IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 06-10

Cellular Automata Based Watermark Copyright Protection Scheme Based On Dct

Prof.Dr.S.A.Khan, Pranali Amle, Vaishnavi Dodke, Sana Khan, Zarmeen Ansari

Electronics And Telecommunications Anjuman College Of Engineering And Technology Nagpur, India
Electronics And Telecommunications Anjuman College Of Engineering And Technology Nagpur, India
Electronics And Telecommunications Anjuman College Of Engineering And Technology Nagpur, India
Electronics And Telecommunications Anjuman College Of Engineering And Technology Nagpur, India
Electronics And Telecommunications Anjuman College Of Engineering And Technology Nagpur, India

Abstract-*Recently, protecting the copyright of digital media has become an imperative issue due to the growing illegal reproduction and modification of digital media. A large number of digital watermarking algorithms have been proposed to protect the integrity and copyright of images. Traditional watermarking schemes protect image copyright by embedding a watermark in the spatial or frequency domain of an image. A blind, low complex, fast, and highly resistant to attacks JPEG watermarking algorithm is proposed. The idea of Moore CA and Cellular Automata Transform (CAT) are introduced into the algorithm. Unlike other JPEG watermarking, a binary image watermark is scrambled by Moore CA firstly. And then is embedded in a certain sub-band, which is further subdivided into non-overlapped blocks, after the original image is disassembled with CAT. Each block embeds a bit of watermark with template, which one of the CAT bases functions. Finally, the watermarked image is compressed into a JPEG image after DCT, quantization, zigzag scan and entropy coding. In the extraction, the watermark bits are determined on the correlation between the blocks and the template. And the experiments show that the proposed algorithm is robust to the common watermark attacks.*

Keywords: *JPEG; Watermark; Cellular Automata; Scramble; Cellular Automata Transform*

I. Introduction

In recent years, the spread of the Internet and the advance in digital techniques for transmitting and storing information have made it possible to copy and edit images, audio, video and other types of multimedia data. Multimedia data by digital format can be duplicated without loss of quality and changed easily at low cost. These situations cause the illicit actions such as interception, duplication, misuse and unauthorized modification of information. One approach to address the problem is watermarking technique. The concept of digital watermarking is associated with the data-hiding technique. Digital watermarking has been proposed as a way to identify the source, creator, owner, distributor, or authorized consumer of multimedia data.

The process of watermarking involves the modification of the original information data to embed watermark information. The embedding method must leave the original information data perceptually unchanged, yet watermark data should be detected by extraction algorithm. And, the following conditions are requested for watermarking:

- It must be difficult or impossible to remove watermark data, at least without visibly degrading the original image.
- The watermark data must survive image modifications that are common to typical applications, such as scaling and color requantization, commonly performed by a picture editor, or lossy compression techniques like JPEG, used for transmission and storage.
- Watermark data should be imperceptible so as not to affect the experience of viewing the image and readily detectable by the proper authorities, even if imperceptible to the average observer.

Various watermarking techniques have been developed. However, these techniques can be grouped into two classes: spatial domain methods and frequency domain methods. The spatial domain techniques are to embed the watermarking data by directly modifying the pixel values of the original images (the lower bit of image's intensity, brightness, geometric transformation, R.G.B color image, etc). The simplest watermarking technique is to just flip the lowest-order bit of chosen pixels in a gray-scale(8-bit) or color(24-bit) image. This

works well only if the image will not be subject to any modification, such as color modification done by a photo editor. Another technique embeds a more robust watermark in much the same way as a watermark is added to paper: A watermark symbol is superimposed over an area of the image and some fixed intensity value for the watermark to the varied pixel values of the image is added. One disadvantage of spatial domain watermarks is that a common picture-cropping process can eliminate the watermark.

In the case of the frequency domain techniques, where original digital data are transformed into frequency components, watermark information is embedded into particular frequency regions of original data. A representative research based on spread spectrum made a further advance in this class [1]. Also DFT, Fresnel or DCT- based methods are proposed [2][3][4][5]. The advantage of frequency domain method is that the watermark is spreaded throughout the whole image or sound and hence is resistant to cropping or cutting. However, a standard frequency filter or a lossy compression algorithm, which usually filters out the less significant frequencies, could damage the watermark information.

In this paper, we propose a new and novel watermarking technique using Cellular Automata Transform (CAT) and show the embedding and extracting results to confirm the validity of our watermarking system. Our watermarking system is different from other frequency domain watermarking methods, which have only one transform plane.

1. Cellular Automata Transform

CA Basics

Cellular Automata are dynamical systems in which space and time are discrete [6]. The cells, which are arranged in the form of a regular lattice structure, have a finite number of states. These states are updated synchronously according to a specified local rule of interaction. For example, a simple 2-state 1-dimensional cellular automaton will consist of a line of cells/sites (See Figure 1). A given node can either be on (assigned a state value 1) or off (value 0). The closest nodes to node P are those to its immediate left and right. In that case, we can have a local neighborhood of three cells. The state of P at time t + 1 will be determined by the states of the cells within its neighborhood at time t[7].

