셀룰러 오토마타 변환을 이용한 집적영상 기반의 강인하고 안전한 3D 워터마킹 방법

박영일* · 김석태**

Robust and Secure InIm-based 3D Watermarking Scheme using Cellular Automata Transform

Yongri Piao* · Seok-Tae Kim**

요 약

본 논문에서는 셀룰러 오토마타 변환을 이용한 집적영상 기반의 강인하고 안전한 3D 워터마킹 방법을 제안한다. 본 집적영상 기반의 워터마킹 방법에서는 먼저 워터마크를 컴퓨터 픽업을 하여 요소영상 워터마크로 변환한 후 보호하려는 영상에 삽입한다. 요소영상의 워터마크는 원 워터마크를 확실하게 복원할 수 있다. 그러나 요소영상의 3D 성질은 보안에 취약하므로 셀룰러 오토마타 변환 영역을 이용하여 보호하려는 영상에 요소영상의 워터마크를 삽입하여 문제를 해결한다. 셀룰러 오토마타 변환 영역을 사용하므로 써 하나의 비밀 키만으로 워터마킹 알고리즘의 안정성이 향상된다. 마지막으로 실험을 통하여 제안 방법은 여러 가지 공격에도 강인성과 안정성을 가지고 있음을 증명한다.

ABSTRACT

A robust and secure InIm(Integral imaging)-based 3D watermarking scheme using cellular automata transform (CAT) is proposed. In the InIm-based 3D watermarking scheme, the elemental image array (EIA) watermark for the target watermark, which has to be detected, is synthesized from the computational pickup process of InIm and embedded in a cover image. The EIA watermark can provide a robust reconstruction of the target watermark. However, the 3D property of the EIA watermark causes a weakening of the security. To overcome this problem, the proposed method uses the CAT domain to embed and extract the EIA watermark in the cover image. The use of CAT significantly improves the security for our watermarking algorithm using a single secure key only. Experiments are presented to show that the proposed scheme shows robust and secure performances against various attacks.

키워드

Cellular automata transform, Basis function, Integral imaging, Elemental image, 3D watermarking

* 광운대학교 전자공학과 3DRC
** 부경대학교 정보통신공학과 (교신저자)

접수일자 2009. 05. 11
심사완료일자 2009. 06. 10

Ⅰ. Introduction

The rapid development of digital techniques for transmitting and storing information have made it possible to copy and edit different types of multimedia data such as images, audio and video. However, copyright protection of digital multimedia data has become a great challenge. To achieve this goal, many techniques have been studied in the last decades, among which digital watermarking is a promising technique not only for copyright protection but also for authentication of digital media and it offers several desirable characteristics such as imprescriptibility, robustness and security [1-7]. Especially, in security, an embedded watermark should be undetectable by illegal pirates while it must be retrieved correctly by the authorized user. The security of a watermarking system depends on the secure key used. To improve watermarking security, complex key structures such as double random phase keys and chaotic sequence keys may be required [8-9].

Until now, various watermarking techniques have been developed. Generally, watermarking techniques can be roughly classified into two main categories according to the operating domain. One is the spatial domain and the other is the transform domain. Spatial approaches are fast but usually susceptible to attacks. Therefore, transform domain approaches are commonly used, such as DCT [4-5] and DWT [6]. Recently, as another spatial domain approach, Shiba et al. [9] proposed an image watermarking technique using cellular automata transform (CAT). CAT is based on cellular automata (CA), which have generated much interest because of their diverse function and usefulness as a discrete model for many processes. A great effort has been invested in associating CA with a wide variety of phenomena including those originating from physics, chemistry, biology, economics, and information systems [9-11]. Along with the development of the CA technology, some efforts are being made in using CA in image processing.

Recently, 3D digital watermark techniques have also been suggested for improving the performance of conventional watermarking schemes [12-13]. Among them, a 3D digital watermarking scheme based on integral imaging (InIm) was proposed by one of this article's authors [13]. In this method, an elemental image array (EIA) is used as a new watermark. This EIA watermark can make a robust reconstruction of the watermark image available even though there are some data losses in the embedded watermark by attacks. It is especially robust to cropping and cutting distortions. However, this information distribution property of EIA watermark may result in a weakening of security. That is, we can fully recover the embedded data by only using the partial data of EIA.

In this paper, to overcome the security problem, we propose a new watermarking scheme using CAT. In our scheme, the EIA for the watermark to be recognized is used as an EIA watermark, which is synthesized from the computational pickup process of InIm. The embedding and extraction processes using EIA watermark are performed in the CAT domain where a single secure key is used. To show the usefulness of the proposed system, some experiments are carried out and the results against attacks are discussed.

