Egyptian Informatics Journal (2014) **15**, 115–127

Cairo University

Egyptian Informatics Journal

www.elsevier.com/locate/eij
www.sciencedirect.com

ORIGINAL ARTICLE

Adaptive and non-adaptive data hiding methods for grayscale images based on modulus function

Najme Maleki, Mehrdad Jalali *, Majid Vafaei Jahan

Department of Computer Engineering, Mashhad Branch, Islamic Azad University, Mashhad, Iran

Received 29 November 2013; revised 3 April 2014; accepted 2 June 2014
Available online 27 June 2014

KEYWORDS

Data hiding;
Non-adaptive steganography;
Adaptive steganography;
Modulus function;
Embedding capacity

Abstract This paper presents two adaptive and non-adaptive data hiding methods for grayscale images based on modulus function. Our adaptive scheme is based on the concept of human vision sensitivity, so the pixels in edge areas than to smooth areas can tolerate much more changes without making visible distortion for human eyes. In our adaptive scheme, the average differencing value of four neighborhood pixels into a block via a threshold secret key determines whether current block is located in edge or smooth area. Pixels in the edge areas are embedded by Q-bit of secret data with a larger value of Q than that of pixels placed in smooth areas. Also in this scholar, we represent one non-adaptive data hiding algorithm. Our non-adaptive scheme, via an error reduction procedure, produces a high visual quality for stego-image. The proposed schemes present several advantages. 1-of aspects the embedding capacity and visual quality of stego-image are scalable. In other words, the embedding rate as well as the image quality can be scaled for practical applications 2-the high embedding capacity with minimal visual distortion can be achieved, 3-our methods require little memory space for secret data embedding and extracting phases, 4-secret keys have used to protect of the embedded secret data. Thus, level of security is high, 5-the problem of overflow or underflow does not occur. Experimental results indicated that the proposed adaptive scheme significantly is superior to the currently existing scheme, in terms of stego-image visual quality, embedding capacity and level of security and also our non-adaptive method is better than other non-adaptive methods, in view of stego-image quality. Results show which our adaptive algorithm can resist against the RS steganalysis attack.

1. Introduction

Nowadays message transmission on the internet still has to face some problems such as data security, and copyright control. Therefore, we need secret communication schemes for transmitting message on the internet. Encryption may provide a safe way, which transforms data into a cipher-text via cipher algorithms. However, encryption makes the message unreadable, but making message suspicious enough to attract

* Corresponding author. Tel.: +98 9153143976.
E-mail addresses: mehrjalali@gmail.com, jalali@mshdiau.ac.ir (M. Jalali).
Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

1110-8665 © 2014 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University.
http://dx.doi.org/10.1016/j.eij.2014.06.001

eavesdropper's attention. For overcoming to this problem, we must utilize of data hiding techniques which hide the secret data behind a cover media. Steganography is a data hiding technique which embeds secret data into a cover media such as text, image, audio and video, so that the result does not notice any third's attention. In the past decade, steganography in image extremely has been studied. The image into which a massage is hidden is called a cover image and the result a stego-image. Application of the data hiding can be used in military, commercial and anti-criminal depended application, transmission of confidential documents between international governments and be anonymous in internet [1]. We can categorize steganography schemes into two types: non-adaptive and adaptive schemes. In non-adaptive schemes, the embedding capacity in each pixel of cover image is a fixed value without taking the image local texture into consideration. In other words, these methods do not consider the differences between adjacent pixels. Non-adaptive means that we did not consider the position, where each embedding change was done. In first category, a well-known steganographic method is the Least Significant Bit (LSB) substitution method, which embeds secret data by replacing k LSBs of a pixel with k secret bits directly [2]. Also for minimizing the image distortion, Chan–Cheng proposed a simple LSB algorithm based on optimal pixel adjustment [3]. In 2006, Zhang and Wang's algorithm [4] represented in $(2n + 1)$-ary notation system. In this method, just one pixel of n pixels into one group is increased or decreased by 1. Also in 2006, Mielikainen [5] proposed LSB matching algorithm for embedding secret message. Both of Zhang and Wang's and Mielikainen's schemes [4,5] had the limited capacity.

