Information Sciences 188 (2012) 346–358

Contents lists available at ScienceDirect

Information Sciences

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

LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis

Der-Chyuan Lou [a,*], Chen-Hao Hu [b]

[a] Department of Computer Science and Information Engineering, Chang Gung University, Kweishan, Taoyuan 33302, Taiwan
[b] Department of Electrical and Electronic Engineering, Chung Cheng Institute of Technology, National Defense University, Taoyuan 33509, Taiwan

ARTICLE INFO

Article history:
Available online 6 June 2011

Keywords:
Information hiding
LSB substitution
Steganography
Steganalysis
x^2 detection
RS attack

ABSTRACT

Statistical steganalysis schemes detect the existence of secret information embedded by steganography. The x^2-detection and Regular-Singular (RS)-attack methods are two well-known statistical steganalysis schemes used against LSB (least significant bit) steganography. The embedded message length can be estimated accurately by these two steganalysis schemes. For secret communication, the resistance of steganography against steganalysis is very important for information security. To avoid the enemy's attempts, the statistical features between stego-images and cover images should be as similar as possible for better resistance to steganalysis. In this manuscript, a reversible histogram transformation function-based LSB steganographic method is proposed to resist statistical steganalysis. The experimental results show that the proposed method resists not only RS-attack but also x^2-detection methods.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

Many methods have been proposed to protect the security of secret information, such as cryptography and steganography techniques. Cryptography techniques can scramble secret information into an unreadable message. However, the unreadable message can easily attract unauthorized attention. Steganography techniques can provide secure transmission by embedding secret information within covert carriers to avoid observation [12,13,30]. The covert carrier can be an image [1,2,12,13,15,16,18,24,25,28], audio [6,20,22], video [5,7,14,26], or document [9–11]. The similarity between cryptography and steganography techniques is that only an authorized person with the right key can recover the secret information. Hence, the best approach is to combine steganography and cryptography techniques to protect the security of secret information. That way, even if stego carriers are obtained by an unauthorized person, the secret message cannot be exposed.

The LSB steganographic method [1,2,16,18,24,25] is the simplest one and is widely used in the field of information security due to its high hiding capacity and quality. It embeds a secret bit stream into the LSB plane of an image. LSB replacement, LSB matching (LSBM), LSB matching revised (LSBMR) [18], and LSBMR-based edge-adaptive (LSBMR-EA) [16] image steganography are well-known LSB-like steganographic methods. The LSB-replacement embedding method replaces the LSB plane with embedded message bits, but the others do not. In LSB matching, if the embedded bit does not match the LSB of the cover image, then the pixel value of the corresponding pixel is randomly changed by ±1. Unlike LSB replacement and LSBM, which embed message bits pixel by pixel, LSBMR deals with two pixels at a time and allows fewer changes to the cover image. The steganalysis resistance and image distortion of LSBMR are better than those of previous two. In general, the choice of embedding positions within a cover image depends on a pseudorandom sequence without consideration of the relationship

[*] Corresponding author.
E-mail addresses: dclouprof@gmail.com, dclou@mail.cgu.edu.tw (D.-C. Lou), chenhao.hu@gmail.com (C.-H. Hu).

0020-0255/$ - see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2011.06.003

between the image content itself and the size of the secret message. LSBMR-EA is proposed to expand the LSBMR and uses an edge-adaptive scheme to select the embedding positions. Based on the size of the embedded message, LSBMR-EA embeds the message from sharper edge regions to smoother edge regions. In [16], Lou et al. showed that LSBMR-EA can enhance security significantly compared with the typical LSB-based approaches, while preserving higher visual quality of the stego-images.

Steganalysis [8,29] is an interesting topic that focuses on the detection of the presence of embedded secret messages. RS attack [4], proposed by Fridrich et al., and x^2 detection [27], proposed by Westfeld and Pfitzmann, are the two most effective LSB steganalytic techniques. The RS-attack technique can detect both sequentially embedded messages and randomly embedded messages. The x^2-detection technique is good at detecting sequential embedding but not random embedding. An extended x^2-detection technique [21] has been proposed by Provos to improve the x^2-detection technique's ability to detect randomly embedded messages. There are other effective LSB steganographic detection methods, such as sample-pair analysis [3], proposed by Dumitrescu et al. All of them can accurately detect and estimate the length of the message embedded in an image.

