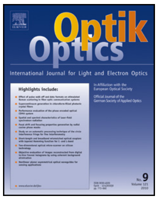
Optik 127 (2016) 5950–5960

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo



Original research article

Ownership protection for progressive image transmission with reversible data hiding and visual secret sharing

Hsiang-Cheh Huang[a], Yuh-Yih Lu[b,*], Jiun Lin[a]

[a] National University of Kaohsiung, No. 700 University Road, Kaohsiung 81148, Taiwan, ROC[1]
[b] Minghsin University of Science and Technology, No.1, Xinxing Rd., Xinfeng, Hsinchu 30401, Taiwan, ROC

ARTICLE INFO

Article history:
Received 1 November 2015
Accepted 6 April 2016

Keywords:
Reversible data hiding
Color planes
Progressive transmission
Visual secret sharing

ABSTRACT

Progressive transmission of multimedia can be commonly encountered in multimedia communications. In this paper, we develop the reversible data hiding and visual secret sharing schemes for ownership protection of digital images, which is suitable for meeting the characteristics of progressive image transmission (PIT). With progressive transmission, data can be partitioned into base and enhancement layers. For reversible data hiding, we consider carefully altering the difference values between base and enhancement layers in the color planes of progressively transmitted images. Moreover, visual secret sharing has integrated into proposed algorithm to guarantee the ownership of images. Simulation results with our schemes have demonstrated the better performances over relating methods, and the effectiveness for practical implementations with color images. Consequently, the ownership protection of progressively transmitted media can be retained, and original color image can be recovered.

1. Introduction

Progressive image transmission (PIT) [1] can be commonly encountered while browsing the Internet. Due to the variation of bitrate for transmission, PIT provides an effective means to let users acquire the low resolution image first, and then obtain the high resolution original image with the reception of progressively transmitted data. With the enormous amount of digital images on the Internet, security issues may be another concern in addition to the effective transmission scheme with PIT. Hence, the ownership protection for progressively transmitted images can consequently be developed.

Data encryption is one of the traditional ways to make ownership protection possible [2]. By doing so, encrypted images look like random noise patterns, and it can easily cause the suspicion by viewers. Besides data encryption, watermarking or data hiding belongs to another practical scheme for ownership protection, which is also commonly employed [3,4]. Because watermarking introduces irreversible degradation of original images, it would be constructive if original image can be recovered back from marked image in addition to ownership protection, and it is the origin of the development of reversible data hiding.

Reversible data hiding is regarded as a new branch in watermarking researches [5,6]. For reversible data hiding, secret information is embedded into original image at the encoder. At the decoder, both the original image and the secret infor-

[*] Corresponding author.
E-mail addresses: huang.hc@gmail.com (H.-C. Huang), yylu@must.edu.tw (Y.-Y. Lu).

[1] http://sites.google.com/site/hch888dr/.

http://dx.doi.org/10.1016/j.ijleo.2016.04.011

mation should be perfectly separated from the marked image, with the provision of reasonable amount of side information. Because the original image and embedded secret can be recovered at the decoder, it is similar to the reversible reaction in chemistry, and people name this category 'reversible data hiding'.

By following the concepts from data encryption or cryptography, a new way named visual cryptography has emerged [7,8]. For visual secret sharing, a binary image containing the ciphers can be divided into shares at the encoder. When parts of the shares are received at the decoder, they can be stacked together to approximately recover the binary image and recognize the ciphers. With this manner, it is possible to hide the shares into different color planes for making visual cryptography possible.

In this paper, we focus on the integration of reversible data hiding and visual secret sharing for protecting the ownership of progressively transmitted images. We can intentionally alter the difference values, originated from the original image, with reversible data hiding. Binary images generated from visual cryptography can be served as the secret information to be embedded in reversible data hiding. By doing so, the advantages of both reversible data hiding and visual cryptography are utilized, and hence the ownership of progressively transmitted image can be assured.

This paper is organized as follows. In Section 2, we discuss about the fundamental schemes in reversible data hiding and visual cryptography. In Section 3 we then describe the proposed algorithm based on prediction techniques in reversible data hiding, and its integration with visual cryptography. Experimental results are demonstrated in Section 4. Finally, we conclude this paper in Section 5.

2. Fundamental schemes

2.1. Reversible data hiding

There are two conventional implementations for making reversible data hiding possible. The first one relates to the alteration of histogram of original image [9], and the other chooses to modify the difference between neighboring pixels in the original image, named the difference expansion (DE) method [10]. Both of them make good use of inherent characteristics of original images from different aspects.

On the one hand, the difference expansion (DE) method is one of the earliest schemes for reversible data hiding [6,10]. It alters the relationships between two neighboring pixels in one pair, and it has the advantage of high embedding capacity because one bit can be embedded into a pair of pixels. For an image with the size of $M \times N$, at most $1/2 \times M \times N$ bits can be reversibly embedded. However, after alteration, the luminance values of the new pair may have overflow problem, meaning that such values may be larger than 255 or may become negative. Thus, coordinates of such a pair should be recorded to prevent from performing the data embedding. The collection of coordinates or such pairs forms the side information, named 'location map', which leads to the reduction of embedding capacity.

On the other hand, the histogram-based method is famous for its ease of implementation and few overhead generated [5,9]. Histogram of original image is generated, and two parameters for reversible data hiding, or the luminance values of the peak and zero points in the histogram, are determined first. Within the histogram, the luminance value corresponding to the maximal occurrence is called the peak point, and the first luminance value with no occurrence, which is larger than that of the peak point, is named the zero point. The portion between peak and zero points are intentionally altered to make data embedding possible. There is no need to prepare for the location map with the histogram-based techniques. Besides, it also has the advantage of guaranteed quality of at least 48.13 dB in PSNR for the marked image [6], which may be required for certain kinds of applications such as medical images. However, due to the guaranteed quality, embedding capacity is limited.

A recently developed branch in reversible data hiding, named prediction-based schemes [11], combines the advantages between the DE-based and histogram-based schemes. With DE, the difference values should be produced first, and then a large amount of secret bits can be embedded by altering the difference values. Considering the ease of implementation with the histogram-based scheme, by use of altering the difference histogram seems a straightforward way for reversible data hiding. Before the embedding of data, in addition to taking the difference of luminance values between two neighboring pixels, how to effectively produce the difference value would be a critical issue, because it may directly influence the performance of proposed method. With the proposed algorithm, we take the relationships between the base and enhancement layers into consideration, and perform the prediction-based scheme to obtain the difference values. Next, difference histogram can be obtained, and with similar concept to histogram-based reversible data hiding, data embedding can be performed subsequently.

2.2. Visual cryptography

Visual cryptography, or visual secret sharing (VSS), was firstly proposed in 1994 [7]. It enables distributing sensitive visual materials to the n involved participants to the scheme, as the produced n shares, which look noise-like, do not reveal any information. Only the qualified sets of k participants, $k \leq n$, are enabled to combine together to reconstruct the image containing the secret message by simply stacking together the shares they own. With this manner, it leads to the (k, n) VSS scheme. For practical applications in this paper, we consider a (2, 2) VSS scheme, where the original image is shared into