Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

A data hiding scheme using pixel value differencing and improving exploiting modification directions

Shu-Yuan Shen [a,b], *Li-Hong Huang* [a,c,*]

[a] *College of Mathematics and Econometrics, Hunan University, Changsha, Hunan 410082, China*
[b] *School of Software South China Normal University, Guangzhou 510631, China*
[c] *Institute of Applied Mathematics and Intelligent Information Processing, Hunan Women's University, Changsha, Hunan 410004, China*

ARTICLE INFO

Article history:
Received 5 January 2014
Received in revised form
15 June 2014
Accepted 28 July 2014
Available online 14 August 2014

Keywords:
Data hiding
Hilbert curve
PVD
Optimization problem
Exploiting modification directions

ABSTRACT

The fundamental requirements of information hiding systems are good visual quality, high hiding capacity, robustness and steganographic security. In this paper, we propose a new data hiding method which can increase the steganographic security of a data hiding scheme because it is less detectable by RS detection attack and the steganalytic histogram attack of pixel-value difference. In our method, a cover image is first mapped into a 1D pixels sequence by Hilbert filling curve and then divided into non-overlapping embedding units with two consecutive pixels. Because the human eyes tolerate more changes in edge and texture areas than in smooth areas, and pixel pairs in these areas often possess larger differences, the method exploits pixel value differences (PVD) to estimate the base of digits to be embedded into pixel pairs. Pixel pairs with larger differences are embedded with digits in larger base than those pixel pairs with smaller differences to maximize the payload and image quality. By using an optimization problem to solve the overflow/underflow problem, minimal distortion of the pixel ternaries cause by data embedding can be obtained. The experimental results show our method not only to enhance the embedding rate and good embedding capacity but also to keep stego-image quality.

1. Introduction

Data hiding techniques can be carried out in three domains (Langelaar et al., 2000), namely, spatial domain (Mielikainen, 2006), compress domain (Chang et al., 2006, 2009, 2009a), and frequency domain (Lee et al., 2007). Each domain has its own advantages and disadvantages in regard to hiding capacity, execution time, and storage space. The fundamental requirements of information hiding systems are good visual quality (i.e., image quality), high hiding capacity, robustness, and steganographic security (i.e., statistically undetectable) (Langelaar et al., 2000).

Designing a new data hiding system achieving good visual quality, high hiding capacity, robustness, and steganographic security is a technically challenging problem. Thus, there are different approaches in designing data hiding systems in the literature. Some of these approaches are as follows. The first

* *Corresponding author*. College of Mathematics and Econometrics, Hunan University, Changsha, Hunan 410082, China.
E-mail addresses: ssyuan02@126.com (S.-Y. Shen), lhhuang@hnu.edu.cn (L.-H. Huang).
http://dx.doi.org/10.1016/j.cose.2014.07.008

approach is to increase hiding capacity (also called embedding capacity or payload) while maintaining a good visual quality or at the cost of lower visual quality (Lan and Tewfik, 2006). This approach is appropriate to applications where high hiding capacity is desired. The second approach purposes to devise a robust data hiding scheme (Ni et al., 2008). This design serves robust watermarking systems. The third approach aims at enhancing visual quality while keeping the same hiding capacity or at the cost of lower hiding capacity (Ni et al., 2006). The fourth approach intends to devise a data hiding scheme with high embedding efficiency (Fridrich et al., 2006; Mielikainen, 2006; Westfeld, 2001). This approach can increase the steganographic security of a data hiding scheme because it is less detectable by statistical steganalysis (Fridrich et al., 2007).

In recent years many researchers are more enthusiastic to improve the embedding efficiency and decrease the possibility of detection. Least-significant-bit (LSB) matching is the conventional efficient steganography method, and it is proved much more difficult to detect than simple LSB replacement.

To defeat the histogram based steganalysis methods, many efforts have been made by researchers to protect the histograms of images. One of the first solutions to defeat these attacks was LSB matching. LSB matching increases or decreases the pixel values with the same probabilities when the least significant bit of the pixel value is not equal to the message bit. In 2006, Mielikainen (2006) developed a pairwise LSB matching method to improve the embedding efficiency. Nevertheless, Mielikainen's scheme is incomplete because the scheme only exploits two modification directions for secret data embedding.

