Information Processing Letters ••• (••••) •••–•••

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Signed digit data hiding scheme

Wen-Chung Kuo [a], Chun-Cheng Wang [b], Hong-Ching Hou [c]

[a] Department of Computer Science and Information Engineering, National Yunlin University of Science & Technology, Taiwan, ROC
[b] Graduate School of Engineering Science and Technology Doctoral Program, National Yunlin University of Science & Technology, Taiwan, ROC
[c] Department of Computer Science and Information Engineering, National Formosa University, Huwei 632, Taiwan, ROC

ARTICLE INFO

Article history:
Received 25 March 2015
Accepted 6 August 2015
Available online xxxx
Communicated by S.M. Yiu

Keywords:
Steganography
Data hiding
LSB replacement
EMD (Exploiting Modification Direction)
MSD (Modified Signed-Digit)

ABSTRACT

The EMD (Exploiting Modification Direction) method by Zhang and Wang uses $(2n+1)$-ary notation to achieve secret message embedding into a cover image. However, the maximum capacity of this method is 1.16 bpp for cover pixel number $n=2$. Its embedding capacity rapidly decreases when selected pixels increase. In order to improve this shortcoming, a new data hiding scheme based on MSD (Modified Signed-Digit) is proposed. There are three major contributions in this proposed scheme. The first is only $\lceil \frac{n}{2} \rceil$ pixels will be modified and the value is $+1$ or -1 when the group has n pixels. Secondly, the embedded capacity maintains at least 1 bpp when n is increasing. The last is the stego image quality is better than 52 dB when the cover image's pixels are greater than 4 for each group.

1. Introduction

Due to the rapid growth of computer and internet technology, multimedia such as images, audio, and video are distributed through the Internet. Protecting digital content security has become a very interesting research topic. Generally, there are two common methodologies for data security: cryptography and steganography. Specifically, steganography hides personal data behind a meaningful image so an unintended observer will not be aware of the existence of the hidden secret message. Until now, many data hiding schemes based on different embedding methods (such as direct replacement or indirect embedding) have been proposed [3,4,6,8–11,14,16].

For direct replacement, the most common data hiding technique is the least significant bit replacement method (LSB). This scheme is very simple, fast and has good stego image quality, but is not secure against bit-plane attack. Alternatively, indirect embedding employs an extraction function such as the Exploiting Modification Direction (EMD) [16]. In 2006, Zhang and Wang proposed a new data hiding scheme based on EMD. The major characteristic of this scheme is that they used n adjacent pixels for a group and only one pixel in group is changed to match the secret data. Therefore, the Zhang-Wang scheme has very good image quality but it needs to transform binary data to $(2n+1)$-ary to get the maximum capacity. The largest embedding capacity is 1.16 bpp (bits per pixel) when $n=2$ and its capacity is less than 1 bpp when $n \geq 3$. Previously, many EMD-type schemes [3,6,9] were proposed to improve embedding capacity or enhance embedded data security. In 2007, Lee et al. proposed the LWC scheme [9] to improve the embedding capacity. LWC scheme uses two pixels for a group and an 8-ary extraction function. Compared to Zhang-Wang scheme, when $n=2$, the embedding capacity of the LWC scheme is larger than 1.16 bpp because the modulus of the Zhang-Wang and LWC schemes are 5-ary and 8-ary, respectively. Note LWC scheme only uses two pixels in a group and cannot use more. Recently, Kuo and Wang [6] provided a novel extraction function and a data hiding scheme based on Generalized Exploiting Modification Direction (GEMD). It maintains high embedding capacity and also has adjustable pixel group size. Accord-

E-mail address: simonkuo@yuntech.edu.tw (W.-C. Kuo).

http://dx.doi.org/10.1016/j.ipl.2015.08.003
0020-0190/

ing to our analysis, all pixels of the group may be modified when secret data is embedded in these EMD-type schemes.

To improve this shortcoming, we will propose a new data hiding scheme based on MSD (Modified Signed-Digit) in this paper. There are three major contributions of this proposed scheme. One is that only $\lceil \frac{n}{2} \rceil$ pixels will be modified and the value is $+1$ or -1 when the group has n pixels. Secondly, embedded capacity always maintains at least 1 bpp when n is increasing and the other is that the stego image quality is better than 52 dB when the cover image's pixels are greater than 4 for each group. According to the experimental results, our proposed scheme keeps the advantages of the EMD data hiding scheme and enhances embedding capacity while also preventing disclosure from some attacks such as visual attack and RS attack.

