Information Sciences 388–389 (2017) 17–36

Contents lists available at ScienceDirect

Information Sciences

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

A novel message embedding algorithm using the optimal weighted modulus

Wei-Sung Chen, Kuo-Chen Wu, Chung-Ming Wang*

Department of Computer Science and Engineering, National Chung Hsing University, 145 Xingda Road, South District, Taichung City, 40227, Taiwan

ARTICLE INFO

Article history:
Received 7 April 2016
Revised 5 November 2016
Accepted 31 December 2016
Available online 4 January 2017

JEL classification:
L8-Industry Studies: Services
L86-Information and Internet Services
Computer Software

Keywords:
Optimal weights
Weighted modulus
Message embedding
Data hiding
Theoretically minimal distortion
Theoretically maximal capacity

ABSTRACT

This paper proposes a novel message embedding algorithm using the optimal weighted modulus. Our algorithm, referred to as a weighted modulus and abbreviated by WM(n, M), conceals an M-ary secret digit in a group of n pixels. Using an n-tuple optimal weight ensures that our algorithm can produce stego pixels with minimal pixel distortion. We adopt four steps to pragmatically accomplish the goal of message embedding. In the first step, we introduce a check-weight algorithm to systematically generate all of the valid weights. Secondly, we classify valid weights by referring to theoretically minimal distortion to produce an optimal weight. Along with the classification, we construct a pixel alteration table which simplifies the process of the message concealment through convenient vector operations. We take advantage of the homogeneous alteration table that is built in this step to decrease the distortion encountered when resolving the problem of pixel underflow or overflow. Finally, we propose a universal bit conversion scheme which transforms a serial secret bit stream into M-ary digits to minimize the transformation loss, thereby achieving maximal embedding capacity. Our algorithm accurately predicts results prior to real message concealment, effectively conveys maximal secret bits and speedily produces stego images with theoretically minimal distortion. The experimental results demonstrate that our algorithm outperforms 11 current state-of-the-art competitors. It is not detectable by the SPAM and RS steganalytic attacks.

1. Introduction

Message embedding algorithms conceal secret messages in a cover image [7,33], with applications in covert communication, security protection, authentication, secret data storing and content annotation. A preferred algorithm should provide reasonable embedding rate in bits per pixel (bpp) and minimize distortion. In addition, the algorithm should withstand steganalytic attacks, which intend to reveal any hidden messages within a stego image [33].

There are a number of message embedding algorithms available, such as the well-known least significant bit substitution (LSB), OPAP algorithm [2], and the LSB matching method [23]. The weighted modulus scheme provides an alternative approach which employs weights to conceal secret messages in a group of pixels.

Exploiting modification direction (EMD) algorithm [38] is a pioneered weighted modulus approach. The EMD algorithm can convey a $(2n + 1)$-ary secret digit in n cover pixels using the regular weight $(1, 2, \ldots, n)$. While the EMD algorithm has

* Corresponding author.
E-mail address: cmwang@cs.nchu.edu.tw (C.-M. Wang).

http://dx.doi.org/10.1016/j.ins.2016.12.049
0020-0255/

two distinct characteristics of using an optimal weight and restricting the pixel change, it also has two drawbacks. First, it only provides a limited embedding rate being less than 1.16 bpp; the larger the n is adopted, the smaller the embedding rate is offered. Second, the algorithm is restricted to conceal an even-ary secret digit; for example, EMD is inapplicable to convey an 8, 12, or 16-ary digit.

Inspired by the EMD algorithm, a number of weighted modulus algorithms were presented to increase the embedding capacity. The most competitive algorithms include APPM [11], WFMO [28], PTM [29], and MEFAG [22] schemes along with other works [4,6,12–14,16–19,21,26,39]. These weighted modulus algorithms demonstrate a common feature: the pixel alteration is removed from ± 1. The embedding capacity is increased by allowing a larger pixel alteration. Unfortunately, they also suffer from four disadvantages, as explicated in the following:

First, these algorithms adopt specific weights which are applicable to concealing a secret digit in a special notational system. In other words, they do not provide flexibility in concealing a secret digit in an arbitrary notational system; nor do they offer flexible embedding capacity. In addition, the cover pixels adopted in a pixel-group are limited, normally being no greater than 3 pixels. For example, it is difficult for these algorithms to adopt 4, 5 or 6 cover pixels to conceal a secret digit in a 36, 43 or 62-ary notational system.

