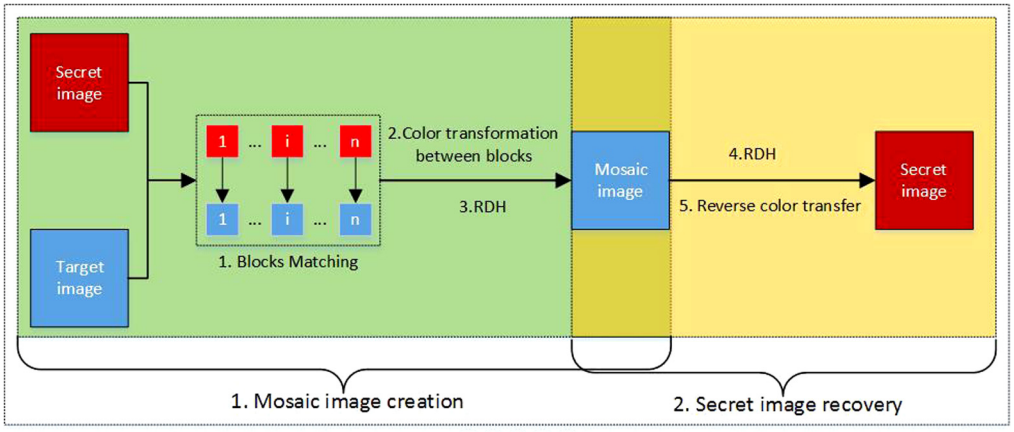

Fig. 1. The framework of mosaic-based secret image transmission.

and Tsai [20] first proposed the new computer art to apply the secret-fragment-visible mosaic image and its application for data hiding. In this method, a secret image is split into the visible fragments at first, and then the fragments undergo a color transform [21–24] to have the same visual appearance of the pre-selected target image. The marked image generated by the color transform is mosaic-like, being made up of the small fragments. The marked image is very similar to the decorative mosaic art, and can be used as a safe carrier without causing attackers' attention. However, the early mosaic transform-based method [20] requires a relatively large picture database. To remedy this, Lee and Tsai [25] proposed to use the Reinhard et al.'s color transfer method [21] to optimize the original color transfer method, and the secret image can be transformed as any freely-selected target image without the need of a huge image database. Hou et al. [26] designed a new mosaic data hiding method that can restored the secret image losslessly by optimizing the color transfer method. Moreover, by utilizing an effective clustering algorithm to reduce the information for recording block indexes, this method can also improve the visual quality of the mosaic image.

As mentioned above, the mosaic-based secret image transmission transforms the secret image into a secret-fragment-visible form to have the same visual appearance of the target image. As shown in Fig. 1, the general mosaic transform consists of three processes, including block matching, color transformation [21–24] and reversible data hiding (RDH) [27–42]. In the mosaic image creation phase, the secret image is transformed using color transfer at first, and then the required information is embedded into mosaic image using RDH. Here, color transfer is an image processing technique to change the color appearance of a source image according to a target image, and RDH is a special data hiding technique by which the cover media can be recovered losslessly after data extraction. For recovery, the embedded information is extracted using RDH, and then the reverse transformation is conducted to recover the secret image. For the color transfer, Reinhard et al. [21] proposed a simple technique that can transfer target image appearance to source image according to the mean and standard deviation of the color values in the source and target images, and can easily apply to $l\alpha\beta$ color space. Pouli and Reinhard [22] proposed a histogram reshaping technique that allowed users to select the color palette of the source image for the target one. The color transfer is implemented by manipulating histograms at different scales, and allowed the coarse and fine features to be considered separately. Instead relying on the color statistics, Wu et al. [23] presented a novel content-based method for transferring the color patterns between images which put an emphasis on the high-level scene content analysis and got a considerable gain. Khan et al. [24] presented a novel approach of local color transfer based on the simple statistics and the locally linear embedding.

In the mosaic transform data hiding, the secret image and the target image are divided into small rectangular image blocks at first, and then the secret blocks match the target blocks one by one before doing color transform. However, the existing works are mainly dedicated to optimizing the color transformation algorithm, and pay less attention to the image block matching. The block matching has an important impact on the color transformation, as it ultimately affects the visual quality of the mosaic image and the restored image. However, the block matching of the method [25] is simply based on the standard variance of the image block, and may not guarantee that all the image blocks can get a good match. There are many factors that affect the block matching, such as the average value of the block image, the total variation [43–45], etc. A single standard deviation is not sufficient to represent the characteristics of the block image. In order to make the restored image with a better visual quality, the matching between image blocks should take more block's statistical characteristics into account.

In this paper, we proposed a new mosaic data hiding method by improving the matching of image blocks. Different from the previous methods, a two-step process is employed in the block matching based on a so-called energy function. The proposed method not only considers the standard deviation, but also takes the total variation of image block into account in the energy function. We employ the zero-mean normalized cross correlation (ZNCC) [46–48] to measure whether the two blocks are matched appropriately, and use the energy function to match the blocks accurately in two steps. The blocks with the unsuitable matching will be picked up and then be re-matched in the second step for a better result. Moreover, by the energy function, the weights of the two statistics can be dynamically adjusted to optimize the overall block matching. An interpolation method is used to obtain the weight of the energy function during matching, and can reduce the optimization time. The experimental results demonstrate that the proposed method can improve the image block matching, and the secret image can be extracted with a better visual quality.

The rest of this paper is organized as follows. In Section 2, the related work is reviewed at first. Section 3 gives the proposed method in details, and the experimental results where the comparisons with some other methods are provided in Section 4. Section 5 concludes this paper.

2. Related work

Lee and Tsai [25] proposed a new secure image transmission technique via secret-fragment-visible mosaic images by a nearly-

Please cite this article in press as: J. Yin et al., Mosaic secret-fragment-visible data hiding for secure image transmission based on two-step energy matching, Digit. Signal Process. (2018), https://doi.org/10.1016/j.dsp.2018.06.014