Contents lists available at ScienceDirect

Information Sciences

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

# A new steganography method which preserves histogram: Generalization of LSB$^{++}$

Kazem Qazanfari, Reza Safabakhsh *

*Department of Computer Engineering and Information Technology, Amirkabir University of Technology, Tehran, Iran*

ARTICLE INFO

*Article history:*
Received 4 September 2013
Received in revised form 25 January 2014
Accepted 1 February 2014
Available online xxxx

*Keywords:*
Steganography
Preserving histogram
LSB$^{++}$ embedding
Co-occurrence matirx

ABSTRACT

Histogram-based steganalysis methods diagnose abnormalities in the stego histogram. LSB$^{+}$ and outguess are two steganography methods which preserve the cover histogram completely. These methods embed some extra bits to retain the cover histogram. However, these techniques adversely affect the statistical and perceptual attributes of the cover media. LSB$^{++}$ was proposed to improve LSB$^{+}$ by prohibiting some pixels from changing, resulting in the reduction of the extra bits. In this paper, we improve the LSB$^{++}$ method by proposing a technique to distinguish sensitive pixels and protect them from extra bit embedding, which causes lower distortion in the co-occurrence matrices. In addition, we extend LSB$^{++}$ to preserve the DCT coefficients histogram of jpeg images and generalize this method to the case where more than one bit of the cover elements are used. The experimental results show that the improved LSB$^{++}$ method produces fewer traces in the co-occurrence matrices than the LSB$^{++}$ method. Furthermore, the histogram based attacks cannot detect stego images produced by the proposed method with or without extra bits embedding. Therefore, the visual quality of the cover can be improved by the elimination of extra bit embedding.

## 1. Introduction

Steganography is the art and science of hidden communication. A steganography system embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. Essentially, the information hiding process in a steganographic system starts by identifying a cover medium's redundant bits. The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message [24]. In an effort to hide a secret message in redundant bits, Yang et al. [35] proposed an adaptive LSB steganography method using adjacent pixel value differencing (PVD). This method determines the number of message bits which could be hidden into these pixels. More message bits are embedded for a higher difference value. Similarly, Hong [9] proposed a new scheme using the concept of pixel value differentiation and a patched reference table (PVD-PRT) to provide a better image quality and extendable embedding capacity. Furthermore, Lee et al. presented a practical method of using a cover image to hide the secret message using tri-way pixel-value differencing. The goal of the proposed approach is to provide secrecy while avoiding the detection by dual statistics steganalysis [15]. In addition, Hong and Chen [10] proposed a steganography method based on pixel pair matching (PPM). This method utilizes the values of pixel pairs as a reference coordinate. To hide the message bits, this method first searches for a coordinate in the

* Corresponding author.
*E-mail addresses:* Kazemmit@aut.ac.ir (K. Qazanfari), Safa@aut.ac.ir (R. Safabakhsh).

http://dx.doi.org/10.1016/j.ins.2014.02.007
0020-0255/© 2014 Elsevier Inc. All rights reserved.

neighborhood set of this pixel pair based on the message bits. Then, this method replaces the pixel pair with the selected coordinate to embed the message bits.

Matrix embedding techniques [5,26,29] and VQ based methods [30,16] are two well known groups of data hiding methods. Fridrich and Soukal proposed two methods based on matrix embedding [5]. The first technique is based on a family of codes constructed from simplex codes and the second one is based on random linear codes of small dimension. One of the weaknesses of matrix embedding techniques is the low robustness against active attacks. Considering this weakness, Sarkar et al. [26] proposed a matrix embedding hiding method using powerful repeat accumulate (RA) codes for error correction, to solve this difficulty. Furthermore, Wang et al. [29] introduced a steganography method to improve the embedding speed of matrix embedding by extending the matrix via some referential columns. Furthermore, Amirtharajan and Balaguru Rayappan proposed an Adaptive Random (AR) k-bit embedding approach which has been attempted to enhance the quality of stego images [2]. VQ based steganography methods hide the message bits into a Vector Quantization (VQ)-compressed image. For example, Wang et al. [30] proposed a technique called Adjoining State-Codebook Mapping (ASCM) to map the content of an image block to an index in the corresponding state-codebooks. Similarly, Lee et al. [16] proposed a VQ based steganography method which explores the correlation of neighboring blocks of a VQ-compressed image to detect some holes for hiding the message bits.