To cope with this new trend, a robust steganographic technique should be developed to withstand the attacks of steganalytic detection. To meet the above requirement, Marçal and Pereira proposed a steganographic method based on reversible histogram transformation functions (RHTF) for digital images [17]. By using a secret key and RHTF, the secret information can be successfully embedded into the LSB of an image. Our experimental results show that the RHTF steganographic method can efficiently resist steganalysis by RS attack, but the secret key of the RHTF algorithm can be extracted easily by analyzing the histogram of the stego-image, and the embedding rate can be effectively estimated by RS attack.

In this manuscript, we have observed three vulnerabilities of the RHTF steganographic method and thus have proposed pixel grouping and a scheme of dynamical secret keys to improve the security of RHTF. The experimental results illustrate that the proposed method is efficient in reducing the vulnerabilities of RHTF and maintaining the resistance to x^2 detection and RS attack. At various embedding rates, most of the detection results of the stego-images are as low as those of cover images.

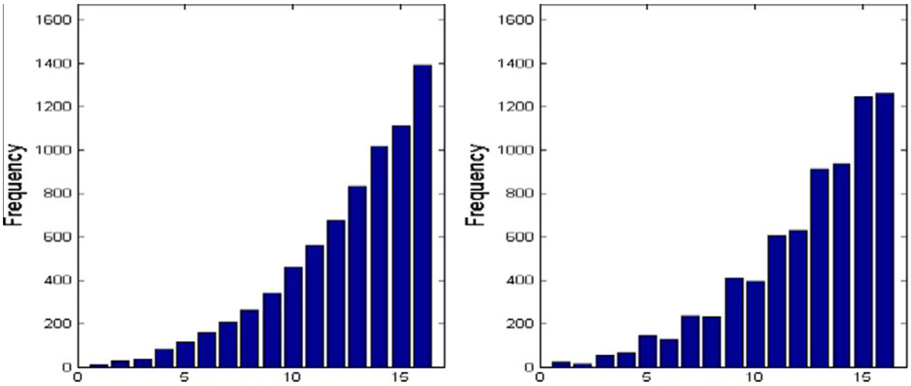
This paper is organized as follows. In Section 2, we introduce the techniques of x^2 detection, RS attack, and the RHTF steganographic method. In Section 3, we analyze the vulnerabilities of the RHTF steganographic method. In Section 4, the improved method is proposed. The experimental results are shown in Section 5. Section 6 gives conclusions.

2. Previous works

2.1. x^2-detection steganalytic technique

The embedding process of LSB steganography replaces the values of the LSB plane with messages. Hence, the pixel values of the LSB plane of the stego-image are different from those of the original image. If the embedding bits are normally distributed, the frequencies of each adjacent value approximate to the equal values. The frequencies of pixel values before embedding the message are shown in Fig. 1(a), and the same statistics after embedding the message are shown in Fig. 1(b). Fig. 1 shows that if the bits used to overwrite the least significant bits are equally distributed, the frequencies of the pairs of values (PoV) will be equal. Westfeld and Pfitzmann observed this PoV phenomenon of the LSB plane and proposed a Chi-Square detection (x^2detection) method [27].

They compared the theoretically expected frequency distribution in steganograms with some sample distributions observed in possible variations of the stego-image. In the cover image, the theoretically expected frequency is the arithmetic mean of two frequencies in a pair of values. The LSB embedding process does not change the sum of two frequencies of a PoV,



(a) Before embedding (b) After embedding

Fig. 1. PoV phenomenon in LSB steganography.

Download English Version:

https://daneshyari.com/en/article/393805

Download Persian Version:

https://daneshyari.com/article/393805

Daneshyari.com