A multiset sharing scheme for color images based on cellular automata

G. ALVAREZ¹, L. HERNÁNDEZ ENCINAS^{1*}
and A. MARTÍN DEL REY²

¹Dpt. Information Processing and Coding
Applied Physics Institute, CSIC
C/ Serrano 144, 28006-Madrid, Spain
{gonzalo, luis}@iec.csic.es

²Dpt. Applied Mathematics, EPS, Universidad de Salamanca
C/ Hornos Caleros 50, 05003-Ávila, Spain
delrey@usal.es

Abstract

In this work a new multiset sharing scheme for secret color images among a set of users is proposed. The protocol allows 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.

Keywords. Secret sharing; Color images; Cryptography; Cellular Automata; Image Processing.

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, $1 \leq k \leq n$, 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 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 exists $m \geq 1$ secrets, $S_1, \dots, S_m$, 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 $(\mathcal{C}, S, V, f)$. $\mathcal{C}$ 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).

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

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

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,

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

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

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

is the configuration at time t of the CA, and $C^{(0)}$ is its initial configuration. Moreover, the sequence $E^{(k)} = \{C^{(t)}\}_{0 \leq t \leq k}$ is called the evolution of order k of the CA. Due to the fact that the number of cells of the CA is finite, boundary conditions must be considered in order to assure the well-defined dynamics of the cellular automaton. In this work periodic boundary conditions are taken: if $i \equiv u \pmod{r}$, and $j \equiv v \pmod{c}$, then $s_{ij}^{(t)} = s_{uv}^{(t)}$.

Let $\mathcal{C}$ be the set of all possible configurations of the CA, then the global function of the CA is a linear transformation, $\Phi: \mathcal{C} \rightarrow \mathcal{C}$, that yields the configuration at the next time step in the evolution of the CA, that is, $C^{(t+1)} = \Phi(C^{(t)})$. If Φ is bijective then there exists another cellular automaton, called its inverse, with global function Φ^{-1} . When such inverse cellular automaton exists, the original CA is called reversible and the backward evolution is possible ([30]).

A particular and very interesting type of bidimensional CA are linear CA (LCA for short) whose evolution is given by means of a linear local transition function, $s_{ij}^{(t+1)} = f(V_{ij}^{(t)})$, such that:

$$\begin{aligned} f(V_{ij}^{(t)}) &= \sum_{\alpha, \beta \in \{-1, 0, 1\}} \lambda_{\alpha, \beta} s_{i+\alpha, j+\beta}^{(t)} \pmod{2} \\ &= \left(\lambda_{-1, -1} s_{i-1, j-1}^{(t)} + \lambda_{-1, 0} s_{i-1, j}^{(t)} + \lambda_{-1, 1} s_{i-1, j+1}^{(t)} \right. \\ &\quad + \lambda_{0, -1} s_{i, j-1}^{(t)} + \lambda_{0, 0} s_{i, j}^{(t)} + \lambda_{0, 1} s_{i, j+1}^{(t)} \\ &\quad \left. + \lambda_{1, -1} s_{i+1, j-1}^{(t)} + \lambda_{1, 0} s_{i+1, j}^{(t)} + \lambda_{1, 1} s_{i+1, j+1}^{(t)} \right) \pmod{2}, \end{aligned} \quad (1)$$

$1 \leq i \leq r$, $1 \leq j \leq c$, and $\lambda_{\alpha, \beta} \in \mathbb{Z}_2$. Note that the sequence of coefficients $\{\lambda_{\alpha, \beta} : \alpha, \beta \in \{-1, 0, 1\}\}$ determines in a univocal manner the LCA. Consequently, every one of these local transition functions can be defined by an integer number called its rule number: ω , which is given by:

$$\begin{aligned} \omega &= \lambda_{-1, -1} 2^8 + \lambda_{-1, 0} 2^7 + \lambda_{-1, 1} 2^6 + \lambda_{0, -1} 2^5 \\ &\quad + \lambda_{0, 0} 2^4 + \lambda_{0, 1} 2^3 + \lambda_{1, -1} 2^2 + \lambda_{1, 0} 2^1 + \lambda_{1, 1} 2^0, \end{aligned} \quad (2)$$

with $\lambda_{\alpha\beta} \in \mathbb{Z}_2$. Note that as $\lambda_{\alpha\beta} \in \mathbb{Z}_2$, it takes two values, 0 or 1; and as ω has 9 addends then there are $2^9 = 512$ possible rule numbers which goes from 0 to 511, each one of them defines a linear CA. The local transition function of the LCA with rule number ω is denoted by f_ω .

The main feature of such cellular automata is that they can be interpreted in terms of Linear Algebra (see, for example, [6]). As an example, in Figure 1 the space-time diagram of the LCA defined by $\lambda_{\alpha\beta} = 1$ for every $\alpha, \beta \in \{-1, 0, 1\}$, that is the LCA with rule number 511, is shown.