Ⅱ. Principle of InIm-based 3D watermarking scheme

The concept of InIm-based 3D digital watermarking scheme is shown in Fig. 1 [13]. It has four steps: generation of the EIA watermark, embedding the EIA watermark, extraction of the EIA watermark and target watermark reconstruction of the finally extracted EIA watermark image. First, from the computational pickup process of InIm, the EIA for the target watermark to be recognized, which is located at a known position z, is synthesized as an EIA watermark. Second, the EIA watermark is embedded into a cover image using DWT and the watermarked cover image is transmitted to the recipient through a noisy communication channel. At the receiver, the EIA watermark is finally extracted from the received

watermarked cover image and its depth-dependent target watermark image at z can be computationally reconstructed by using the computational integral imaging reconstruction (CIIR) technique [14-16].

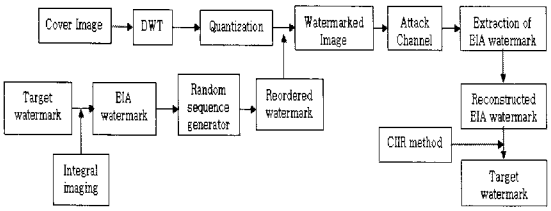


그림 1. 집적영상 기반의 워터마킹 방법의 순서도
Fig. 1 Flowchart of the InIm-based watermarking scheme.

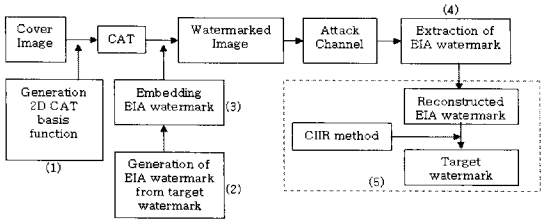


그림2. 제안한 방법의 순서도
Fig. 2 Flowchart of the proposed scheme.

Ⅲ. Proposed method

Generally, a DFT or DCT transform provides only one spectrum plane for embedding hidden data, so that the embedded information can be removed easily. To increase the flexibility in data hiding, we propose a secure 3D watermarking scheme using CAT. Figure 2 shows a flowchart of the proposed scheme, which consists of five steps: (1) generation of 2D CAT basis function, (2) generation of EIA watermark from target watermark, (3) embedding of EIA watermark, (4) extraction of EIA watermark, (5) target watermark reconstruction of EIA watermark.

3.1 CAT and 2D CAT Basis function

The CA system is a dynamical system, in which space and time are discrete [9-11]. The cell, which is structured in form of a regular lattice structure, has a finite number of states. These states are updated synchronously according to a specified local rule of interaction. The neighborhood of a cell is chosen as the cell itself and some of the adjacent cells. By using a specified rule of neighborhood, the states are updated synchronously in discrete time steps for all cells.

In general, CA is described as a k-state, r-site neighborhood CA. In the k-state CA, each cell can take any of the integer values between 0 and (k-1). The state of each cell for k-state, r-site neighborhood CA is represented by the Boolean variable a. The quantity a(i,t) means the state of the i-th at discrete time t, whose two neighbors are in states a(i-1,t) and a(i+1,t). At the next t+1 time step, the state a(i,t+1) is calculated synchronously form the states of the cells in the neighborhood. The possible CA evolutions can be given as

$$a(i,t+1)=F[a(i-m,t),\cdots,a(i,t),\cdots,a(i+m,t)] \quad (1)$$

where F[·] is a Boolean function defining the rule and m=(r-1)/2 .

To understand the basic concept of CA, we describe a 1D 2-state, 3-site CA. In this case, there are 8 possible configurations for each neighborhood in a 2-state 3-site neighborhood automaton. The relation between the configuration of CA and the Boolean value C_n is shown in Table 1. Then, we can obtain 2^8=256 rules for the 2-state, 3-site CA. That is, the number of rules can be calculated by

$$R=\sum_{n=0}^{7} C_n 2^n \quad (2)$$

If there are N cells in the entire 1-D CA space, there is total of k^N possible initial states for the evolution of the CA. Furthermore, if the CA is run over T discrete time steps, the number of rules that we can evolve from a 1D, k-state, r-site, N-cell CA is in the order of $k^{k^r}+k^N+k^{2T}$.

표1 CA 구조와 Boolean 값의 관계
Table 1. Relationship between Configuration of CA and Boolean value

CONFIGURATION	BOOLEAN VALUE, C
111	C_0
110	C_1
101	C_2
100	C_3
011	C_4
010	C_5
001	C_6
000	C_7

Now, for the use of CAT, consider a 1D space consisting of N cells. We generate the basis functions $A=A_{ik}$(i,k=0,1, ···, N-1) for domain transform. Here, we can see that there is a very large number of ways by which A_{ik}(can be expressed as a function of a state of CA. Then the data sequence f_i can be represented using the transform bases. This is given by

$$f_i = \sum_{k=0}^{N-1} c_k A_{ik} \quad i = 0,1,2,\cdots N-1 \tag{3}$$

where ck are the transform coefficients. The basis functions are related to the evolving field of the CA. Equation (3) represents a mapping of the process f (in the physical domain) to c (in the CA domain) using the building blocks A as transfer functions.

