

Sharing secret color images using cellular automata with memory

G. Álvarez Marañón, L. Hernández Encinas*

Dpt. Tratamiento de la Información y Codificación, Instituto de Física Aplicada, CSIC

C/ Serrano 144, 28006-Madrid, Spain

E-mails: {gonzalo, luis}@iec.csic.es

A. Martín del Rey

Dpt. de Matemática Aplicada, E.P.S., Universidad de Salamanca

C/ Santo Tomás s/n, 05003-Ávila, Spain

E-mail: delrey@usal.es

Abstract

A (k, n) -threshold scheme based on two-dimensional memory cellular automata is proposed to share images in a secret way. This method allows to encode an image into n shared images so that only qualified subsets of k or more shares can recover the secret image, but any $k - 1$ or fewer of them gain no information about the original image. The main characteristics of this new scheme are: each shared image has the same size that the original one, and the recovered image is exactly the same than the secret image; *i.e.*, there is no loss of resolution.

Keywords: Cellular automata, Graphic cryptography, Image processing, Secret sharing, Threshold scheme.

1 Introduction

A *secret sharing scheme* is a method which allows to share a secret among a set of users in such a way that only qualified subsets of these users can recover the secret. Consequently, the basic idea in secret sharing schemes is

*Corresponding author. Tel.: (+34) 915 618 806 (ext. 458), Fax: (+34) 914 117 651, Email: luis@iec.csic.es

to divide the secret into a fixed number of pieces, called *shares* or shadows, which are distributed among the participants so that the pooled shares of certain subsets of users allow the reconstruction of the secret.

Secret sharing schemes were independently introduced by Shamir ([1]) and Blakley ([2]), and their original motivation was to safeguard cryptographic keys from loss. These schemes also have been widely employed in the construction of several types of cryptographic protocols (see, for example, [3]) and consequently, they have many applications in different areas such as access control, opening a bank vault, opening a safety deposit box, or even launching of missiles.

The basic example of a secret sharing scheme is the (k, n) -*threshold scheme* (or k -out- n scheme) for integers $1 \leq k \leq n$. In such scheme there exists a *dealer* (or mutually trusted party) and n participants. The dealer computes n secret shares S_i , $0 \leq i \leq n - 1$, from an initial secret S , and securely distributes them to the users P_0, \dots, P_{n-1} , in such a way that any k or more users who pool their shares may easily recover the original secret S , but any group knowing only $k - 1$ or fewer shares is unable to recover the secret. In other words, each group of $k - 1$ or fewer shares reveals absolutely no information about the secret image. Shamir's scheme, which is based on polynomial interpolation, and Blakley's scheme, based on the intersection of affine hyperplanes, are examples of (k, n) -threshold schemes.

Subsequently, Ito *et al.* ([4]) and Benaloh *et al.* ([5]) described a more general situation based on the specification of the subsets of participants that should be able to determine the secret and the subsets of participants that should not. These general secret sharing methods are intimately related to the notion of *access structure* (see [6, 7]).

For secret sharing schemes, the *information rate for a particular participant* is the bit-size ratio:

$$R_p = \frac{\text{size of the shared secret}}{\text{size of the participant's share}}. \quad (1)$$

Moreover, the *information rate for a secret sharing scheme* is the minimum rate over all participants. In this sense, an *ideal* secret sharing scheme is a scheme in which the size of the shares given to each participant is equal to the size of the secret; consequently, for ideal secret sharing schemes the information rate is 1. Moreover, secret sharing schemes satisfying the additional property that unqualified subsets can gain absolutely no information about the secret are called *perfect*. For a more detailed description we refer the reader to [3, 8, 9].

Usually, the secret to be shared consists in text data, but also images can be considered. The first scheme to share images was due to Naor and

Shamir ([10]) and it is called *visual cryptography*. It is based on *visual threshold schemes* k of n , *i.e.*, the original image is divided in n shares. Each of them is photocopied in a transparency and then, the original image is recovered by superimposing any k transparencies but no less. Moreover, no cryptographic protocol is used to recover it. Its main feature is the use of human vision properties in order to recover the original image.

