International Journal of Innovative
Computing, Information and Control
Volume 8, Number 10(B), October 2012
 ISSN 1349-4198
pp. 7249–7262

IMAGE WATERMARKING ALGORITHM USING 2D CELLULAR AUTOMATA TRANSFORM

Xiao-wei Li[1], Sung-jin Cho[2] and Seok-tae Kim[1,*]

[1]Department of Information and Communications Engineering
[2]Department of Applied Mathematics
Pukyong National University
599-1, Daeyeon 3-Dong, Nam-Gu, Busan, Republic of Korea
lixiaowei@nate.com; sjcho@pknu.ac.kr
*Corresponding author: setakim@pknu.ac.kr

Received August 2011; revised December 2011

Abstract. *Cellular automata are discrete dynamical systems that provide the basis for the synthesis of complex emergent behavior. Starting from a basic unit, the cell, the use of cellular automata not only provides insight into the evolution of life but also opens vistas into the creation of intelligent computer systems. This paper proposes a secure and novel digital watermarking system based on Maximum-Length Cellular Automata (MLCA) and a Two-Dimension Cellular Automata Transform (2D CAT). First, the original image is decomposed into a level-1 CAT algorithm and the sub-bands LL1, HL1, LH1 and HH1 are obtained, and further using level-1CAT to sub-bands HL1 and LH1, the middle-frequency: HL2 and LH2 are obtained. Then, the original watermark, which is encrypted by the Maximum-Length Cellular Automata (MLCA), is embedded into the CAT domains of the original image. Finally, the watermarked image is obtained using the inverse Cellular Automata Transform (ICAT) for the CAT-transformed image. This is a novel scheme because it has the capability of robustness and invisibility simultaneously. However, the traditional watermarking algorithm based on CAT cannot achieve. The experimental results show that our CAT-based watermarking system can simultaneously improve the security, robustness and image quality of the watermarked image.*
Keywords: Cellular automata, Digital watermarking, Maximum-length cellular automata, Middle-frequency, 2D cellular automata transform

1. **Introduction.** Because of the popularity of Internet use, the ability to embed an owner's identity and other information securely into multimedia is becoming an urgent need. The protection and enforcement of intellectual property rights for digital multimedia have become important issues. Digital media, including images, audio and video, suffer from copyright infringement because of their digital nature, which facilitates unlimited copying, ease of modification and the ability to be quickly transferred over the Internet [2,6]. Digital watermarking refers to techniques used to protect digital data by imperceptibly embedding information (a watermark) into the original data in such a way that it remains present.

Most multimedia applications require imperceptible and robust watermarks [1]. Watermarking schemes based on secret keys are intensively used in modern security systems to ensure data integrity [3,8,9]. 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 enough, and the calculation time of the algorithm is very long. Digital watermarking is also called watermark insertion or watermark embedding. After inserting or embedding the watermark by specific algorithms, the original media will be slightly modified. The modified media are

called the watermarked media. There might be little to no perceptible difference between the original media content and the watermarked content.

Watermarking methods can be classified into two types: those that embed the watermark into the spatial domain and those that embed the watermark into the frequency domain. The first type provides good computing and visibility but usually has a degraded robustness, while the second type, which is based on a transformed domain technique, for watermark embedding in the CAT or discrete cosine transform (DCT) [8] domain, if we embed the watermark in the higher frequency bands, even though the watermarked image quality is good, it is vulnerable to the low pass filtering (LFP) attack. Thus, embedding in the higher frequency bands coefficients is not robust, although the watermarked image quality is assured. In contrast, if we embed the watermark into the coefficient in the lower frequency bands, it should be robust against common image proceeding attacks such as the LPF attack. However, embedding in the lower frequency band will cause the resulting watermarked image quality greatly degrade to compare with the original image. This comes from the fact that the energies of most natural images are concentrated in lower frequency bands, and the human eyes are more sensitive to the noise caused by modifying the lower frequency coefficients. Therefore, aside from the two observations above, some researchers claim to embed the watermarks into the middle-frequency bands to serve as a trade-off for watermark embedding in the transform domain.

Cellular automata are discrete dynamical systems whose behavior is completely specified in terms of a local relation [4]. A cellular automaton can be thought of as a stylized universe [5,6]. Space is represented by a uniform grid, with each cell containing a few bits of data. Time advances in discrete steps and the laws of the "universe" are expressed in a small look-up table through which at each step, each cell computes its new state from that of its close neighbors. Thus, the systems' laws are local and uniform. All cells on the lattice are updated synchronously [7]. Von Neumann conceived the first cellular automaton in the late forties. (Von Neumann's work on self-reproducing automata was completed and described by Arthur Burks). Different from previous schemes, in this paper, we propose a novel watermarking scheme for image data using two-dimensional cellular automata transform (2D CAT) algorithms. The CAT technique provides hierarchical multi-resolution: three parts multi-resolution representation (MRR) and one part multi-resolution approximation (MRA). Level n-resolution CAT decomposition will result in a pyramid structure. The sub-bands labeled LH1, HL1 and HH1 of (MRR) represent the high-frequency information, such as the edges and textures of an image. Generally, the human visual system is not sensitive enough to detect changes in such sub-bands. The sub-band LL1 of MRA represents the low-frequency information which contains important data about the original image.

