A Novel Watermarking Scheme Based on Two Dimensional Cellular Automata

OMAR ADWAN¹, AIMAN AYYAL AWWAD², AZZAM SLEIT¹, ABDEL LATIF ABU ALHOUM¹

(1) King Abdulla II School for Information Technology
University Of Jordan, Queen Rania Street, Amman, JORDAN
(2) Department of Mathematics and Computer Science, Faculty of Science, Tafila Technical University
Tafila, JORDAN
{ adwanoy;azzam.sleit;a.latif}@ju.edu.jo, AimanAwwad@ttu.edu.jo

Abstract: - Cellular automata are a powerful computation model that provides a simple way to simulate and solve many difficult problems in different fields. The most widely known example of Cellular Automata is the Game-of-Life. In this paper, we propose a novel watermarking scheme based on Conway game. For embedding gray watermark image at LSB to different positions of host image, our method is performed using the positions of the live cells in the Game-of-Life generations. The experimental results show that perceptually the watermark is not visible in the watermarked image. Our model is simple, robust and secures enough to resist passive attacks as described in the experimental results section.

Key-words: - Two Dimensional Cellular Automata, Game-of-Life, Image Watermarking

1 Introduction

With the development of multimedia technology and internet communications, digital information can be easily distributed, copied and modified. However, the changes of digital information are always not being discovered because it is very easy to be modified and copied by the unauthorized coping and malicious tampering. Therefore, more attention is focused on the copyright protection of digital information. Digital watermarking technology is a field in computer science, cryptography and signal processing [1]. Digital watermarking is the process of embedding or hiding watermark into digital information such as a photo and video for the purpose of authenticating and verifying digital contents [2].

Indeed a watermark is a special logo, image, pattern, etc. Furthermore, the information is hidden in the multimedia to protect itself, so that the unauthorized users will not be able to notice or extract the existence of hidden information. Digital watermarking methods in still images can be classified in two categories based on the embedding domain: spatial and transform domain. In spatial domain method, a watermark is embedded in the pixels of image. The Least Significant Bit altering algorithm (LSB) is one of the well known examples in this domain. In transform domain, watermarking is based on altering the transform coefficients [3].

Cellular Automata are widely used in different applications, such as art (generated images and music), random number generation, pattern recognition, routing algorithms and games. The application of cellular automata in the area of digital image processing includes image enhancement, compression, encryption and watermarking

The Game-of-Life (GL) is a Two Dimensional Cellular Automata (CA) that produces large amounts of patterned data. The ability to obtain complex global behavior from simple local rules makes CA an interesting platform for digital image watermarking. It is possible for GL to embed the watermark image pixels to specific original image pixels depending on the position of the live cells on the GL generations, where GL provides the complex behavior which would be best to produce useful operations.
In this paper, an algorithm to embed watermark image to a gray image based on (2-D) CA GL is presented. Randomly, the two most significant bits for each pixel in the watermark image are embedded to the host image pixels depending on the positions of the live cells in the GL generations to improve the security and robustness. The attacker without a correct secret key (the initial random configuration for Conway game and the number of iterations) cannot extract or detect the watermark image.

Our proposed scheme will ensure:
1] The difference between the host image and the embedded watermarked image should be perceptually invisible
2] An invisible watermark must be undetectable by an unauthorized user
3] The owner of the image is the only one who holds the secret key
4] For high quality images the amount of individual pixels modification should be as small as possible

The rest of the paper is organized as follows. In section 2, we introduce the (2-D) CA GL. In section 3, we describe the proposed watermarking scheme. In section 4, experiment results are given to demonstrate the effectiveness and robustness of our scheme. Finally, we give conclusion and indicate future work in section 4.

2 Cellular Automata
Cellular Automata (CA) are dynamical complex space and time discrete systems [4]. They were originally proposed by Stanislaw Ulam and John von Neumann in the 1940s, as formal models for self-reproducing organisms [5]. They consist of a certain number of identical cells, each of which can take one in a finite number of states. The cells are distributed in space in a rectangular grid, in one or more dimensions. At every time step, all the cells update their state synchronously by applying rules (transition function) which take as input the state of the cell under consideration and the states of its neighboring cells.

