Watermarking Based on Complemented MLCA and 2D CAT

Xiao-Wei Li, Jae-Sik Yun, Sung-Jin Cho, and Seok-Tae Kim, *Member, KIMICS*

***Abstract*— Digital watermarking has gained importance in recent years in copyright protection and multimedia. This paper proposes a secure and novel watermarking system based on complemented Maximum Length Cellular Automata (MLCA) and Two-Dimension Cellular Automata Transform (2D CAT). In this watermarking scheme, the original watermark is first encrypted by complemented MLCA with the private keys, and then the encrypted watermark is embedded into the CAT domain of the cover image, at last use the inverse CAT for the transformed image, the watermarked image is obtained. Experiment results show that this new method is more secure and provides robust performance against watermarking attacks.**

***Index Terms*—watermarking, complemented MLCA, 2D CAT, private key.**

I. INTRODUCTION

WITH the widespread use of internet and the development in computer industry, the digital media, including images, audio, and video, suffer from infringing upon the copyrights with the digital nature of unlimited copying, easy modification and quick transfer over the internet. Digital watermarking refers to techniques used to protect digital data by imperceptibly embedding information (watermark) into the original data in such a way that it remains present. 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 usually not robust and the amount of calculation of algorithm is very great.

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 based on complemented MLCA and 2D CAT. In our scheme, cover image will be CAT decomposed a pyramid structure. The sub bands labeled LH1, HL1 and HH1 represent the high frequency information such as edges and textures of an image. The sub band LL1 represents the low frequency information which contains important data. The encrypted watermark which is generated by MLCA and complemented MLCA is embedded into the low frequency (LL1).This proposed method of encrypted watermark embedding into our CAT-based watermarking system can simultaneously improve security, robustness, and image quality of the watermarked images.

II. IMAGE WATERMARKING BASED ON CELLULAR AUTOMATA TRANSFORM

1) MLCA and Cellular Automata Transform

What are cellular automata? Cellular automata are dynamical systems in which space and time are discrete. The cells are arranged in the form of a regular lattice structure and each must have a finite number of states. The cellular automata are also a collection of n storage elements. The elements are called the cells which take on discrete values. At each clock (discrete time step) the value of each cell is set to the value of the output of a function, the function which called a transition function or a rule [1]. An n cell CA at time *t*, the next state can be described by the matrix operation:

$$f_{t+1} = T \times f_t \tag{1}$$

where $ft = [f1(t), f2(t), f3(t) \ldots fn(t)']$(' denotes the transpose) and T is the state-transition matrix. A state s_0 is called a cycle state if there exists an inter p such that

$$s_0 = Tp \times s_0 \tag{2}$$

Manuscript received January 17, 2011; revised January 25, 2011; accepted February 10, 2011.

Seok-T ae Kim(Corresponding Author) is with the Department of Information & Communications Engineering, Pukyong National University, 599-1, Daeyeon 3-Dong, Nam-Gu, Busan, 608-737, Korea (Email: setakim@pknu.ac.kr)

The smallest integer p that satisfies Eq.2 is called cycle length of the CA [2], [3]. If the length of an n-cell CA is 2^n-1, it will be called Maximum Length Cellular Automata (MLCA) [4].The complemented CA evolution is expressible in the form:

$$\overline{(x_{i(t+1)})} = f[x_{i-1(t)}, x_{i(t)}, x_{i+1(t)}] \oplus F(x) \tag{3}$$

We consider a three-site neighborhood, dual-state, one dimension CA, f is a Boolean function where defining the rule, F is complemented vector and ⊕ devotes XOR logic.

One Dimension transform CAT base function A_{ik} can be used as transform bases:

$$Type1: \quad A_{ik}=\alpha+\beta a_{ik} \tag{4}$$

$$Type2: \quad A_{ik}=\alpha+\beta a_{ik}a_{ki} \tag{5}$$

2)2-D Cellular Automata Transform

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

$$A_{ijkl}=A_{ik}A_{jl} \tag{6}$$

Or

$$A_{ijkl}=L_w\{(a_{ik}a_{ki}+a_{jl}a_{lj}) \bmod L_w\}-(L_w-1) \tag{7}$$

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

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

$$f_{ij}=\sum_{k=0}^{M-1}\sum_{l=0}^{N-1} c_{kl}\times A_{ijkl} \tag{8}$$

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

$$c_{kl}=\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} f_{ij}\times B_{ijkl} \tag{9}$$

If A_{ijkl} are orthogonal, the bases B_{ijkl} are the inverse of A_{ijkl}, the Eq.9 is called Cellular Automata Transforms (CAT) and Eq.8 is called Inverse Cellular Automata Transforms (ICAT)[5][6].