Due to the characteristics of this model, only black & white images were suitable to be shared. Nevertheless, in recent years, a wide variety of new proposals based on visual cryptography have emerged not only for processing gray-level images ([11, 12, 13]), but also for color images ([14, 15, 16]). In these visual threshold schemes each pixel of the secret image is ciphered by means of h subpixels (the *pixel expansion*) for the n shares; consequently, the size of the shared images is much bigger than the original one. Moreover, another disadvantage of these schemes is that there is a great contrast loss between the secret image and the recovered one.

Furthermore, other algorithms for sharing images, not based in the visual cryptography paradigm, have appeared (see, for example, [17, 18]).

In this paper, we propose a new graphic sharing scheme; *i.e.*, a secret sharing scheme for black & white (b&w), gray-level and color images, by means of two-dimensional memory cellular automata. The proposed scheme is based on cellular automata and the properties of these kind of discrete dynamical systems permit us to define an algorithm for sharing secret images. In the scheme, the shares obtained for each participant have the same size than the secret image and the recovered image is exactly the same than the original one, without loss of resolution. These properties are not satisfied by any other graphic scheme.

Roughly speaking, two-dimensional cellular automata are time delay dynamical systems for which time and space are discrete. They consist of a collection of a finite two-dimensional array of simple objects, called cells, interacting locally with each other. Each cell can assume a state such that it changes in every time step according to a local rule whose variables are the states of some cells at previous time steps. The prize, compared to visual cryptography, is that in this new protocol some computations are needed to recover the original image.

The design of cryptographic protocols by means of two-dimensional cellular automata is a recent event, and their use are only restricted to symmetric ciphers for images (see [19, 20]), by the moment. On the other hand, one-dimensional cellular automata has been widely used not only for symmetric ciphers: stream ciphers (see, for example [21, 22]) and block ciphers ([23]), but also for asymmetric ciphers ([24]).

The rest of the paper is organized as follows: In Section 2, some basic

concepts regarding memory cellular automata are introduced. In Section 3, the new secret sharing scheme for b&w, gray-level and color images is presented. The security of the proposed scheme is analyzed and proved in Section 4. In Section 5 several examples for different classes of images and different schemes, are given. Finally, the conclusions of this paper are presented in Section 6.

2 Memory Cellular Automata

Two-dimensional finite cellular automata (2D-CA for short) are discrete dynamical systems formed by a finite two-dimensional array of $r \times s$ identical objects called *cells*, such that each of them can assume a state. The state of each cell is an element of the *finite state set*, S . Throughout this paper we will consider $S = \mathbb{Z}_c$, where $c = 2^b$ is the number of colors of the image; *i.e.*, if the image is a b&w image, then $b = 1$; for gray-level images the value is $b = 8$, and if it is a color image, then $b = 24$.

The (i, j) -th cell is denoted by $\langle i, j \rangle$, and the state of this cell at time t is $a_{ij}^{(t)} \in \mathbb{Z}_c$. The 2D-CA evolves deterministically in discrete time steps, changing the states of all cells according to a *local transition function*,

$$f: (\mathbb{Z}_c)^n \rightarrow \mathbb{Z}_c.$$

The updated state of each cell depends on the n variables of the local transition function, which are the previous states of a set of cells, including the cell itself, and constitute its *neighborhood*. For 2D-CA there are some classic types of neighborhoods, but in this work only the *extended Moore neighborhood* will be consider; that is, the neighborhood of the cell $\langle i, j \rangle$ is formed by its nine nearest cells:

$$V_{i,j} = \{ \langle i-1, j-1 \rangle, \langle i-1, j \rangle, \langle i-1, j+1 \rangle, \langle i, j-1 \rangle, \langle i, j \rangle, \langle i, j+1 \rangle, \langle i+1, j-1 \rangle, \langle i+1, j \rangle, \langle i+1, j+1 \rangle \}.$$

Graphically it can be seen as follows:

$\langle i-1, j-1 \rangle$	$\langle i-1, j \rangle$	$\langle i-1, j+1 \rangle$
$\langle i, j-1 \rangle$	$\langle i, j \rangle$	$\langle i, j+1 \rangle$
$\langle i+1, j-1 \rangle$	$\langle i+1, j \rangle$	$\langle i+1, j+1 \rangle$

