Information Sciences 254 (2014) 197–212

Contents lists available at ScienceDirect

Information Sciences

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

# Secret sharing with multi-cover adaptive steganography

Hai-Dong Yuan *

*Zhengzhou Information Science and Technology Institute, Zhengzhou, Henan, China*
*State Key Laboratory of Mathematical Engineering and Advanced Computing, China*

ARTICLE INFO

*Article history:*
Received 11 September 2012
Received in revised form 14 July 2013
Accepted 5 August 2013
Available online 14 August 2013

*Keywords:*
Secret sharing
Steganalysis
Steganography

ABSTRACT

More and more studies have been dedicated to investigating secret sharing with steganography. Unfortunately, no previous work has ever reported its capability to resist steganalysis. In this paper, we pose the multi-cover adaptive steganography problem. Two secret sharing methods for natural images based on multi-cover adaptive steganography have been proposed. The secret information is adaptively shared into textured regions of covers by a spatial ±1 operation. In comparison to previous secret sharing methods, each of the proposed methods uses a simple share-constructing operation and each has lossless secret reconstruction and high quality shares. More importantly, the proposed methods are more secure in terms of resistance against state-of-the-art steganalysis techniques. In comparison to previous steganographic methods, the proposed methods hide secret bits among textured regions with different covers and are thus difficult to detect. Moreover, the proposed methods can be used to adaptively embed location-sensitive secrets (e.g., secret images) and require no stego key for extracting the encrypted message. These results also have significance in individual cover steganography. The experimental results show the effectiveness of the proposed methods.



## 1. Introduction

The concept of a $(k,n)$ secret sharing (SS) scheme was proposed by Shamir [37]. The main idea of the $(k,n)$ SS scheme $(k \leqslant n)$ is to encode and divide a secret message into $n$ shares, where each share individually reveals no information about the original secret. Then, any $k$ or more shares can reveal the secret. However, by inspecting any $k-1$ or fewer shares, one cannot reveal any information about the original secret, even if infinite computational power is available.

Visual secret sharing (VSS), also called visual cryptography (VC) [32], encodes a binary secret image into $n$ randomly appearing binary shares (printed on transparencies), and the decryption is performed by directly stacking $k$ or more transparencies together. VSS has been studied intensively in recent years. Most of the previous research has focused on resolving the problems of large pixel expansion and low contrast reconstruction [29], and the single binary secret image-sharing method has been extended to share grayscale, color or multiple secret images [7,38–40]. Another disadvantage of traditional VSS schemes is that the shares are random-like images. A malicious intruder might be attracted to such meaningless shares delivered over an insecure channel. Extended visual cryptography (EVC) eliminates such a disadvantage by constructing meaningful halftone shares (called share constructing) [17,19] or embedding random shares into meaningful halftone covers to form stego images (called share embedding) [28]. Unfortunately, all of the EVC methods mentioned above still cannot reconstruct the original secret image exactly and especially cannot be used to share a halftoning or dithering secret image. Consequently, these techniques are not suitable to some rigorous tasks, such as military and medical applications.

* Address: Zhengzhou Information Science and Technology Institute, Zhengzhou 450004, Henan, China.
*E-mail address:* authoryhd@msn.com

0020-0255/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2013.08.012

### 1.1. Secret sharing with steganography

Generally speaking, the usage of natural images (photographic scenes or scanned photos) is more popular than that of halftone images in reality, and therefore, a natural image share is preferred to a halftone share in terms of concealing shares from suspicion. From this point of view, an SS method for natural images can also be regarded as a technique of digital steganography, namely, secret sharing with steganography.

Steganography, cryptography and watermarking are tightly related topics in information security. Steganography is the art and science of covert communication. While cryptography is about protecting the content of the messages, steganography is about concealing their existence [33]. A steganographic method embeds a secret message as undetectable alterations in a digital cover object (an innocuous-looking object such as an image, video, or audio), to produce a stego object. The primary goal of steganography is always to conceal the very existence of the embedded message. In contrast, steganalysis aims to uncover the existence of secret messages. Steganography and watermarking are both forms of information hiding. However, there are also essential differences between steganography and watermarking. A watermarking method's main concern is to achieve a high level of robustness [2,3,9,10,12–14]. Steganography, on the other hand, strives for high undetectability and embedding capacity, which often entails that the embedded message is fragile [36]. A detailed comparison of steganography and related techniques can be found in [8].

