Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

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

Binary power data hiding scheme

Wen-Chung Kuo[a], Chun-Cheng Wang[b], Yu-Chih Huang[c]

[a] *Department of Computer Science and Information Engineering, National Yunlin University of Science & Technology, No. 123 University Road, Section 3, Douliou, Yunlin 64002, Taiwan, ROC*
[b] *Graduate School of Engineering Science and Technology Doctoral Program, National Yunlin University of Science & Technology, Taiwan, ROC*
[c] *Department of Information Management, Tainan University of Technology, No. 529, Zhongzheng Rd., Yongkang District, Tainan City 71002, Taiwan, ROC*

ARTICLE INFO

Article history:
Received 10 August 2014
Received in revised form 23 March 2015
Accepted 10 July 2015

Keywords:
Data hiding
General exploiting modification direction(GEMD)
Signed-digit method
Embedding capacity

ABSTRACT

In 2006, Zhang and Wang developed the EMD (exploiting modification direction) method for embedding secret message into pixels. Their scheme gives a maximum capacity of 1.16 bpp (bits per pixel) when the cover pixel number is 2. However, the embedding capacity rapidly decreases when the selected pixels increase. In addition, the binary data must be converted to a different radix before it is embedded. In this paper, we will propose a binary power data hiding scheme for digital images. According to our analysis, there are four major contributions in this proposed scheme: enhanced embedding data speed, embedded capacity of at least 1 bpp, stego image quality is better than 51 dB when the number of cover image pixels approach to infinity in a pixel group and it can prevent visual attack and RS attack.

© 2015 Elsevier GmbH. All rights reserved.

1. Introduction

The rapid growth of information and technology allows multimedia such as images, audio, and video to be transmitted over the Internet. However, there is often private personal information included in this multimedia. How to maintain digital content security has become a very interesting research topic. Generally speaking, the two common methodologies of cryptography and steganography are used to prevent data security. In particular, steganography can hide 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 [2,3,6,9,12,14,15,19].

For direct replacement, the most common data hiding technique is the least significant bit replacement method (LSB). The LSB scheme is very simple, fast and has good stego image quality. Unfortunately, it is not secure against the bit-plane attack. Alternatively, indirect embedding employs an extraction function such as the exploiting modification direction (EMD) method.

In 2006, a new data hiding scheme based on EMD was proposed by Zhang and Wang [19]. The major contribution of this paper is very good image quality compared to the conventional LSB scheme, but its embedding capacity decreases quickly when the pixel group is large. Since then, many EMD-type schemes [2,6,8,12] were proposed to improve the embedding capacity. In 2007, Lee et al. [12] proposed an improved scheme (LWC) where three binary bits can be embedded into two pixels as a group. The most important contribution of the LWC scheme is the secret binary data stream can be embedded directly. However, the number of pixels for each group is restricted to two. That is to say, the LWC scheme loses the flexibility of changing pixel group size compared with EMD. To overcome this disadvantage, the general EMD (GEMD) data hiding scheme [6] was proposed by Kuo and Wang in 2013. The major contributions of this scheme are the flexible pixel group size and also the ability to embed the binary secret data steam directly without conversion. Obviously, the LWC scheme structure is the special case of Kuo-Wang scheme. Recently, Kieu and Chang [2] proposed a robust data hiding scheme based on the fully exploiting modification direction (FEMD) to improve data hiding capacity from 1 bpp to 4.5 bpp (bits per pixel) while maintaining good stego image quality. However, they use a search matrix method to embed the secret data and the problem of overflow is not discussed in detail. In order to improve on these shortcomings, a new data hiding scheme based on the *formula fully exploiting modification directions* method is proposed in [7].

Moreover, in binary system, the multiple operation is very easier than in decimal. As we know, no real binary EMD data hiding scheme has been proposed where the coefficient and modulus are radix 2. In this paper, we propose a binary power data hiding scheme where the coefficient and modulus of the extraction function are binary power which can directly utilize the binary secret data stream and speedup embedding or extraction. There are four

E-mail address: t00232@mail.tut.edu.tw (Y.-C. Huang).

http://dx.doi.org/10.1016/j.aeue.2015.07.007
1434-8411/© 2015 Elsevier GmbH. All rights reserved.

major contributions in this proposed scheme: enhanced embedding speed, embedded capacity of at least 1 bpp when the number of pixels in a group increases, stego image quality is better than 51 dB when the number of cover image pixels approach to infinity in a pixel group and it can prevent the modern attacks such as visual attack and RS attack.

The rest of paper is organized as follows: in Section 2, some data hiding schemes such as EMD, GEMD and MSD (modified signed-digit) are reviewed briefly. In Section 3, a new data hiding method based on binary power is described. Experimental results and security analysis are provided in Section 4. Finally, concluding remarks are given in Section 5.

2. Review data hiding schemes

Previously, LSB and many EMD-type data hiding schemes have been proposed. In this section, we review a selection of data hiding schemes such as LSB along with the EMD, GEMD and MSD data hiding schemes proposed by Zhang–Wang [19], Kuo–Wang [8] and Kuo et al. [4], respectively. We will describe the embedding algorithm and then give an example to explain it for each reviewing scheme.

2.1. LSB data hiding scheme

In the LSB data hiding scheme, we convert the pixel values of the cover image and the secret data from decimal to binary bitstream. Then, we sequentially replace the k-rightmost bits of each pixel with the binary data of the secret stream. The LSB algorithm [5]is as follows:

Algorithm LSB (embedding algorithm for LSB replacement)
Input: cover image I_C and binary secret data stream M
Output: stego image I_S

LSB-1 For each pixel, transform k bits to decimal value m.
LSB-2 Compute stego image's pixel $y = x - (x \bmod 2^k) + m$.
LSB-3 Repeat LSB-1 until all secret data are embedded.