Consequently the local transition function $f: (\mathbb{Z}_c)^9 \rightarrow \mathbb{Z}_c$ is

$$a_{ij}^{(t+1)} = f \left(a_{i-1,j-1}^{(t)}, a_{i-1,j}^{(t)}, a_{i-1,j+1}^{(t)}, a_{i,j-1}^{(t)}, a_{i,j}^{(t)}, a_{i,j+1}^{(t)}, a_{i+1,j-1}^{(t)}, a_{i+1,j}^{(t)}, a_{i+1,j+1}^{(t)} \right),$$

or equivalently,

$$a_{ij}^{(t+1)} = f \left(V_{ij}^{(t)} \right), \quad 0 \leq i \leq r-1, \quad 0 \leq j \leq s-1,$$

where $V_{ij}^{(t)} \subset (\mathbb{Z}_c)^9$ stands for the states of the neighbor cells of $\langle i, j \rangle$ at time t . The matrix

$$C^{(t)} = \begin{pmatrix} a_{00}^{(t)} & \cdots & a_{0,s-1}^{(t)} \\ \vdots & \ddots & \vdots \\ a_{r-1,0}^{(t)} & \cdots & a_{r-1,s-1}^{(t)} \end{pmatrix}$$

is called the *configuration at time t* of the 2D-CA, and $C^{(0)}$ is the *initial configuration* of the CA. Moreover, the sequence $\{C^{(t)}\}_{0 \leq t \leq k}$ is called the *evolution of order k* of the 2D-CA, and \mathcal{C} is the set of all possible configurations of the 2D-CA; consequently $|\mathcal{C}| = c^{r \cdot s}$.

As the number of cells of the 2D-CA is finite, boundary conditions must be considered in order to assure the well-defined dynamics of the CA. In this paper, *periodic boundary conditions* are taken:

$$a_{ij}^{(t)} = a_{uv}^{(t)} \Leftrightarrow i \equiv u \pmod{r}, \quad j \equiv v \pmod{s}.$$

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 during 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 cellular automaton is called *reversible* and the evolution backwards is possible ([25]).

Let us consider the set of 2D-CA whose local transition functions are of the following form:

$$a_{ij}^{(t+1)} = \sum_{\alpha, \beta \in \{-1, 0, 1\}} \lambda_{\alpha, \beta} a_{i+\alpha, j+\beta}^{(t)} \pmod{c},$$

with $0 \leq i \leq r-1$, $0 \leq j \leq s-1$, and $\lambda_{\alpha\beta} \in \mathbb{Z}_2$. They are called *2D-Moore linear cellular automata* (2D-LCA). As there are 9 cells in the extended Moore neighborhood, then there exist $2^9 = 512$ two-dimensional LCA, and every one of them can be conveniently specified by a decimal integer called the *rule number*: w , which is defined as follows:

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

where $0 \leq w \leq 511$.

The standard paradigm for CA considers that the state of every cell at time $t + 1$ depends on the state of some cells (its neighborhood) at time t . Nevertheless, one can consider CA for which the state of every cell at time $t + 1$ not only depends on the states of some cells at time t , but also on the states of (possible) other different groups of cells at times $t - 1$, $t - 2$, etc. This is the basic idea of *memory cellular automata*, MCA for short, (see [26]). In this paper, we consider a particular type of MCA called *k-th order linear MCA* (LMCA for short) for which the local transition function is of the following form:

$$a_{ij}^{(t+1)} = \sum_{m=0}^{k-1} f_{m+1} \left(V_{ij}^{(t-m)} \right) \pmod{c}, \quad (2)$$

with $0 \leq i \leq r - 1$, $0 \leq j \leq s - 1$, and where f_l , $1 \leq l \leq k$, are the local transition functions of k particular 2D-LCA.

Note that the initial configuration of a 2D-LMCA is formed by k components, $C^{(0)}, \dots, C^{(k-1)}$, in order to initialize the evolution of the MCA of order k .

A particular type of reversible MCA with local transition function (2) is characterized by means of the following result.

Proposition 1 *If the global function defining the 2D-CA with local transition function f_k is the identity, i.e., if*

$$f_k \left(V_{ij}^{(t-k+1)} \right) = a_{ij}^{(t-k+1)},$$

then the LMCA given by (2) is a 2D-reversible MCA, whose inverse CA is another LMCA with local transition function:

$$a_{ij}^{(t+1)} = - \sum_{m=0}^{k-2} f_{k-m-1} \left(V_{ij}^{(t-m)} \right) + a_{ij}^{(t-k+1)} \pmod{c}, \quad (3)$$

for $0 \leq i \leq r - 1$, $0 \leq j \leq s - 1$.

