Int. J. Electron. Commun. (AEÜ) 69 (2015) 1745–1754

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

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

Reversible and adaptive image steganographic method

Mingwei Tang[a,*], Jie Hu[b], Wen Song[a], Shengke Zeng[a]

[a] School of Computer and Software Engineering, Xihua University, Chengdu 610039, China
[b] School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China

ARTICLE INFO

Article history:
Received 10 October 2013
Accepted 26 August 2015

Keywords:
Information hiding
Image interpolation
Reversibility
Peak signal-to-noise ratio
Adjacent pixels

ABSTRACT

Reversible image steganographic scheme has become one of main research contents in information hiding field in recent years. Reversibility allows the original images to be completely reconstructed without any distortion after the embedded information has been extracted. Image interpolation is a key image processing method and has been widely applied in imaging processing relevant areas, such as image reconstruction by simulating image adjacent pixels between two-dimensional images. This paper proposed a reversible and adaptive image steganographic algorithm based on a novel interpolation technology, which can improve the performance of information hiding schemes proposed before. The proposed scheme has the benefits of higher embedding capacity with lower computational complexity and better image quality. The experimental results show that the proposed scheme can gain better performance than other state-of-the-art algorithms.

1. Introduction

Information hiding (or data hiding) is the art of secret information communication via public networks [1]. In the past 10 years, information hiding techniques have become an important information security technology. It is widespread in a great deal of application fields [2]. It, for example, is used for protecting secret information not to be perceptible. Secret information sender can apply the information hiding technique to embed secret information which can avoid being detected, stolen, or destroyed by unauthorized persons in the process of transmission. It mainly concerns with embedding of information in a "cover file" so that the very existence of hidden information is concealed. Anyone should not doubt or know the presence of secret messages except for the sender and the authorized users of the stego files. Information hiding is able to avoid suspicion from the visual view, which is lacking in traditional encryption system.

Steganography (or steganographic algorithm) is one of main branches of information hiding which refers to a number of disciplines. Security, capacity, and robustness are three main aspects that affect an information hiding system and its applications. Steganographic methods are concerned primarily with high security and capacity. Robustness is usually one of main research contents in the watermarking technology. Because of their inherent redundant information, digital files (such as digital images, videos, sound files, and other computer files) have widespread application for information hiding and steganography using as "cover files" or carriers to embed secret information.

In the information hiding systems, there are two types of information hiding algorithms. Methods based on spatial domain techniques are a kind of image steganographic techniques. In the spatial domain, information hiding algorithms can embed secret messages into the intensity of pixels value of images directly. The least significant bits (LSB) embedding is the simplest and most popular scheme for digital images. The LSBs of image pixel values have pseudo random and noise-like characteristics. So, embedding information in them cannot be visually detected. Methods based on spatial domain are a widely used technique due to its superior capacity, good image quality and its low computational complexity [3]. Hence, information hiding in the LSBs was one of the most early steganographic methods and its variations are still being considered by the researchers in this field. Methods based on transform domain techniques are another kind of image information hiding techniques. In the transform domain, images are first transformed to another domain (such as DCT domain), and then secret messages are embedded into transform domain coefficients in Ref. [2]. The LSBs of transform coefficients have also the same characteristics, such as pseudo random and noise-like characteristics.

The capacity or embedding rate is an important characteristic of a steganographic algorithm which is defined as the number of information bits that can be embedded in each pixel of a cover image. The embedding rate is one bit per pixel (bpp) in the two mentioned steganographic methods of LSB-F and LSB-M. When the hidden messages contain a smaller number of bits than the number

[*] Corresponding author. Tel. +86 02887720101.
E-mail address: tang4415@126.com (M. Tang).

http://dx.doi.org/10.1016/j.aeue.2015.08.011
1434-8411/© 2015 Elsevier GmbH. All rights reserved.

of the cover-image pixels, we assume that the information hiding is distributed randomly throughout the cover image based on a secret key (or stego key) shared with the authorized users of the stego image. Some of the classic algorithms will be presented as follows.

Mielikain proposed an information hiding method based on LSB matching revisited (LSB-MR) which has also better performance than the powerful LSB [4]. Using a pair of pixels as an information hiding unit, the secret information is embedded in the image pixels in LSB-MR. The LSB of the first pixel hides one bit of message, and a function of the two pixel values embeds another bit of message. Experimental results demonstrate that the proposed method is with fewer revisions to the pixels of the cover image than LSB-M when embedding the same capacity messages. The embedding rate is 0.5 bit per pixel (bpp) in LSB-MR. Omoomi et al. proposed a novel efficient high payload ±1 steganographic scheme based on a special two variable binary functions [5]. Embedding capacity is 1.00 bit per pixel (bpp) in the EPES method.

The proposed information hiding methods can also be classified into two kinds, such as irreversible information hiding schemes (e.g., [6–10]) and reversible information hiding algorithms (e.g., [11–20]). Irreversible steganographic techniques may generally obtain better embedding capacity and higher image quality. Reversible information hiding methods get the advantages of the exact recovery of the original images when extraction of the embedded information. The latter is the fundamental research content of this paper.

