Secure and Novel Watermarking System Based on Complemented MLCA and 2D CAT

Xiao-wei Li · Jae-sik Yun · Sung-jin Cho · Seok-tae Kim
Pukyong National University
E-mail : lixiaowei@nate.com · yffyjs@gmail.com · sjcho@pknu.ac.kr · setakim@pknu.ac.kr

ABSTRACT

A secure and novel watermarking system based on complemented Maximum Length Cellular Automata (MLCA) and Two-Dimension Cellular Automata Transform (2D CAT) is proposed. In this watermarking scheme, the original watermark which is first encrypted by complemented MLCA with the private keys, and the encrypted watermark is embedded into the CAT domain of the cover image. Experiment results show that this new method is more secure and provides robust performance against watermarking attacks.

KEYWORD
Watermarking, Complemented MLCA, 2D CAT

I. INFORMATION

With the widespread use of internet and the development in computer industry, network security and copyright protection have become a great focus in the world. And meantime, watermarking has been proposed, not only for protecting the copyright of the multimedia data but also preventing illegal copying and distribution. Watermarking scheme based on secret Keys is intensively used in modern security systems to ensure data integrity. To improve watermarking security, some researchers try to use complex key structures such as double random phase (DRP) keys and chaotic sequence (CS) keys, however, the watermark is not usually robust and calculating is not good.

Watermarking methods can be classified into two types: embedding the watermark into the spatial domain, and imbedding the watermark into frequency domain. The first type provides good computing and visibility but usually degraded robustness while the second type is more robust especially when the watermarking is done by compression methods.

Different from previous schemes, in this paper, we proposed more secure and novel watermarking system. In our scheme, the cover image will be decomposed a pyramid structure based CAT. The sub bands labeled LH, HL and HH represent the high frequency information such as edges and textures of an image. The sub band LL represents the low frequency information which contains important data of cover image. The encrypted watermark which is generated by complemented MLCA is embedded into the low frequency (LL). This proposed method of encrypted watermark embedding into our CAT-based watermarking system, which can simultaneously improve security, robustness, and image quality of the watermarked images.

II. IMAGE WATERMARKING BASED ON CELLULAR AUTOMATA TRANSFORM

2.1 MLCA and Cellular Automata Transform

Cellular Automata are dynamical systems in which space and time are discrete[1]. CA is a collection of \( n \) storage elements. The elements are called the cells which take on discrete values. At each clock (discrete times step) the value of each cell is set to the value of the output of a function, the function, called a transition function or a rule[2]. In this paper, complement MLCA can be generated by
90/150 NBCA (Null Boundary CA). Shown in Fig.1, the first and the last input cells are 0, such that

\[
\begin{align*}
\overline{s_1} & = (0 \oplus s_2) \oplus F \\
\overline{s_2} & = (s_1 \oplus s_2 \oplus s_3) \oplus F \\
\overline{s_3} & = (s_2 \oplus s_3) \oplus F \\
\overline{s_4} & = (s_3) \oplus F \\
\overline{s_5} & = (s_4) \oplus F \\
\overline{s_6} & = (s_5) \oplus F \\
\overline{s_7} & = (s_6) \oplus F \\
\overline{s_8} & = (s_7 \oplus s_8 \oplus 0) \oplus F
\end{align*}
\]

where \( \overline{s_t} \) is the complement MLCA \( s_t \) at the time \( t+1 \), \( F \) is the complement vector.

### 2.2 2D Cellular Automata Transform

Two Dimension Cellular Automata based \( A_{ijkl} \) derived from one-dimensional automata:

\[
A_{ijkl} = A_{ik} \times A_{jl}
\]

Or

\[
A_{ijkl} = L_w(a_{ik}a_{jl} + a_{ik}a_{lj}) \mod L_w - (L_w - 1)
\]

where \( L_w \geq 2 \) is the number of state of the automaton.

In a two dimension \( (M \times N) \) space, the data \( f \) is measured by the independent discrete variable \( i, j \). We seek a transformation in the form:

\[
f_{ij} = \sum_{k = 0}^{M-1} \sum_{l = 0}^{N-1} c_{kl} \times A_{ijkl}
\]

here \( k, l \) are vector of non negative integers, \( c_{kl} \) is transform coefficient whose values is obtained from the inverse transform:

\[
c_{kl} = \sum_{i = 0}^{M-1} \sum_{j = 0}^{N-1} f_{ij} B_{ijkl}
\]

If \( A_{ijkl} \) is orthogonal, the bases \( B_{ijkl} \) is the inverse of \( A_{ijkl} \), the (5) called Cellular Automata Transforms (CAT) and (4) which we called Inverse Cellular Automata Transforms (ICAT)[5][6].