In this research, a watermarking algorithm based on MLCA and 2D CAT is presented. First, the host image will be decomposed into a pyramid structure based on level-2 2D CAT. The sub-bands labeled LL2, HH2, LH2 and HL2 are obtained. Here, sub-bands LH2 and HL2 are named the Middle frequency of the original image. The encrypted watermark generated by MLCA is embedded into the CAT-transformed frequency. This proposed method of embedding an MLCA-based encrypted watermark into our CAT-based watermarking system can greatly improve security and simultaneously improve the robustness and image quality of the watermarked images. The goal of this method is to apply the 2-D CAT algorithm to enhance the robustness to different attacks to minimize the drawbacks of the previous algorithm.

2. Watermarking Algorithm Based on a Cellular Automata Transform.

2.1. **MLCA and 2D CAT.** Cellular automata are dynamical systems in which space and time are discrete. A CA is a collection of n storage elements. The elements are called cells, and the cells 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. The function is called a transition function or a rule [9,10]. For 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 $f_t = [f1(t), f2(t), f3(t), \ldots, fn(t)]'$, ($f'$ denotes the transpose) and T is called the state-transition matrix. A state s_0 is called a cycle state if there exists an integer p such that

$$s_0 = T^p \times s_0 \tag{2}$$

The smallest integer p that satisfies Equation (2) is called the cycle length of the CA. If the length of an n-cell CA is $2^n - 1$, it will be called the Maximum-Length Cellular Automata (MLCA) [11,12]. An N-cell MLCA is characterized by the presence of the entire non zero states of the CA in a single cycle. In the case of an N cell dual-state $(0, 1)$ CA, the length of this cycle is $2^n - 1$. The characteristic polynomial of such a CA is a primitive polynomial. The definition of a primitive polynomial remains invariant in the extension that is field the lowest value of k for which the characteristic polynomial will divide $x^k + 1$ is $2^n - 1$. The 3-cell CA having the following T matrix is an MLCA. Example:

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

The characteristic polynomial of the T polynomial is $x^4 + x^3 + 1$. The lowest value k for this polynomial dividing $x^k + 1$ is $2^4 - 1 = 15$. This CA is an MLCA.

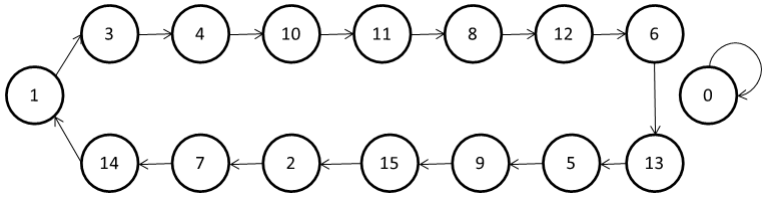


FIGURE 1. The state transition graph

2.2. **2-D cellular automata transform.** The cellular automata transform presents a more direct way of achieving the linkage between a given phenomenon and the evolving CA field [12]. CA transforms can be utilized in the way other transforms (e.g., Fourier, Laplace and wavelets) are utilized. Cellular automata are capable of generating billions of orthogonal, semi-orthogonal, bi-orthogonal and non-orthogonal bases [13-16]. For a two-state, three-site CA, the state a_{it+1} from the state of the neighborhood at the t-th time level, the cellular automaton evolution is expressible by the function:

$$a_{it+1} = F(a_{i-1t}, a_{it}, a_{i+1t}) \tag{3}$$

k → / i ↓	0	1	2	3	4	5	6	7
0	_	+	_	_	_	_	_	_
1	+	+	_	_	_	+	_	_
2	_	_	_	+	_	_	_	_
3	_	_	+	+	_	_	_	+
4	_	_	_	_	_	+	_	_
5	_	+	_	_	+	+	_	_
6	_	_	_	_	_	_	_	+
7	_	_	_	+	_	_	+	+

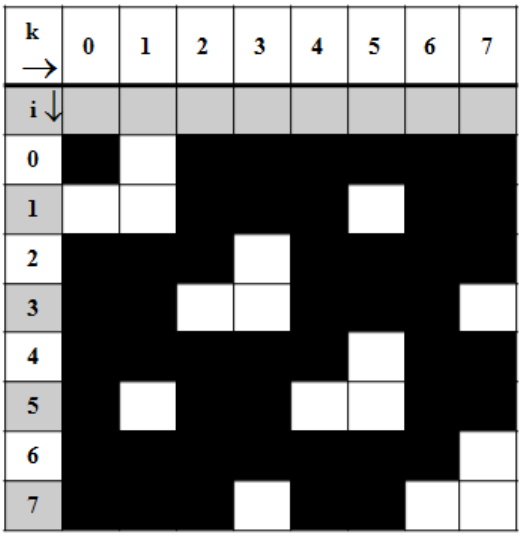


FIGURE 2. Basis functions of one-dimensional CAT, dual-coefficient basis function Wolfram Rule = 11; $N = 8$. Initial configuration = 011011000. Boundary configuration = Cyclic. CAT type = 2 and the graphical display.