Image interpolation is a rather important technique in digital image processing by which a small image is scaled-up larger. High speed and low time complexity are two main advantages of image interpolation method. Based on the existence information of image to estimate unknown approximation pixel values at the adjacent pixel positions, the size of the image is magnified by image interpolating methods up to several times or more. An interpolated image will always lose some quality after image interpolation is performed each time [9]. Image interpolation is widely used in the medical imaging processing in Ref. [21]. Moreover, medical imaging processing requires enormous amounts of information and extreme precision. So, it is essential for a better interpolating technique to reduce the processing time and remain or improve good quality of reconstructed images. It is important for a speedy and efficient interpolating technique that provides extremely good image quality.

It is a hot topic for combination interpolation technology with information hiding in recent years. In 2009, Jung and Yoo first proposed the use of image interpolation to information hiding in the spatial domain in Ref. [11]. The interpolating method proposed by Jung and Yoo in [11] is Neighbor Mean Interpolation (NMI). Using image interpolation technique, Luo et al. presented a reversible image watermarking method [12]. In [13], Lee et al. presented an interpolation technique by Neighboring Pixels (INP). By the interpolation technique, INP method hides secret information based on maximum adjacent pixels difference values. Using optional prediction error histogram modification, Ou et al. put forward a reversible watermarking method which reduced the image distortion of high capacity in Ref. [14]. Using the idea of reference pixel and multilayer hiding, Zeng et al. presented a Reversible Data Hiding Scheme (RDHS) based on the pixel difference histogram shifting to spare space for embedding secret information [15]. Based on image interpolation and direction order mechanism, Wang et al. proposed a reversible data hiding for high quality images in spatial domain [16]. Qian et al. presented a framework of reversible information hiding method in an encrypted JPEG bitstream [17]. Utilizing a multi-layer information embedding technique, Tang et al. proposed a high Capacity Reversible Steganography (CRS) [18]. When the good visual quality being retained, Wu et al. presented a novel reversible digital images information hiding algorithm [19]. Based on the minimum rate criterion and optimized histograms modification, Hu et al. [20] designed a reversible information hiding scheme by applying a pixel prediction method to embed secret information. Depending on adjacent pixels when image interpolation, information hiding scheme produces the estimated pixel values to fill in the blanks and hides secret sub-messages within them. This research may contribute to the improvement of embedding capacity. But, image quality is affected by introducing an image interpolation by neighboring pixels.

Based on the above analysis and research, the paper proposed a high capacity, Reversible and Adaptive Steganographic (RAS) method based on a novel image interpolation and image compensation technique. The rest of the paper is organized as follows. Section 2 introduces the image interpolation technique and information hiding algorithm proposed by Jung and Yoo [11], Lee and Huang [13], Zeng et al. [15] and Tang et al. [18]. Section 3 describes the proposed information hiding scheme and shows how the embedding capacity in the image interpolating method can be improved as well as good image quality being retained. The experimental results and performance analysis are presented in Section 4. Conclusions are finally outlined in Section 5.

2. Theoretical background

In this section, some classic reversible information hiding algorithms using image interpolation are reviewed, including NMI method [11], INP on maximum difference values [13], High Capacity Reversible Steganography using multilayer embedding (CRS) [18] and Reversible Data Hiding Scheme (RDHS) [15]. Let an input image, original image, cover image (or scaling-up), and stego image be I_i, O_i, C_i and S_i, respectively.

2.1. Neighbor Mean Interpolation (NMI)

The NMI method calculates the mean based on the neighboring pixel values, and inserts it into the blanks of scaling-up image C_i as a pixel. The calculation process of NMI method is as follows: for a 3×3 overlapping sub-block, $C_i(0, 0) = O_i(0, 0)$, $C_i(0, 1) = (O_i(0, 0) + O_i(0, 2))/2$, $C_i(1, 0) = (O_i(0, 0) + O_i(2, 0))/2$ and $C_i(1, 1) = (C_i(1, 0) + C_i(0, 1) + O_i(1, 1))/3$. A large amount of secret information can be embedded by the NMI method while maintaining good image quality. The experimental results of NMI method show that the average stego image quality is 24.44 (dB) measured by peak signal-to-noise ratio (PSNR), which is superior to the similar algorithms proposed before. Meanwhile, the NMI method gets the advantages of high speed and low time complexity. Therefore, the NMI method is appropriate for application of interpolation calculation with a large number of images. Please refer to [11] for the more detailed descriptions and contents of embedding and extracting procedures.

2.2. Interpolation by Neighboring Pixels (INP) on maximum difference values

At first, the INP scheme changes a $H \times G$ size input image I_i down to 1/4 (that is, $H/2 \times G/2$) of itself, and uses the reduced scale image as an original image O_i. Secondly, the INP method uses an interpolation method to enlarge O_i to form a four times image (that is a $H \times G$ cover image C_i). And then, after embedding secret information, a $H \times G$ stego image S_i comes into being from the cover image C_i. The authorized users can recover the original image O_i after the embedded secret information is extracted from the stego image S_i. Please refer to [13] for the more detailed descriptions and contents of embedding and extracting procedures.