In case of a 2D square space consisting of $N \times N$ cells, the transform base is $A=A_{ijkl}$ (i,j,k,l=0,1,···, N-1). For generating 2D CA transform bases, our approach is as follows.

Step 1: We obtain gateway values as shown in Fig. 3. In general, gateway values consist of the wolfram rule number, number of cells in lattice, number of cells per neighborhood, and descriptions of the initial configuration and boundary configuration. This gateway values are considered as a secure CAT key in our watermark scheme using CAT.

Step 2: The cyclic boundary conditions imposed on the end sites are of the form of the Eq. (4):

$$a_{-1,k} = a_{N-1,k} \qquad a_{N,k} = a_{0k} \tag{4}$$

Step 3: Then a 1D CA basis function is generated as described by Eq. (5):

$$A_{ik} = 2a_{ik}a_{ki} - 1 \tag{5}$$

where a_{ik} is the state of the CA at node i and time $t=k$.

Step 4: The CA basis function is derived from the 1D CA basis function as in the following Eq. (6):

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

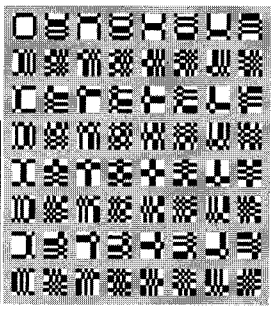
Step 5: 2D basis functions are derived from the evolving 1D Automata as in the Eq. (7):

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

where L_W>1 is the number of states of the automaton.

Wolfram Rule Number	158
Number of Cells per Neighborhood	3
Number of Cells in Lattice	8
Initial Configuration	01100101
Boundary Configuration	Cyclic
Basis Function Type	2

(a)



(b)

그림 3. (a) 게이트웨이 값 (b) 2D A_{ijkl} 기저함수
Fig. 3 (a) Gateway values (b) 2D A_{ijkl} basis functions.

Figure 3 shows an example for the generation of a 2D basis function. The gateway values (CAT key) are presented in Fig. 3(a) and the generated basis functions are shown in Fig. 3(b). Here, A_{00kl} is the block at the top left corner. The top row represents $0 \le j < 8$; i=0. The left column is j=0; $0 \le i < 8$. A_{ij00} is the upper left corner of each block. The white rectangular dots represent "1" while the black dots are "-1".

3.2 Generation of EIA watermark

In the previous InIm-based 3D watermarking scheme, the EIA is employed as an EIA watermark. It can be generated from the computational pickup process of InIm. Figure 4(a) shows a process of EIA generation through a k-th pinhole for a 3D object. The EIA is easily calculated in the pickup plane by using a computational pickup scheme based on ray optics [14]. The EIA is synthesized as described in the following. First, we consider 3D objects located at z. If z>0, then the intensity distribution of a sectioned image is mapped inversely through corresponding pinholes onto the pickup plane and if z<0, the intensity distribution is mapped directly onto the pickup plane.

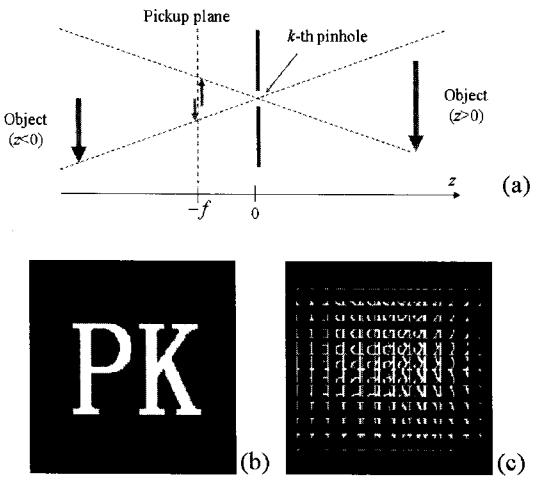


그림 4. (a) k번째 핀홀에 의한 EIA 생성 원리
(b) 원 워터마크 (c) 생성된 EIA 워터마크
Fig. 4 (a) The principle of EIA generation for k-th pinhole. (b) Original watermark
(c) Generated EIA watermark

For InIm-based watermarking, the target watermark to be recognized is used as 3D object. The target watermark, Fig. 4(b) shows the example of a 2D character pattern of 'PK', is located at the pickup plane z and rays coming from the target watermark are mapped inversely through the pinhole on the pickup plane and they are recorded as EIA. The entire EIA can be obtained by repeating the process through all pinholes in the same way. The computationally generated EIA is shown in Fig. 4(c). It is used as EIA watermark in the InIm-based watermarking system.

3.3 Embedding of EIA watermark

Figure 5 shows the embedding procedure of the EIA watermark into 2D CAT coefficients. To obtain CAT coefficients, we assume that we are using an orthogonal 2-state, 2D CA basis function A_{ijkl} as shown in Fig. 3(b). First, after an input cover image is transformed into the CA domain by using the 2D basis function Aijkl, the CAT coefficients of c_{kl} are decomposed using Eq. (3).

