The Journal of Systems and Software 84 (2011) 803–809

Contents lists available at ScienceDirect

The Journal of Systems and Software

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

Secret image sharing with authentication-chaining and dynamic embedding

Z. Eslami*, J. Zarepour Ahmadabadi

Department of Computer Science, Shahid Beheshti University, G.C., Tehran, Iran

ARTICLE INFO

Article history:
Received 3 March 2010
Received in revised form
14 November 2010
Accepted 1 January 2011
Available online 6 January 2011

Keywords:
Secret image sharing
Steganography
Authentication
Visual quality

ABSTRACT

A popular technique to share a secret image among n participants is to divide it first into some shadow images and then embed the shadows in n"cover" images. The resulting "stego" images, which contain the embedded data, are distributed among intended recipients. In order not to attract any attacker's attention, it is important to apply a suitable embedding such that high quality stego images are produced. Moreover, to ensure the integrity of stego data, a robust authentication mechanism which can detect tampering with high probability should be implemented.

Recently, a series of papers (Lin and Tsai, 2004; Yang et al., 2007; Chang et al., 2008; Yang and Ciou, 2009) have considered polynomial-based secret image sharing with steganography and authentication. The embedding technique employed in all these papers is static, i.e. hidden bits are embedded in predetermined fixed-size blocks of each cover image. It is therefore possible that all the hidden data is replaced in only a subset of blocks of cover images while other blocks remain intact. As for authentication, the best of these schemes detects a tampered stego block with probability 15/16, however, since this is obtained at the cost of using 4 authentication bits per block, the visual quality of stego images is seriously degraded. In this paper, we propose a novel polynomial-based secret image sharing scheme with two achievements. First, a new embedding is proposed so that the block size is determined dynamically according to the size of hidden data and therefore, all the capacity of cover images is used for data hiding. Second, we introduce a new authentication-chaining method which achieves 15/16 as its tamper-detection ability while using only 2 authentication bits. Experimental results are provided to confirm the theory.

1. Introduction

Recent technological advances in computer networks have turned transmission of digital data quite a popular task and digital images are no exception. In particular, there are important confidential images that should be transferred securely over open channels such as the Internet. A common approach to accomplish this is to share the secret image among n entities by using the so-called (t, n)-threshold secret sharing schemes, introduced first independently by Shamir (1979) and Blakley (1979). The secret image is divided (by an entity called the dealer) into n shadow images in such a way that the original secret image can be restored from any t (or more) of shadows, however, the information obtained from $(t-1)$ or fewer shadows is insufficient for reconstruction. This approach adds a fault-tolerant property to image sharing procedure as well. In other words, even if $n-t$ entities are inaccessible for some reasons, the remaining t users are able to restore the secret. In this respect, there are two major approaches. One is visual cryptography schemes in which any t participants may photocopy their shadows on transparencies and stack them on an overhead projector to visually decode the secret image through the human visual system. Naor and Shamir first proposed this idea (Naor and Shamir, 1994). The interested reader can find more on visual cryptography in Yang (2004); Lin and Tsai (2003); Yang and Chen (2006, 2007, 2008); Liu et al. (2010); Tuyls et al. (2005); Tsai et al. (2007); Feng et al. (2008). The other approach is polynomial-based schemes which recover the secret image by adopting Shamir's secret sharing scheme.

However, two problems still exist. First, the above procedure usually produces noise-like shadows which if transmitted would attract attention of attackers. Therefore, for sensitive data some steganographic (data-hiding) method should be utilized to transform shadows to high quality images. In these methods n ordinary images are selected as cover and then the shadow data is embedded in these cover images. The resulting images, called stego images, are then distributed among participants. It is clearly important that high embedding capacity is achieved in a manner that the visual quality of stego images would not be damaged (Lou et al., 2010; Wu and Hwang, 2007). The second problem pertains to ensuring the integrity of stego images during the reconstruction phase. In many applications, any tampering of the stego images should be

* Corresponding author.
E-mail addresses: z_eslami@sbu.ac.ir (Z. Eslami), J.zarepour@mail.sbu.ac.ir (J.Zarepour Ahmadabadi).

0164-1212/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2011.01.002

Nomenclature

SI	the secret image
t	threshold value, such that t or more shadows can recover SI, while $t-1$ shadows cannot
$P_1, \ldots, P_n$	the participants
CI_i	the cover image corresponding to P_i
$\langle\langle bitstring\rangle\rangle_i$	the leftmost i bits of $bitstring$
$\langle bitstring\rangle_i$	this operator divides $bitstring$ from right to left into substrings of length i and then XORs them to obtain a string of length i, with padding done if necessary
H_K	a collision-free keyed hash function

detected with high probability and this makes a robust authentication technique quite indispensable.