Figure 1: Space-time diagram of a linear CA

The standard paradigm for CA states the state of every cell at time $t + 1$ only depends on the state of its neighbor cells at time t . However, it is possible to consider CA for which the state of every cell at time $t + 1$ also depends on the states of its neighbor cells at times $t - 1, t - 2, \dots$. In this case the CA is called memory cellular automata, MCA for short (see, for example, [1]). In this work, we will consider k -th order linear MCA (LMCA) whose local transition function takes the form $s_{ij}^{(t+1)} = F(V_{ij}^{(t)}, \dots, V_{ij}^{(t-k+1)})$, such that:

$$F(V_{ij}^{(t)}, \dots, V_{ij}^{(t-k+1)}) = (f_{\omega_1}(V_{ij}^{(t)}) + \dots + f_{\omega_k}(V_{ij}^{(t-k+1)})) \pmod{2}, \quad (3)$$

where $1 \leq i \leq r$, $1 \leq j \leq c$, $\omega_1, \omega_2, \dots, \omega_k \in [0, 511]$, and the computation considers modulo 2 because the arithmetic is performed in $\mathbb{Z}_2$. Note that, in order to compute the evolution of a LMCA it is necessary to know its k initial configurations: $\{C^{(0)}, \dots, C^{(k-1)}\}$. For example, if we consider the 3-th order

LMCA defined by:

$$\begin{aligned}
& F\left(V_{ij}^{(t)}, V_{ij}^{(t-1)}, V_{ij}^{(t-2)}\right) \\
&= \left(f_{511}\left(V_{ij}^{(t)}\right) + f_{511}\left(V_{ij}^{(t-1)}\right) + f_{511}\left(V_{ij}^{(t-2)}\right)\right) (\bmod 2) \\
&= \left(s_{i-1,j-1}^{(t)} + s_{i-1,j}^{(t)} + s_{i-1,j+1}^{(t)} + s_{i,j-1}^{(t)} + s_{i,j}^{(t)}\right. \\
&\quad \left.+ s_{i,j+1}^{(t)} + s_{i+1,j-1}^{(t)} + s_{i+1,j}^{(t)} + s_{i+1,j+1}^{(t)}\right) (\bmod 2) \\
&\quad + \left(s_{i-1,j-1}^{(t-1)} + s_{i-1,j}^{(t-1)} + s_{i-1,j+1}^{(t-1)} + s_{i,j-1}^{(t-1)} + s_{i,j}^{(t-1)}\right. \\
&\quad \left.+ s_{i,j+1}^{(t-1)} + s_{i+1,j-1}^{(t-1)} + s_{i+1,j}^{(t-1)} + s_{i+1,j+1}^{(t-1)}\right) (\bmod 2) \\
&\quad + \left(s_{i-1,j-1}^{(t-2)} + s_{i-1,j}^{(t-2)} + s_{i-1,j+1}^{(t-2)} + s_{i,j-1}^{(t-2)} + s_{i,j}^{(t-2)}\right. \\
&\quad \left.+ s_{i,j+1}^{(t-2)} + s_{i+1,j-1}^{(t-2)} + s_{i+1,j}^{(t-2)} + s_{i+1,j+1}^{(t-2)}\right) (\bmod 2), \tag{4}
\end{aligned}$$

then its space-time diagram is shown in Figure 2.

Figure 2: Space-time diagram of a 3-th order LMCA

Note that it is very easy to construct a reversible LMCA: it is sufficient to take $f_{\omega_k}\left(V_{ij}^{(t-k+1)}\right) = s_{ij}^{(t-k+1)}$ in equation (3) (note that this is the local transition function of the LCA with rule number 16). Consequently, the LMCA defined by

$$\begin{aligned}
& F\left(V_{ij}^{(t)}, \dots, V_{ij}^{(t-k+1)}\right) \\
&= \left(f_{\omega_1}\left(V_{ij}^{(t)}\right) + \dots + f_{\omega_{k-1}}\left(V_{ij}^{(t-k+2)}\right) + s_{ij}^{(t-k+1)}\right) (\bmod 2), \tag{5}
\end{aligned}$$

is reversible and its inverse CA is another k -th order LMCA with the following local transition function, $s_{ij}^{(t+1)} = G(V_{ij}^{(t)}, \dots, V_{ij}^{(t-k+1)})$, where:

$$G(V_{ij}^{(t)}, \dots, V_{ij}^{(t-k+1)}) = \left(-f_{\omega_{k-1}}(V_{ij}^{(t)}) - \dots - f_{\omega_1}(V_{ij}^{(t-k+2)}) + s_{ij}^{(t-k+1)} \right) \pmod{2}. \quad (6)$$

This type of cellular automata was introduced by Fredkin (see [13]). In Figure 3 the space-time diagram of the reversible MCA constructed starting from the MCA of the last example, is shown.