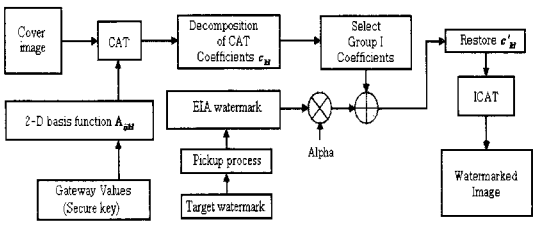


그림 5. 워터마크 삽입과정 블록도
Fig. 5 Block diagram of a watermark embedding procedure

The transform coefficients c_{kl} can be divided into four groups as shown in Fig. 6. Those CA bases at even k and l locations represent the low-low frequency CA bases and belong to the so-called 'Group I' bases. The 'Group II' bases are those at even k and odd l locations, which represent the low-high frequency CA bases and which are used to generate the low-high frequency CAT coefficients. Similarly, the 'Group III' bases are those at odd k and even l locations, which represent the high-low frequency CA bases and are used to generate the high-low frequency

CAT coefficients. Finally, the high-high frequency CA bases are denoted as 'Group IV' and are used to generate the high-high frequency CAT coefficients. In our watermarking scheme, we chose 'Group I' coefficients. For the embedding process, the EIA data is embedded into the 'Group I' coefficients of the input cover image by using the following Eq. (8):

$$C'_{GroupI}(k,l) = C_{GroupI}(k,l) + alpha \cdot W_{EIA}(k,l) \quad (8)$$

where k,l =1,..., $N/2$, alpha is a scaling parameter, $C_{GroupI}(k,l)$ is the CAT coefficient of 'Group I' and $C'_{GroupI}(k,l)$ is the EIA watermark embedded coefficient after using the 'Group I' CAT coefficient. For obtaining the watermarked cover image, we finally use the inverse CAT.

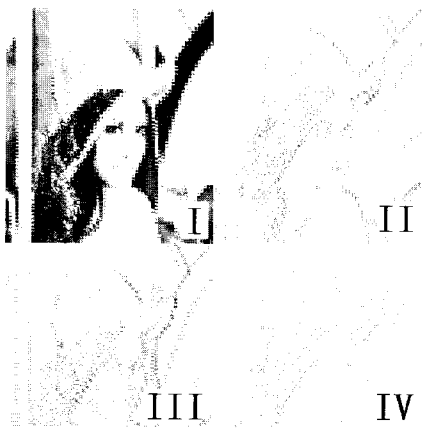


그림 6. 4개 대역으로 분해된 CAT계수
Fig. 6 Decomposition of CAT coefficients into four bands

3.4 Extraction of EIA watermark

The EIA watermark is detected by using the CAT basis function A_{ijkl} and the scaling parameter α after the decomposition of the CAT coefficients of the watermarked cover image and the original cover image. The detailed procedure of the EIA watermark extraction is shown in Fig. 7. First, the A_{ijkl} are used to transform the watermarked image and original image into the CA domain. Second, we can obtain the coefficients $C''_{GroupI}(k,l)$ using the algorithm in the embedding method from the watermarked image. Finally, we use the following Eq. (9) to get the extracted EIA watermark:

$$W'_{EIA}(k,l) = [C_{GroupI}(k,l) - C''_{GroupI}(k,l)] / alpha \quad (9)$$

where W'_{EIA} is the extracted EIA watermark.

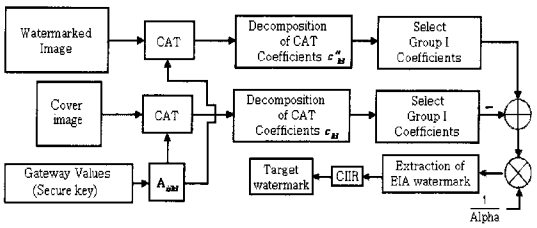


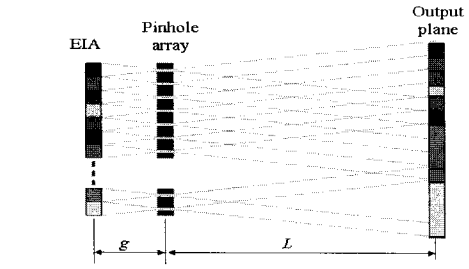
그림 7. 워터마크의 추출과정 블록도
Fig. 7 Block diagram of a watermark extraction procedure

3.5 Reconstruction of target watermark

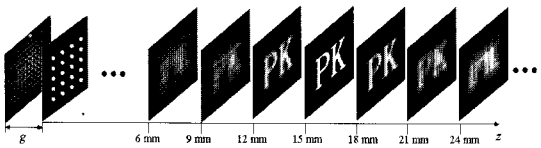
In the InIm technique, the EIA can be reconstructed as a 3D plane image using a computational reconstruction method. This method is called computational integral imaging reconstruction (CIIR). Figure 8(a) illustrates the CIIR technique based on a pinhole array model [14]. At the fixed distance L, each elemental image obtained by the pickup process is projected inversely through each virtual pinhole. Each projected image is simply magnified by the ratio of the distance between the virtual pinhole array and the reconstruction image plane (L) to the distance between the pinhole array and the elemental image plane (g). Furthermore, the through each virtual pinhole inversely mapped images are overlapped and summated at each pixel. To display the 3D information of an object, this process is repeated for many different distances.