Proof. Suppose that $\{C^{(t)}\}_{t \geq 0}$ is the evolution of the LMCA given by (2), where

$$C^{(t)} = \begin{pmatrix} a_{00}^{(t)} & \cdots & a_{0,s-1}^{(t)} \\ \vdots & \ddots & \vdots \\ a_{r-1,0}^{(t)} & \cdots & a_{r-1,s-1}^{(t)} \end{pmatrix}$$

is the configuration at time t , and let $\{\tilde{C}^{(t)}\}_{t \geq 0}$ be the evolution of the LMCA given by (3), where:

$$\tilde{C}^{(t)} = \begin{pmatrix} \tilde{a}_{00}^{(t)} & \cdots & \tilde{a}_{0,s-1}^{(t)} \\ \vdots & \ddots & \vdots \\ \tilde{a}_{r-1,0}^{(t)} & \cdots & \tilde{a}_{r-1,s-1}^{(t)} \end{pmatrix}.$$

The proof ends if we show that $\tilde{C}^{(k+1)} = C^{(t-k+1)}$ when $\tilde{C}^{(1)} = C^{(t+1)}$, $\tilde{C}^{(2)} = C^{(t)}$, \dots , $\tilde{C}^{(k)} = C^{(t-k+2)}$, for every t . Consequently, by simply applying (3) we obtain:

$$\tilde{a}_{ij}^{(k+1)} = -f_{k-1}(\tilde{V}_{ij}^{(k)}) - f_{k-2}(\tilde{V}_{ij}^{(k-1)}) - \dots - f_1(\tilde{V}_{ij}^{(2)}) + \tilde{a}_{ij}^{(1)} \pmod{c}, \quad (4)$$

for $0 \leq i \leq r-1, 0 \leq j \leq s-1$. As $\tilde{C}^{(m)} = C^{(t-m+2)}$ with $1 \leq m \leq k$, then $\tilde{V}_{ij}^{(m)} = V_{ij}^{(t-m+2)}$ with $1 \leq m \leq k$. As a consequence, taking into account the value of $C_{ij}^{(t+1)}$ given by (2), the equation (4) yields:

$$\begin{aligned} \tilde{a}_{ij}^{(k+1)} &= -f_{k-1}(V_{ij}^{(t-k+2)}) - \dots - f_1(V_{ij}^{(t)}) + a_{ij}^{(t+1)} \pmod{c} \\ &= -f_{k-1}(V_{ij}^{(t-k+2)}) - \dots - f_1(V_{ij}^{(t)}) \\ &\quad + f_1(V_{ij}^{(t)}) + \dots + f_{k-1}(V_{ij}^{(t-k+2)}) + a_{ij}^{(t-k+1)} \pmod{c} \\ &= a_{ij}^{(t-k+1)} \pmod{c}, \end{aligned}$$

for every $0 \leq i \leq r-1, 0 \leq j \leq s-1$, thus $\tilde{C}^{(k+1)} = C^{(t-k+1)}$ and we conclude. ■

3 A new graphic secret sharing scheme based on MCA

In this section we propose a new graphic secret sharing scheme, specifically a graphic (k, n) -threshold scheme, based on memory cellular automata, in order to apply it to images. Basically, it consists of considering the secret image as the first component of the initial configuration for a 2D reversible LMCA of order k , and the rest of $k-1$ components of the initial configuration are $k-1$ random matrices. The shares to be distributed among the n participants are n consecutive configurations of the evolution of the LMCA. In the next subsections, the scheme is more detailed.

3.1 The representation of an image as a matrix

An image I defined by c colors and $r \times s$ pixels, p_{ij} , with $1 \leq i \leq r$, $1 \leq j \leq s$, can be considered as a matrix M with coefficients in \mathbb{Z}_c , as follows:

1. If I is a b&w image, then M is an $r \times s$ matrix whose (i, j) -th coefficient is 1 (*resp.* 0) if the pixel p_{ij} is black (*resp.* white); *i.e.*, the coefficients of M are in \mathbb{Z}_2 ($c = 2$, and hence $b = 1$).
2. If I is a gray-level image, then the RGB code of each pixel, p_{ij} , is given by the three-dimensional vector (R, G, B) , where $0 \leq R, G, B \leq 255$ and $R = G = B$. Consequently, each pixel can be defined by a number $0 \leq R \leq 255$. Hence, M is an $r \times s$ matrix with coefficients in \mathbb{Z}_{2^8} .
3. Finally, if I is a color image, then each pixel is given by 24 bits (8 bits representing each basic color: red, green and blue). As a consequence M is an $r \times s$ matrix with coefficients in $\mathbb{Z}_{2^{24}}$.