Figure 3: Space-time diagram of a reversible 3-th order MCA

Figures 1, 2, and 3 show the space-time diagrams (for time steps $t = 0, 1, 2, \dots, 14$) obtained from three CA which are related in some way. These diagrams are similar, but they are obtained in a different way. The first diagram corresponds to a LCA with rule number 511; whereas the other two diagrams are space-time diagrams of two invertible CA. In fact, the second diagram is a diagram of a 3-th order LMCA with rule numbers 511, 511, and 511, and the last diagram is the space-time diagram of its inverse CA. This last diagram is the diagram of a LCA with rule number 16.

3 The new multiset sharing scheme

In this section we propose a new multiset sharing scheme. The scheme is a (n, n) -threshold scheme such that each participant $P_1, \dots, P_n$ shares a secret color image, $S_1, \dots, S_n$. All participants can recover all secret images if all of them share their shares.

Set S_m with $m = 1, \dots, n$ the secret images to be shared, which are defined by $r \times c$ pixels. It is possible that some secret images have different size and different color palette. In this case white pixels are padded around the original image to get the same size for all secret images (this way of padding the images is secure due to the fact that a truly random sequence is used in the step 5 of the setup phase), and we consider the biggest color palette used by the secret images.

These images can be considered as one of the components of the initial configuration of a $(n + 1)$ -th order LMCA of, at most, $24(r \times c)$ cells, $C^{(m)}$, as follows: It is well-known that the numeric value of the color of each pixel of an image, for example S_m , can be encoded (via RGB) with b bits by means of a palette of $p = 2^b$ colors, where $b = 1, 8$ or 24 . Consequently each image can be represented by means of a binary matrix of order $b(r \times c)$. This binary image stands for the configuration of the cellular automata.

The multisecret sharing scheme is divided in the following three phases.

3.1 Setup phase

In this phase, the trusted party or dealer defines the LMCA of order $n + 1$ and its initial configuration as follows:

1. D receives from each of the n participants his secret color image and pads them, with white pixels around each image, in order to obtain a set of n images, S_m , $m = 1, \dots, n$, defined by the same number of pixels. Moreover, in order to obtain the same color palette for all images, D considers that each pixel is codified by b bits ($b \in \{1, 8, 24\}$), taking into account the biggest color palette of all secret images.
2. D generates n random integer numbers $\omega_m \in [0, 511]$, $m = 1, \dots, n$, in order to define m local functions of n LCA, f_{ω_m} .
3. D constructs the local transition function of the LMCA, of order $n + 1$, $s_{ij}^{(t+1)} = F(V_{ij}^{(t)}, \dots, V_{ij}^{(t-n)})$, which is similar to that given in equation (3):

$$F(V_{ij}^{(t)}, \dots, V_{ij}^{(t-n)}) = \left(\sum_{m=1}^n f_{\omega_m}(V_{ij}^{(t-m+1)}) + s_{ij}^{(t-n)} \right) \pmod{2}. \quad (7)$$

4. D defines n components of the initial configuration of LMCA: $C^{(m)} = S_m$, with $m = 1, \dots, n$, which are the n secret color images shared by the n participants.
5. D generates a random color image, S_0 , with the same size and the same color palette than the other images and considers $S_0 = C^{(0)}$, in order to complete the initial configuration of LMCA of order $n + 1$. Note that the security of the system relies on the use of a truly random generator to generate S_0 .

3.2 Sharing phase

In this phase, D computes the shares to be distributed in a secure way to the n participants as follows:

1. D generates at random an integer number $l \geq n + 2$.
2. D computes the evolution of order $(l + n - 1)$ of the LMCA defined in the setup phase:

$$\{C^{(0)}, C^{(1)}, \dots, C^{(n)}, C^{(n+1)}, \dots, C^{(l-1)}, C^{(l)}, \dots, C^{(l+n-1)}\}.$$

Each configuration $C^{(t)}$, $t > n$, is a noise-like image which can be identified as a shadow of an original image.

3. D distributes in a secure way a share, (m, ω_m, R_m) , $m = 1, \dots, n$, to each participant $P_1, \dots, P_n$. This share is composed by three elements: (1) the order number of the participant, m , (2) its rule number, ω_m , and (3) the shadow R_m . The shadows $R_m = C^{(l+m-1)}$, $m = 1, \dots, n$, are the last n configurations of the evolution of the LMCA.
4. D publishes the number l and the last component of the initial configuration for the inverse CA, i.e, $R_0 = C^{(l-1)} = \tilde{C}^{(n+1)}$.

3.3 Recovering phase

In this phase, as the sharing scheme is a (n, n) -threshold scheme, all participants have to share their shadows so that all of them can recover the n secret color images.