In our InIm-based watermarking scheme, the extracted EIA watermark data is identical with the EIA of InIm. In order to obtain the embedded target watermark image from the extracted EIA watermark data, a CIIR process is used. When using a CIIR technique, many depth-dependent 3D plane images can be reconstructed along the output plane

from the EIA watermark data as shown in Fig. 8(b). Particularly, the images reconstructed on the output planes, where the target watermark images were originally located, are clearly focused, while moving away from these planes, the reconstructed images appear to be blurred. This characteristic of CIIR reconstructs the depth-dependent target watermark images.



(a)



(b)

그림 8. (a) CIIR 기술의 개념도
(b) 워터마크를 깊이에 따라 재생한 평면 영상
Fig. 8 (a) Conceptual diagram of the CIIR technique
(b) Depth-dependently reconstructed plane image of target watermark

3.6 Estimation Parameters

To objectively evaluate the performance of our watermarking scheme, we measure the similarity between the original watermark and reconstructed watermark using the following Eq. (10):

$$SIM = \sum_{p=1}^{P}\sum_{q=1}^{Q} W_{pq} \cdot W'_{pq} \Big/ \sum_{p=1}^{P}\sum_{q=1}^{Q} W_{pq} \cdot W_{pq} \qquad (10)$$

where W is the original watermark having a total of $P \times Q$ pixels and W' is the extracted watermark.

The peak signal-to-noise ratio (PSNR) is used to evaluate the quality of the watermarked image. The PSNR and MSE are defined as follows:

$$PSNR = 10\log\left(\frac{255^2}{MSE}\right), \quad MSE = \frac{1}{XY}\sum_{x=1}^{X}\sum_{y=1}^{Y}(O_{xy} - O'_{xy})^2 \qquad (11)$$

where O represents the original image and O' represents the watermarked image.

Ⅳ. Experiments and results

4.1 Embedding and extraction of the EIA watermark

The performance of the proposed watermarking scheme was tested on various types of images. The cover image was the gray scale 8-bit 'Lena' image of size 512×512 pixels as shown in Fig. 9(a). The target watermark image shown in Fig. 4(b) had 256×256 pixels and was used to generate the EIA watermark. The target watermark was located at L=15mm from the origin of the pinhole array as shown in Fig. 4(a) and the pinhole array consisted of 32×32 pinholes. The distance g between the pickup plane and the pinhole array and the pitch of the pinhole array was set to be 3 mm and 1.08 mm, respectively. Then, the EIA watermark of the 'PK' target watermark was computationally synthesized through the computational pickup system, in which each elemental image consisted of 16×16 pixels. Using the 2D CAT filter, which is shown in Fig. 3, the EIA watermark was finally generated as shown in Fig. 9(b). We decomposed the CAT coefficients c_{kl} into four bands and used the "Group I" band for embedding the watermark, for which the scaling parameter α was 0.05.

The EIA watermark was embedded into the cover image through the embedding process shown in Fig. 5. The watermarked 'Lena' image is shown in Fig. 10(a) and has a PSNR value of 54.73 dB. From this result, we could not find any perceptual degradation between the original image and the watermarked image. Next, the embedded EIA watermark was extracted from the watermarked 'Lena' image through the extraction process described by Eq. (9) and is shown in Fig 10(b).

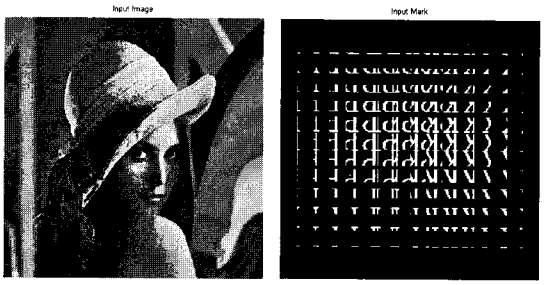


그림 9. (a) 원 영상 (b) EIA 워터마크
Fig. 9 (a) Original Image (b) EIA watermark

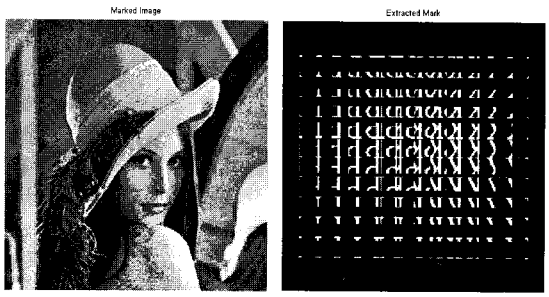


그림 10. (a) 워터마킹된 영상 (PSNR=54.73dB)
(b) 추출된 EIA 워터마크
Fig. 10 (a) Watermarked Image (PSNR=54.73dB)
(b) Extracted EIA watermark

4.2 Experiments and analysis of robustness

Each paper will be charged according to the number of pages. 20 prints will be supplied without additional charge if requested. Additional reprints are available with actual cost.