3.2 The graphic sharing scheme

As it is mentioned, the secret sharing scheme proposed is a (k, n) -threshold scheme based on the use of a 2D-reversible LMCA. The protocol contains three phases: The setup phase, the sharing phase and the recovery phase.

3.2.1 The setup phase

This first phase is given by the following steps:

1. The dealer generates a sequence of $k - 1$ random integers numbers:

$$\{w_1, \dots, w_{k-1}\} \quad (5)$$

such that $0 \leq w_l \leq 511$ with $1 \leq l \leq k - 1$. These numbers stand for the rule numbers of the 2D-LCA constituting the memory cellular automata.

2. The dealer constructs the 2D-LMCA with local transition function:

$$a_{ij}^{(t+1)} = f_{w_1} \left(V_{ij}^{(t)} \right) + \dots + f_{w_{k-1}} \left(V_{ij}^{(t-k+2)} \right) + a_{ij}^{(t-k+1)} \pmod{c}, \quad (6)$$

where $f_{w_l}: (\mathbb{Z}_c)^9 \rightarrow \mathbb{Z}_c$, and $0 \leq i \leq r - 1$, $0 \leq j \leq s - 1$. The set of random numbers given in (5) should be securely distributed to the participants if the dealer's role is limited to elaborate the shares, and his help is not necessary to recover the secret image.

3. The matrix representing the secret image to be shared is considered as the first component of the initial configuration, $C^{(0)} = M$. Moreover, to complete the initial configuration, the dealer generates $k - 1$ random components: $C^{(1)}, \dots, C^{(k-1)}$, by means of a cryptographic secure pseudorandom number generator (see [3, Section 5.5]), in order to avoid an attack to the scheme by supposing the values of these $k - 1$ matrices. These $k - 1$ configurations must be destroyed after generating the shares.

3.2.2 The sharing phase

1. The dealer chooses a integer number m , such that $m \geq k$ in order to avoid possible overlaps between the initial conditions and the shares. (Note that the number of iterations increases with m , so this number would not be much bigger than k .)
2. Starting from the initial configurations $C^{(0)}, \dots, C^{(k-1)}$, the dealer computes the $(m + n - 1)$ -th order evolution of the 2D-LMCA:

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

3. The shares to be distributed among the n participants, P_0, \dots, P_{n-1} , are the last n configurations computed: $S_0 = C^{(m)}, \dots, S_{n-1} = C^{(m+n-1)}$. Moreover, each participant receives the set of random numbers generated by the dealer in the step 1 of the setup phase, in order to construct the inverse function of the local transition function given by formula (6). In this way, each participant knows how to recover the original image, without the cooperation of the dealer.

3.2.3 The recovery phase

To recover the secret image, any consecutive k (of n) shared images are needed, but no less. The following steps define this phase.

1. To recover the secret, $C^{(0)}$, a set of k consecutive shares of the form

$$S_\alpha = C^{(m+\alpha)}, \dots, S_{\alpha+k-1} = C^{(m+\alpha+k-1)}, \quad 0 \leq \alpha \leq n - k,$$

is needed.

2. Taking $\tilde{S}_0 = C^{(m+\alpha+k-1)}, \dots, \tilde{S}_{k-1} = C^{(m+\alpha)}$, and iterating $m+\alpha+k-1$ times the inverse LMCA, the secret initial configuration (the original image), $C^{(0)}$, is obtained.

Note that the recovered image is exactly the same than the original one because the LMCA is reversible. This property of the proposed scheme is not verified by any other graphic sharing scheme. Moreover, as every participant knows the local transition function, they do not need the collaboration of the dealer for recovering the original image.

