J. Vis. Commun. Image R. 40 (2016) 225–236

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

Image camouflage by reversible image transformation ☆,☆☆

Dongdong Hou, Weiming Zhang *, Nenghai Yu

School of Information Science and Technology, University of Science and Technology of China, Hefei 230027, China

ARTICLE INFO

Article history:
Received 23 September 2015
Revised 14 May 2016
Accepted 20 June 2016
Available online 30 June 2016

Keywords:
Image camouflage
Image transformation
Image encryption
Reversible data hiding

ABSTRACT

A new reversible image transformation technique is proposed, which not only improves the visual quality of the camouflage image created by transforming a secret image to a freely-selected target image, but also can restore the secret image without any loss. Effective clustering algorithm is utilized to reduce the information for recording block indexes that is vital for restoring the secret image. Therefore, the transformation can be made between the blocks with relatively small size, thus greatly improving the visual quality of the camouflage image. The root mean square error of camouflage image was reduced by 6 in most cases compared with the previous method. Since the proposed technique is reversible, we can further realize two-round transformation by transforming the camouflage image to another target image and thus hide two images into only one.

1. Introduction

Nowadays, outsourcing photos to cloud or sharing photos through social media is more and more popular, which at the same time make it challenging to protect the privacy of photos' owners. For instance, recently many private photos of Hollywood actress leaked from iCloud [1].

There are two common approaches, encryption and data hiding, to protect image contents from leakage. Although encryption solves the privacy problem in a certain extent, but the messy codes of ciphertext with special form are easy to cause the attention of attackers who will plan to breakout the accounts of encryption users.

Data hiding technology embeds message into covers such as the image, audio or video, which not only protects the content of secret file, but also hides the communication process itself to avoid the attacker's attention. The most secure approach of data hiding is to embed the message while minimizing a suitably defined distortion, such as methods proposed in [2–4], which have strong ability to resist detection, but can only achieve a relatively small payload, less than 1 bit per pixel (bpp). Traditional data hiding method is suitable for embedding a small message into a large cover, e.g., an image. However, in the applications of image outsourcing or sharing, the message itself is just an image. Therefore, we need large capacity data hiding (LCDH) methods to hide images. Although, LCDH is hard to resist detection of strong steganalysis [5–7], it will be very useful in the applications of privacy protection of photos.

LCDH can be used for "secret image sharing" by hiding one image into several other images [8,9]. Typical secret image sharing model is based on the well known (t, n) threshold scheme originated from Blakley [10] and Shamir [11], which generates n shadow images and any t $(t \leqslant n)$ of n shadow images can be used to reconstruct the secret image. However, in such scheme, t is larger than 1, that is, we need more than one image to reconstruct the secret image. How to hide one image into another one with the same size is a more challenging problem, which we call "image transformation".

As shown in Fig. 1(a), by image transformation, the sender can transform a secret image A to a target image B, getting a camouflage image B' which is similar with the target image B. From B', the recipient can reconstruct a A', and usually A' is a good estimation of A. If A can be losslessly reconstructed from B', i.e., A' is equal to A, we call the scheme reversible image transformation, just as Fig. 1(b) shows. Image transformation technique can be viewed as a special kind of data hiding method, which embeds image A into B.

Lai et al. [12] propose an image transformation method, which selects a target image similar to the secret image in a database, then replaces each block of the target image by a similar block of the secret image and embeds the map between secret blocks and target blocks, finally generates a camouflage image as the

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

☆☆ This work was supported in part by the Natural Science Foundation of China under Grant 61170234 and Grant 60803155, and by the Strategic and Piloted Project of CAS under Grant XDA06030601.

* Corresponding authors.
E-mail addresses: houdd@mail.ustc.edu.cn (D. Hou), zhangwm@ustc.edu.cn (W. Zhang), ynh@ustc.edu.cn (N. Yu).

http://dx.doi.org/10.1016/j.jvcir.2016.06.018
1047-3203/

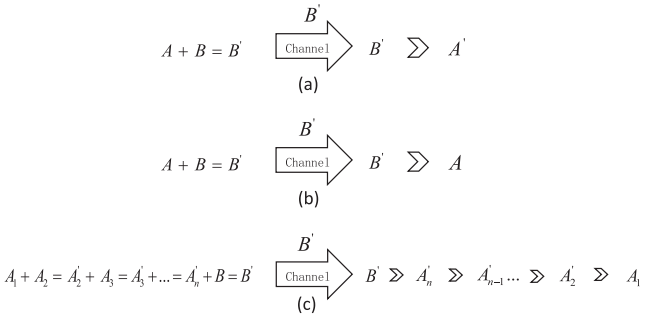

Fig. 1. Diagram of image transformation. $A, A_1, A_2, \ldots, A_n$ are secret images; B is a target image. (a) Nearly-reversible image transformation. (b) Reversible image transformation. (c) Multi-round transformation.

camouflage of the secret image. A greedy search is used to find the most similar block. Although Lai et al.'s method is reversible, it is only suitable for a target image similar with the secret image, and the visual quality of the created camouflage image is not so good.