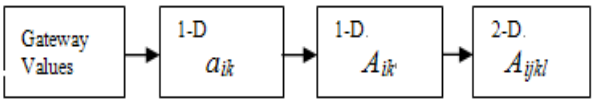

Fig.1. 2D basis function A_{ijkl} generation process.

TABLE I
GATEWAY VALUES

Gateway	Values
'Wolfram' Rule number	14
Initial configuration	11010100
Boundary configuration	Cyclic
N	8
Basis function type	Type 2

The cyclic boundary conditions imposed on the end sites (i=-1and i=N) are of the form: $a_{-1k}=a_{N-1k}$, $a_{Nk}=a_{0k}$.

In this paper, the CAT basis function type is type 2: $A_{ik}=2a_{ik}xa_{ki}$. Using the Eq.4: $A_{ijkl}=A_{ik}A_{jl}$, the 2-D CAT basis function is obtained.

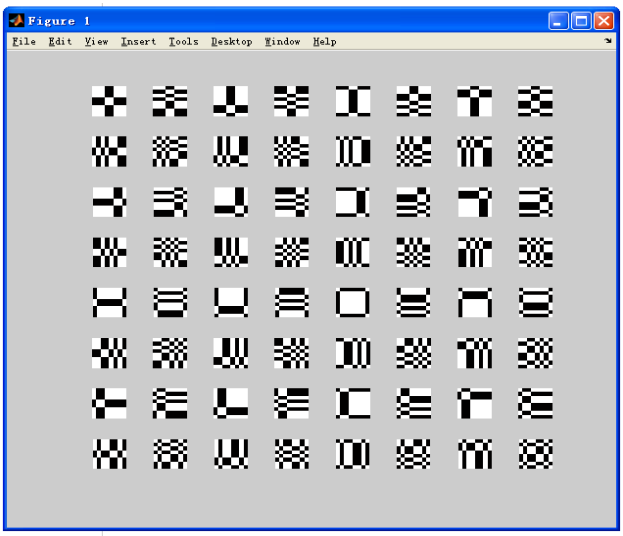

Fig.2. 2-D CAT basis function A_{ijkl}.

Here, Fig.2 is 2-D CAT basis function, 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 [7]. 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:

$$a_{1(t+1)}=(W_0a_{0t}+W_1a_{1t}+W_2a_{2t}+W_3a_{0t}a_{1t}+W_4a_{1t}a_{2t} +W_5a_{2t}a_{0t}+W_6a_{0t}a_{1t}a_{2t}+W_7)^{W_8} \bmod K \tag{10}$$

III. GENERATION OF ENCRYPTED WATERMARK

In this watermarking scheme, the encrypted watermark can be generated from the linear MLCA and complemented MLCA.

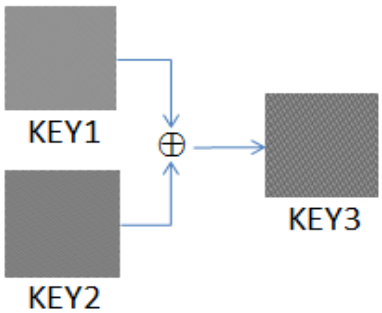

Fig.3. Private Key generation process.

The 'KEY1' is the MLCA based image (256×256 pixels) and 'KEY2' is the complemented MLCA based image (256×256 pixels). The two keys do exclusive-or (*XOR*) operation, the private key 'KEY3' is obtained.

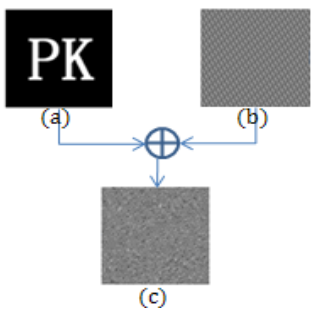

Fig.4. Private watermark generation process.

Here, Fig.4 shows the encrypted watermark generation process, (a) Original watermark, (b) Private Key and (c) encrypted watermark.

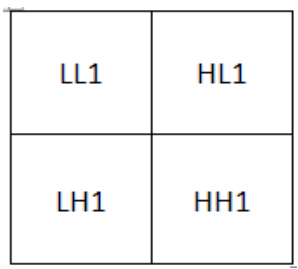

Fig.5. Multi-resolution sub bands of the original image.

The pyramid structure (Fig.5) of the CA-transformed**.** The LL1 sub band is called low frequency of the transformed image.

IV. EMBEDDING INTO ENCRYPTED WATERMARK

The embedding procedure of encrypted watermark of the watermarking system can be summarized as below, and the block diagram is shown in Fig.6.

