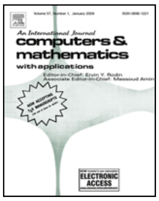
Computers and Mathematics with Applications 60 (2010) 319–325

Contents lists available at ScienceDirect

Computers and Mathematics with Applications

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



Improved modification direction methods

H.J. Kim [a,*], C. Kim [b], Y. Choi [a], S. Wang [c], X. Zhang [c]

[a] *Department of Information Management and Security, Korea University, Seoul, 136-701, Republic of Korea*

[b] *Department of Computer Science and Engineering, Sejong University, Seoul 143-747, Republic of Korea*

[c] *School of Communication and Information Engineering, Shanghai University, Shanghai 200072, China*

ARTICLE INFO

Keywords:
Data hiding
Number theory
Steganography

ABSTRACT

The original exploiting modification direction (EMD) method proposed by Zhang and Wang is a novel data hiding technique which can achieve large embedding capacity with less distortion. The original EMD method can hide $(2n+1)$-ary numbers by modifying at most one least-significant bit (LSB) of n pixel values. The proposed methods in this paper, 2-EMD and EMD-2, modify at most two pixels of the LSB values. Efficiency of the proposed methods is shown theoretically and through experiments. The 2-EMD and EMD-2 can hide even larger numbers than the EMD with similar distortion under the same conditions. This paper shows that the EMD-2 is much better than the EMD, and slightly better than 2-EMD when n is 3, 4 and 5. The way to generate basis vector can be used for the generalization of the n-EMD and EMD-n where $n > 1$.

1. Introduction

Two important issues of data hiding techniques are preserving good image quality and increasing the embedding capacity altogether at the same time. However, this is an irreconcilable requirement. If we try to reduce image distortion, we have to sacrifice the embedding capacity. If we increase embedding capacity, image quality gets worse. The first generation approach has modified the least-significant bit (LSB) values. This simple method is called LSB replacement technique. This method can embed as many bits as the total number of pixels. However, statistical analysis based on the chi-square test using neighboring pixel value pairs can detect the presence of a hidden message [1]. Two values whose binary representations differ only in the LSB level are called a pair of values. For example, two consecutive numbers – 70 (i.e., 01000110 in binary representation) and 71 (i.e., 01000111 in binary format) – are a pair of values. In general, the frequencies of two neighboring values are statistically rarely equal in number. However, after the LSB replacement embedding, observation of Westfeld and Pfitzmann [1] conclude that most of their frequencies are getting closer. If the message to be hidden is really random, the frequencies of the pairs become nearly equal after embedding message due to its true randomness. If the message is not random, the pair of values may be normal and does not give us any hint. However, practitioners do not want to hide plain text. They believe that hiding plain text is more dangerous than cipher text. As a conclusion, the chi-square test is an effective technique against LSB modification methods.

Therefore, reducing the embedding capacity becomes an alternative solution to reduce image degradation. Tseng et al. [2] hide as many as $\lfloor \log_2(mn+1) \rfloor$ bits of data in an $m \times n$ binary image block by changing at most two bits in the block. Matrix encoding technique in F5 algorithm [3] changes at most one LSB value to embed k bits into p pixels where $p = 2^k - 1$. Thus, this encoding technique uses a $(1, p, k)$ Hamming code. Modified matrix encoding technique [4] uses a $(2, p, k)$ Hamming

[*] Corresponding author. Tel.: +82 2 3290 4895.
E-mail addresses: khj-@korea.ac.kr (H.J. Kim), mipsan@paran.com (C. Kim), ciechoi@korea.ac.kr (Y. Choi), shuowang@shu.edu.cn (S. Wang), xzhang@shu.edu.cn (X. Zhang).

0898-1221/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.camwa.2010.01.006

Table 1
Numbers generated by a basis vector [1, 2] when n is 2 in the EMD.

	1	2
0	0	0
1	1	0
2	0	1
3	0	−1
4	−1	0

code to modify at most two pixels. This modified matrix encoding technique allows more degree of freedom than the original matrix encoding technique.

