Information Sciences 178 (2008) 4382–4395

Contents lists available at ScienceDirect

Information Sciences

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

A multisecret sharing scheme for color images based on cellular automata

G. Alvarez [a], L. Hernández Encinas [a,*], A. Martín del Rey [b]

[a] Department of Information Processing and Coding, Applied Physics Institute, CSIC, C/Serrano 144, 28006 Madrid, Spain
[b] Department of Applied Mathematics, EPS, Universidad de Salamanca, C/Hornos Caleros 50, 05003 Ávila, Spain

ARTICLE INFO

Article history:
Received 9 July 2007
Received in revised form 6 June 2008
Accepted 6 July 2008

Keywords:
Secret sharing
Color images
Cryptography
Cellular automata
Image processing

ABSTRACT

In this work a new multisecret sharing scheme for secret color images among a set of users is proposed. The protocol allows that each participant in the scheme to share a secret color image with the rest of participants in such a way that all of them can recover all the secret color images only if the whole set of participants pools their shadows. The proposed scheme is based on the use of bidimensional reversible cellular automata with memory. The security of the scheme is studied and it is proved that the protocol is ideal and perfect and that it resists the most important statistical attacks.

1. Introduction

Secret sharing schemes were independently introduced by Shamir [26] and Blakley [4] in 1979. These schemes are cryptographic procedures to share a secret among a set of participants in such a way that only some qualified subsets of these participants can recover the secret. The original motivation for such schemes was to safeguard cryptographic keys from loss. Currently, they have many applications in different areas such as access control, opening safety deposit boxes, etc.

The most extended secret sharing schemes are the (k,n)-threshold schemes. For this class of schemes k and n are integer numbers, $1 \leqslant k \leqslant n$, and its protocol is as follows: There exists a mutually trusted party (a dealer) which computes n secret shares from an initial secret and later he distributes them to the n participants in a secure way. The (k,n)-threshold scheme has to verify two conditions: (1) any k, or more, participants can recover the original secret by joining their shares, and (2) any group of $k-1$ or less participants is unable to recover the secret. The most extended (k,n)-threshold schemes are due to Shamir, which is based on polynomial interpolation, and Blakley, which is based on the intersection of affine hyperplanes. Recently, several cryptographic protocols for (k,n)-threshold cryptography have been proposed in the literature [9,20,32].

A (k,n)-threshold scheme is called ideal if the size of every share is equal to the size of the shared secret, and a (k,n)-threshold scheme is said perfect if the knowledge of any $k-1$ or fewer shares provides no information about the original secret (for more information about these schemes see [23,27,28]).

The first (k,n)-threshold scheme proposed to share images is the visual cryptography [25]. This scheme is perfect but not ideal since the size of the shared images is bigger than the original one. Moreover, the quality of the contrast of the recovered secret images is degraded. Several modifications to this first proposal have been made. For example, in [21] (k,n)-threshold visual secret sharing (VSS) schemes were studied and the authors provided a new characterization of the VSS schemes for

* Corresponding author. Tel.: +34 91 561 8806; fax: +34 91 411 7651.
E-mail addresses: gonzalo@iec.csic.es (G. Alvarez), luis@iec.csic.es (L. Hernández Encinas), delrey@usal.es (A. Martín del Rey).

0020-0255/$ - see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2008.07.010

which black pixels in a secret black and white image are perfectly recovered as black pixels. Moreover, Chen et al. [7] proposed a multiple-level VSS scheme (MLVSS) in order to avoid the loss of contrast obtained in the recovered secret image. This scheme has the advantages that an enhancement of contrast is obtained and there is no expansion of the image.

Other visual secret sharing schemes have been proposed: In [5], a method for intellectual property protection of grey level images was presented; a secret sharing scheme for 250 grey-level images which elaborates shares of smaller size than the original image and based on Shamir scheme, was presented in [29]; a scheme for color images by using additive cellular automata was published in [2]. However, in visual schemes, there is, in general, a great contrast loss between the secret image and the recovered one.

A scheme for sharing several secrets and not only one secret is called a multisecret sharing scheme. In this case, there exits $m \geqslant 1$ secrets, $S_1, \ldots, S_m$, to be shared among a set of n participants. This type of cryptographic protocol is very useful when several secrets must be protected by using no more information than when only one secret must be protected, or when the size of the secret to protect is so big that it must be broken into several parts.