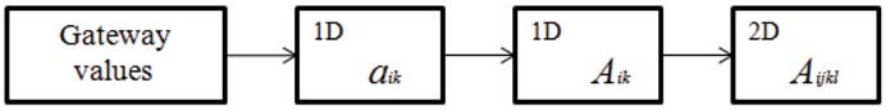


FIGURE 3. 2D basis function generation process

Here, F is the Boolean function that is defined by the rule.

The one-dimensional transform base function can be used as a transform base:

$$A_{ik} = \alpha + \beta a_{ik} a_{ki} \tag{4}$$

where a_{ik} is the state of the CA at the mode i at time $t = k$ while α and β are constants. The states are obtained from N cells evolved from a specific initial configuration for N time steps.

The two-dimensional cellular automata base function A_{ijkl} is derived from a one-dimensional base function:

$$A_{ijkl} = A_{ik} A_{jl} \tag{5}$$

There are as many canonical 2D bases as there are permutations of the 1D base. One interesting 2D basis function is derived from the evolving one-dimensional automata as:

$$A_{ijkl} = L_W((a_{ik}a_{ki} + a_{jl}a_{lj}) \bmod L_W) - (L_W - 1) \tag{6}$$

where $L_W \geq 2$ is the number of states of the automaton. In this paper, we use (Equation (5)). Here, $A_{ik} = (\alpha + \beta a_{ik})(\alpha + \beta a_{ki})$. 2D basis function generation process is shown in Figure 3.

Here, 1D a_{ik} is the state of CA at the cell i at time $t = k$, and according the CAT type 8: $A_{ik} = (\alpha + \beta a_{ik})(\alpha + \beta a_{ki})$, 1D basis function A_{ik} is obtained. 2D CAT-bases derived from the one-dimensional automata.

TABLE 1. Gateway values

Gateway	Values
Wolfram Rule number	...14/43...
Number of cells of per neighborhood	8
Initial configuration	(01101010)/(01011101)
Boundary configuration	Cyclic
Basis function type	$A_{ik} = (2a_{ik} - 1) \times (2a_{ki} - 1)$

In this paper, we use gateway values of Table 1, the CAT basis function type given $\alpha = -1$, $\beta = 2$. For the coefficients for a typical orthogonal $(1, -1)$, the cyclic boundary conditions imposed on the end sites ($i = -1$ and $i = N$) are of the form: $a_{-1k} = a_{N-1k}$, $a_{Nk} = a_{0k}$.

FIGURE 4. 2D CAT basis function A_{ijkl}, (a) Rule = 14 and (b) Rule = 43

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

$$f_{ij} = \sum_{k=0}^{M-1} \sum_{l=0}^{N-1} c_{kl} \times A_{ijkl} \tag{7}$$

Here, k and l are vectors of nonnegative integers, and c_{kl} is a transform coefficient whose values are obtained from the inverse transform:

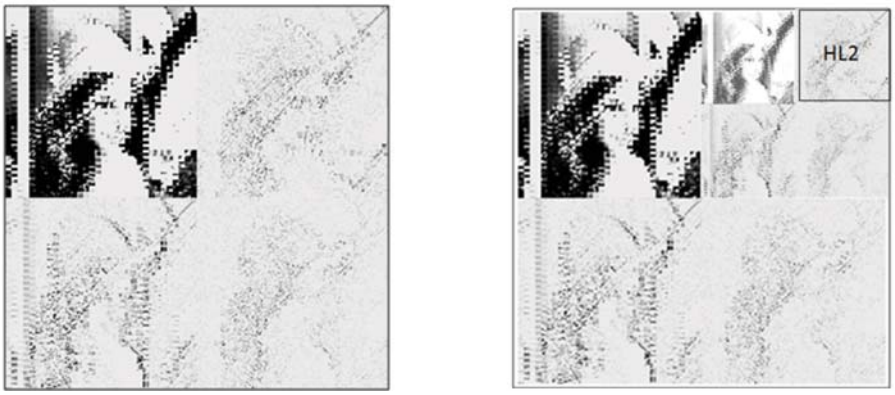
$$c_{kl} = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f_{ij} \times B_{ijkl} \tag{8}$$

If A_{ijkl} are orthogonal, the bases B_{ijkl} are the inverse of A_{ijkl}, Equation (8) is called the Cellular Automata Transform (CAT), and Equation (7) is called the Inverse Cellular Automata Transform (ICAT) [15,16].