Table 2. Gateway Values

<table>
<thead>
<tr>
<th>GATEWAY</th>
<th>VALUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Wolfram&quot; Rule number</td>
<td>243</td>
</tr>
<tr>
<td>( N )</td>
<td>8</td>
</tr>
<tr>
<td>Initial configuration</td>
<td>01100101</td>
</tr>
<tr>
<td>Boundary configuration</td>
<td>Cyclic</td>
</tr>
<tr>
<td>Basis function type</td>
<td>type2: ( A_{00} = 2a_0a_0 - 1 )</td>
</tr>
</tbody>
</table>

Here, 2D CAT gateway values is shown in table 2, the basis function, type2: \( A_{00} = 2a_0a_0 - 1 \), and Rule number is 243.

Fig.2 2D CAT basis function

Here, \( A_{00} \) is the block at the top left corner and \( A_{000} \) is the upper left corner of each block. The white rectangular dots represent "1" while the black dots are "-1".
Consider a three-site neighborhood, one-dimensional CA, since site \( m=3 \), there are 2\(^3\)=8 inter \( W \) values. The states of the cells are from (left to right) \( a_0, a_1, a_2 \) at time \( t \). The state of middle cell at time \( t+1 \) is:

\[
a_{3(t+1)} = (W_0a_0 + W_1a_1 + W_2a_2 + W_3a_0a_2 + W_4a_1a_2 + W_5a_0a_1a_2 + W_6a_3a_4) \mod K
\]  

III. GENERATION OF ENCRYPTED WATERMARK

In this watermarking scheme, the encrypted watermark can be generated from the private key-complemented MLCA based image (256 x 256 pixels).

![Fig.4 Encrypted watermark generation process](image)

Fig.4 (a) Original watermark, (b) Private Key, (c) encrypted watermark, which displays the encrypted watermark generation process. In this paper, we use the Fig.4(c) “encrypted watermark” as the target watermark.

IV. EMBEDDING INTO ENCRYPTED WATERMARK

The embedding procedure of encrypted watermark into watermarking system can be summarized as below, and the block diagram is shown in Fig.5.

![Fig.5 Watermark imbedding procedure](image)

The 2-D CAT transform coefficients \( c_{kl} \) can be divided into four groups. Those CA based at even \( k \) and \( l \) locations represent the low frequency we call “Group I”. The rest of the coefficients are the high frequency components.

In our watermarking scheme, the encrypted watermark is embedded into the “Group I” coefficient by using the following (7):

\[
O' = O_{\text{groupI}} \times (1 + awi)
\]  

Here, \( wi \) is the watermark data, \( O_{\text{groupI}} \) is the data of \( c_{kl} \) (Low frequency), \( a \) is the imbedding parameter. The watermarked image is generated as described by (8):

\[
O'' = \text{ICAT}(O')
\]

where \( O'' \) is the watermarked information.

V. EXPERIMENTAL RESULTS AND ANALYSIS

4.1 Estimate Parameters

To demonstrate the performance of the scheme, we use the famous test image LENA (gray-valued,512 x 512 pixels) as the test image and image PK (256 x 256 pixels, binary-valued) as the watermark. We use the Peak Signal to Noise Ratio (PSNR) for evaluating the quality of the watermarked image, and Bit Correct Ratio (BCR) to judge the difference between the watermarks and extracted watermarks.

\[
\text{PSNR} = 10 \log_2 \left( \frac{255^2}{\text{MSE}(O, O'')} \right),
\]

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

\[
\text{BCR} = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} W(i,j) \oplus W''(i,j)}{M \times N}
\]

Where \( O, O' \) are the original images and watermarked images respectively, \( W, W' \) are the watermark data and extract watermark data, and \( \oplus \) denotes the Exclusive-or operator. \( M, N \) is the size of images.

For testing the invisibility, Fig.6 (d) PSNR = 42.25DB is greater than 30DB. It means that the invisibility is better.
VI. CONCLUSION

A secure and novel watermarking system based on complemented Maximum Length Cellular Automata (MLCA) and Two-Dimension Cellular Automata Transform (2D CAT) is presented in this paper. Watermarking is done by embedding the encrypted watermark into the first level CAT sub band LL of the cover image. Experiments show that this method provides a secure and robust digital watermarking system, the watermark is encrypted by the private key which improve the watermark security and provides robust performance against different watermarking attacks.

REFERENCES