Recently, more and more studies have been dedicated to investigating secret sharing with steganography. Based on Shamir's $(k,n)$ SS scheme, Lin and Tsai [24] proposed an SS method with the additional capabilities of steganography wherein the stego images were formed by embedding shares into natural cover images via a least significant bit (LSB) replacement. Yang et al. [43] presented an improved method that rearranged the embedded bits (also by LSB replacement) to improve the visual quality of the stego images and could reconstruct a secret image exactly. Chang et al. [5,6] further improved the visual quality of the stego images to approximately 45 dB (by means of PSNR). However, these methods are computationally expensive. Lin et al. [25,26] employed a modulus operator to embed shares into a cover image. The advantages of their methods are high secret capacity and lossless secret reconstruction. The disadvantages of their methods are still computationally intense, and the cover images must be the same.

For most of the previous methods of secret sharing with steganography, the visual perception of the stego images is the main concern. However, a visual comparison between cover and stego images looks meaningless in terms of resistance against steganalysis when the stego image is confronted by an experienced steganalyst. Unfortunately, in the field of secret sharing with steganography, none of the previous studies have ever reported a capability of resistance against steganalysis.

### 1.2. Individual cover steganography and multi-cover steganography

In the field of digital steganography, it is generally accepted that the LSB plane of a natural image is insignificant and sufficiently random (except for flat or saturated regions) to hide secret bits [31]. LSB-based steganographic approaches are widely used in the spatial domain [1,30,31,35,42]. One of the most popular steganographic techniques is LSB replacement because of its extreme simplicity and visual imperceptibility. LSB replacement directly replaces the LSBs of cover pixels with message bits (usually encrypted), i.e., it increases even pixel values by 1 or decreases odd pixel values by 1 or leaves them unmodified. As a result, embedding uniformly distributed message bits (simply as encrypted data) reduces the difference between adjacent bins in the gray-level histogram of a cover image. With this statistical bias, LSB replacement can be reliably detected by current steganalytic techniques, even when the embedding rate (secret bits embedded per pixel) is low [22].

LSB matching (often called ±1 embedding) also hides the secret message into the LSB plane of a cover image. If the secret bit does not match the LSB of the cover pixel, then +1 or $-1$ is randomly added to the pixel value (except for the boundary of the dynamic range). The random ±1 embedding scheme is no longer unbalanced in comparison to LSB replacement and, therefore, makes LSB matching harder to detect.

For many LSB-based approaches, the selection of cover pixels and the order of embedding are generated by a keyed pseudo-random number generator (PRNG). The key (called a stego key) is shared by the recipients; therefore, they can reconstruct the stego pixel sequence and extract the encrypted message by reading off the LSBs from the stego pixels. It is well known that values of neighboring pixels in natural images are not independent; therefore, the random cover pixels selecting scheme makes LSB matching can be detected [4,23]. Moreover, recent results from digital image steganalysis [34] suggest that the secure payload for individual cover is far below 0.25 bits per pixel (bpp).

Certainly, one can extend most of the existing VC/EVC schemes to secret sharing with steganography by simply substituting the LSB planes of natural cover images with the produced shares (similar to [24,43]) or by performing randomly the ±1 process to make the LSB of the covers match with the shares. However, as mentioned above, such "steganographic" methods of share embedding are easy to detect by state-of-the-art steganalysis methods.

More recently, some content-adaptive steganographic methods for individual cover [16,31,35] embed secret messages into edges and texture regions that are difficult for steganalysis, thus leading to highly undetectable steganography. However, in these methods, the stego key is still required, and the adaptive embedding works on the intra-image manner; thus, it is difficult to hide a *location-sensitive secret* (e.g., a meaningful secret image). Furthermore, when multiple cover images are required (e.g., for communicating a large payload), one might wonder whether these steganographic schemes are adaptive enough: (1) how many secret bits should be dispatched to each cover, and (2) where should the secret bits be embedded? We use the term *multi-cover adaptive steganography* as a shortened form of these two questions.