For the CAT coefficient c_{kl}, we can decompose a pyramid structure using the CA-transformed. We first decompose the original images using the CAT, and the coefficient c_{kl} is obtained. When k and l are even, the c_{kl} (Group I) represents low frequency, which is located in upper left part of Figure 6(a). The rest (Group II: k is even, l is odd, the upper right part. Group III: k is odd; l is even, the lower left part. Group IV: k is

(a) (b)

FIGURE 5. (a) 256 × 256 Lena as the original data f_{ij} and (b) 2D-CAT transform coefficient c_{kl}



(a) (b)

FIGURE 6. (a) Decomposition of CAT coefficients c_{kl} into four bands, (b) the image formed by the Group II components in Figure 6(a) is further CAT decomposed and sorted into another four groups, HL2-domain is equivalent to middle frequency of CAT coefficients c_{kl}

odd, l is odd, the lower right part of Figure 6(a)) of the coefficients are in high frequency components.

As shown in Figure 7, sub-band LL2 is equivalent to the low-low frequency components. Sub-band HH2 is equivalent to the high-high frequency components. Sub-band HL2 is the Middle frequency components.

3. Generation of an Encrypted Watermark and the Watermarking Algorithm.

3.1. Encryption and decryption process.

In this watermarking scheme, the encrypted watermark can be generated from the linear MLCA. We first generate the MLCA basis image, and then the original watermarks perform the XOR operation on every pixel of the basis image.

Figure 8 shows ROSE (binary value, see Figure 10) as the original watermark. We use the MLCA basis image as the encryption key, and (a) the watermark encryption process, (b) the private watermark decryption process.

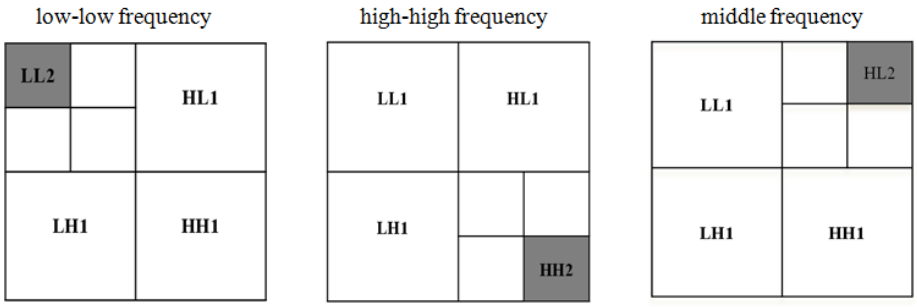


FIGURE 7. Level-2 CAT transformed. The image formed by Figure 6(a) is further CAT decomposed and sort into another four bands.

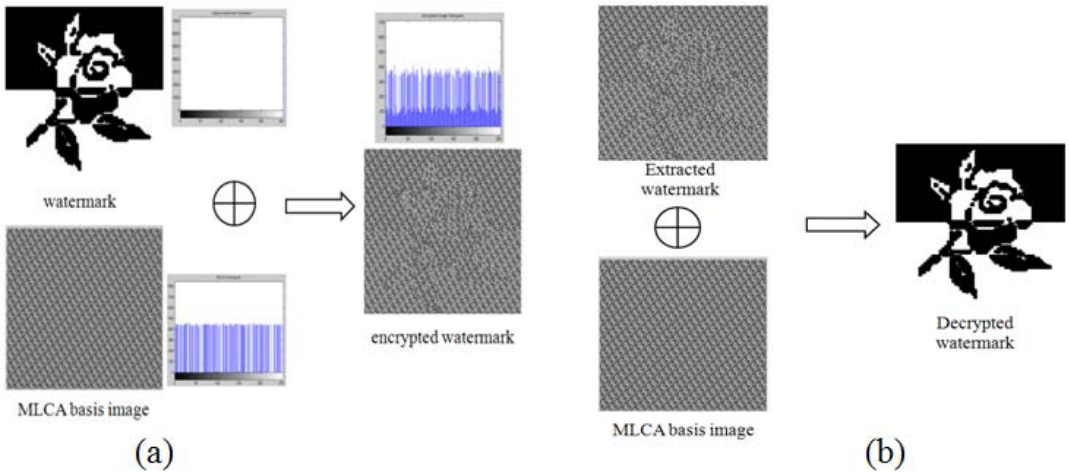


FIGURE 8. Private watermark generation process

3.2. **Watermark algorithm.** The watermark data embedded into the CAT low-frequency coefficient give the following (Equation (9)):

$$O' = O \times (1 + \alpha w_i) \tag{9}$$

Then, we use 2D inverse CAT (ICAT) to transform,

$$O'' = ICAT(O') \tag{10}$$

Here, O is the data from the CAT-transformed image, w_i is the watermark data, α is the embedding parameter, and O'' is the watermarked image data.