Figure 1: 1-dimensional cellular space

Using a specified rule (usually deterministic), the values are updated synchronously in discrete time steps for all cells. With a k-state automaton, each cell can take any of the integer values between 0 and k - 1. In general, the rule governing the evolution of the cellular automaton will encompass r sites up to a finite distance away. We say the cellular automaton is a k-state, r-site neighborhood CA.

Theory of CAT

Given a process described by a function f, defined in a physical space of lattice grid i, we seek basis functions A and their associated transform coefficients c, defined in cellular automata "frequency" space k, which allow us to write

$$f_i = \sum_k c_k A_{ik}$$

The basis functions are related to the evolving field (i.e., the states) of the cellular automata. Note that each point on the physical grid i has an associated basis function A (spanning the entire physical space i and CA space, k). Equation (1) represents a mapping of the process f (in the physical domain) into c (in the cellular automata domain) using the building blocks A as transfer functions. In many applications we seek to obtain transform coefficients c, with properties not necessarily possessed by the original function, f. Alternatively, the transformation process should reveal things about f not readily observed in the physical domain.

The essence of CAT is that we can always find CA rules (and its associated neighborhood, initial/boundary configuration, lattice arrangement, etc.) which will result in basis functions and transform coefficients with properties we desire for a given problem. The chief strength is the huge number and varied nature of the basis functions available to us.

2. Watermarking Using Cat

Generally, Fourier or DCT transform provides only one spectrum plane for embedding hidden data, so the embedded information can be removed easily. To increase the flexibility in data hiding, we propose a new technique using CAT.

Our watermarking system, diagrammed in Figure 2, is a kind of frequency domain method which embeds a data stream by modulating the transform domain coefficients.

CAT and Watermarking

There are two benefit points using CAT on watermarking. The first one is to provide many transform patterns verifying CA bases. So our method can recover the weak point having only one transform plane in DFT and DCT domain methods. Using CAT with various CA bases and rule number, it is possible to get many channels embedding information. The second one is the complexity of CA, and it provides difficulty to attacker to find or guess the position embedded watermark data.

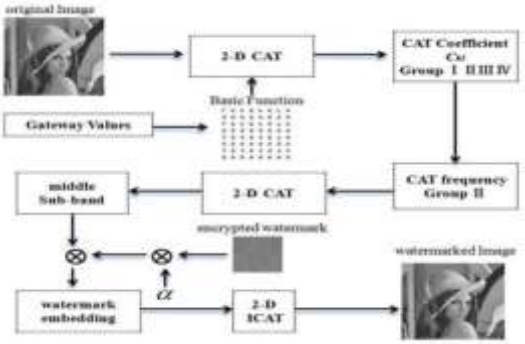

Figure 2: Watermarking system block diagram using CAT

Data Embedding and Extracting Process

3.2.1. Embedding calculation formula

Selection of Rule Number:

$$O' = CAT(O)$$
$$W_{code} = W * w$$
$$E = O' + W_{code}$$
$$O'' = ICAT(E)$$

where

O : original image
O' : CA-transformed pattern of O
W_{code} : embedding pattern of watermark data
W : watermark data
w : embedding parameter
E : embedded pattern
O'' : watermarked version of O

3.2.2. Extracting calculation formula

Selection of Rule Number:

$$O''_{CAT} = CAT(O'')$$
$$W'_{code} = O''_{CAT} - O'$$
$$W' = W'_{code} * w'$$

O''_{CAT} : CA-transformed pattern of O''
W'_{code} : extracted coding pattern
w' : extracting parameter($w' = (1/w)$)
W' : extracted watermark data

2.3 Embedding phase

In general, most of the image energy is concentrated at the lower-frequency sub-bands, LLx, and therefore, embedding watermarks in these sub-bands may degrade the image significantly. Embedding in the low-frequency sub-bands, how-ever, could increase the robustness significantly. However, the high-frequency sub-bands, HHx, include the edges and textures of the image, and the human eye is not generally

As shown in Figure 2 the flow chart of the embedding phase of the watermarking system can be summarized as below.

Watermark embedding:

Step-1 Apply level-1 2D CAT to decompose the N x N image 0 into four non-overlapping multi-resolution sub-bands: LL1, HH1, HL1 and LH1.

