J. Vis. Commun. Image R. 25 (2014) 1093–1101

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

Secret image sharing scheme with hierarchical threshold access structure

Nasrollah Pakniat, Mahnaz Noroozi, Ziba Eslami *

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

ARTICLE INFO

Article history:
Received 10 July 2013
Accepted 7 March 2014
Available online 19 March 2014

Keywords:
Cryptography
Secret image sharing
Hierarchical threshold access structure
Cellular automata
Birkhoff interpolation
Information hiding
Reversibility
Tamper detection

ABSTRACT

A hierarchical threshold secret image sharing (HTSIS) scheme is a method to share a secret image among a set of participants with different levels of authority. Recently, Guo et al. (2012) [22] proposed a HTSIS scheme based on steganography and Birkhoff interpolation. However, their scheme does not provide the required secrecy needed for HTSIS schemes so that some non-authorized subsets of participants are able to recover parts of the secret image. In this paper, we employ cellular automata and Birkhoff interpolation to propose a secure HTSIS scheme. In the new scheme, each authorized subset of participants is able to recover both the secret and cover images losslessly whereas non-authorized subsets obtain no information about the secret image. Moreover, participants are able to detect tampering of the recovered secret image. Experimental results show that the proposed scheme outperforms Guo et al.'s approach in terms of visual quality as well.

1. Introduction

Sharing images over open channels such as the Internet has attracted considerable attention in recent years [1–8]. However, when it comes to sharing secret images, some challenging problems should be solved first. The first one is the number of parties that can access the secret image. It is definitely a risk to consider a single party due to the accidental or intentional loss/corruption of such images that might occur. On the other hand, if several participants share parts of the secret image, care must be taken to ensure that no malicious shareholder is able to manipulate his/her data. The second concern is the need to keep invaders unaware not only of the content of the secret image itself but also of the very fact that an image is being transferred. Secret sharing schemes which protect and distribute a secret content among a group of participants provide solutions to the first issue. In this regard, the basic example, proposed first by Shamir [9] and Blakley [10], is the concept of a (t, n)-threshold secret sharing scheme which encodes a secret data set into n shares and distributes them among n participants in such a way that any t or more of the shares can be collected to recover the secret data, but any $t-1$ or fewer of them provides no information about the secret. Moreover, to ensure recovery of the original secret information some authentication process must be employed so that any manipulation of shares is detected with high probability. To tackle the second concern, steganographic techniques are usually employed [11–14]. In these methods, first some innocent looking images, called **cover** images, are selected. Then the secret data are embedded into cover images and the resulting **stego** images are distributed among participants using some secret sharing scheme. Clearly, in order not to invoke suspicion, the embedding should create high-quality stego images such that the changes are not visually perceptible. So far, two most popular steganographic methods used in steganographic secret sharing schemes were the least significant bits (LSBs) replacement and the modulus operation.

A method of secret image sharing with steganography and authentication proposed by Lin and Tsai [15] in 2004. Their scheme is an example of a lossy polynomial-based image sharing and the reconstructed secret image may be distorted slightly. Wu et al. [16] in 2004 proposed another scheme in which the secret image is compressed firstly, and then embedded into the cover images by modulus operation. This approach can generate smaller stego images, but the original secret image cannot be retrieved completely in the reconstruction procedure. To recover the secret image losslessly, the method introduced by Thien and Lin [17] can be utilized which splits every pixel with value more than 250 into two pixels. Their method is effective, but the output images are random-looking which attracts the attention of malicious attackers. In order to overcome the defects in Lin and Tsai's scheme, Yang et al. [18] used Galois field $GF(2^8)$ instead of modulo 251 and

* Corresponding author. Fax: +98 2122431655.
E-mail addresses: n_pakniat@sbu.ac.ir (N. Pakniat), m.noroozi@mail.sbu.ac.ir (M. Noroozi), z_eslami@sbu.ac.ir (Z. Eslami).

http://dx.doi.org/10.1016/j.jvcir.2014.03.004
1047-3203/

proposed an improved approach in 2007. The scheme proposed by Eslami et al. [4] in 2009 is another example of a secret image sharing scheme with steganography and authentication. Their scheme is an effective lossless sharing scheme based on cellular automata, but their access structure is restricted, i.e., only a subset of some consecutive participants from an ordered set of participants can form an authorized subset. Eslami and Ahmadabadi [5], Ulutas et al. [6] and Yang and Chu [7] are more recent examples on this line of research.

In the above mentioned schemes, it is not possible for participants to recover the cover image losslessly. However, in some applications, such as medical diagnosis, law enforcement, military imaging system, remote sensing and high-energy particle physical experimental investigation, it is important to reverse the stego media back to original after the embedded data is retrieved from it. Therefore, designing a secret image sharing scheme which allows authorized participants to restore the distorted stego image to original without distortion after retrieving the shared data is necessary. Lin and Chan [19] proposed an invertible sharing scheme with steganography to recover the secret image and cover image losslessly. Wu et al. [20] proposed another secret image sharing based on cellular automata and steganography which retrieves the secret and cover images both losslessly.