We carried out experiments in order to analyze the robustness of the proposed watermarking scheme against attacks. We compared our results with those of the conventional method in terms of PSNR and SIM of the extracted watermark patterns as given by Eqs. (10) and (11). To this end, various types of image distortions were tested. Here, four kinds of attacks were considered: Gaussian noise, median filtering, blurring and sharpening on the watermarked cover image. Some examples of attacked images are shown in Fig. 11 and the extracted EIA watermarks are shown in Fig. 12. In Fig. 12, it is visible that there were some noises in the extracted EIA watermark image and that these noises degraded the image quality of the EIA watermark. But as mentioned above, the EIA watermark itself is not the final watermark data in the proposed method. The final data was generated after these EIA watermark underwent the further processing of CIIR. Consequently, the extracted EIA images only are meaningless but they can be made meaningful for the use of copyright identification through the CIIR technique.

그림 11. 4가지 공격후의 워터마킹 된 영상
Fig. 11 Watermarked images of four kinds of attacks

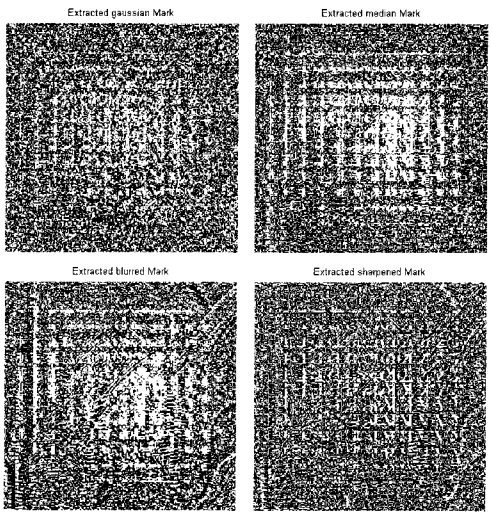


그림 12. 추출된 EIA 워터마크 영상
Fig. 12 Extracted EIA watermark images.

Fig. 13 shows the computationally reconstructed target watermark from the extracted EIA watermark by using CIIR process. These results reveal that target watermarks can be extracted exactly although the watermarked images are severely attacked by several noises. The Similarity between the original target watermark and the reconstructed target watermark was calculated and found to be 0.8662, 0.9459, 0.8387 and 0.8907 for Gaussian noise, median filtering, blurring and sharpening attacks, respectively. In consequence, we can state that the proposed scheme is robust against image processing attacks.

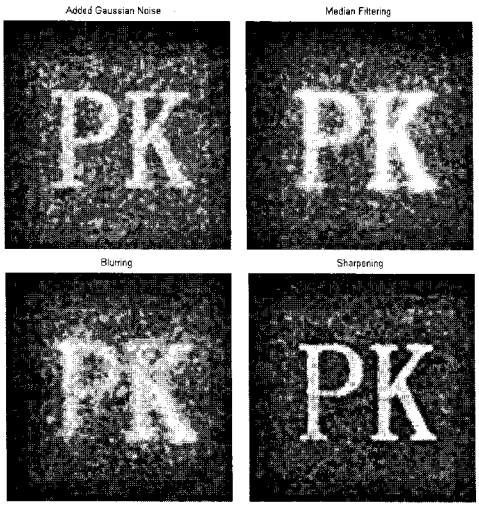


그림 13. CIIR 기술을 이용하여 4가지 공격 후 추출된 EIA 워터마크를 재생한 결과
Fig. 13 Reconstructed target watermarks from the extracted EIA watermarks by using the CIIR technique for four cases of attacks.

Next, we performed some experiments for image compression. Digital images are usually stored and transmitted after image compression. Among others, JPEG is a popular image compression technique for still images. Here, we examined the robustness of the proposed scheme by compressing the watermarked images with different JPEG quality factors. Figure 14 shows some experimental results of the extraction of target watermarks from the extracted EIA watermark by using the CIIR technique for different JPEG compression quality factors. The SIM was calculated for different compression factors as shown in Fig. 15. The results show that the proposed scheme is robust against JPEG image compression.