So far, two most popular steganographic embedding methods are the least significant bits (LSB) replacement (Chan and Cheng, 2004; Chang et al., 2003; Wang et al., 2001) and the modulus operation (Wu et al., 2004; Chang et al., 2006; Thien and Lin, 2003). In this paper, we are only concerned with LSB-based methods and provide a literature review of the research done in this category. Thien and Lin (2002) shared the secret image into noise-like shadows using a (t, n)-threshold scheme based on Shamir sharing scheme. In 2004, Lin and Tsai (2004) proposed an image sharing scheme equipped with steganography and authentication. However, their scheme could introduce distortion to the original secret and their authentication ability was rather weak. Afterwards, Yang et al. (2007) proposed an improvement to overcome these defects and enhanced authentication to some degree. In 2008, Chang et al. (2008) employed the Chinese remainder theorem (CRT) to compute authentication bits and obtained better tamper-detection capabilities so that the probability of successful verification for a fake stego block was 1/16. They also claimed to obtain better visual quality for stego images, however, in Yang and Ciou (2009), the authors showed that because of using 4 authentication bits, this quality is indeed degraded. For the sake of completeness, we also mention that in Eslami et al. (2010), Eslami et al. employed the concept of cellular automata to propose an image sharing scheme. They use configurations of the automata to store authentication data and detect a fake stego block with probability 255/256. Therefore, the visual stego quality is enhanced, however, the cost is that consecutive shares must be presented to recover the original secret. In this paper, we only consider polynomial-based schemes.

In all of the above-mentioned schemes, the embedding technique is static, i.e. the cover image is divided into predetermined fixed-size blocks and then the hidden data is embedded into the LSBs of each block. Consequently, it is possible that only a subset of a cover image is used for this purpose and therefore, the number of bits that should be replaced in each block increases unnecessarily. This in turn might have a downside on the visual quality of the resulting stego images. In this paper, we propose a novel embedding method which is dynamic and uses all the capacity of cover images for the purpose of data hiding. Therefore, the block size is determined dynamically according to the size of hidden data and embedding takes place throughout the entire cover image.

We also propose a new authentication method in which chaining of embedded data is used such that computing authentication bits for one block of hidden data depends on previous authentication bits as well. Therefore, while the current best tamper-detection probability (15/16 by Chang et al.) is achieved by allocating 4 authentication bits, our scheme uses only 2 authentication bits to obtain the same result.

X $x = (x_1, x_2 \ldots, x_8)$	V $v = (v_1, v_2 \ldots, v_8)$
W $w = (w_1, w_2 \ldots, w_8)$	Z $x = (x_1, x_2 \ldots, x_8)$

Fig. 1. A 4-pixel block (B) of a cover image.

The rest of the paper is organized as follows: Section 2 reviews briefly recent polynomial-based schemes with steganography and authentication. In Section 3, we explain dynamic embedding, authentication chaining and the proposed secret image sharing scheme. Experimental results are provided in Section 4. Finally, conclusions of the paper are presented in Section 5.

2. Related works

In this section, we review briefly recent secret image sharing schemes. Since all the schemes considered in this section are based on Shamir's sharing scheme, we deliberately omit some detail so as to highlight the essential improvements achieved by our proposed scheme regarding embedding and authentication. We use the following notations throughout the paper.

2.1. Lin et al.'s secret image sharing scheme

This Shamir-based (t, n)-threshold secret image sharing scheme is proposed in 2004 (Lin and Tsai, 2004). Different phases of the scheme are as follows.

2.1.1. Share generation

The secret image SI and cover images.
Each pixel of SI is considered as a secret and is shared by Shamir's (t, n)-scheme Shamir (1979) among $P_1, \ldots, P_n$. Input for Shamir polynomials are pixels of cover images and all calculations are done mod 251.
n shared pixels of the form $(s_1, \ldots, s_8)$ corresponding to each secret pixel.

2.1.2. Computing authentication data for shares

The share $(s_1, \ldots, s_8)$.
The parity bit: $p = s_1 \ldots s_8$.

2.1.3. Embedding of secret data in a given cover image

The cover image (CI) and the secret data (the shares plus corresponding authentication bits).
CI is divided into non-overlapping 4-pixel blocks B as in Fig. 1. Each share $(s_1, \ldots, s_8)$ plus the authentication bit p are embedded in B such that the resulting stego block $\widehat{B}$ in Fig. 2 is obtained. Note that the number of modified bits in the 4 pixels of $\hat{B}$ is (0, 3, 3, 3).
The corresponding stego image.

$\hat{X}$ $\hat{x} = (x_1, x_2 \ldots, x_8)$	$\hat{V}$ $\hat{v} = (v_1, v_2 \ldots, v_5, \boxed{s_1, s_2, s_3})$
$\hat{W}$ $\hat{w} = (w_1, w_2 \ldots, w_5, \boxed{s_4, s_5, s_6})$	$\hat{Z}$ $\hat{z} = (z_1, z_2 \ldots, z_5, \boxed{s_7, s_8, p})$

Fig. 2. Stego block ($\hat{B}$) of Lin et al.'s scheme.