1. Each participant shares his shadow with the rest of them. In this way, a (or the same) dealer D receives the following data: (m, ω_m, R_m) , $1 \leq m \leq n$, and moreover, D knows l and R_0 as they are public.
2. The dealer D computes the secret color images by considering the initial configuration of the inverse CA of the original LMCA:

$$\tilde{C}^{(1)} = R_n = C^{(l+n-1)}, \dots, \tilde{C}^{(n)} = R_1 = C^{(l)}, \tilde{C}^{(n+1)} = R_0 = C^{(l-1)},$$

and by iterating $l - 1$ times the LMCA of order $n + 1$ given by the local transition function, $s_{ij}^{(t+1)} = G(V_{ij}^{(t)}, \dots, V_{ij}^{(t-n)})$, similar to that of the expression (6):

$$G(V_{ij}^{(t)}, \dots, V_{ij}^{(t-n)}) = \left(- \sum_{m=n}^1 f_{\omega_m}(V_{ij}^{(t+m-n)}) + s_{ij}^{(t-n)} \right) \pmod{2}.$$

Then, D obtains the n secret color images:

$$\tilde{C}^{(l)} = C^{(n)} = S_n, \tilde{C}^{(l+1)} = C^{(n-1)} = S_{n-1}, \dots, \tilde{C}^{(n+l+1)} = C^{(1)} = S_1.$$

Note that l and R_0 can be made public by the first dealer due to the fact that knowing these values does not reduce the security of the scheme. Moreover, to recover the secrets it is necessary that the (new) dealer knows those values.

In relation to the complexity and efficiency of the protocol, it is necessary to determine the computations needed in each phase. In the setup phase, the computations are reduced to generate n random integer numbers in the interval $[0, 511]$ and, at most, $24(r \times c)$ random bits. It is obvious that the time for these computations is negligible. Moreover, the computations for the sharing and for the recovering phases are the same and they consist in obtaining $l - 1$ shadows in the evolution of the CA considered. Each new pixel of a shadow is computed by adding, at most, 9 pixels with, at most, 24 bits each. Due to the fact that each shadow has $r \times c$ pixels, the computation of all shadows requires $9(l - 1)(r \times c)$ binary additions of numbers of 24 bits. Hence, the protocol is reduced to compute a number of additions which depends, basically, on the size of the secret images.

4 Experimental results

As an example, we present the experimental results of a multisecret sharing scheme with $n = 4$ participants. The participants will share the secret color images shown in Figures 4 and 5, respectively.

The first secret color image is a black and white photo of 512×512 of Lena. The second image is a smaller secret of peppers with 236-grey level image of 256×256 pixels, the third image is a color photo of 332×504 pixels of Marilyn with 8514 colors; and the fourth image is a color photo of a baboon of 512×512 pixels and with 230655 colors.

Figure 4: The first and second secret color images to be shared

In this case, the dealer, D , receives from the participants the $n = 4$ secret images shown in Figures 4 and 5, and D proceeds with the setup phase.

First of all, D consider the following values: $r = 512$, $c = 512$, and $p = 2^{24}$, in order to pad the four secret images (step 1). After that, D generates four

Figure 5: The third and fourth secret color images to be shared

integer numbers, ω_i , in the interval $[0, 511]$. In the present example, these values are $\omega_1 = 93$, $\omega_2 = 316$, $\omega_3 = 477$, and $\omega_4 = 398$ (step 2).

From these values, D constructs the local transition function of the LMCA, F , to be used in the protocol, from the four local transitions functions of LCA, f_{ω_i} . To do this, D considers that the coefficients $\lambda_{\alpha,\beta}$ defined in the equation (2) determine whether the cell in the position (α, β) of the Moore neighborhood is taken into account or not.

In fact, from the values of ω_i , $i = 1, \dots, 4$, we have:

$$\begin{aligned}\omega_1 &= 93 = 1 \cdot 2^6 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1, \\ \omega_2 &= 316 = 1 \cdot 2^8 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2, \\ \omega_3 &= 477 = 1 \cdot 2^8 + 1 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1, \\ \omega_4 &= 398 = 1 \cdot 2^8 + 1 \cdot 2^7 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1,\end{aligned}$$

hence, the functions f_{ω_i} of LCA are the following:

$$\begin{aligned}f_{93} \left(V_{ij}^{(t)} \right) &= s_{-1,1}^{(t)} + s_{0,0}^{(t)} + s_{0,1}^{(t)} + s_{1,-1}^{(t)} + s_{1,1}^{(t)}, \\ f_{316} \left(V_{ij}^{(t-1)} \right) &= s_{-1,-1}^{(t-1)} + s_{0,-1}^{(t-1)} + s_{0,0}^{(t-1)} + s_{0,1}^{(t-1)} + s_{1,-1}^{(t-1)}, \\ f_{477} \left(V_{ij}^{(t-2)} \right) &= s_{-1,-1}^{(t-2)} + s_{-1,0}^{(t-2)} + s_{-1,1}^{(t-2)} + s_{0,0}^{(t-2)} + s_{0,1}^{(t-2)} + s_{1,-1}^{(t-2)} + s_{1,1}^{(t-2)}, \\ f_{398} \left(V_{ij}^{(t-3)} \right) &= s_{-1,-1}^{(t-3)} + s_{-1,0}^{(t-3)} + s_{0,1}^{(t-3)} + s_{1,-1}^{(t-3)} + s_{1,0}^{(t-3)},\end{aligned}$$

These expressions mean that, for example, the local transition function f_{93} , only considers the states of the cells in the positions $(-1, 1)$, $(0, 0)$, $(0, 1)$, $(1, -1)$, and $(1, 1)$.