Example 1. Given grayscale cover image $I_C = \{23, 26, 27, \ldots\}$ and binary secret data stream $M = 10010011\ldots_2$, the stego image is calculated as $I_S = \{22, 25, 24, \ldots\}$ using LSB scheme.

Step 1 Transform 2 bits 10_2 to decimal value $m = 2$.
Step 2 Compute the stego pixel $y = 23 - (23 \bmod 2^2) + 2 = 22$.
Step 3 Repeat the above steps until all secret data is embedded.

2.2. EMD data hiding scheme

In order to enhance embedding capacity, Zhang and Wang provided a new extraction function Eq. (1) and a robust data hiding scheme based on EMD [19].

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

where x_i is the ith pixel value and n is the number of pixels.

The EMD-scheme uses the relationship of n adjacent pixels to embed a $2n+1$ radix secret data stream. For example, the 5 radix secret data stream will be embedded in two adjacent pixels. In other words, it only modifies one of two adjacent pixels by adding one, subtracting one, or no action.

Algorithm EMD (Embedding algorithm for EMD Scheme)
Input: the grayscale cover image I_C and binary secret data stream M
Output: stego image I_S

EMD-1 Divide I_C into non-overlapping n-pixel blocks and transform M to $(2n+1)$-ary secret data stream M'.
EMD-2 Get the cover pixel block and compute $t = f_e(x_1, x_2, \ldots, x_n)$ by Eq. (1).
EMD-3 Access $(2n+1)$-ary data m from M' and compute the difference $d = (m - t) \mathrm{mod}(2n+1)$.
EMD-4 If $d = 0$, then $y_i = x_i$, for $\forall i \in \{1, 2, \ldots, n\}$,elseif $(d < n)$, then $y_d = x_d + 1$ and $y_i = x_i$, for $\forall i \in \{1, 2, \ldots, n | i \neq d\}$else $y_{2n+1-d} = x_{2n+1-d} - 1$ and $y_i = x_i$, for $\forall i \in \{1, 2, \ldots, n | i \neq (2n+1-d)\}$.
EMD-5 Go to step EMD-2 until all secret data is embedded.

where x_i is the cover image's pixel and y_i is the stego image's pixel. These two parameters (x_i and y_i) are used to GEMD algorithm, MSD algorithm and the proposed binary-EMD algorithm.

Example 2: Given three grayscale pixels of cover image (23, 26, 27) and binary secret data stream $M = 100_2$,the stego image's pixels are (23, 27, 27) using the EMD scheme when $n = 3$.

Step 1 Divide I_C into non-overlapping 3-pixel blocks (23, 26, 27) and transform M to $M' = 4_7$.
Step 2 Get the cover pixel block and compute $t = f_e(23, 26, 27) = 2$.
Step 3 Access 7-ary data $m = 4$ and compute the difference $d = (4 - 2) \bmod 7 = 2$.
Step 4 Since $d = 2 < 3$, we compute $y_2 = x_2 + 1 = 27$, $y_1 = x_1 = 23$, $y_3 = x_3 = 27$.

From the EMD algorithm, the largest embedding capacity of EMD is $\log_2(5)/2 = 1.16$ bpp (bits per pixel) when using radix 5. If the number of pixels in a group increases (i.e. n increases) then the hiding secret data rate will decrease [19]. For example, the hiding secret data rate is $\log_2(21)/10 = 0.439$ bpp when $n = 10$(10 pixels in the pixel group). For the purpose of enhancing secret data embedding capacity, many EMD-type data hiding schemes were proposed [3,8,10–13,17].

2.3. The general EMD method

In order to improve the embedding capacity of the EMD method and embed the binary secret data stream directly, a GEMD (general EMD) data hiding scheme was proposed by Kuo and Wang in 2013 [8]. Previous work by Lee et al. [12]in 2007, where the parameter n is limited to 2, is a special case of GEMD scheme.

Algorithm GEMD (Embedding algorithm for Kuo–Wang scheme)
Input: the grayscale cover image I_C and binary secret data stream M
Output: stego image I_S

GEMD-1 Divide I_C into non-overlapping n-pixel blocks.
GEMD-2 Get the cover pixel block and calculate $t = f_g(x_1, x_2, \ldots, x_n)$ where

$$f_g(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} x_i \times (2^i - 1) \, mod \, 2^{n+1}. \tag{2}$$

GEMD-3 Access $(n+1)$ bits secret data from M and transform to 2^{n+1}-ary data m. Compute the difference $D_g = (m - t) \bmod 2^{n+1}$.
GEMD-4 If $D_g = 2^n$ then $k = 1$; else if $(D_g < 2^n)$ then $k = 2$ else $k = 3$.
GEMD-5 Switch (k)

Case 1 Let $y_n = x_n + 1, y_1 = x_1 + 1$ and $y_i = x_i$, for $\forall i \in \{2, 3, \cdots, n-1\}$.
Case 2 Transform D_g to $(b_n b_{n-1} b_{n-2} \cdots b_1 b_0)_2$,for $i = n - 1$ to 1 doif $(b_i = 0$ and $b_{i-1} = 1)$ then $y_i = x_i + 1$;else if $(b_i = 1$ and $b_{i-1} = 0)$ then $y_i = x_i - 1$;otherwise, $y_i = x_i$end.

Download English Version:

https://daneshyari.com/en/article/447481

Download Persian Version:

https://daneshyari.com/article/447481

Daneshyari.com