Since LSB-Based methods just modify the LSB of image pixels, that can be detected the present secret data easily by the proposed steganalysis algorithms, e.g. the well-known RS detector [6]. Hence, level of security in these methods is poor. Of other aspect, all Pixels in a cover image cannot tolerate equal values of changes without causing noticeable distortion. Such that, the 4-bit LSB methods can make the smooth areas of cover image very dirty. Thus, easily the hiding effects resulted from embedding notice by eavesdropper. Because, the changes occur in edge areas can be difficultly discerned to the human eyes, therefore adaptive methods for steganography have been presented [7–13] in which the amount of embedding data in pixels is variable. These schemes provide a more imperceptible result than those employed by simple LSB s substitution and other non-adaptive schemes. Wu–Tsai proposed a novel steganographic method that uses the different values between two neighboring pixels to estimate how many secret bits should be embedded [7]. Chang–Tseng used the side information of neighboring pixels for each input pixel to help the capacity estimation in edge and smooth areas [8]. In Zhang–Wang scheme, three neighbor pixels are employed to assess the size of secret message for each pixel in the original image [9]. Wu et al. proposed a novel steganographic method based on LSB substitution and PVD method. In their algorithm, the secret bits in pixels located into edge areas embed using of PVD algorithm and those in pixels placed into smooth areas, embed using 3-LSB substitution algorithm [10]. Yang–Weng proposed a multi-pixel differencing method that to determine how many secret bits should be embedded, that used of three different values in a four-pixel block [11]. For improving the stego-image quality in Wu–Tsai scheme, Wang et al. [12] presented a steganographic method which instead of the different values, that utilizes the remainder of two consecutive pixels to record the information of secret data [12]. Yang et al. [13] proposed an adaptive LSB steganographic method using the different values of two consecutive pixels based on k-bit modified LSB substitution method to discriminate between edge and smooth areas [13]. Weiqi and Sivaranjani in [14,15] have proposed the LSB matching revisited image steganography. In [14,15] for low capacities only edge regions of cover image have changed and the smooth regions remained constant and hence had preserved the statistical and visual features of cover image (because the regions located at the edges present more complicated statistical features and observation changes in these regions is hard and difficult). In Weiqi and Sivaranjani's schemes [14,15], the embedding regions can select according to the size of secret message and the difference between two corresponding pixel in the cover image. Those use the absolute difference between two adjacent pixels as the criterion for classification of edge and smooth regions of cover image. Manoj and others in [16] in 2011, represented an overview of image steganography and its applications with a basic image steganographic model. In this method [16], for maximizing the embedding capacity into each pixel, has been utilized of an adaptive encoding algorithm along with LSB insertion method. The method [16] used StegSan for implementation. Indeed, StegSan uses of an adaptive encoding algorithm to optimize the use of embedding space in a specific cover image. Using StegSan tool in [16] allowed the users to hide various large files so stego-image maintains good imperceptible. This technique has been implemented only on 4-LSB [16]. In [17] in 2011 presented an adaptive steganographic method based on just noticeable distortion (JND) profile measurement. To compute how much information can be embedded and also final value determination of the stego-pixel, different impact factors had used ((1) JND value of the target pixel, (2) a predefined embedding capacity control factor, (3) the contents of various length secret data bits). To preserve the visual features of cover image, method [17] like more adaptive methods embedded more secret data bits within edge areas.

In 2013 [18], is presented a new adaptive embedding scheme namely adaptive steganography by oracle (ASO). It is based on an oracle which is used to calculate the detectability map. This approach preserves both cover image and sender's database distributions during the embedding process, which improves the security. In addition, it offers to the sender the opportunity to choose the most reliable image(s), during his secret communication [18]. Also in 2013 [19], Yu and Wang represent an adaptive steganography algorithm in the sparse domain. Image blocks whose entropy is higher than the threshold Used in this paper, are selected for sparse decomposition as complex texture image regions. The secret message is embedded into the decomposition coefficients, and then the stego image is reconstructed with modified coefficients [19].

Three criteria are used to evaluate the performance of data hiding schemes: the embedding capacity, the visual quality of the stego-image and the security. However, existing data hiding schemes seldom consider all these factors in their methods. But in 2010, Lee and Chen [20] used a simple modulus function to imply all the performance factors listed above. However, in Lee–Chen scheme the embedding capacity into each image pixel was fixed and thus that was a non-adaptive method. In order to provide better stego-image quality, larger embedding