These local transition functions permit D to construct F , the local transition

function of LMCA of order $5 = n + 1$, to be used in the protocol, as follows:

$$F\left(V_{ij}^{(t)}, V_{ij}^{(t-1)}, V_{ij}^{(t-2)}, V_{ij}^{(t-3)}, V_{ij}^{(t-4)}\right) = \left(f_{93}\left(V_{ij}^{(t)}\right) + f_{316}\left(V_{ij}^{(t-1)}\right) + f_{477}\left(V_{ij}^{(t-2)}\right) + f_{398}\left(V_{ij}^{(t-3)}\right) + s_{ij}^{(t-4)}\right) \pmod{2}.$$

To end this phase (steps 4 and 5), D generates a truly random image of size 512×512 and 2^{24} colors and defines $C^{(0)}$ = “Random image”, $C^{(1)}$ = “Lena”, $C^{(2)}$ = “Peppers”, $C^{(3)}$ = “Marilyn”, and $C^{(4)}$ = “Baboon” (see the first image of Figure 6, and Figures 7 and 8).

In the sharing phase, D generates at random an integer number, $l \geq n + 2 = 6$, in this case, $l = 10$ (step 1) and computes the evolution of order $l + n - 1 = 13$ of the LMCA defined in the setup phase (step 2). Figure 6 shows the random image defined in the step 5 of the setup phase, $C^{(0)}$, and the next space-time diagram following to the four secret images, that is, the configuration $C^{(5)}$ (we do not include all the space-time diagrams of the evolution of the LMCA defined in the protocol because the configurations $C^{(6)}$ - $C^{(9)}$ are of the same type, i.e., they are like random-noise images).

Figure 6: Configurations $C^{(0)}$ and $C^{(5)}$

At the end of this step 2, D have obtained the four shadows to be distributed amongst the four participants. Figures 7 and 8 show the shadows of the $n = 4$ participants.

To finish the sharing phase (steps 3 and 4), D distributes in a secure way the following values to each participant:

$$\begin{aligned} P_1: & \quad (1, \omega_1 = 93, R_1 = C^{(10)}), \\ P_2: & \quad (2, \omega_1 = 316, R_2 = C^{(11)}), \\ P_3: & \quad (3, \omega_1 = 477, R_3 = C^{(12)}), \\ P_4: & \quad (4, \omega_1 = 398, R_4 = C^{(13)}), \end{aligned}$$

and finally, D publishes the value $l = 10$ and the configuration $R_0 = C^{(9)}$.

To recover the original secret images, the participants only have to join their shares, consider the data made public for the dealer, i.e., $l = 10$, and R_0 (step

1); and follow the step 2 of this phase, which is similar to the step 2 of the sharing phase, but with different parameters. In fact, in this step, the LMCA is defined by the configurations

$$\tilde{C}^{(1)} = R_4, \tilde{C}^{(2)} = R_3, \tilde{C}^{(3)} = R_2, \tilde{C}^{(4)} = R_1, \tilde{C}^{(5)} = R_0,$$

and by the local transition function G given by

$$G\left(V_{ij}^{(t)}, V_{ij}^{(t-1)}, V_{ij}^{(t-2)}, V_{ij}^{(t-3)}, V_{ij}^{(t-4)}\right) = \left(-f_{398}\left(V_{ij}^{(t)}\right) - f_{477}\left(V_{ij}^{(t-1)}\right) - f_{316}\left(V_{ij}^{(t-2)}\right) - f_{93}\left(V_{ij}^{(t-3)}\right) + s_{ij}^{(t-4)}\right) \pmod{2}.$$

The secret images recovered are shown in Figures 9 and 10 which are exactly the same than the original ones considered by D after to pad them, that is, their contents are the same, although their sizes and color palettes are not the same in all cases.

Figure 7: Shadows of the first and second participants: $C^{(10)}$ and $C^{(11)}$

Figure 8: Shadows of the third and fourth participants: $C^{(12)}$ and $C^{(13)}$

Figure 9: Secret color images recovered by the participants

Figure 10: Secret color images recovered by the participants

5 Security analysis

In this section we analyze the security of the proposed protocol. In particular, we prove that the protocol is ideal-like and perfect, and it resists the most important statistical attacks.