There are different types of CA models that differ in the number of dimensions, the number of possible states, the neighborhood relationship and the state update rules. A typical CA neighborhood in one dimension makes the next state of the CA depend on its current state and those of its two nearest neighbors. Two typical (2-D) neighborhoods in two dimensions are von Neumann neighborhood (where the next state depends on the current state and those of the nearest neighbors in the four rectangular directions) and Moore neighborhood, (where the next state depends on the current state and those of the nearest neighbors in the eight rose-of-winds directions).

In spite of their simple construction, CA can produce quite complex behavior, capable of generating useful operations. Wolfram has classified one-dimensional CA into four broad categories: (i) Class 1: ordered behavior; (ii) Class 2: periodic behavior; (iii) Class 3: random or chaotic behavior; (iv) Class 4: complex behavior [4]. CA with 'ordered' or 'periodic' behaviors are boring, in the sense that it is very easy to predict or describe what they do. On the other hand, 'random' or 'chaotic' CA is unpredictable and therefore not exciting. Somewhere in between, in the transition from periodic to chaotic, a complex, interesting behavior can occur. For One-Dimensional (1-D) automata, Chris Langton has defined the $\lambda$ (lambda) parameter, which can be used to determine the behavior of each CA [6, 7]. Langton $\lambda$ parameter has recently been extended to (2-D) CA [7].

So far, CA have proved very powerful to simulate many real life applications and phenomena, as in [8] and [9]. It has also been proved that some (1-D) and (2-D) CA, such as the GL, are equivalent to the Universal Turing Machine [5].

The bi-dimensional CA called the GL was designed by Conway. It consists of an $[M \times N]$ matrix of cells, where each cell may take only two states: alive (represented by one) or dead (represented by zero). Each cell has eight neighbors, according to the Moore neighborhood. At every time step, also called a generation, each cell computes its new state by determining the states of the cells in its neighborhood and applying the transition rules to compute
its new state. Every cell uses the same update rule, and all the cells are updated simultaneously. The next state of a cell is determined as follows:

- "Birth": A cell dead at time t becomes alive at time t+1 if exactly three of its neighbors are alive at time t.
- "Death by overcrowding": A cell alive at time t dies at time t+1 if four or more of its neighbors are alive at time t.
- "Death by exposure": A cell alive at time t dies at time t+1 if one or none of its neighbors are alive at time t.
- "Survival": A cell alive at time t will remain alive at time t+1 if two or three of its neighbors are alive at time t.

In this paper, we will describe the use of (2-D) GL generations to embed the digital watermark to the host image. This procedure can easily be generalized and used for any type of digital media.

### 3 Watermarking Embedding and Extraction

Digital image watermarking is hiding information in a host image in perceptually invisible and visible manner. We can express it as a linear combination as shown in the below notation [10]:

\[
WM(x, y) = 4 \left( \frac{H(x, y)}{4} \right) + \frac{W(x, y)}{64} \quad \ldots \ldots \ldots \quad (3.1)
\]

Where, WM(x,y): Watermarked Image, H(x,y) : Host Image, and W(x,y) : Watermark(logo).

However, Dividing and multiplying by 4 sets the two least significant bits(LSB) of H to 0, dividing W by 64 shifts its two most significant bits(MSB) into the two LSB positions and adding the two results generates the LSB watermarked image[10].

### 3.1 Proposed Embedding Scheme

First of all, our proposed scheme will be implemented in a spatial domain, also it is a blind scheme, because a blind technique does not require the original host image or any feature of it to extract the watermark.