Zhang and Wang [5] has proposed a novel data hiding technique to transform the binary secret data into a stream of secret digits using a $(2n+1)$-ary notational system. Their embedding method called exploiting modification direction (EMD) uses n cover pixels to carry one secret digit in the $(2n+1)$-ary number system. The maximum possible error of the modified pixel is ± 1 because their scheme changes only one LSB value. The pixel segmentation system proposed by Lee et al. [6] can hide more large numbers by modifying two pixel values. However, image quality gets considerably degraded and worse than 8 dB.

Two new EMD methods proposed in this paper, 2-EMD and EMD-2, are very simple to implement. The embedding capacity of these methods is larger than the pixel segmentation method, and much larger than the EMD. However, the average image quality of the EMD-2 is around 52 dB which is 8 dB higher than the pixel segmentation method, but similar to the EMD and 2-EMD. The efficiency of the 2-EMD and EMD-2 is compared with the EMD under the same condition.

2. EMD embedding method

The EMD method proposed by Zhang and Wang [5] is a novel method for hiding data. Each secret digit in a $(2n+1)$-ary notational system is carried by n cover pixels, where $n \geq 2$, and at most one pixel value is increased or decreased by 1 in the EMD method. A group of pixel values is represented as a vector G, where $G_n = [g_1, g_2, \dots, g_n]$. A vector $[g_1, g_2, \dots, g_n]$ in an n-dimensional space is mapped to a value f, which is computed by Eq. (1) as a weighted sum modulo $(2n+1)$:

$$f(g_1, g_2, \dots, g_n) = \left[\sum_{i=1}^{n} (g_i \cdot i)\right] \bmod (2n+1). \tag{1}$$

No modification is needed if a secret digit d equals the extraction function f of the original pixel group. When the secret data d is not equal to f, we calculate $s = d - f \bmod (2n+1)$. If s is not larger than n, we increase the value of g_s by 1; otherwise, we decrease the value of g_{2n+1-s} by 1. Eq. (1) can be represented as an inner product between an image pixel value vector G_n and a basis vector $B_n = [1, 2, \dots, n]$ such as

$$f(g_1, g_2, \dots, g_n) = G_n \cdot B_n^T \bmod (2n+1). \tag{2}$$

The basis vector for EMD can be easily derived since only one pixel value is changed. Consider a case where n is 2. The basis vector B_2 is given as [1, 2]. Note that the number 0 can be generated by nullifying the basis vector (see Table 1) such as $0 = (0) \cdot 1 + (0) \cdot 2$. The number 1 is generated by setting the associated element 1 in the basis vector (i.e., b_1) by 1 and also nullifying the basis vector element 2 (i.e., b_2) such as $1 = (1) \cdot 1 + (0) \cdot 2$. The coefficients for the basis vector for the number 1, C_1, is [1, 0]. On the other hand, 3 can be generated by resetting the first element by 0 and setting the second element by −1 and taking modulus 5 based on Eq. (2). Thus, C_3 is $[0, -1]$. In other words, $(0) \cdot 1 + (-1) \cdot 2$ is -2, but $[(-2) \bmod 5]$ becomes 3. It is obvious that all five numbers from 0 to 4 can be generated according to Eq. (2) by the linear combination of the basis elements with their associated coefficients. Note that the five numbers are uniquely decided since we can choose 1 or −1 only once for each case.

3. The proposed EMD-2 scheme

In this section, we shall present our data hiding scheme based on $(2w+1)$-ary notational system in a group of pixels. The proposed data hiding scheme is composed of the embedding and extracting procedures, which are described below. This paper proposes a novel steganographic embedding method, EMD-2, that fully exploits the modification directions by allowing at most two pixels to be modified. In this method, modifications in different directions are used to represent different secret data, leading to a higher embedding efficiency. For the EMD-2 embedding method, the basis vector should be generated first.

3.1. Basis vector

The EMD-2 allows at most two pixels to be modified. Since one more pixel value is changed compared with the EMD, that changes at most one pixel value, the numbers generated by the new basis vector should be larger than that of the EMD. The