5.1 The sharing scheme is ideal-like and perfect

If the original secret color images are of different size or they are defined by different color palettes, the scheme is not ideal in a strict sense, because there is not ‘a size’ for all the secrets. In this case, the size of the shadows is equal to the biggest secret image and the color palette is also the biggest of the images. Nevertheless, if all secret images have the same size and the same color palette, the scheme is ideal as the shadows are configurations of the same LMCA. Hence, we can consider that the scheme is ideal-like.

Moreover, the scheme is also perfect due to the fact that if only one shadow

is unknown, say $\tilde{C}^{(n-q)} = C^{(l+q)}$, for a q with $0 \leq q \leq n-1$, then there is no information about the configuration $\tilde{C}^{(n+2)} = C^{l-2}$, and hence for any other $\tilde{C}^{(n+p)} = C^{l-p}$, with $3 \leq p \leq l$. This is because the evolution of the LMCA is given by the following linear system:

$$s_{ij}^{(n+2)} = \left(u_{ij} + s_{ij}^{(n-q)} + v_{ij} \right) \pmod{2}, \quad 0 \leq i \leq r-1, 0 \leq j \leq c-1,$$

where u_{ij} and v_{ij} are values obtained from the known configurations; whereas $s_{ij}^{(n+2)}$ and $s_{ij}^{(n-q)}$ are unknown values. In this situation, a system with $r \cdot c$ equations with $2r \cdot c$ unknowns is obtained which can not be solved. A harder situation to be solved will be obtained if the number of unknown configurations is greater than one.

5.2 Statistical analysis

We have carried out a statistical analysis by means of several statistical tests in order to determine the security of the new multisecret sharing scheme. The results allows us to state that it strongly resists the statistical attacks.

The first statistical test we have carried out is the set of tests stated by FIPS ([11, 23]) in order to ensure the randomness of a binary sequence of 20000 bits. This set of test is formed by the following tests: Monobit, Poker, Runs, Long runs, and Autocorrelation. We have implemented these tests in Matlab and all the shadows shown in Figure 7 and 8 have passed these tests.

As it is well known, the linear complexity of a bit sequence s is defined as the length of the shortest LFSR that generates the given sequence, and it is denoted by $L(s)$. If L_i , $i \geq 1$, is the linear complexity of the finite subsequence $s^i = s_1, s_2, \dots, s_i$, of the sequence s , then the sequence $L_1, L_2, \dots$ is called the linear complexity profile of s . This sequence can be plotted by representing the points (i, L_i) , $i \geq 1$, and joining them by horizontal and vertical segments. It is clear that the graph of a linear complexity profile is not decreasing and that the expected linear complexity of a random sequence should closely follow the line $L = i/2$. Here we have used the Berlekamp-Massey algorithm ([23, §6.2.3]) to determine the linear complexity of the finite sequences formed by the 10000 first bit of each shadow. In all cases, we have obtained a value of $L(s) = 5000$.

As an example, in Figure 11, the runs test and the linear complexity profile of the share 1 are shown (see Figure 7).

The second statistical test tries to determine the confusion and diffusion properties of the proposed scheme. This test is performed by a correlation test of adjacent pixels of the original image and its shadows. The correlation test between adjacent pixels in the images has been made selecting in a random way 1000 pairs of two vertically adjacent pixels, 1000 pairs of two horizontally adjacent pixels, and 1000 pairs of two diagonally adjacent pixels, for each original image as well as for its shadows. In each case, the correlation coefficient of each pair has been computed and the results are shown in Tables 2 and 3. From these tables it is observed that the correlation coefficients of the images and the shadows are different enough, which guarantees the confusion and diffusion of

Figure 11: Runs test and Linear complexity profile of the shadow 1

the pixels. It is observed, in addition, that the correlations in the shadows are very small indeed.

	Image 1	Image 2	Image 3	Image 4
Horizontal	-0.3546	0.9553	0.9654	0.9169
Vertical	-0.0534	0.9704	0.9685	0.8683
Diagonal	0.2902	0.9191	0.9439	0.8497

Table 2: Correlation coefficients of adjacent pixels for the secret color images

	Shadow 1	Shadow 2	Shadow 3	Shadow 4
Horizontal	0.0086	-0.0008	-0.0298	-0.0405
Vertical	0.0065	0.0104	-0.0057	0.0567
Diagonal	-0.0103	0.0277	-0.0081	-0.0367

Table 3: Correlation coefficients of adjacent pixels for the shadows

Figure 12 and 13 show the correlation distribution of 1000 couples of horizontal adjacent pixels of secret images and shadows, respectively. One can observe how in the first case, the distributions follow, approximately, the principal diagonal, which gives an idea of the strong correlation among the pixels of the secret images; whereas in the second case, the clouds of points seem to distribute in a random way, which indicates the weak correlation among the pixels of the shadows.

The third test has been designed in order to test the influence of one-pixel change on the whole share. This test uses two measures: the number of pixels change rate, *NPCR*, which measures the percentage of different pixel numbers

Figure 12: Correlation of horizontal adjacent pixels of the secret images

between two images; and the unified average changing intensity, $UACI$, which measures the average intensity of differences between two images.