4 Analysis of the security of the scheme

In this section, the security of the proposed graphic sharing scheme is analyzed. First of all, note that from the formula (1), the information rate of each participant of this scheme is 1, and consequently, the information rate for this secret sharing scheme is also 1. Furthermore, the scheme proposed is ideal. It is also perfect, as it is proved in the following

Proposition 2 *Let us consider the LMCA given by the local transition function (2). If one configuration of the form $C^{(t-i)}$, $0 \leq i \leq k-1$, is unknown, then no information about the configuration $C^{(t+1)}$ can be obtained.*

Proof. Note that the evolution of the LMCA with local transition function (2) can be expressed in terms of global functions as follows:

$$C^{(t+1)} = \Phi_1(C^{(t)}) + \dots + \Phi_{k-1}(C^{(t-k+2)}) + \Phi_k(C^{(t-k+1)}) \pmod{c}, \quad (7)$$

where Φ_i stands for the global function of the 2D-LCA with transition function f_i . Now, without loss of generality, we can assume that the unknown configuration is $C^{(t-k+1)}$. Then the formula (7) yields:

$$C^{(t+1)} = U + V \pmod{c},$$

where $U = (u_{ij})$ is a known matrix, and $V = (v_{ij})$ is the unknown matrix $\Phi_k(C^{(t-k+1)})$, where $0 \leq i \leq r-1$, $0 \leq j \leq s-1$. Both matrices have coefficients in \mathbb{Z}_c . As a consequence, the following linear system holds:

$$a_{ij}^{(t+1)} = u_{ij} + v_{ij} \pmod{c}, \quad 0 \leq i \leq r-1, \quad 0 \leq j \leq s-1,$$

which is formed by $r \cdot s$ equations with $2r \cdot s$ unknowns. Consequently, it can not be solved and, obviously, no information about the configuration

$$C^{(t+1)} = \left(a_{ij}^{(t+1)} \right), \quad 0 \leq i \leq r-1, \quad 0 \leq j \leq s-1,$$

is obtained. ■

Remark that a similar result holds if the number of unknown configurations is greater than one. As a consequence, for the secret sharing scheme proposed it is impossible to recover the secret image from $k - 1$ (or less) shares.

Furthermore, it is assumed that each participant knows the local transition function, but this knowledge does not suppose a weakness of the scheme and it permits to recover the secret image without the collaboration of the dealer.

5 An example

In this section, an example for a (k, n) -threshold scheme will be presented. The random matrices (configurations) $C^{(1)}, C^{(2)}, \dots, C^{(k-1)}$, for the step 3 in the setup phase have been generated by using the BBS pseudorandom bit generator ([27]). This generator is a cryptographically secure pseudorandom bit generator and it is defined by iterating the function $x^2 \pmod n$, where $n = p \cdot q$ is the product of two large prime numbers, each of them congruent to 3 modulo 4. In other words, the BBS generator produces a sequence of bits by taking the least significant bit of the sequence defined by $x_{i+1} \equiv x_i^2 \pmod n$, $i \geq 0$, where x_0 is the seed of the generator. The conditions for choosing the modulus n and the seed x_0 , in order to obtain orbits of maximal periods have been established in [28].

In the practical implementation of the proposed scheme for the following example, we have decided to obtain shared images of the same type than the original one, that is, as the original image is a gray-level image, the shares also will be gray-level images. An easier implementation could determine shares with 2^{24} colors, in all cases, *i.e.*, without taking into account the number of colors of the secret image.

The image used in the following example has 181×157 pixels and 249 gray-levels (see Figure 1). Moreover, the local function used is defined by means of the number $w_1 = 232$, and the parameters are:

$$k = 3, \quad n = 5, \quad m = 3.$$

In this way, 5 iterations for the CA have been needed in order to obtain the following images:

$$C^{(0)}, C^{(1)}, C^{(2)}, S_0 = C^{(3)}, S_1 = C^{(4)}, S_2 = C^{(5)}, S_3 = C^{(6)}, S_4 = C^{(7)}.$$

The five shares are shown as images in Figures 2, 3, 4, 5, and 6, respectively.

For this example we have used the shares S_2 , S_3 and S_4 to recover, after 5 iterations, the original image (see Figure 1).

6 Conclusions

In this paper a new graphic (k, n) -threshold scheme for sharing secret b&w, gray-level and color images is presented. The scheme is based on two-dimensional reversible linear memory cellular automata. The two main characteristics of this new scheme, which are not satisfied by any previous proposed graphic schemes, are: (1) The size of each shared image is exactly the same than the size of the secret image to be shared, and (2) There is no loss of resolution in the recovery secret image.