Tan and Li (2012) showed that the readjusting step of LSB matching revised-based edge-adaptive (Luo et al., 2010) produces some effects in the long exponential tail of the histogram of the absolute difference of the pixel pairs. By using these effects, they proposed a steganalysis technique that could detect stego images and could estimate the used threshold in the data hiding process. In addition, Ghazanfari et al. (Qazanfari and Safabakhsh, 2012, 2013) proposed an adaptive steganography method based on the LSB matching which increases the capacity up to 150% (Qazanfari and Safabakhsh, 2012) and 158% (Qazanfari and Safabakhsh, 2013). Their second work (Qazanfari and Safabakhsh, 2013) is the extension of their previous scheme (Qazanfari and Safabakhsh, 2012) into the DCT domain. The $LSB^{=}$ method suggested by Wu et al. (Wu, 2008) preserved the image histogram in spatial domain by embedding some extra bits in images. This method, however, results in statistical and perceptual distortions. A new technique for image steganography, called LSB^{++}, was proposed in Kazem et al (2011), which improves the LSB^{+} by keeping some pixels from changing, results in reducing the number of extra bits. Their later work (Qazanfari and Safabakhsh, 2014), they improved the LSB^{++} method by proposing a technique to distinguish the sensitive pixels and keep them from extra bit embedding, as the embedding process causes fewer traces in the co-occurrence matrixes.

To fully exploit different modification directions for secret data embedding. Zhang and Wang (2006) also proposed the exploiting modification direction (EMD) method, which employs n pixels as an embedding unit, and embeds digits in $2n + 1$ base. Its maximum payload is $1/2\log_2 5 \approx 1.161$ bpp when $n = 2$. Zhang and Wang claimed that the modification directions of Mielikainen's scheme are not explored fully. Specifically, the PSNR value of the EMD method is slightly smaller than that of Mielikainen's scheme at hiding capacity of 1 bpp. In addition, for $n = 2$, Zhang and Wang's method only utilizes four modification directions. Kieu and Chang (2011) (FEMD) proposed a novel extraction function (also called the modified extraction function) by modifying the extraction function proposed by Zhang and Wang (2006). The modified extraction function allows the proposed method to exploit eight modification directions for embedding secret data, restrict the embedding distortion into a square of various sizes (e.g. 2×2, 3×3, and so on) and use the minimum distortion embedding (MDE) process. By this way, the proposed method can achieve various hiding capacities and good visual qualities compared to two recently published works, namely Mielikainen's method (Mielikainen, 2006), Zhang and Wang's method (Zhang and Wang, 2006). To solve the irreversibility of the EMD method in (Zhang and Wang, 2006; Qin et al. 2014) proposed a novel data hiding scheme based on EMD with reversibility by using two steganographic images, which can also achieve satisfactory performances of the hiding capacity and the stego image quality.

Inspired by EMD, Chao et al. (2009) proposed a diamond encoding (DE) method to greatly improve the payload of EMD. DE employs a search region of $B = 2k^2 + 2k + 1$ elements to increase the payload because digits in base B can be embedded into a pixel pair, where $k \geq 1$. A larger k indicates that a larger payload can be embedded with greater image distortion. DE employs an extraction function to generate diamond characteristic values (DCV), and uses an embedding parameter k to control the payload. A digit in a B-ary notational system can be concealed into two pixels by modifying the pixel pairs according to their DCV's neighborhood set. However, DE can't embed digits in any notation system and the distortion caused by DE is larger than some other embedding methods with the same payload. Although DE has these advantages, it does not allow embedding digits in multiple bases, Which is the essential requirement for an embedding method with the consideration of HVS. Besides, to prevent the overflow and underflow problems from occurring, the pixel values exceed 0 or 255 will be added or subtracted by B to keep the pixel values within the range [0, 255]. This adjustment may cause a large distortion, and may result in image noise when the embedding parameter k is large. For example, if $k = 5$, then the base B used to conceal data is $2 \times 5^2 + 2 \times 5 + 1 = 61$. However, a pixel value that is subtracted by 61 or added by 61 will cause a large distortion.

The aforementioned methods regard all pixels within an image can tolerate equal amounts of changes without causing visual artifacts to an observer. However, the tolerance of the changes to pixel values is different in smooth and edge areas according to human visual system (HVS). Based on the fact that edge areas can tolerate more severe changes than smooth areas, edge adaptive schemes have been proposed, which conceal more data in edge areas to acquire more embedding capacity whereas conceal less data in smooth area to preserve the visual quality. Moreover, in the kieu-Chang's scheme