Suppose that $R = C^{t_0} = (s_{ij}^{t_0})$ and $\tilde{R} = \tilde{C}^{t_0} = (\tilde{s}_{ij}^{t_0})$ are two shadows obtained from original secrets that differ in only one-pixel. Define a bipolar array of size $r \times c$, $D = (d_{ij})$, such that $d_{ij} = 0$ if $s_{ij}^{t_0} = \tilde{s}_{ij}^{t_0}$, and $d_{ij} = 1$ otherwise. The $NPCR$ and $UACI$ are defined as follows:

$$NPCR = \frac{\sum_{i=1}^r \sum_{j=1}^c d_{ij}}{r \cdot c} \times 100\%, \quad (8)$$

$$UACI = \frac{1}{r \cdot c} \left(\sum_{i=1}^r \sum_{j=1}^c \frac{|s_{ij}^{t_0} - \tilde{s}_{ij}^{t_0}|}{\text{number of colors}} \right) \times 100\%, \quad (9)$$

From the previous definition, a high value of $NPCR$ and a high value of $UACI$ mean that the change of a pixel in the secret image influences significantly in the shares. The range for $NPCR$ is between 0-100 and in the present example

Figure 13: Correlation of horizontal adjacent pixels of the shadows

these values are bigger than 99. For this reason, we can state that the proposed scheme is very sensitive with respect to small changes in the secret images.

The results for the NPCR test and for the UACI test comparing the corresponding pairs of shares are shown in Table 4 and Table 5, respectively.

6 Conclusions and Future work

In this work a new multisecret sharing scheme for color images has been presented. The scheme is developed by a (n, n) -threshold scheme and it is based on bidimensional reversible cellular automata with memory. We have shown that the scheme is ideal-like and perfect. Moreover, we have studied its statistical properties and we have proved that the multisecret sharing scheme is secure against statistical attacks.

Our future work consists of extending the previous multisecret sharing scheme to more general (k, n) -threshold schemes, where $k < n$. Moreover, we will try

Shadows	Red	Green	Blue
0 – 0	99.6040	99.5972	99.5975
1 – 1	99.5975	99.6201	99.5808
2 – 2	99.6025	99.6212	99.6269
3 – 3	99.5964	99.5892	99.6136
4 – 4	99.6162	99.6174	99.6132

Table 4: NPCR test comparing the corresponding pairs of shares

Shadows	Red	Green	Blue
0 – 0	33.4249	33.4396	33.4449
1 – 1	33.5108	33.4930	33.4973
2 – 2	33.3500	33.4339	33.4945
3 – 3	33.4758	33.4463	33.4672
4 – 4	33.5025	33.4019	33.3772

Table 5: UACI test comparing the corresponding pairs of shares

to define a new multisecret scheme in order to authenticate the dealer of the protocol, for example, by adding a signature scheme.

Acknowledgement

Author thanks to Julio Gómez for his comments and to the anonymous referees for their valuable suggestions. This work has been supported by Ministerio de Educación y Ciencia (Spain) under grant TSI2007-62657; by CDTI, Ministerio de Industria, Turismo y Comercio (Spain) in collaboration with Telefónica I+D (Project SEGUR@) with reference CENIT-2007 2004; and by Consejería de Educación y Cultura of Junta de Castilla y León (Spain), under grant SA110A06.

References

- [1] R. Alonso-Sanz, Reversible cellular automata with memory: two-dimensional patterns from a single seed. *Physica D* **175**(2003), 1–30.
- [2] G. Álvarez Marañón, L. Hernández Encinas and A. Martín del Rey, A new secret sharing scheme for images based on additive 2-dimensional cellular automata, *Lecture Notes in Comput. Sci.*, Pattern Recognition and Image Analysis, **3522** (2005), 411–418.
- [3] F. Bao, Cryptanalysis of a Partially Known Cellular Automata Cryptosystem, *IEEE Trans. Comput.* **53** (2004), 1493–1497.