Step-2 Apply level-1 2D CAT again to transform the four sub-bands yielding sub-bands LL2, HH2, HL2 are and sub-band HL2 is called Middle frequency domain.
Step-3 Apply the MLCA theory to generate the basis image and obtain the encrypted watermark by performing the XOR operation on the original watermark.
Step-4 Embed the private watermark data with the size (Nw x Nw) in the Middle frequency of CAT-domain, 0' = 0 x (1 + awi) i = 1, . , .
, . , Nw.
Step-5 Use the level-2 ICAT to produce the watermarked cover image.
Watermark extraction:
Step-1 Apply level-1 2D CAT to the whole watermarked image 0", map the CAT coefficient into four non-overlapping bands: LL1*, HH1*, HL1* and LH1*.
Step-2 Apply level-1 2D CAT again to transform the sub-band HL1* yielding sub-band HL2*.
Step-3 Extract the encrypted watermark values from the Middle frequency sub-band: w: Step 3. Extract the encrypted watermark values from the Middle frequency sub-band:

w K = OK)/a, K =1,...,N .
: 2 w
Step-4 Apply the MLCA basis image and obtain the recovered watermark by performing the XOR operation on the extracted encrypted watermark Step 4. Apply the MLCA basis image and obtain the recovered watermark by perform¬ing the XOR operation on the extracted encrypted watermark

II. Experimental Results and Analysis

In order to confirm the validity of the proposed method, we conducted experiments with a Lena image(as original image) and a signature image(as watermark data) as shown in Figure 3 and 256 * 256 sampling points(256 grey-scaled) and 64 * 64 sampling points(binary value) are chosen respectively Embedding phase.

Figure 3: Original image and watermark data

Two images of the left side of Figure 4 show the watermarked versions of original image, where the rule numbers are chosen as 86 and 134 for CAT of an original image from left to right respectively and embedding parameter is chosen as The right side of Figure 4 shows the extracted image from watermarked versions, where the extracting parameters are chosen as 0.1 for extraction.


I&

(a) **(b)**

(a)RN=84, PSNR=44.0 watermarked versions
(b)RN=134, PSNR24.1 extracted data

Figure 4: Watermarked versions and extracted data

To demonstrate the performance of the scheme, we use the Peak Signal to Noise Ratio (PSNR) to evaluate the quality of the watermarked image and the Bit Correct Ratio (BCR) to judge the difference between the watermarked images and the original image.

$$PSNR = 10 \times \log\left(\frac{255^2}{MSE(O, O')}\right)$$

$$MSE(O, O') = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (O, O')$$

$$BCR = \left(1 - \frac{\sum_{i=1}^{L_M} (w_i \oplus w_i')}{L_M}\right)$$

where 0 and 0' represent the original image data and the watermarked image data, respectively, and w_i and w_i' are the original watermarks and the extracted watermarks.

III. Conclusion

A new watermarking technique by Cellular Automata Transform (CAT) is proposed and experiments are done resulting in confirming the validity of the proposed technique. To vary our method is further subject to study in order to extend the proposed technique to the public watermarking system. From the experimental results, it is said that our technique using CAT has a possibility to embed image data in watermarking process, and the quality of watermarked versions is related to the choice of rule number. Though this watermarking technique is limited in embedding and extracting of watermark data, to increase the robustness to the attacks and image processing is left as a future study.

References

[1]. R. Shiba, S. Kang and Y. Aoki, An image watermarking technique using CAT, 2004 IEEE Region 10 Conference, vol.1, pp.303-306, 2004.
[2]. M. Mukherjee, N. Ganguly and P. Pal Chaudhuri, Cellular automata based authentication, A CRI, Switzerland, pp.259-269, 2002.
[3]. S. Wolfram, Theory and Applications of Cellular Automata, World Scientific Publishing Company, Singapore, 1986.
[4]. S. Wolfram, Cryptography with Cellular Automata, Springer- Verlag, Beilin, 1986.
[5]. 0. Adwan, A. A. Awwad et al., A novel watermarking scheme based on two dimensional cellular automata, Proc. of the 2011 International Conference on Computers and Computing, pp.88-94, 2011.
[6]. R. J. Chen, Y. H. Chen, C. S. Chen and J. L. Lai, Image encryption/decryption system using 2-D cellular automata, ISCE, pp.1-6, 2006.
[7]. J. W. Shin, S. Yoon and D. S. Park, Contents-based digital image protection using 2-D cellular automata transforms, IEICE Electronics Express, vol.7, no.11, pp.772-T78, 2010.
[8]. W. C. Rong, L. J. Jing and L. G. Ying, A DCT-SVD domain watermarking algorithm for digital image based on Moore-model cellular automata scrambling, /C/SS, pp.104-108, 2010.
[9]. S. D. Lin, Y. Kuo and M. Yao, An image watermarking scheme with tamper detection and recovery, International Journal of Innovative Computing, Information and Control, vol.3, no.6(A), pp.1379- 1387, 2007.
[10]. 0. E. Lafe, Method and apparatus for data encryption/decryption using cellular automata transform, U.S. Patent No.5677956, 1997.