The rest of paper is organized as follows: In Section 2, some data hiding schemes are reviewed briefly and the sparse modified signed-digit (MSD) representation method is introduced. In Section 3, the new data hiding method based on MSD method is described. Experimental results and security analysis are provided in Section 4. Finally, the conclusion is given in Section 5.

2. Review of data hiding schemes and MSD representation

In this section, we will review data hiding schemes from two different embedding approaches. For direct replacement method, the least significant bit replacement will be introduced. For indirect embedding using the extraction function, the EMD data hiding scheme [16] and GEMD data hiding scheme [6] will be described. In addition, we will introduce the sparse modified signed-digit (MSD) representation method to present the number which no two adjacent entries are nonzero.

2.1. LSB data hiding

The least significant bit replacement method is the most common data hiding technique because the scheme is very simple, fast and has good stego image quality. There are two phases in the LSB data hiding scheme: First, the secret information is converted from decimal to binary. Then, the k-rightmost bits of each pixel are replaced sequentially with the binary data of the secret stream.

Embedding Algorithm for the LSB replacement method [7]
Input: cover image I_C and secret data $(S)_{10}$
Output: stego image I_S

(**LSB-1**) Convert the secret data $(S)_{10}$ to binary stream $(S)_2 = (s_n, s_{n-1}, \ldots, s_2, s_1, s_0)_2$, where $s_j \in \{0, 1\}$.
(**LSB-2**) Calculate secret $s = \sum_{j=0}^{k-1} s_j \times 2^{k-1-j}$ and $y_i = x_i - (x_i \bmod 2^k) + s$ for each pixel i to embed k binary bits, where y_i is the ith stego pixel of I_S.

Extraction Algorithm for the LSB replacement method [7]
Input: stego image I_S
Output: binary secret data stream S

(**ELSB-1**) For each stego pixel i, calculate the secret $s = y_i \bmod 2^k$.
(**ELSB-2**) Transform s to binary secret data stream S.

Example 1. Given four pixels $(201, 195, 192, 203)$ and secret data $S = [1, 1, 0, 1, 0, 0, 1, 0]$, embedded two bits for each pixel to get stego pixels $(203, 197, 196, 202)$ from following steps:

(**Step 1**) Calculate $S^* = [s_1, s_2, s_3, s_4] = [3, 1, 0, 2]$.
(**Step 2**) By using the LSB algorithm, we can get the stego pixels $(203, 193, 192, 202)$.

The secret data can be recovered.

The LSB replacement hiding technique is simple and fast, and has good imperceptibility (PSNR) and capacity. However, this data hiding scheme is not secure because attackers can determine the secret easily by analyzing the bit-plane.

2.2. Data hiding scheme based on EMD

In 2006, Zhang and Wang introduced a new extraction function as Eq. (1) and then proposed a data hiding scheme based on the exploiting modification direction method [16].

$$f_e(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} x_i \times i \bmod (2n+1), \tag{1}$$

where x_i is the i-th pixel value and n is the number of pixels.

The characteristic of the EMD-scheme uses the relationship of n adjacent pixels to embed a $(2n+1)$-ary secret data stream. For example, the 5-ary secret data stream will be embedded in two adjacent pixels, i.e., it at most modifies one of two adjacent pixels by adding one, subtracting one, or doing nothing. In this method, the two following functions are introduced.

- $O_{EMD}(\cdot)$ is a function which gives all n-tuples $(x_1, x_2, \ldots, x_n)$ obtained from partitioning the image I_C into the non-overlapping n-pixel blocks by scanning each line of pixels from left to right and from top to down manner.
- $O_{EMD-S}(\cdot)$ is a function which can obtain (2^{n+1})-ary data s from secret data stream S for each block.

Embedding Algorithm for the EMD Scheme
Input: cover image I_C and binary secret data stream S
Output: stego image I_S

(**EMD-1**) Obtain all n-pixel blocks $(x_1, x_2, \ldots, x_n)$ from I_C by using $O_{EMD}(I_C)$ and secret data s from $O_{EMD-s}(S)$.
(**EMD-2**) For each block, calculate $t = f_e(x_1, x_2, \ldots, x_n)$ by Eq. (1).
(**EMD-3**) Calculate the difference $d = (s - t) \bmod (2n+1)$.