Step1. Using the gateway values generate the CAT basis function A_{ijkl}.
Step2. Apply 1-level CAT to decompose image into four non-overlapping multi-resolution sub bands: LL1, HL1, LH1, and HH1.
Step3. Apply the MLCA and complemented MLCA to generate the private key.
Step4. Embed the private watermark into the low frequency of the CAT coefficient.
Step5. Use the ICAT for '*Step 4'* and the watermarked image is obtained.

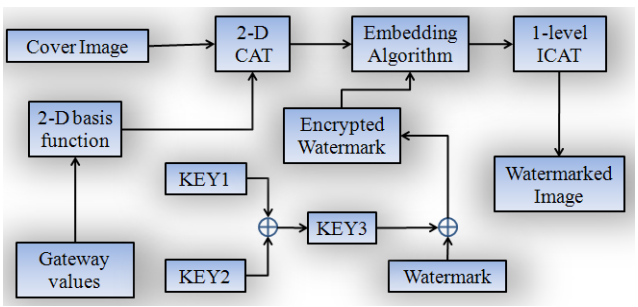

Fig.6. Watermark embedding procedure.

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 work, the encrypted watermark is embedded into the "Group I" coefficient by using the following Eq.11:

$$O' = O_{group1} \times (1 + \alpha wi) \tag{11}$$

here, wi is the watermark data, $O_{\text{group I}}$ is the data of c_{kl}(Low frequency), α is the embedding parameter. The watermarked image is generated as described by Eq.12:

$$O'' = ICAT(O') \tag{12}$$

where O'' is the watermark information.

V. EXPERIMENTAL RESULTS AND ANALYSIS

Estimate Parameters To demonstrate the performance of the scheme, we use the famous test image Body-Disk (gray-valued, 512x512 pixels) as test image and PK (256x256 pixel, 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 embedded watermarks and extracted watermarks.

$$PSNR = 10\log(\frac{255^2}{MSE(O,O')}) \quad (13\text{-}1)$$

$$MSE = \frac{1}{M \times N}(\sum\sum(O-O'))^2 \quad (13\text{-}2)$$

$$BCR = \frac{\sum_{i=0}^{(Wh\times Ww)-1}\overline{(W \oplus W')}}{Wh \times Ww} \times 100\% \quad (14)$$

where *O, O'* are the original images and watermarked images information respectively, *W, W'* is the watermark data and extract watermark data, and $\oplus$ denotes the Exclusive-Or operator.

Imperceptibility For testing the invisibility and robustness, we compare the test image 'BODY-DISK' with the watermarked image, the PSNR=43.56dB is greater than 30DB. It means the invisibility is better.

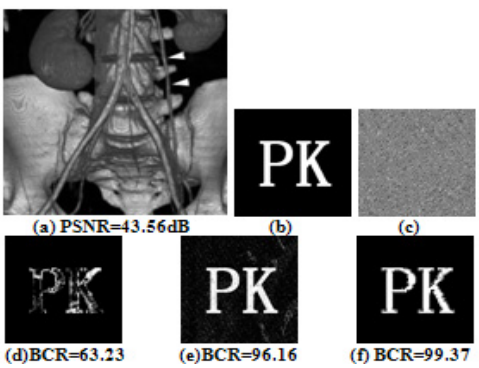

Fig.7. (a) Watermarked image of BODY-DISK(512x512), (b)original watermark(256x256), (c)Encrypted watermark, (d)Recovered watermark from watermarked image (CAT Rule=11), (e) Recovered watermark with the Rule is 243, (f) Recovered watermark with the Rule is 14.

In this work, the test image 'BODY-DISK' and watermark 'PK' is shown in Fig.7. Different CAT Rules to put to use, compare with the Rules, the CAT Rule=14 is the best 'Wolfram' Rule number for this experiment. We evaluated imperceptibility comparison with DCT and DWT algorithm by using BCR values. In contrast, and show in TABLE 2 the PSNR values of the CAT is relatively large. This indicates that improvement in imperceptibility can be achieved by applying CAT transformed LL1 sub band.

TABLE II
PSNR VALUES WITH DIFFERENT METHODS

PSNR Values			
Methods	CAT	DCT	DWT
BODY-DISK	43.56	32.55	27.36
Monkey	46.32	34.23	28.49
Lena	51.38	38.12	29.65
Pepper	46.28	30.95	30.19
Plane	51.69	33.64	26.75

Table 2 shows the CAT method with the rule=14 and test images with gray images (512x512), in this paper we use the same test image and watermark with the different methods, from the result, the CAT method is better than DCT and DWT methods.

Robustness Table3 shows the Bit Correct Ratio values between the original watermark and the watermark extracted from the watermarked image.