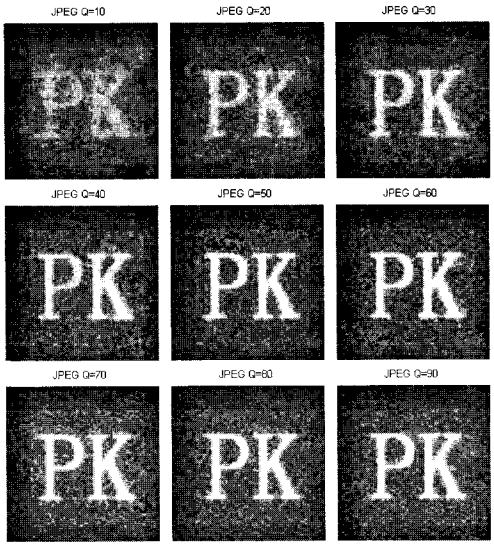


그림 14. CIIR 기술을 이용하여 서로 다른 JPEG율로 압축을 한 후에 추출한 EIA 워터마크를 재생한 결과
Fig. 14 Reconstructed target watermark images from the extracted EIA watermark by using the CIIR technique for different JPEG compression factors.

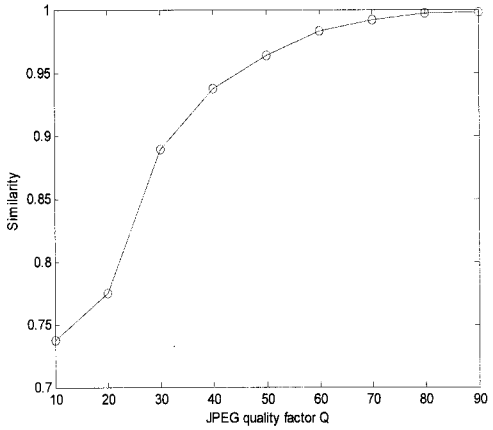


그림 15. 서로 다른 JPEG 압축율에서 측정한 SIM
Fig. 15 SIM for different JPEG compression factors

In addition, we repeated our experiments for five different cover images, which are shown in the top row of Table 2. Below in Table 2, the SIM results for these cover images are presented. According to the above-mentioned experimental results, we can see that the proposed InIm-based 3D watermarking scheme can be an effective digital watermarking in terms of robustness.

표 2. 유사도
Table 2. Similarity

	Lena	Baboon	Peppers	Boats	Tiger
Test Image					
Attacks	Similarity				
Gaussian	0.866	0.858	0.864	0.865	0.945
Median	0.946	0.830	0.955	0.938	0.819
Blurring	0.839	0.745	0.872	0.824	0.783
Sharpening	0.891	0.818	0.916	0.894	0.782
JPEG Q=10	0.737	0.734	0.772	0.789	0.785

4.3 Experiments and analysis of security

InIm-based 3D watermarking schemes requires the use of EIA watermark, which itself can be regarded as meaningless data. Nevertheless, this provides the possibility to reach an effective level of robustness, i.e. we can easily reconstruct the target watermark using CIIR process even though there are partial data of EIA watermarks, which can be obtained when the secure CAT key is partially known. This useful feature of the EIA watermark may decrease the security of the previous InIm-based 3D watermarking scheme. However, the proposed 3D watermarking scheme using CAT shows characteristics of higher security.

To analyze the secure characteristics, we assumed that the secure CAT key was partially known. This analysis method is called a partial-key attack. First, we will describe the partial-key attack for previous InIm-based 3D watermarking scheme. Figure 16(a) shows the EIA watermark for a certain partial loss attack, in which the boundary key information was known. The target watermark image was reconstructed from the partial EIA watermark using the CIIR technique and is shown in Fig. 16(b). It can be seen that we can easily and exactly reconstruct the target watermark using the CIIR process from the partial data of EIA watermarks. According to the known degree of the secure EIA watermark, the PSNR for reconstructed target watermark was calculated. These results are shown in Fig. 16(c) and a main result is that the PSNR increases and the security decreases as the known degree of the secure EIA watermark increases.

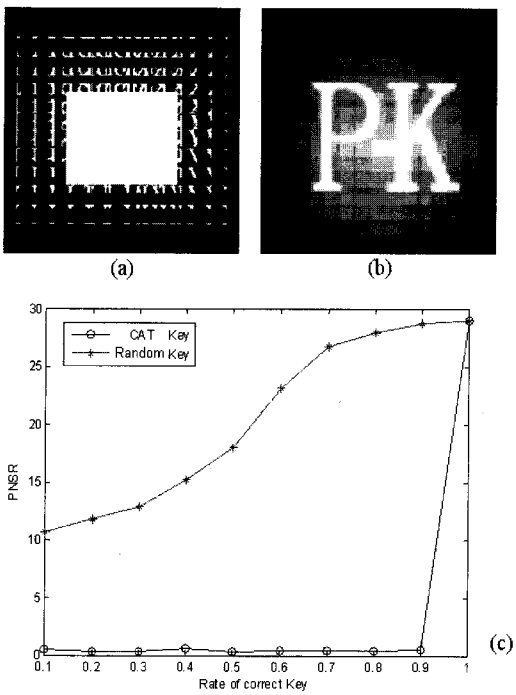


그림 16. (a) 공격에 부분적으로 손실된 EIA워터마크 영상.
(b) EIA 워터마크로부터 재생한 원 워터마크
(c) 워터마크의 손실에 따른 PSNR 결과 값
Fig. 16 (a) EIA watermark from the partial loss attack (b) Reconstructed target watermark from EIA watermark (c) PSNR results according to the known degree of EIA watermark