Moreover, the security of the scheme has been analyzed and it has been proved that in order to obtain the original image it is necessary to join, at least, k shares. If $k - 1$ or less shares are pooled, no information of the secret image is obtained.

Acknowledgments

This work is supported by Ministerio de Ciencia y Tecnología (Spain), under grant TIC2001-0586, and by the Consejería de Educación y Cultura of Junta de Castilla y León (Spain), under grant SA052/03.

References

- [1] A. Shamir, How to share a secret, Commun. ACM 22 (1979) 612-613.
- [2] G.R. Blakley, Safeguarding cryptographic keys, AFIPS Conference Proceedings 48 (1979) 313-317.
- [3] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of applied cryptography, CRC Press, Boca Raton, FL, 1997.
- [4] M. Ito, A. Saito, T. Nishizeki, Secret sharing scheme realizing general access structure, Proc. of IEEE Global Telecommunication Conf. Globecom 87 (1987), pp. 99-102.
- [5] J.C. Benaloh, J. Leichter, Generalized secret sharing and monotone functions, Advances in Cryptology-CRYPTO'88, LNCS 403 (1990) 27-35.
- [6] G. Ateniese, C. Blundo, A. De Santis, D. Stinson, Extended capabilities for visual cryptography, Theoret. Comput. Sci. 250 (2001) 143-161.
- [7] W. Tzeng, C. Hu, A new approach for visual cryptography, Des. Codes Cryptogr. 27 (2002) 207-227.

- [8] D.R. Stinson, An explication of secret sharing schemes, *Des. Codes Cryptogr.* 2 (1992) 357-390.
- [9] D.R. Stinson, *Cryptography. Theory and practice*, Second Edition, CRC Press, Boca Raton, FL, 2002.
- [10] M. Naor, A. Shamir, Visual Cryptography, *Advances in Cryptology-Eurocrypt'94*, LNCS 950 (1995), pp. 1-12.
- [11] C. Lin, W. Tsai, Visual cryptography for gray-level images by dithering techniques, *Pattern Recognition* 24 (2003) 349-358.
- [12] C. Thien, J. Lin, Secret image sharing, *Computers and Graphics* 26 (2002) 765-770.
- [13] E.R. Verheul, H.C.A. van Tilborg, Construction and properties of k out of n visual secret sharing schemes. *Des. Codes Cryptogr.* 11 (1997) 179-196.
- [14] C.C. Chang, C.S. Tsai, T.S. Chen, A technique for sharing a secret color image, *Proc. Ninth National Conf. on Information Security*, Taichung, 1999, pp. 63-72.
- [15] Y. Hou, Visual cryptography for color images, *Pattern Recognition* 36 (2003) 1619-1629.
- [16] V. Rijmen, B. Preneel, Efficient colour visual encryption or 'Shared colours of Benetton', *Rump Session of Eurocrypt'96*, available in <http://www.iacr.org/conferences/ec96/rump/preneel.ps>.
- [17] C. Chang, R. Hwang, Sharing secret images using shadow codebooks, *Inform. Sci.* 111 (1998) 335-345.
- [18] C. Tsai, Ch. Chang, T. Chen, Sharing multiple secrets in digital images, *J. Syst. Software* 64 (2002) 163-170.
- [19] G. Álvarez Marañón, A. Hernández Encinas, L. Hernández Encinas, A. Martín del Rey, G. Rodríguez Sánchez, Graphic cryptography with pseudorandom bit generators and cellular automata, *Proc. of Seventh Internat. Conf. on Knowledge-Based Intelligent Information & Engineering Systems*, LNAI 2773 (2003), pp. 1207-1214.
- [20] L. Hernández Encinas, A. Martín del Rey, A. Hernández Encinas, Encryption of images with 2-dimensional cellular automata, *Proc. of 6-th Multiconference on Systemics, Cybernetics and Informatics*, Vol. I: Information Systems Development, Orlando, USA, 2002, pp. 471-476.