In reconstruction of the secret image of these schemes, each stego image plays an equivalent role. However, a general threshold access structure can have other useful properties for some applications. For example, when the participants differ in their authority, an access structure which takes this difference into account may be useful. A hierarchical threshold access structure is beneficial in such situations. In a scheme with hierarchical threshold access structure, the secret is shared among a group of participants that is partitioned into levels. The access structure is then determined by a sequence of threshold requirements for these levels, e.g., considering $t_0 < t_1 < t_2 < \cdots$ as the sequence of threshold requirements, a subset of participants is authorized to reconstruct the secret if it has at least t_0 participants from the highest level, as well as at least $t_1 (> t_0)$ participants from the two highest levels and so forth. In 2007, Tassa proposed a new secret sharing scheme based on Birkhoff interpolation to deal with hierarchical threshold access structures [21]. However, unlike Shamir's secret sharing scheme, Tassa's scheme is not able to use all potentials of underlying polynomial to share multiple secrets. Using Tassa's scheme to share more than t_0 secrets makes it possible for some non-authorized subset of participants to recover some of the secrets.

Based on Tassa's scheme, Guo et al. in [22] proposed a hierarchical threshold secret image sharing scheme with steganographic properties. To the best of our knowledge, their scheme is the only existing hierarchical threshold secret image sharing. In their scheme, after sharing each block of the secret image using Tassa's scheme, modulus operation is used to hide the shadow data into some cover images. However, their scheme has the following weaknesses:

- As the authors have mentioned in their paper, some non-authorized subsets of participants can obtain parts of the secret image.
- The cover image can not be losslessly recovered.
- There is no authentication in their scheme. Therefore, a malicious participant can make honest participants obtain a fake secret image.
- Compared to existing schemes in the literature with the same threshold parameter, image quality of this scheme is not acceptable (see Section 2.2).

The aim of this paper is to employ cellular automata to propose a hierarchical threshold secret image sharing scheme which overcomes the weaknesses of Guo et al.'s scheme. In the proposed scheme, secret and cover images are recovered losslessly. Moreover, participants are able to check the originality of the recovered secret image. We also formally prove that non-authorized subsets of participants can obtain no information about the secret image. As for the steganographic security, we follow the common methodology considered so far in the context of secret image sharing, i.e., steganographic methods are employed only to prevent noise-like shadow data. Therefore, we consider visual quality of stego images to measure how (visually) susceptible stego images are. The experimental results indicate that the proposed scheme achieves a better visual quality for stego images compared to Guo et al.'s scheme. Despite this, we would like to emphasize that the steganographic method employed in our paper is rather weak (the same as almost all existing literature on steganographic secret image sharing) and well-designed steganalysis algorithms are able to detect the presence of hidden data in our stego images.

The rest of this paper is organized as follows. Section 2 reviews Guo et al.'s hierarchical threshold secret image sharing scheme and discusses its weaknesses. An overview of cellular automata is also provided in this section. In Section 3, we describe the proposed scheme. Security analysis and experimental results of our proposed scheme are provided in Sections 4 and 5, respectively. Finally, the conclusions of this paper are presented in Section 6.

2. Related work

In this section, we first describe Guo et al.'s scheme and then we explain its weaknesses. The necessary background on cellular automata which is the basis of our approach is also covered in this section.

2.1. Review of Guo et al.'s hierarchical threshold secret image sharing scheme

Let U be a group of n participants $P_1, P_2, \ldots, P_n$ divided into $m+1$ levels $U_0, U_1, \ldots, U_m$ and suppose that the sequence of threshold requirements $t_0, t_1, \ldots, t_m$ determines the hierarchical threshold access structure. Let SI be the secret image and let $CI_1, \ldots, CI_n$ be the cover images corresponding to $P_1, \ldots, P_n$. The stego image STG_i corresponding to P_i is constructed using CI_i and the P_i's share from SI, for $i = 1, \ldots, n$. The details of Guo et al.'s scheme are as follows:

Setup: The dealer:

(1) Chooses a large prime number p.
(2) Divides SI into (t_m)-pixel units $D_1, \ldots, D_l$, where $l = \left\lceil \frac{M_{SI} \times N_{SI}}{t_m} \right\rceil$ and M_{SI} and N_{SI} are the width and height of the secret image.

Sharing: For each unit $D_j (1 \leqslant j \leqslant l)$, the dealer:

(1) Constructs a $(t_m - 1)$th degree polynomial $F_j(x) = D_j^1 + D_j^2 x + \cdots + D_j^{t_m} x^{t_m - 1} (mod\ p)$, where $D_j^i (1 \leqslant i \leqslant t_m)$ is ith pixel of D_j.
(2) Assigns to each participant P_i his share from D_j as $SH_j^i = F_j^{(t_{k-1})}(i)$, where k is such that $P_i \in U_k$ and $F_j^{(t_{k-1})}(x)$ is the (t_{k-1})th derivative of $F_j(x)$.

Embedding: The dealer uses modulus operation to embed each participant's share from the secret image into his cover image CI_i and obtains his stego image STG_i.

Recovery: Given the stego images corresponding to an authorized subset of participants which satisfy the sequence of threshold requirements, one can recover the secret image as follows:

- Extracts the embedded data from each stego image.