Expert Systems with Applications 39 (2012) 11517–11524

Contents lists available at SciVerse ScienceDirect

Expert Systems with Applications

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

A novel technique for image steganography based on a high payload method and edge detection

Anastasia Ioannidou [a], Spyros T. Halkidis [b,*], George Stephanides [b]

[a] Department of Applied Informatics, University of Macedonia, Egnatia 156, GR-54006, Greece
[b] Computational Systems and Software Engineering Laboratory, Department of Applied Informatics, University of Macedonia, Egnatia 156, GR-54006, Greece

ARTICLE INFO

Keywords:
Image steganography
High payload techniques
Hybrid edge detection
Information hiding
Image processing

ABSTRACT

Image steganography has received a lot of attention during the last decade due to the lowering of the cost of storage media, which has allowed for wide use of a large number of images. We present a novel technique for image steganography which belongs to techniques taking advantage of sharp areas in images in order to hide a large amount of data. Specifically, the technique is based on the edges present in an image. A hybrid edge detector is used for this purpose. Moreover, a high payload technique for color images is exploited. These two techniques are combined in order to produce a new steganographic algorithm. Experimental results show that the new method achieves a higher peak signal to noise ratio for the same number of bits per pixel of embedded image.

1. Introduction

Steganography, which means covered writing, is an art that traces back to ancient times (Petitcolas, Anderson, & Kuhn, 1999). It separates itself from cryptography from the fact that one of its basic aims is that the fact that a secret message is hidden, in contrast to cryptography, should be not known to anybody but the communicating entities. Image steganography (Morkel, Eloff, & Olivier, 2005; Queirolo, 2011), where information is embedded within an image has been widely used during the last decade due to the lowering of the cost of image storage and communication and also due to the weaknesses of the human visual system (HVS).

Regarding the terminology related to image steganography, we note that the original image without the embedded secret message is termed as cover or host image, while the image resulting from embedding this message is termed as stego image. The secret message can be plain text, images, audio or video. After the embedding process, the stego image should look identical to the cover image and be resistant to standard analysis in order to avoid raising suspicion. A stego key is usually used in the embedding process to enhance security since only the person who knows it will be able to extract the secret message. The term payload is used to describe the size of the secret message that can be embedded in a particular image.

Image steganography methods can be separated into two categories: spatial domain and frequency domain based methods. In the first case, the secret message is embedded directly in the intensity of the pixels, while in the second case, images are first transformed to frequency domain and then, the secret message is embedded in the transform coefficients.

Many image file formats, such as jpeg, bmp, and gif, have been used so far in the literature for image steganography. 8-bit and 24-bit images are the most typical, the first due to their small size and the second due to the high payload they offer and to the fact that the large number of colors they contain make the changes from the secret message undetectable from the human visual system.

In this paper we present a novel technique for image steganography which is based on a high payload method for color images (EL-Emam, 2007) and another high payload steganography mechanism using a hybrid edge detector (Chen, Chang, & Hoang Ngan Le, 2010).

The rest of the paper is organized as follows: Section 2 presents related work, Section 3 describes the proposed method, Section 4 presents the experimental results in terms of peak signal to noise ratio and bits per pixel (bpp), Section 5 presents an experiment, where the number of embedded bits in edge pixels is gradually increased and possible visual attacks are investigated. Finally, Section 6 provides some conclusions and proposes future work.

2. Related work

The most obvious method to hide information within an image is the least significant bit (LSB) technique. In this method, information is embedded in the least significant bit of every pixel

* Corresponding author.
E-mail addresses: ioananas@csd.auth.gr (A. Ioannidou), halkidis@java.uom.gr (S.T. Halkidis), steph@uom.gr (G. Stephanides).

0957-4174/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.eswa.2012.02.106

in the image. However it has been shown (Fridrich, Goljan, & Du, 2001) that this technique does not resist statistical attacks. More recent techniques (Chang & Tseng, 2004; Chen et al., 2010; Thien & Lin, 2003; Wang, Wu, Tsai, & Hwang, 2008; Wu & Tsai, 2003) exploit the fact that more information can be hidden in sharp areas than in smooth areas, without the embedded image to be detectable.

In Wu and Tsai (2003) a steganographic method for images by pixel value differencing is presented. The cover image is partitioned in non-overlapping blocks of two consecutive pixels. A difference value is calculated from the values of the two pixels in each block. All possible difference values are classified into a number of ranges. The selection of the range intervals is based on the characteristics of the human vision's sensitivity to gray value variations from smoothness to contrast. The difference value is then replaced by a new value to embed the value of a substream of the secret message. The number of bits which can be embedded in a pixel pair is decided by the width of the range that the difference value belongs to. They use the differences of the gray values in the two-pixel blocks of the cover image as features to cluster the blocks into a number of categories of smoothness and contrast properties. Different amounts of data can be embedded in different categories according to the degree of smoothness or contrast. The main observation is that changes in the gray values of pixels in smooth areas in images are more easily noticed by the human eyes. A large difference value indicates that we examine an edged area. The image is scanned in a zigzag manner. If the difference value d is close to 0, this indicates that we are located in an extremely smoothed block. Conversely a value of d close to -255 or 255 shows that we are located in a sharply edged block. Only the absolute values of d can be considered (0 through 255) and classified into a number of contiguous ranges say R_i, where i = 1, 2, ..., n. The lower and upper values of R_i are denoted by l_i and u_i, respectively, where l_1 is 0 and u_n is 255. The widths of the ranges which represent the difference values of smooth blocks are chosen to be smaller, while those which represent the difference values of edged blocks are chosen to be larger. That is, ranges with smaller widths are created when d is close to 0 and ones with larger widths are created when d is far away from 0 for the purpose of yielding better imperceptible results. A difference value which falls in a range with index k is said to have index k. In the proposed method some bits of the secret message are embedded into a two-pixel block by replacing the difference value of the block with one with an identical index. The number of bits that can be embedded is given by:

$$n = \log_2(u_k - l_k + 1). \tag{1}$$

The new difference d' is given by:

$$d' = \begin{cases} l_k + b, & \text{if } d \geqslant 0, \\ -(l_k + b), & \text{if } d < 0, \end{cases} \tag{2}$$

where b is the value of the sub-streams. The embedding process is finished when all the bits of the secret message are embedded.