Lee et al. [13] improve Lai et al.'s method by transforming the secret image to a freely-selected target image without the need of a database. In Lee et al.'s method, each block of the secret image is transformed to a block of the target image with a nearly-reversible color transformation [14], and then the accessorial information for restoring secret image, such as transformation parameters, indexes of block, is embedded into the transformed blocks, getting the ultimate camouflage image. Lee et al.'s method can transform a secret image to a freely-selected target image, and greatly improves the visual quality of the camouflage image. However, by Lee et al.'s method, the secret image cannot be losslessly reconstructed because the transformation is not reversible.

Reversible image transformation is important especially for the applications of medical images and military images. Moreover, the reversibility enables us to realize multi-round transformation as shown in Fig. 1(c), in which the image A_1 is transformed to A_2 getting A_2', and then A_2' is transformed to A_3 getting A_3', and so on. Finally we hide n secret images, $A_1, \ldots, A_n$, into one target image B getting B'. From B', the receiver can in turn reconstruct $A_n', A_{n-1}', \ldots, A_2'$ and A_1. Note that the receiver only completely restores A_1 and gets similar versions for other secret images. Without the reversibility, the accessorial information will be destroyed in the process of restoration, and thus only one round transformation is possible. In the multi-round transformation, $A_2, \ldots, A_n$ are secret images and target images at the same time. Therefore, to realize multi-round transformation, the target image must be freely-selected, because secret images may be arbitrary.

Such multi-round transformation can be used for different purposes such as follows:

- Hiding several secret images, $A_1, A_2, \ldots, A_n$, into one target image B.
- If only A_1 is the secret image, deeply hiding A_1 into several images by using different keys in each round and thus realizing multi-layered camouflage.
- Compressing $n+1$ images, $A_1, A_2, \ldots, A_n$ and B, into one image B'. Such compression is transparent, because B' is similar to B, and thus B' can be viewed as the envelop of the compressed files.

In this paper, we propose a reversible image transformation for freely-selected target images. To keep the reversibility, we transform the secret block to the target block only by shifting the mean of pixels in the secret block. A clustering algorithm is used to divide all blocks into K classes according to their standard deviations (SDs). The clustering can efficiently reduce the information for recording the indexes of block, which enables us to set small block size and thus greatly improves the visual quality of the created camouflage images. To accelerate the speed of transformation, the parallel framework proposed in [15,16] may be useful. Because the proposed method is reversible and is suitable for arbitrary target images, we can further realize two-round transformation.

The rest of the paper is organized as follows: Section 2 introduces the related work. The proposed method is elaborated in Section 3. Experimental results are shown in Section 4, and the paper is concluded with a discussion in Section 5.

2. Previous arts

The proposed method is an improvement of Lee et al.'s method [13], which we will briefly introduce firstly. Both the proposed method and Lee et al.'s method do transformation for channel R, G, B of a color image separately, so we just take the transformation on gray images (one channel) as an example in Sections 2 and 3. In Lee et al.'s method, the secret image and the target image are divided into N non-overlapping blocks with the same size, which are called tiles. The secret tiles are sorted into a sequence $\mathbf{B}_i$ $(1 \leqslant i \leqslant N)$, and the target tiles are sorted into another sequence $\mathbf{T}_i$ $(1 \leqslant i \leqslant N)$ according to the SD of the pixels in each tile. And then the ith secret tile is transformed to the ith target tile with the following near-reversible transformation.

Let secret tile $\mathbf{B}$ be a set of pixels such that $\mathbf{B} = \{p_1, p_2, \ldots, p_n\}$, and the corresponding target tile $\mathbf{T} = \{p_1', p_2', \ldots, p_n'\}$. Firstly calculate the mean and SD of each tile.

$$u = \frac{1}{n}\sum_{i=1}^{n} p_i, \quad u' = \frac{1}{n}\sum_{i=1}^{n} p_i'. \tag{1}$$

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(p_i - u)^2}, \quad \sigma' = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(p_i' - u')^2}. \tag{2}$$

A new set of pixels $\mathbf{T}' = \{p_1'', p_2'', \ldots, p_n''\}$ is generated by calculating as

$$p_i'' = q(p_i - u) + u', \tag{3}$$

where $q = \sigma'/\sigma$. Obviously $\mathbf{T}'$ has the same mean and variance as the target tile $\mathbf{T}$. Replace each $\mathbf{T}$ with the corresponding $\mathbf{T}'$, we get a transformed image (Before embedding accessorial information.) similar with the target image. At the receiver side, the original pixel p_i can be recovered by

$$p_i = 1/q(p_i'' - u') + u. \tag{4}$$

To recover the original pixels, the parameter q, u and u' must be embedded into the transformed image and sent to the receiver. To embed the real number q, it is represented as a number in the range of 0.1–12.8 with 7 bits. These parameters are embedded into the transformed image with a reversible data hiding (RDH) scheme [17] and the yielded camouflage image will be sent to the receiver. The RDH scheme enables the receiver to losslessly reconstruct the transformed image after extracting these parameters and then recover the secret image from the transformed image with the help of the parameters. Note that p_i'' yielded with Eq. (3) is also a real number which must be truncated to be an integer in the range of 0–255, so the original pixel value cannot be recovered exactly by Eq. (4). That is why Lee et al.'s method is not reversible.

Besides the parameters of transformation, the sender must embed the indexes of secret tiles into the transformed image, according to which the receiver rearranges the restored tiles to get the secret image. With the smaller tile size, we can get a trans-