3.3. **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, however, 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

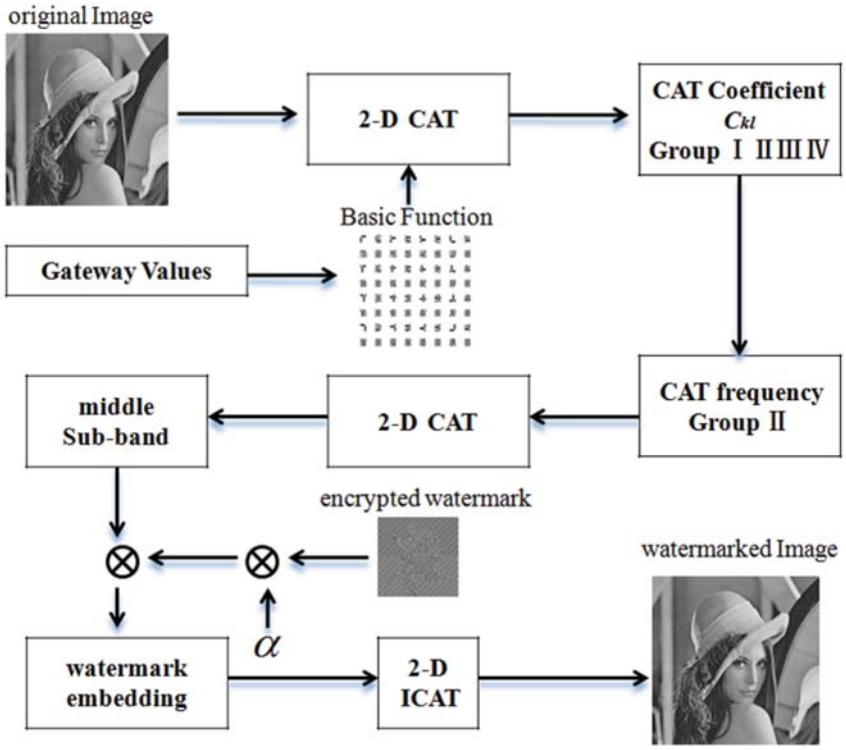


FIGURE 9. The flow chart of the cellular automata transform algorithm

sensitive to changes in such sub-bands [17,18]. This allows the watermark to be embedded without being perceived by the human eye. However, it is not robust, and it is vulnerable to image-processing attacks. The compromise adopted by the 2D CAT-based watermarking algorithm is to embed the watermark in the Middle frequency sub-bands, HLx and LHx. To provide credibility for this approach, compare the sub-band Middle frequency with other CAT sub-bands and the DWT watermarking method. Experiments show that embedding the watermark in the Middle frequency sub-bands led to acceptable performance for imperceptibility and robustness.

As shown in Figure 9, 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 $N \times N$ image O 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 shown in Figure 7, 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 $(N_W \times N_W)$ in the Middle frequency of CAT-domain, $O' = O \times (1 + \alpha w_i)$ $i = 1, \ldots, N_W$.

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 O'', 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: $w_i^{*K} = (O_{HL2}^{'*K} - O_{HL2}^{'K})/a$, $K = 1, \ldots, N_w$.

Step 4. Apply the MLCA basis image and obtain the recovered watermark by performing the XOR operation on the extracted encrypted watermark.

4. Experimental Results and Analysis.

4.1. **Embedding phase.** 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.

$$PSNR \equiv 10 \times \log\left(\frac{255^2}{MSE(O, O')}\right) \tag{11}$$

$$MSE(O, O') \equiv \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (O, O') \tag{12}$$

$$BCR \equiv \left(1 - \frac{\sum_{i=1}^{L_M} (w_i \oplus w_i')}{L_M}\right) \tag{13}$$

where O and O' 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.

4.2. **Experimental results and analysis.** The performance of proposed 2D CAT image watermarking algorithm is evaluated using the performance using the gray-scale 512×512 cover image 'Lena', as test image, and ROSE (binary-valued) as the watermark (see Figure 10). The 2D CAT rules (14, 15, 42, 43 and 143) are used for this scheme. The watermarked images are subjected to attack via JPEG compression, cropping, rotation and scaling. Watermarking algorithms are usually evaluated with respect to their imperceptibility and robustness.

Imperceptibility

FIGURE 10. The original image of the proposed technique Lena and the original watermark ROSE

For the obtained watermarked image (Figure 11) for which we chose the CAT rule of 43 and embedded the watermark in the Middle frequency, the quality of the images is good, and the PSNR values are considered. The PSNR of other CAT Rules show below.

Table 2 shows the PSNR values under different CAT rules. For watermarking based on 2D CAT, determining how to choose the best CAT rule is the key point. In this work, the 2-state, 3-site CA has $2^{2^3} = 256$ CAT rules. From the experiment, Rule = 43 is the most desirable rule.