- [4] G.R. Blakley, Safeguarding cryptographic keys, *AFIPS Conference Proceedings* **48** (1979), 313–317.
- [5] C.C. Chang and J.C. Chuang, An image intellectual property protection scheme for gray-level images using visual secret sharing strategy, *Pattern Recogn. Lett.* **23** (2002), 931–941.
- [6] P. Chaudhuri, D. Chowdhury, S. Nandi, and S. Chattopadhyay, *Additive cellular automata. Theory and Applications. Volume 1*, IEEE Computer Society Press, Los Alamitos, 1997.
- [7] Y.F. Chen, Y. K. Chan, C. C. Huang, M. H. Tsai, and Y. P. Chu, A multiple-level visual secret-sharing scheme without image size expansion, *Inform. Sciences* **177**, 21 (2007), 4696–4710.
- [8] H.Y. Chien, J.K. Jan and Y.M. Tseng, A practical (t, n) multi-secret sharing scheme, *IEICE Transactions on Fundamentals* E83-A (2000), 2762–2765.
- [9] C. K. Chu and W. G. Tzeng, Optimal resilient threshold GQ signatures, *Inform. Sciences* **177**, 8 (2007), 1834–1851.
- [10] R. Díaz Len, A. Hernández Encinas, L. Hernández Encinas, S. Hoya White, A. Martín del Rey, G. Rodríguez Sánchez, and I. Visus Ruíz, Wolfram cellular automata and their cryptographic use as pseudorandom bit generators, *Internat. J. Pure Appl. Math.* **4** (2003), 87–103.
- [11] FIPS 140-2, Security requirements for cryptographic modules, Federal Information Processing Standards Publication 140-2. U.S. Department of Commerce/National Institute of Standards and Technology, Springfield, VA, Issued May 25, 2001.
- [12] C. Fraile Rubio, L. Hernández Encinas, S. Hoya White, A. Martín del Rey, and G. Rodríguez Sánchez, The use of linear hybrid cellular automata as pseudorandom bit generators in cryptography, *Neural Parallel Sci. Comput.* **12** (2004), 175–192.
- [13] E. Fredkin, Digital mechanics. An informal process based on reversible universal cellular automata, *Physica D* **45** (1990) 254–270.
- [14] P. Guan, Cellular automaton public-key cryptosystem, *Complex Systems* **1** (1987), 51–57.
- [15] L. Harn, Comment: Multistage secret sharing based on one-way function, *Electronic Letters* **31** (1995), 262.
- [16] L. Harn, Efficient sharing (broadcasting) of multiple secret, *IEE Proceedings, Computers and Digital Techniques* **142** (1995), 237–240.
- [17] J. He and E. Dawson, Multisecret-sharing scheme based on one-way function, *Electronic Letters* **30** (1994), 1591–1592.

- [18] J. He and E. Dawson, Multisecret-sharing scheme based on one-way function, *Electronic Letters* **31** (1995), 93–95.
- [19] R.J. Hwang and C.C. Chang, An on-line secret sharing scheme for multisecrets, *Computer Communications* **21** (1998), 1170–1176.
- [20] K. Kaya and A. A. Selçuk, Threshold cryptography based on AsmuthBloom secret sharing, *Inform. Sciences* **177**, 19 (2007), 4148–4160.
- [21] H. Koga and E. Ueda, Basic properties of the (t, n) -threshold visual secret sharing scheme with perfect reconstruction of black pixels. *Des. Codes Cryptogr.* **40**, 1 (2006), 81–102.
- [22] W. Meier and O. Staffelbach, Analysis of pseudorandom sequences generated by cellular automata, *Lecture Notes in Comput. Sci.*, Advances in Cryptology - EUROCRYPT '91, **547** (1991), 186–189.
- [23] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1997.
- [24] S. Nandi, B.K. Kar, and P.P Chaudhuri, Theory and applications of cellular automata in cryptography, *IEEE Trans. Comput.* **43** (1994), 1346–1357.
- [25] M. Naor and A. Shamir, Visual cryptography, *Lect. Notes Comput. Sci.*, Advances in Cryptology EUROCRYPT'94, **950**, (1995), 1–12.
- [26] A. Shamir, How to share a secret, *Commun. ACM* **22** (1979) 612–613.
- [27] D.R. Stinson, An explication of secret sharing schemes, *Des. Codes Cryptogr.* **2** (1992), 357–390.
- [28] D.R. Stinson, *Cryptography Theory and Practice*, Second Edition, CRC Press, Boca Raton, FL., 2002.
- [29] C. Thien and J. Lin, Secret image sharing, *Computers & Graphics* **26** (2002), 765–770.
- [30] T. Toffoli and N. Margolus, Invertible cellular automata: A review, *Physica D* **45** (1990), 229–253.
- [31] C.S. Tsai, C.C. Chang, and T.S. Chen, Sharing multiple secrets in digital images, *J. Systems Software* **64** (2002) 163–170
- [32] L. Wang, Z. Cao, X. Li, and H. Qian, Simulatability and security of certificateless threshold signatures, *Inform. Sciences*, **177**, 6 (2007), 1382–1394.
- [33] F. H. Wang, K. K. Yen, L. C. Jain, and J. S. Pan, Multiuser-based shadow watermark extraction system, *Inform. Sciences* **177**, 12 (2007), 2522–2532.
- [34] S. Wolfram, Random sequence generation by cellular automata, *Adv. Appl. Math.* **7** (1986), 123–169.

- [35] S. Wolfram, Cryptography with cellular automata, *Lecture Notes in Comput. Sci.*, Advances in Cryptology - CRYPTO '85, **218** (1986), 429–432.
- [36] C.C. Yang, T.Y. Chang, and M.S. Hwang, A (t, n) multi-secret sharing scheme, *Appl. Math. Comput* **151** (2004), 483–490.