In other works on embedding secret messages in cover objects, Fakhredanesh et al. [3,4] presented two image steganography methods. The first method locates regions suitable for embedding by the contourlet transform [3], whereas the second one assumes Watson's visual model for the cover image statistics and presents a new steganography method which uses this model to improve perceptual undetectability [4].

Modifying the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is called statistical steganalysis [25]. Many steganalysis methods are proposed which use these properties to detect stego images. Furthermore, Lyu and Farid [20] proposed a novel steganalysis method which extracts the first and higher order magnitude and phase statistics of images to detect stego from cover images. In another effort, Pevny et al. [23] investigated the difference between neighboring pixels before and after embedding using the first and second order Markov chains. They extracted some statistical features from the transition probability matrices and used a SVM classifier to detect stego images.

Histogram and co-occurrence matrices are two important statistical representations used in some steganalysis methods. These techniques utilize the changes made by data hiding to these properties to detect stego covers, and can be applied to any digital media in any embedding domain.

Westfeld and Pfitzmann [31] proposed a histogram based steganalysis method. They found that the embedding process alters the frequencies of cover values. Therefore, they proposed a Chi-Square test as a method for detecting stego images from clear covers. Furthermore, Harmsen and Pearlman [8] defined a Histogram Characteristic Function Center of Mass (HCF-COM) to detect the changes in image histogram after embedding. By extracting this feature, they were able to detect stego signal. To detect the stego images under more general conditions, this method was extended by Ker [13]. He then proposed a steganalysis method for the case when the two least significant bits of the pixels are used [14]. In addition, Liu et al. presented a scheme of steganalysis of the least significant bit (LSB) matching steganography based on feature mining and pattern recognition techniques [17], and Zhang et al. presented a least significant bit (LSB) matching steganography detection method based on the statistical modeling of the pixel difference distributions [36].

To defeat the histogram based steganalysis methods, many efforts have been made by researchers to protect the histograms of images. One of the first solutions to defeat these attacks was LSB matching. LSB matching increases or decreases the pixel values with the same probabilities when the least significant bit of the pixel value is not equal to the message bit. The LSB matching revised (LSBMR) [22], Near-optimal solution-pair-wise LSB matching via an immune programming strategy [33], and LSBMR-based edge-adaptive [19] are three versions of the LSB matching steganography methods. Tan and Li [28] showed that the readjusting step of LSBMR-based edge-adaptive [19] produces some effects in the long exponential tail of the histogram of the absolute difference of the pixel pairs. By using these effects, they proposed a steganalysis technique that could detect stego images and could estimate the used threshold in the data hiding process. In addition, Ghazanfari et al. [6,25] proposed an adaptive steganography method based on the LSB matching which increases the capacity up to 150% [6] and 158% [25]. Their second work [25] is the extension of their previous scheme [6] into the DCT domain. Sun et al. [27] presented a low capacity data hiding approach which completely preserved the histogram of the image.

Marçal and Pereira [21] proposed a steganography method based on reversible histogram transformation functions (RHTF) for the digital images. By using a secret key and RHTF, the secret information can be successfully embedded into the LSBs of an image. Lou and Hu [18] showed that this method causes some artifacts; so the stego images could be detected easily. They proposed an improved version of this method by using multi embedding keys. Although both methods are secure against histogram based steganalysis, they do not preserve the cover histogram completely.

The LSB$^+$ method suggested by Wu et al. [32] preserved the image histogram in spatial domain by embedding some extra bits in images. This method, however, results in statistical and perceptual distortions. Similarly, Provos [24] proposed a similar approach which preserves the primary histogram, but in the discrete cosine transform (DCT) domain. In our previous work [7], a new technique for image steganography, called LSB$^{++}$, was proposed, which improves the LSB$^+$ by keeping some pixels from changing, results in reducing the number of extra bits.

In this paper, we improve the LSB$^{++}$ method by proposing a technique to distinguish the sensitive pixels and keep them from extra bit embedding, as the embedding process causes fewer traces in the co-occurrence matrixes. Our previous work

Please cite this article in press as: K. Qazanfari, R. Safabakhsh, A new steganography method which preserves histogram: Generalization of LSB$^{++}$, Inform. Sci. (2014), http://dx.doi.org/10.1016/j.ins.2014.02.007