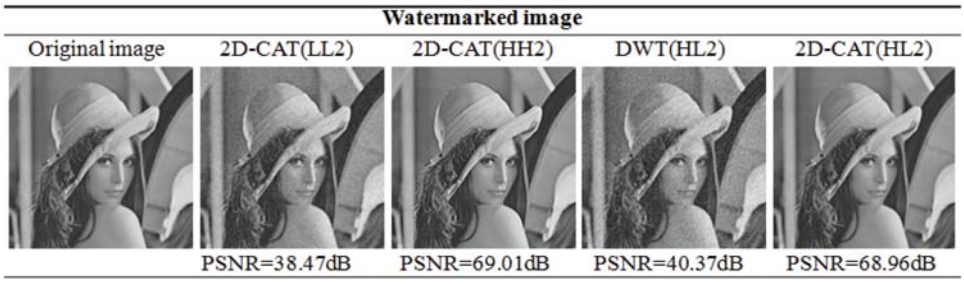


FIGURE 11. The watermarked image Lena at different CAT sub-bands and DWT sub-band

TABLE 2. PSNR values (Lena) under different CAT rules

Rule	14	15	42	43	143
CAT-HL2	56.38	38.12	25.39	68.96	46.38
CAT-LL2	41.26	22.10	21.65	38.47	38.74
CAT-HH2	58.73	32.14	29.54	69.02	45.29

We evaluated the imperceptibility of the CAT algorithm by measuring PSNR for the CAT-based sub-bands. The Middle frequency HL2 gave very high PSNR values. The High-High frequency gave slightly greater PSNR values than the Middle domains. However, the PSNR values of low-low frequency are not considered.

Robustness:

To test the robustness of the proposed scheme, we first attack the watermarked image and then extract the watermark. The possible attacks include rotating, JPEG compression, scaling and cropping. In this work, a comparative analysis is performed between our proposed method and an existing watermarking method (Yuan, Yao, Joo, et al. 2002), discrete wavelet transform (DWT) [19-21]. Like our scheme, the original image is decomposed into a level-2 DWT algorithm and the sub-band HL2 was obtained, then, the watermark data was embedded into the DWT-domain (HL2). The host image is analyzed, a two-level decomposition is applied to the host image, and watermark information is embedded into the frequency domain. The bit correct ratio values of different schemes are described in Tables 3-6.

(a) (b) (c) (d)

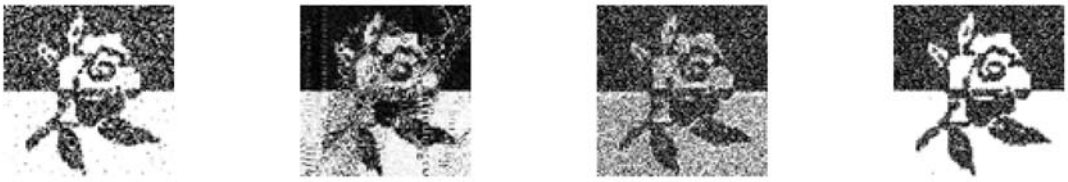
FIGURE 12. Attacked images, (a) rotation attack (angle = pi/20), (b) JPEG compression (Q = 0.3), (c) scaling attack (scaling factor = 0.8) and (d) cropping attack (size = 160)

Figure 12 shows the watermarked image 'Lena' which watermark was embedded into middle-frequency of 2D CAT, under rotating, JPEG compression, scaling and cropping

attacks. The compromise adopted by CAT-based watermarking algorithm, is to embed the watermark in the Middle frequency sub-bands, for proving credibility of this view point, comparison with sub-band middle frequency and other watermarking methods. In contrast, we embed watermark into the coefficients in the other frequency bands LL2-domain, HH2-domain and DWT frequency domain. The extracted watermarks show below (Figures 13-16).

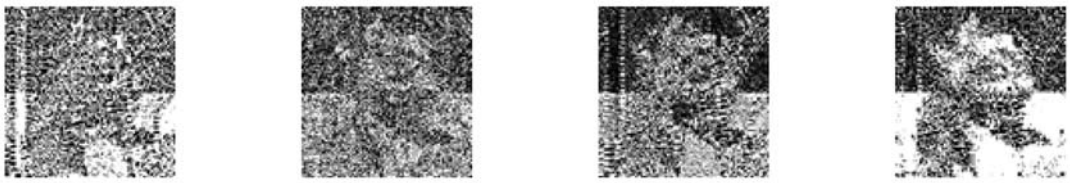
(a) Rotation (b) JPEG (c) Scaling (d) Cropping

FIGURE 13. Recovered watermarks from the HL2-domain of attacked watermarked image (see Figure 13)



(a) Rotation (b) JPEG (c) Scaling (d) Cropping

FIGURE 14. Recovered watermarks from the LL2-domain of the CAT scheme



(a) Rotation (b) JPEG (c) Scaling (d) Cropping

FIGURE 15. Recovered watermarks from the HH2-domain of the CAT scheme

(a) Rotation (b) JPEG (c) Scaling (d) Cropping

FIGURE 16. Recovered watermarks from the HL2-domain of the DWT scheme

As shown in Figures 13-16, the quality of the extracted watermarks, we find that our proposed method offers the more robustness than other CAT methods (J. W. Shin, S. Yoon and D. S. Park, 2010) which embedded other frequency domain.