In the last years several multisecret sharing schemes have been proposed. Some of them are based on hash functions (see [15,17,18]), on Lagrange interpolation polynomials [16,36] or in coding theory [8]. Nevertheless, most of them are schemes to share texts and there are only a few proposals for sharing images. The proposal given in [19] was based on the RSA cryptosystem and the threshold scheme by Shamir; whereas the scheme presented in [31] was based on visual cryptography. Moreover, secret sharing schemes with multi-users have been proposed to be used in watermarking schemes [33]. In this proposal, the original watermark is split into two shares so that the first share is embedded into the cover image in order to increase the security; whereas the second one is used to generate several keys.

In this work, a new multisecret sharing scheme for color images is proposed. The generation of the shares from the secret color images is based on bidimensional reversible cellular automata with memory. As it is known, cellular automata are discrete dynamical systems which simulate complex behaviors by means of simple computational models. Cellular automata have been widely used in cryptography [3,10,12,14,22,24,34,35].

The rest of this work is organized as follows: In Section 2, the basic definitions about bidimensional cellular automata are recalled; in Section 3, the multisecret sharing scheme based on reversible cellular automata with memory is presented. Some experimental results are shown in Section 4; the security analysis of the scheme is carried out in Section 5; and the conclusions and future work are included in Section 6.

2. Bidimensional cellular automata

Bidimensional cellular automata (CA) are discrete dynamical systems defined by a 4-uplet $(\mathbb{C}, S, V, f)$. $\mathbb{C}$ is the cellular space formed by a finite two-dimensional array of $r \times c$ identical objects called cells, where the (i,j)th cell is denoted by $\langle i,j\rangle$ (see Table 1).

At each discrete time step t, each cell $\langle i,j\rangle$ is endowed with a state, $s_{ij}^{(t)}$, belonging to a finite set S. In this work we will consider $S = \mathbb{Z}_2 = \{0,1\}$.

The CA evolves deterministically in discrete time steps changing the states of all cells according to a local transition function, f. The updated state of the cell $\langle i,j\rangle$ depends on the states of a set of cells called its neighborhood which is defined by means of a set $V \subset \mathbb{Z} \times \mathbb{Z}$. This work deals with Moore neighborhoods, that is, the neighbor cells of $\langle i,j\rangle$, V_{ij}, are the eight nearest cells around it and itself:

$$V = \{(-1,-1),(-1,0),(-1,1),(0,-1),(0,0),(0,1),(1,-1),(1,0),(1,1)\},$$
$$V_{ij} = \{\langle i-1,j-1\rangle,\langle i-1,j\rangle,\langle i-1,j+1\rangle,\langle i,j-1\rangle,\langle i,j\rangle,\langle i,j+1\rangle,\langle i+1,j-1\rangle,\langle i+1,j\rangle,\langle i+1,j+1\rangle\}.$$

As a consequence,

$$s_{ij}^{(t+1)} = f(V_{ij}^{(t)}), \quad 1 \leqslant i \leqslant r, 1 \leqslant j \leqslant c,$$

where $V_{ij}^{(t)}$ stands for the set of states of the neighbor cells of $\langle i,j\rangle$ at time t.

The $(r \times c)$th order matrix

$$C^{(t)} = \begin{pmatrix} s_{11}^{(t)} & s_{12}^{(t)} & \cdots & s_{1c}^{(t)} \\ s_{21}^{(t)} & s_{22}^{(t)} & \cdots & s_{2c}^{(t)} \\ \vdots & \vdots & \ddots & \vdots \\ s_{r1}^{(t)} & s_{r2}^{(t)} & \cdots & s_{rc}^{(t)} \end{pmatrix}$$

Table 1
Cellular space of a bidimensional cellular automata with $r \times c$ cells

$\langle 1,1\rangle$	$\langle 1,2\rangle$	$\cdots$	$\langle 1,c\rangle$
$\langle 2,1\rangle$	$\langle 2,2\rangle$	$\cdots$	$\langle 2,c\rangle$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\langle r,1\rangle$	$\langle r,2\rangle$	$\cdots$	$\langle r,c\rangle$