We propose performing pixel embedding with the help of a number of generations of the game of life, which will add the diffusion property to the embedding technique. The algorithm for the proposed scheme can be described as follows:

1. An M×N game of life automaton is set up with an initial random configuration A0, and is set to run for K generations, thus obtaining \{A1, A2, … Ak\} matrices.
2. Let HI denote the Host image (after dividing and multiplying H by 4); WM denotes the Watermarked image, WI denotes the Watermark image (after dividing W by 64) and A1 is the first generation produced by the game of life.
3. Get in succession the gray value of two LSB of pixel WI(i,j) where A1(i,j)=1, and add it with the gray value of two LSB of pixel HI(row,col) to produce WM(row,col) starting from row=1, col=1.
4. Starting at q=2, get in succession the gray value of two LSB of pixel WI(i,j), where Aq(i,j)=1 and An(i,j) ≠ , (for n=1, …, q-1) and add it with the gray value of two LSB of pixel HI(row,col). Repeat this step for q=q+1 while q<k.
5. After k iterations, get the gray value of two LSB of the remaining pixels in WI(i,j) for all Aq(i,j) = 0 (where q=1, 2 , …, K), and add them with the gray value of two LSB of pixel HI (row,col).

The digital watermarking embedded process which is based on Conway game generations is shown in the Fig.1.
3.2 Watermark Extraction

Definitely, the embedding key plays an important role in extracting the watermark information from watermarked images. The embedding key is automatically generated during the process of embedding along with the respective security levels. This embedding key has to be shared with the receiver through a secret channel.

The purpose of the proposed scheme is to make the watermark looks like a random one meanwhile keeping a capability of countering most common cryptographic attacks. Therefore, the proposed algorithm is highly secured.

We note that the inverse process of the Embedding algorithm can be implemented to extract the watermark image. However, we will use the same GL's generations to extract the watermark image, and we get the gray value of two LSB of pixel $WM(row, col)$ where $Aq(i, j) = 1$ and $An(i, j) != 1$ (n=1, ..., q-1) successively and put them in $EM(i, j)$, where $EM$ is the Extracted watermark.

4 Experimental Results

In this section, the effectiveness of the proposed algorithm is tested. However, the MatLab is used to simulate the Conway game, watermarking embedment and extraction. For this, several original gray level images and gray watermark images are used. Original gray scale image of Barbara (size of 256×256) and gray scale watermark image of Flower (size 128×128 pixels) and it is 2MSB are taken as shown in Fig.2 (a), (b) and (c). Moreover, Original gray scale image of Cameraman (size of 256×256) and gray scale watermark image of Google logo (size 64×64 pixels) are tested.
To achieve our goal, the algorithm proposed in this paper is used to embed the gray host image to gray watermark image. The GL is run to produce K generations that are used to embed and extract the watermark.

Valuable to note that the watermark is invisible, the original gray image and the gray watermark are involved in the formation of a new watermarked image, any modification by the attacker to watermarked image pixels can lead to detect of any change. The results show that the algorithm is secure; the tiny tampering can be detected and located, as shown in Fig.3.

Fig.2: (a) Original Barbara image of size of 256×256 (b) Watermark Flower of size 128×128 (c) 2MSB of Flower image
The similarity of the original host image \( H \) and the watermarked image \( W \) is measured by peak signal-to-ratio (PSNR), and PSNR in this paper is defined as follows:

\[
PSNR = 10 \log_{10} \left( \frac{L^2}{\frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} [H(i, j) - W(i, j)]^2} \right)
\]  \hspace{1cm} \text{……………………(4.1)}

Where \( L \) is the maximum fluctuation in the input image data type. For example, if the image has a double-precision floating-point data type, then \( L = 1 \). If it has an 8-bit unsigned integer data type, \( L = 255 \), etc.

The PSNR value between the Barbara in Fig.2(a) and Watermarked Barbara in Fig.3(c) is 40.830 dB, and the PSNR value between the cameraman in Fig.3(e) and Watermarked Cameraman in Fig.3(g) is 43.882 dB.
5 Conclusions

In this paper, we propose a novel watermarking scheme based on Conway game. To embed a gray watermark pixel to a gray host pixel, our model is performed using the positions of the live cells in the GL generations. Also, we have used blind method for watermark extraction.

The proposed scheme is secure enough to resist attacks. Primarily, when the complex behavior of GL is used, the diffusion process is in high degree, thus, it becomes more difficult that the attackers extract the watermark. The algorithm used different keys to strengthen the impossibility of being attacked, event if the algorithm is open.

References