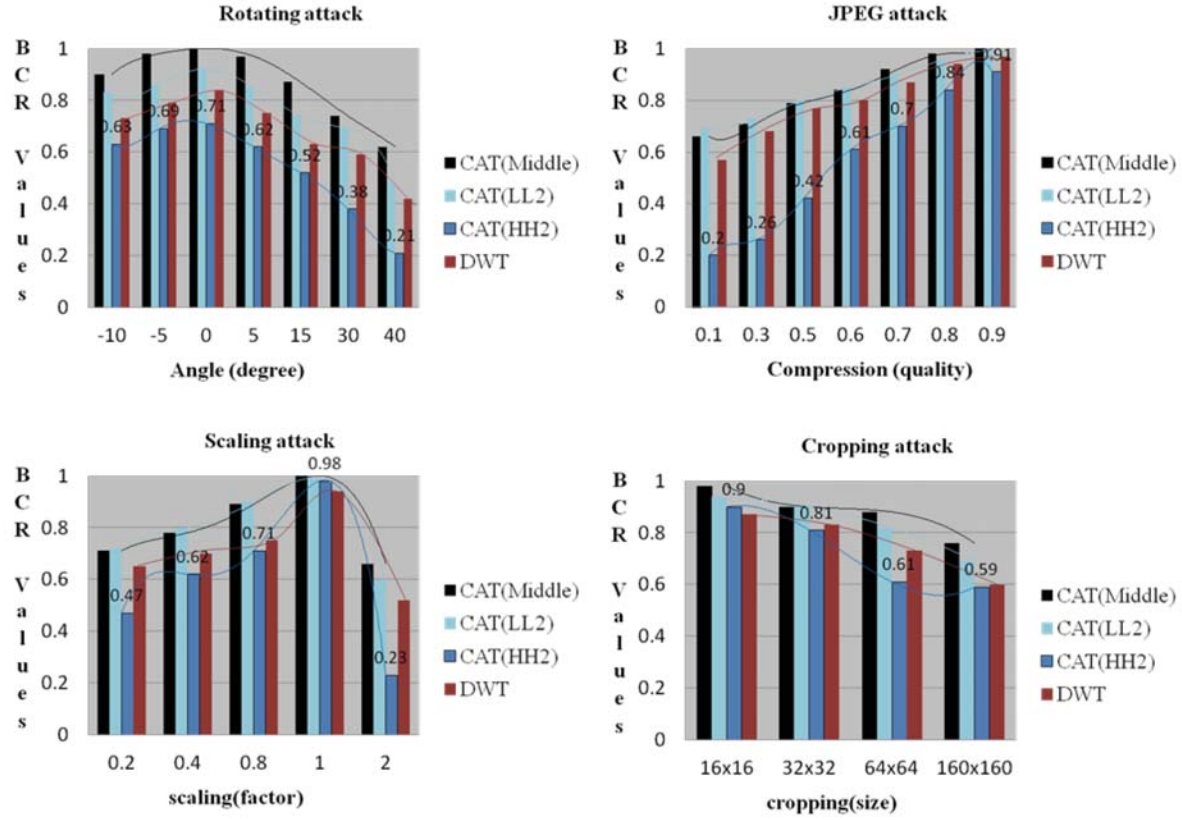


FIGURE 17. Comparison under rotating attack, JPEG compression attack, scaling attack and cropping attack

TABLE 3. Bit correct ratio values under rotating attack

Angle (degree)	CAT Middle(HL2)	CAT Low-Low(LL2)	CAT High-High(HH2)	DWT-based DWT-domain
−10	0.90	0.83	0.63	0.73
−5	0.98	0.86	0.69	0.79
0	1	0.92	0.71	0.84
5	0.97	0.85	0.62	0.75
15	0.87	0.74	0.52	0.63
30	0.74	0.69	0.38	0.59
40	0.62	0.48	0.21	0.42

TABLE 4. Bit correct ratio values under compression attack

JPEG (quality)	CAT Middle(HL2)	CAT Low-Low(LL2)	CAT High-High(HH2)	DWT-based DWT-domain
0.1	0.66	0.69	0.20	0.57
0.3	0.71	0.73	0.26	0.68
0.5	0.79	0.80	0.42	0.77
0.7	0.92	0.90	0.70	0.87
0.9	1	0.99	0.91	0.97

