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, completement 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

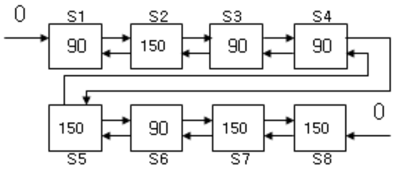

Fig.1 90/150 NBCA 8-cells structure

Table 1. Complemented Rule

	$s_i(t+1)$	$\overline{s_i(t+1)}$
90	$s_{i-1}^t \oplus s_{i+1}^t$	$\overline{s_{i-1}^t \oplus s_{i+1}^t}$
150	$s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t$	$\overline{s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t}$

According to the fig.1 and table 1 values, the completement MLCA matrix can generate using the following:

$$\begin{aligned} \overline{s}_1^+ &= (0 \oplus s_2) \oplus F \\ \overline{s}_2^+ &= (s_1 \oplus s_2 \oplus s_3) \oplus F \\ \overline{s}_3^+ &= (s_2 \oplus s_4) \oplus F \\ &\bullet\ \bullet\ \bullet \quad \bullet\ \bullet\ \bullet \\ \overline{s}_8^+ &= (s_7 \oplus s_8 \oplus 0) \oplus F \end{aligned} \qquad (1)$$

where $\overline{s_i^+}$ is the completement MLCA $\overline{s_i^t}$ at the time t+1, F is the completement vector.

2.2 2D Cellular Automata Transform

Two Dimension Cellular Automata based *Aijkl* derived from one-dimensional automata:

$$A_{ijkl} = A_{ik} \times A_{jl} \qquad (2)$$

Or

$$A_{ijkl} = L_w(a_{ik}a_{ki} + a_{jl}a_{lj}) \mathrm{mod} L_w - (L_w - 1) \qquad (3)$$

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:

$$f_{ij} = \sum_{k=0}^{M-1} \sum_{l=0}^{N-1} c_{kl} \times A_{ijkl} \qquad (4)$$

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

$$c_{kl} = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f_{ij} B_{ijkl} \qquad (5)$$

If *Aijkl* is orthogonal, the bases *Bijkl* is the inverse of *Aijkl*, the (5) called Cellular Automata Transforms (CAT) and (4) which we called Inverse Cellular Automata Transforms (ICAT)[5][6].

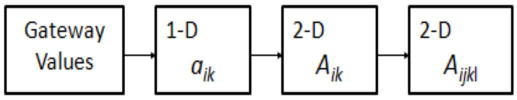

Fig.2 2D A_{ijkl} generation process

where the 2-D CAT basis function *Aijkl* is generated based on 1-D CAT.

Table 2. Gateway Values

GATEWAY	VALUES
"Wolfram" Rule number	243
N	8
Initial configuration	01100101
Boundary configuration	Cyclic
Basis function type	type2:A_{ik}=2$a_{ik}a_{ik}$-1

Here, 2D CAT gateway values is shown in table 2, the basis function, type2: A_{ik}=2$a_{ik}a_{ik}$-1, and Rule number is 243.

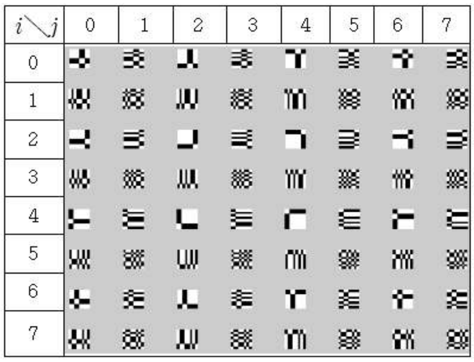

Fig.3 2D CAT basis function

Here, A_{00kl} is the block at the top left corner and A_{ij00} 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_{0k}, a_{1k}, a_{2k} at time t. the state of middle cell at time t+1 is:

$$a_{1(t+1)} = (W_0a_{0t} + W_1a_{1t} + W_2a_{2t} + W_3a_{0t}a_{1t} + W_4a_{1t}a_{2t} + W_5a_{2t}a_{0t} + W_6a_{0t}a_{1t}a_{2t} + W_7)^{W_8} \bmod K \quad (6)$$

III.GENERATION OF ENCRYPTED WATERMARK

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

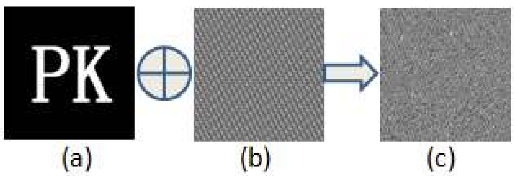

Fig.4 Encrypted watermark generation process

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.