- [21] R. Díaz Len, A. Hernández Encinas, L. Hernández Encinas, S. Hoya White, A. Martín del Rey, G. Rodríguez Sánchez, I. Visus Ruíz, Wolfram cellular automata and their cryptographic use as pseudorandom bit generators, *Internat. J. Pure Appl. Math.* 4 (2003) 87-103.
- [22] S. Wolfram, Random sequence generation by cellular automata, *Adv. Appl. Math.* 7 (1986) 123–169.
- [23] H.A. Gutowitz, Cryptography with dynamical systems, in *Cellular Automata and Cooperative Systems*, Proc. of the NATO Advanced Study Institute, Dordrech, 1993, pp. 237–274.
- [24] P. Guan, Cellular automaton public-key cryptosystem, *Complex Systems* 1 (1987) 51–57.
- [25] T. Toffoli, N. Margolus, Invertible cellular automata: A review, *Physica D* 45 (1990) 229–253.
- [26] R. Alonso-Sanz, Reversible cellular automata with memory: two-dimensional patterns from a single seed, *Phys. D* 175 (2003) 1–30.
- [27] L. Blum, M. Blum, and M. Shub, A simple unpredictable pseudorandom number generator, *SIAM J. Comput.* 15 (1986) 364–383.
- [28] L. Hernández Encinas, F. Montoya Vitini, J. Muñoz Masqué, A. Peinado Domínguez, Maximal periods of orbits of the BBS generator, Proc. of the 1998 Int. Conf. on Inf. Security and Cryptology, Seul, 1998, pp. 71–80.

Figure captions



Figure 1: Secret image

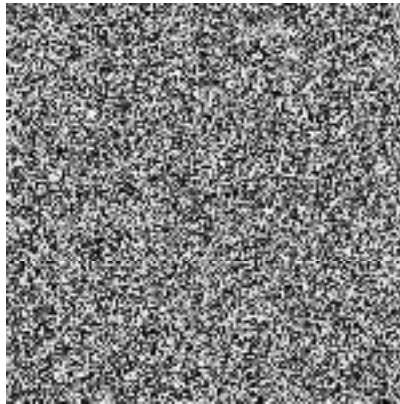


Figure 2: First share

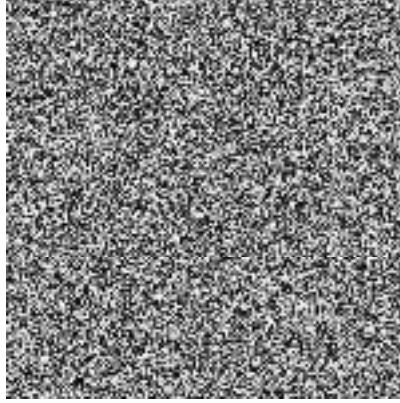


Figure 3: Second share

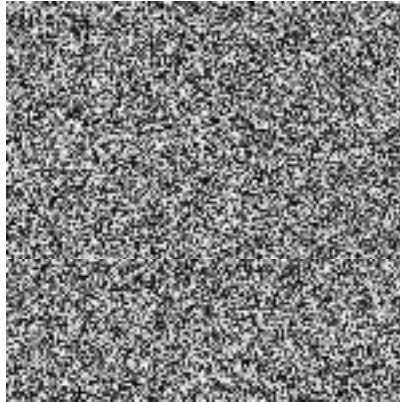


Figure 4: Third share

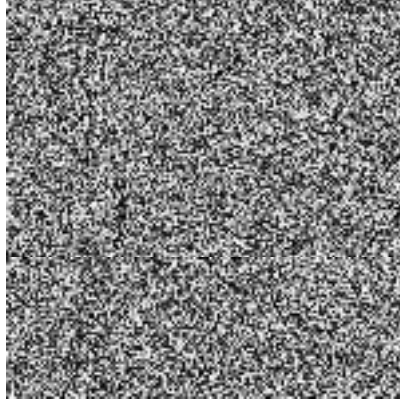


Figure 5: Fourth share

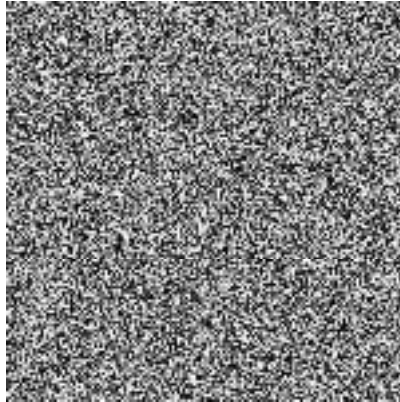


Figure 6: Fifth share