Additionally, we repeated the experiments with our 3D watermarking scheme using CAT and compared the result with previous ones. These results are also shown in Fig. 16(c) and show that we can only obtain a high PSNR of the target watermark when the known degree is 1. This is due to the fact that different CAT keys will results in totally different basis functions and transform coefficients, i.e. the proposed method is very sensitive to the CAT key and a small change of the key may generate a completely different results. From the results of Fig. 16(c), one can conclude that our scheme can dramatically improve the security of watermarking.

V. Conclusions

In this work, we have proposed a watermarking scheme using CAT to improve security in InIm-based 3D watermarking schemes. For this purpose, we first generated a 2D CA basis function and transformed the cover image into the CA domain. Next, the EIA for a target watermark was applied as the EIA watermark for robust attacks and the embedding and extraction process using EIA watermark was performed in the CAT domain. To show the usefulness of the proposed watermarking system, some experiments for both robustness and security were carried out and the results against attacks were discussed. From the experimental results of robustness, we found that the proposed scheme is robust against various noises and JPEG image compression. Additional experiments for security revealed that compared to previous watermarking schemes, our scheme could dramatically improve the security of watermarking. These good experimental results suggest a possibility of implementing a secure and robust 3D digital watermarking system based on integral imaging.

References

[1] N. F. Johnson, Z. Duric, and S. Jajodia, "Information Hiding, Steganography and Watermarking-Attacks and Countermeasures Advances in Information Security," Vol. 1, Kluwer Academic, 2001.

[2] G. C. Langelaar, I. Setyawan and, R. L. Lagendijk, "Watermarking digital image and video data. A state of the art overview", IEEE Signal Proc. Mag. 17, pp. 20-46, 2000.

[3] M. Arnold, M. Schmucker, and S. D. Wolthusen, "Techniques and Applications of Digital Watermarking and Content Protection," Artech House, 2003.

[4] Chuan-Fu Wu and Wen-Shyong Hsieh, "Digital watermarking using zerotree of DCT," IEEE Trans. Consum. Electron. Vol. 46, pp. 87-94, 2000.

[5] M. A. Suhail and M. S. Obaidat, "Digital watermarking based DCT and JPEG model," IEEE Trans. Instrum. Meas. Vol. 52, pp.1640-1647, 2003.

[6] H.-j. Wang, P.-C. Su, and C.-C. J. Kuo, "Wavelet-based digital image watermarking," Opt. Express 3, pp. 491-496, 1998.

[7] S. Kishk and B. Javidi, "Information hiding technique with double phase encoding," Appl. Opt. 41, pp. 5462-5470, 2002.

[8] W. Xiao, Z. Ji, J. Zhang, and W. Wu, "A watermarking algorithm based on chaotic encryption," Proc. IEEE TENCON'02, pp. 545-548, 2002.

[9] R. Shiba, S. Kang, and Y. Aoki, "An image watermarking technique using CAT," TENCON 2004, 2004 IEEE Region 10 Conference 1, pp. 303-306, 2004.

[10] B. Viher, A. Dobnikar, and D. Zazula, "Cellular automata and follicle recognition problem and possibilities of using cellular automata for image recognition purposes," Int. J. Med. Inform. Vol. 49, pp. 231-241, 1998.

[11] C. L. Chang, Y. J. Zhang, and Y. Y. Gdong "CA for Edge detection of Images," IEEE International Conference on Machine Learning and Cybernetics, Shanghai, pp. 3830-3834, 2004.

[12] S. Kishk and B. Javidi, "3D object watermarking by a 3D hidden data," Opt. Express 11, pp. 874-886, 2003.

[13] D.-C. Hwang, D.-H. Shin, and E.-S. Kim, "A novel three-dimensional digital watermarking scheme basing on integral imaging," Opt. Commun. 277, pp. 40 - 49, 2007.

[14] S. Hong, J.-S. Jang and B. Javidi, "Three-dimensional volumetric object reconstruction using computational integral imaging," Opt. Express 12, pp. 483-491, 2004.

[15] D. -H. Shin and H. Yoo, "Image quality enhancement in 3D computational integral imaging by use of interpolation methods," Opt. Express 15, pp. 12039-12049, 2007.

[16] H. Yoo and D. -H. Shin, "Improved analysis on the signal property of computational integral imaging system," Opt. Express 15, pp. 14107-14114, 2007.

저자소개

박영일 (Yongri Piao)

한국해양정보통신학회 논문지
제13권 제8호 참조

김석태 (Seok-Tae Kim)

한국해양정보통신학회 논문지
제13권 제8호 참조