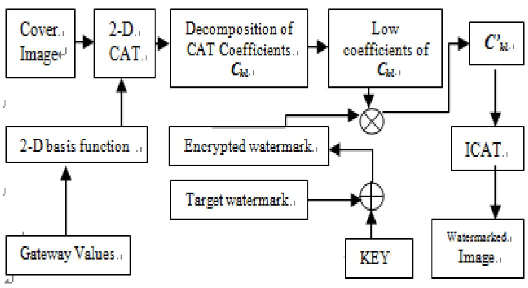

Fig.5 Watermark imbedding procedure

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):

$$O' = O_{groupI} \times (1 + awi) \quad (7)$$

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

$$O'' = ICAT(O') \quad (8)$$

where O'' is the watermark 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,512×512 pixels) as the test image and image PK (256×256 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.

$$PSNR = 10\log(255^2/(MSE(O,O'))), \quad MSE = \frac{1}{M \times N}\left(\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(O(i,j) - O'(i,j))\right) \quad (9)$$

$$BCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} W(i,j) \oplus W'(i,j)}{M \times N} \quad (10)$$

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.

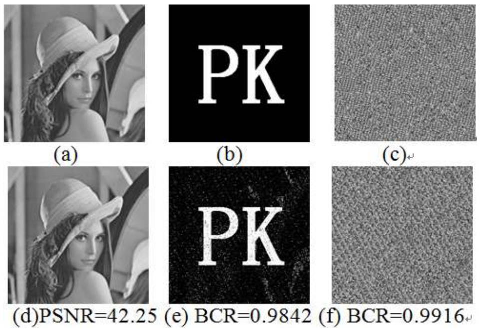

Fig.6 (a)Original image of "LENA",(b) original watermark "PK", (c) Encrypted watermark, (d) watermarked image "LENA", (e) Reconstructed watermark from the extracted encrypted watermark, (f) Extracted encrypted watermark

The attack result of the experiment is shown in Fig.7. BCR values are very high and the reconstructed watermark is recognizable.

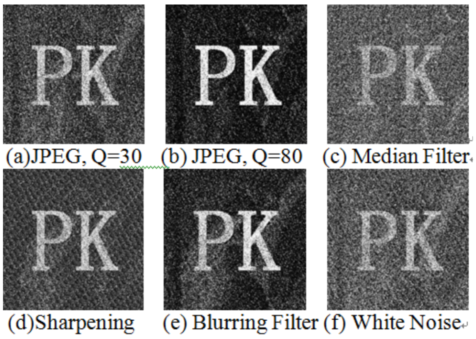

Fig.7 Reconstructed Watermarks

The Reconstructed watermarks from the extracted encrypted watermarks under different attacks while using LENA as the test image.

Table 3. BCR Values Under Different Attacks

Attacks	BCR
JPEG,Q=30	0.8843
JPEG,Q=80	0.9546
Median Filter	0.8154
Sharpening	0.8439
Blurring Filter	0.9135
White Noise	0.8729

According to the result of experiment in Fig.7 and Table 3.The BCR values are considered and all extracted watermarks under different attacks are recognized.

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

[1] T.L.Booth, "Sequential Machines and Automata Theory", Wiley,London,1967.

[2] S.Nandi and P.P. Chaudhuri, etcs, "Theory and application of cellular automata", Proc.IEE, Stevenage, U.K., Vol.137, pp.81-87, Jan.1990.

[3] T.H.Nam, S.T.Kim and S.J.Cho,"image encryption using Non-linear FSR and complemented MLCA",2009 international conference of maritime information and communication science, Vol.2,No.1,pp.168-171, Jun.2009.

[4] Olu Lafe,"Data Compression and Encryption Using Cellular Automata Transforms,", EngAAI, No. 6, pp. 581-591, December 1997.

[5] Seok-Tae Kim and Yongri Piao,"Robust and Secure InIm-based 3D Watermarking Scheme using Cellular Automata Transform", International Journal of Maritime Information and Communication Sciences, Korea, pp.1767-1778, 2009.

[6] B.Viher, A.Dobnikar and D.Zazula,"CA and Follicle Recognition problem and Possibilities of using CA for Image Recognition Purposes", International Journal of Medical Informatics. Vol. 49 ,pp.231-241,1998.