Secondly, most algorithms are unaware that there exists more than single weight available for message concealment. Using various weights certainly offers greater security in hindering malicious eavesdroppers from extracting the secret messages. Worse still, most algorithms do not even notice that optimal weights do exist; they can lower the distortion, thus providing a higher stego image quality and achieving higher embedding efficiency.

It is common that the problem of pixel illegality occurs when pixels are outside of a normal range due to conveying secret messages. Most algorithms present ad hoc techniques rather than offering a systematic approach to resolving the problem of pixel illegality. This situation is perhaps due to the fact that these algorithms are not designed to achieve general-purpose message concealment. In addition, due to the lack of a systematic approach, despite solving the problem of pixel illegality, the stego pixels produced do not perform with minimal distortion.

Finally, when secret messages are a serial bit stream, we need to convert the bit stream into secret digits in the target, say T-ary, notational system before conveying these secret digits. Unfortunately, most algorithms pay little attention to the transformation subject despite the fact that a transformation loss occurs between a binary and target notational system. This means that in real implementation, it is difficult to provide maximal embedding capacity.

In this paper, we propose a novel weighted modulus message embedding algorithm. We abbreviated our algorithm by WM(n, M), where a secret M-ary digit is conveyed in a group of n pixels. Using an optimal weight, our algorithm offers concrete and pragmatic solutions for four problems encountered, while not compromising the current state-of-the art weighted modulus others. In particular, we systematically generate valid weights and effectively classify them to produce optimal weights. During the process of weight generation, we develop two auxiliary tables, allowing our algorithm to conceal secret messages producing the least embedding distortion and achieving high embedding efficiency. The experimental results demonstrate that our algorithm outperforms 11 current state-of-the-art schemes.

This paper is organized as follows. We review related works in Section 2, and present our algorithm in Section 3. In Section 4, we demonstrate our analysis to validate weights before we introduce an approach to classify them, in order to derive optimal weights. The experimental results and comparisons are presented in Section 5. Our conclusions and future work suggestions are described in the final section.

2. Related works

This section reviews related works that examine the weighted modulus for message embedding. In particular, we will elaborate only four algorithms because they provide better performance representing the most competitive works with respect to the weighted modulus algorithm. These four algorithms include the APPM [11], WFMO [28], PTM [29], and MEFAG [22] schemes due to the space limit. Nevertheless, we will compare our experimental results with 11 current state-of-the-art algorithms [6;11;12;18;19;21;22;26;28;29;39] to reveal the superiority of our WM algorithm. A detailed survey of message embedding algorithms can be referenced in literature by authors in [5,20,27].

2.1. EMD algorithm

The EMD algorithm [38] can be featured as EMD[n, $(2n + 1)$, $\boldsymbol{W}(1, 2,\ldots, n)$]. Each secret digit in a $(2n + 1)$-ary notational system is conveyed by a group of n cover pixels; at most, only one pixel is increased or decreased by 1 (± 1) using the optimal weight $\boldsymbol{W}(1, 2,\ldots, n)$.

The EMD algorithm produces a high quality stego image and the problem of pixel illegality is solved by changing the saturated pixel by 1 before conducting the secret digit embedding again. Unfortunately, the EMD algorithm offers a small payload, the maximum being appropriate to $log_2 3$ for the case when $n = 1$. Another disadvantage is that it employs a single weight and secret messages are confined to the $(2n + 1)$ notational system.

A variety of algorithms were proposed to increase the embedding capacity. The EMD-2 algorithm [14] can be featured as EMD-2[n, 9, $\boldsymbol{W}(1, 3)$] if $n = 2$ or EMD-2[n, $(10n - 13)$, $\boldsymbol{W}(1, 2, 6,\ldots, 5n - 9)$] if $n \geq 3$. Despite the weights derived being optimal, the maximal embedding rate is 1.585 bpp when $n = 2$ and the capacity decreases along with the increase of n. In contrast, our WM algorithm can provide a variety of payloads using different n and M.