The Bit Correct Ratio values given in table 3 show clearly that the CAT watermarking algorithm outperforms the conventional DCT and DWT approach with respect to robustness against the JPEG Compression and Gaussian noise and Median Filter attacks. The results are better regardless of whether the watermark was embedded in CAT domain or other conventional transformed (DCT, DWT) domains, however, CAT-based algorithm gave better robustness. Fig.8 shows the watermarks extracted from LL1 when CAT was used. Fig.9 and Fig.10 show the watermarks extracted from sub band LL1 when DCT and DWT were used respectively.

TABLE III
BCR VALUES UNDER DIFFERENT ATTACKS

Bit Correct Ratio Values			
Attacks	CAT	DCT	DWT
JPEG,Q=30	87.12	27.42	49.42
JPEG,Q=80	94.33	30.25	53.25
Median Filter	82.52	38.66	51.66
Gaussian	88.13	49.21	50.21
White Noise	85.38	42.19	40.19

Fig.8. Extracted watermarks from the LL1-watermarked image using CAT method.

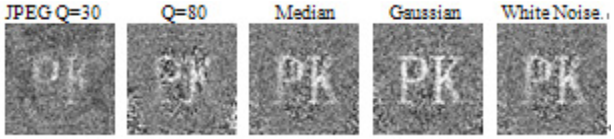

Fig.9. Extracted watermarks from the LL1-watermarked image using DCT method.

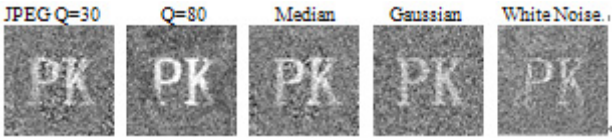

Fig.10. Extracted watermarks from the LL1-watermarked image using DWT method.

According the result of expriment in Table 3.The BCR values of CAT-based are considered and all extracted watermarks under different attackss are recognized.

VI. CONCLUSIONS

In this work a secure and novel watermarking system based on complemented Maximum Length Cellular Automata (MLCA) and Two-Dimension Cellular Automata Transform (2D CAT) is presented and tested on the original image, 'BODY-DISK'. Watermarking mainly introduces that the encrypted watermark is embedded into the CAT-domain of the cover image. The experiments show that this method provides a secure and robust digital watermarking system.

REFERENCES

[1] T.L.Booth, "Sequential Machines and Automata Theory", London, 1967.
[2] S. Nandi, B.KKar and P.P. Chaudhuri, "Theory and application of cellular automata", Proc.IEE, Stevenage, U.K., Vol.137, pp.81-87, Jan.1990.
[3] S.J.Cho, U.S.Choi and Y.H.Hwangi, "Computing phase shifts of Maximum-Length 90/150 cellular automata sequences", lecture notes in computer science, pp.31-39, Oct.2004.
[4] 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.
[5] Olu Lafe, "Cellular Automata Transforms: Theory and Application in Multimedia Compression, Encryption, and Modeling", Kluwer Academic Publishers, Boston/Dordrecht/London, pp.581-591, 1997.
[6] S.T.Kim, Y.R.Piao, "Robust and Secure InIm-based 3D Watermarking Scheme using Cellular Automata Transform", IJMICS, pp.1767-1778, 2009.
[7] 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, pp.231-241, 1998.

Xiao-Wei Li is a master degree student at department of information and communications in Pukyong National University of Korea. He received his B.S degree in computer science and technology from Dalian Ocean University of China, in 2009. His area of interest is digital watermarking about image processing.

Jae-Sik Yun received the B.S. degree in Dept. of Electronics and Telecommunication Engineering from Pukyong National University, Busan, Korea in 2010. He is currently pursuing the M.S. in Dept. of Information and Communications Engineering at Pukyong National University. His research interests include Image Processing and Machine Vision.

Sung-Jin Cho received the B.S. degree in Dept. of Mathematics Education from Kangwon National University, Korea in 1979. He received the B.S. and the Ph.D. degree in Dept. of Mathematics from Korea University in 1981 and 1988. Since 1988, he has been a Professor in Dept. of Applied Mathematics, Pukyong National University, Busan, Korea. His research interests include Cellular Automata, Coding Theory and Cryptography.

Seok-Tae Kim received B.S. degree in Dept. of Electronics Engineering from Kwangwoon University, Korea in 1983. He received M.S. degree in Dept. of Electronics Engineering from Kyto Institute of Technology, Kyoto, Japan in 1988. He received Ph.D. degree in Dept. of Communication Engineering from Osaka University, Osaka, Japan in 1991. He had worked as an inviting professor from University of Washington, USA in 1999 and at Simon Fraser University, Canada in 2006. Since 1991, he has been a Professor in Dept. of Electronics, Computer and Telecommunication Engineering, Pukyong National University, Busan, Korea. His research interests include Image Processing, Pattern Recognition, Watermarking and Cellular Automata.