TABLE 5. Bit correct ratio values under scaling attack

Scaling (factor)	CAT Middle(HL2)	CAT Low-Low(LL2)	CAT High-High(HH2)	DWT-based DWT-domain
0.2	0.71	0.72	0.47	0.65
0.4	0.78	0.80	0.62	0.70
0.8	0.89	0.90	0.71	0.75
1	1	0.99	0.98	0.94
2	0.66	0.60	0.23	0.52

TABLE 6. Bit correct ratio values under cropping attack

Cropping (size)	CAT Middle(HL2)	CAT Low-Low(LL2)	CAT High-High(HH2)	DWT-based DWT-domain
16×16	0.98	0.94	0.90	0.87
32×32	0.90	0.90	0.81	0.83
64×64	0.88	0.82	0.61	0.73
160×160	0.76	0.69	0.59	0.60
256×256	0.65	0.53	0.32	0.42

The bars graph in Figure 17 and the data in Tables 3-6 were generated from the experimental results. We can see that, when embedding the watermark in the Middle frequency domain and sub-band LL2, the BCR values become similar to each other under the image-processing attacks, however, embedding the watermark in sub-band HH2 and the DWT-domain yields BCR values smaller than the Middle frequency after rotating, scaling and cropping attacks and watermarks are not legible. Here, we can obtain high BCR values from watermark embedded into LL2 sub-band. However, watermarks embedding in the LL2 sub-band provided poor imperceptibility in the above-mentioned experiment. From the above, embedding the watermark in the Middle frequency sub-band gave a good level of imperceptibility and was more robust against some attacks. This is a novel scheme because it has the capability of robustness and invisibility simultaneously. However, the traditional watermarking algorithm based on CAT cannot achieve. Comparing our proposed method and the DWT-based method, we may conclude that the 2D CAT-based watermarking method using Middle frequency band is more robust under various attacks.

5. **Conclusions.** A novel watermarking approach based on a 2D cellular automata transform (CAT) is presented in this paper. Based on 2D CAT, we designed a perceptually invisible and robust watermarking system to satisfy the current requirements. The experiments show that watermarking according to our algorithm provides good robustness against common signal processing, noise disturbances and some hostile assaults.

Our experimental results were satisfactory compared with most recent works in this field. In our future work, we plan to investigate the possibility of embedding encrypted watermarks in more exact and rational sub-bands of high levels of 3D CAT to provide more accurate forgery detection on 3D image or video. In addition, we believe that it is possible to make an adaptive method (fuzzy system) based on host image content for determining the strength of watermark parameters.

Acknowledgment. This work is partially supported by the National Research Foundation of Korea Grant funded by the Korean Government (NRF-2010-371-B00008).

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, *ACRI*, 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] O. 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.772-778, 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, *ICISS*, 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] O. E. Lafe, Method and apparatus for data incryption/decryption using cellular automata transform, *U.S. Patent No.5677956*, 1997.

[11] O. Lafe, *Cellular Automata Transforms: Theory and Application in Multimedia Compression, Encryption, and Modeling*, Kluwer Academic Publishers, Boston/Dordrecht/London, 2000.

[12] T. H. Nam, S. T. Kim and S. J. Cho, Image encryption using non-linear FSR and complement MLCA, *ICMICS*, vol.2, no.1, pp.168-171, 2009.

[13] S. J. Cho, U. S. Choi et al., Analysis of complemented CA derived from linear hybrid group CA, *Computers and Mathematics with Applications*, vol.53, no.1, pp.54-63, 2007.

[14] O. E. Lafe, Data compression and encryption using cellular automata transforms, *Engineering Applications of Artificial Intelligence*, vol.10, pp.589-591, 1997.

[15] Y. R. Piao and S. T. Kim, Two-dimensional cellular automata transform for a novel edge detection, *Computability in Europe 2008 Logic and Theory of Algorithms*, Greece, 2008.

[16] S. T. Kim and Y. R. Piao, Robust and secure inIm-based 3D watermarking scheme using cellular automata transform, *IJMICS*, pp.1767-1778, 2009.

[17] X. W. Li, J. S. Yun, S. J. Cho and S. T. Kim, Watermarking using low and high bands based on CAT, *IEEE ICCSIT*, 2011.

[18] J. Jin and H. P. Shu, Secure multiple image watermarking based on cellular automata, *Journal of Xidian University (Natural Science)*, vol.37, no.1, 2010.

[19] Q. Yuan, H. X. Yao, W. Gao and S. Joo, Blind watermarking method based on DWT middle frequency pair, *2002 IEEE International Conference on Multimedia and Expo*, vol.2, pp.473-476, 2002.

[20] J. W. Wang, G. Liu et al., Locally optimum detection for barni's multiplicative watermarking in DWT domain, *International Journal of Signal Processing*, vol.88, no.1, pp.117-130, 2008.

[21] D. Huangn, J. Liu, J. Huang and H. Liu, A DWT-based image watermarking algorithm, *ICME*, pp.313-316, 2001.