The inverse calculation for computing (g'_i, g'_{i+1}) from the original gray values (g_i, g_{i+1}) of the pixel pair is given by:

$$f((g_i, g_{i+1}), m) = (g'_i, g'_{i+1}) = \begin{cases} g_i - ceiling_m, g_{i+1} + floor_m, \\ \text{if } d = \text{is an odd number}, \\ g_i - floor_m, g_{i+1} + ceiling_m, \\ \text{if } d = \text{is an even number}, \end{cases} \tag{3}$$

where $m = d' - d$, $ceiling_m = \lceil \frac{m}{2} \rceil$ and $floor_m = \lfloor \frac{m}{2} \rfloor$. Care is also taken of boundary values. For the inverse process of extracting the original gray values from the stego-image, we note that the values which are computed from $f((g^*_i, g^*_{i+1}), u_k - d^*)$ (where d^* is the difference of the two gray values which have index k) are identical to the gray values which were computed in the embedding process. A related proof is given in the paper. The gray values of the stego-image are used to determine the index k. The value b, which was embedded in the two-pixel block is extracted by using the equation:

$$b = \begin{cases} d^* - l_k, & \text{if } d^* \geqslant 0, \\ -d^* - l_k, & \text{if } d^* < 0. \end{cases} \tag{4}$$

Note that in the recovery of the secret message from the stego-image using the previously described extraction process, there is no need of referencing the cover image.

A technique not directly but indirectly related to our context, by a method described later, (Wang et al., 2008) is analyzed by Thien and Lin (2003), who illustrate a steganographic method based on the modulus function. Suppose that people wish to embed the i-th digit x_i ($0 \leqslant x_i < m$; $m = 2^k$) of the data into a pixel with a gray value of y_i ($0 \leqslant y_i \leqslant 255$) in the cover image. Assume that

$$y_i = m \times t_i + b_i, \tag{5}$$

where $b_i = y_i \bmod m$, $t_i = \lfloor y_i / m \rfloor$.

The resulting gray value y'_{iLSB} replacing y_i is

$$y'_{iLSB} = (y_i - b_i) + x_i. \tag{6}$$

In later days the embedded data digit x_i can be extracted from y'_{iLSB} by

$$x_i = y'_{iLSB} \bmod m. \tag{7}$$

The resulting gray value y'_i generated by the proposed method of Thien and Lin is given by

$$y'_i = y_i - b_i + x_i + lm, \tag{8}$$

where l is an integer suitably chosen from 0, 1, -1. m kinds of symbols are used in the data. The ith digit x_i ($0 \leqslant x_i < m$) of the data is embedded into the pixel with a gray value of y_i ($0 \leqslant y_i \leqslant 255$) in the cover image. First $b_i = y_i \bmod m$, $d_i = x_i - b_i$.

$$d'_i = \begin{cases} d_i, & \text{if } \left(-\lfloor \frac{m-1}{2} \rfloor\right) \leqslant d_i \leqslant \lceil \frac{m-1}{2} \rceil, \\ d_i + m, & \text{if } (-m+1) \leqslant d_i < \left(-\lfloor \frac{m-1}{2} \rfloor\right), \\ d_i - m, & \text{if } \lceil \frac{m-1}{2} \rceil < d_i < m. \end{cases} \tag{9}$$

Finally $y'_i = y_i + d'_i$ is used as the resulting gray value to replace y_i

$$y'_i = \begin{cases} y_i + d'_i + m, & \text{if } y_i + d'_i < 0, \\ y_i + d'_i - m, & \text{if } y_i + d'_i > 255. \end{cases} \tag{10}$$

The embedded information can be extracted as $x_i = y'_i \bmod m$ just as with the LSB method.

A technique that combines pixel value differencing with the modulus function is proposed by Wang et al. (2008). The remainder of the two consecutive pixels can be computed using the modulus operation and then secret data can be embedded into the two pixels by modifying their remainder. There is an optimal approach to alter the remainder so as to greatly reduce the distortion caused by the hiding of the secret data. Instead of the difference value the proposed scheme modifies the remainder of two consecutive pixels $P_{(i,x)}$ and $P_{(i,y)}$ for better stego-image quality. The method is divided into various steps.

Step 1: Given a sub-block F_i composed of two continuous pixels $P_{(i,x)}$ and $P_{(i,y)}$ from the cover image, obtain the difference value d_i, the sub-range R_j, such that $R_j \in [l_j, u_j]$, the width $w_j = u_j - l_j + 1$, the hiding capacity t_i bits and the decimal value t'_i of t_i for each F_i by using Wu and Tsai's scheme.

Step 2: Compute the remainder values $P_{rem(i,x)}$, $P_{rem(i,y)}$ and $F_{rem(i)}$ of $P_{(i,x)}$ and $P_{(i,y)}$ and sub-block F_i respectively by using the following equations: