Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2013, Article ID 632043, 8 pages
http://dx.doi.org/10.1155/2013/632043

Research Article

An Extended DCT Domain Watermarking for Robot Vision against Geometric Image Attacks

Okkyung Choi,[1] InBae Jeon,[2] Seung-Wha Yoo,[2] and Seungbin Moon[1]

[1] *Department of Computer Engineering, Sejong University, Seoul 143-747, Republic of Korea*
[2] *Department of Knowledge Information Engineering, Graduate School of Ajou University, Suwon 443-749, Republic of Korea*

Correspondence should be addressed to Seungbin Moon; sbmoon@sejong.ac.kr

Received 26 September 2013; Accepted 23 October 2013

Academic Editor: Jongsung Kim

With the rapid development of the Internet and the mobile service robot, the digital services are becoming important factors for robots to recognize things in the real world. Advances in computer technology and the risk of copyright infringement have increased in the way that anyone replicates and copies digital media easily. Therefore, ways to prevent and suppress copyright infringement, digital watermarking technologies that insert copyrights information into the work, are being researched. Digital watermark, depending on the actual insert domain, can be categorized into the spatial domain and transform domain. In this paper, we propose an extended DCT domain watermarking for robot vision. The suggested method is by distributing and duplicating watermark images that are including copyright information on the original images. By doing this, it can be strong on geometric image attacks such as partial cutting, resizing, rotating, and so forth. For the success of watermark extraction, invertible process can be used to recover a disfigured image. Experimental results are provided to support these methods, through the process of recombination by complete image pieces.

1. Introduction

With the rapid development of robot services on the Internet, the digital services between robots and things using mobile terminals are becoming important issues. Unlike the robotic technologies from the past, robots are holding greater performance in our lives. Digital watermarking is the process of inserting unique identification information to prevent the piracy or unauthorized use of digital information, thus providing protection for owner's unique contents. Given that intellectual property of books, pictures, music, and so forth in digital format is reproduced in large quantities and distributed readily on the Internet, digital watermarking is drawing attention as key technology for copyright protection [1]. Digital watermarking algorithm is made up of two algorithms: one embeds a watermark, which is a piece of uniquely identifying information, into multimedia content; and the other extracts and verifies the embedded watermark in order to confirm copyright information [2].

This digital watermarking technology is classified into spatial domain watermarking and transforms domain watermarking depending on the domain into which the actual information is embedded. In spatial domain watermarking, the original signal is not converted but specific pixel values are embedded as they are in the spatial domain [3]. Specific methods of this type include probabilistic labeling of a patchwork, as proposed by Bender et al. [4] and others. In addition, it includes a scheme proposed by Pitas and Kaskalis [5], "which divides a digital image into two sets of the same size, adds specific values to one of the sets, and then uses the difference in the mean values of pixels for the two sets so as to detect the inserted watermark [3]." However the above spatial domain watermarking schemes have a drawback that they are vulnerable to compression and noise.

In transform domain watermarking, the original signal is converted and a watermark is embedded. The different types of transform used include DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform), and DWT (Discrete Wavelet Transform). Specific methods of this type include "embedding a watermark into a phase using DFT" proposed by Ruanaidch [6] and "partitioning an image to apply

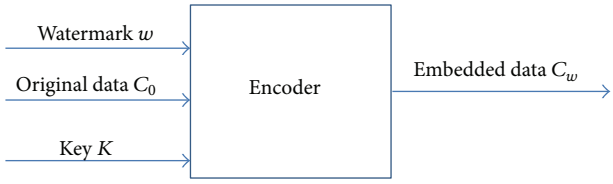


Figure 1: Insertion unit of watermark.

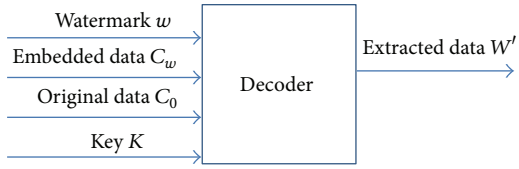


Figure 2: Extraction unit of watermark.

watermarking after DCT" [1] proposed by Koch and Zhao [7]. In addition, Cox et al. [8] proposed "a scheme that uses DCT for the whole image without partitioning the image, selects important frequency coefficients other than DC components from the image, and inserts a desired watermark signal into them [1]." The existing spatial domain watermarking method has vulnerabilities against attacks when processing images, such as noise and compression.

To overcome this shortcoming, in this paper an integrity verification system using a DCT-domain watermarking method is designed and implemented, which can be used to protect copyright of original contents and prevent forgery. Lastly, experimental results show that the process of image reverse conversion and extraction of the watermark image by recombining undamaged image pieces among overlapped watermark pieces can improve the extraction rate efficiently.

The rest of the paper is organized as follows. Several related works are compared and reviewed in the next section. Then, proposed methods for watermark insertion and extraction are proposed in Section 3. In Section 4, the experimental results and analysis are given and conclusion provided in the final section, along with plans for further studies.

2. Related Work

2.1. Composition of a Digital Watermark. A digital watermarking scheme is largely composed of the insertion part and the extraction part.

As shown in Figure 1, the typical watermark insertion part processes the original data C_0, using w, watermark information the owner tries to insert, and K, the owner's own proper key, and creates and distributes watermark-embedded C_w [3].

As shown in Figure 2, the typical watermark extraction part extracts W', watermark information included in distributed C'_w, using w, watermark information inserted by the owner, C_0, the original information, and K, the owner's own proper key [3].

2.2. DCT. DCT is a frequency linear transformation domain approach, which is characterized as more robust against attacks compared to the spatial (time) domain approach [9]. DCT is a method in which conversion is done to frequency information in units of blocks by focusing widespread energy into several coefficients, as a result of which energy can be maximized in concentration [10].

DCT was introduced in a paper on a new type of orthogonal transformation called discrete cosine transform in 1974 by a team of three researchers at University of Texas, one of whom was Professor Rao. With DCT, contrary to how DFT calculates even complex numbers, only the real part is dealt with, so signal processing can be done effectively in the area of image processing, without having to deal with the imaginary part [11].

First, in the forward DCT stage, the image in the spatial domain is transformed into a frequency domain in the units of 8×8 blocks, in order to obtain low frequency DC components and high frequency AC components. In the inverse DCT stage, the frequency components are converted into an image in the spatial domain [12].

2.3. Comparative Analysis of Previous Research. The method by Saeed [9], which is a DCT-domain watermarking method, supports the following methods: Method 1A, Method 1B, and Method 1C. In Method 1A, a single watermark image is embedded and extracted. In Method 1B, two watermark images are embedded redundantly, which are extracted. Then a new single watermark image is created by averaging the two watermark image information. Method 1C is basically the same as Method 1B except that three redundant watermark images are embedded. For Method 1B, it is strong against geometrical attacks such as size adjustment and rotation as the average of the redundant watermarks is used. For Method 1A, it is strong against noise attacks. For Method 1C, although the average is calculated as with Method 1B, it is relatively small because of the high number of redundancies.

Table 1 shows the analytic results of comparing the existing schemes of Saeed's [9] Method 1A and Method 1B and the scheme proposed in this paper in terms of five requirements of watermark, the number of inserted watermarks, reverse conversion, and the speed of watermark insertion and extraction.

3. Proposed Method

The proposed scheme falls under robust watermarking. The embedded watermark should be extractable in its intact or slightest damaged condition even against malicious outside attack as well as general signal processing.

As for the spatial domain-based watermarking, it has the advantage that the watermark can be inserted and extracted with a small amount of computations, leaving no damage to the quality of an image. However, information added to a specific bit is very sensitive to image processing such as general signal processing, compression, image editing, linear/nonlinear filtering [3]. As methods for overcoming such a limitation of the spatial domain-based watermarking,

Table 1: Comparison with previous studies.

Content	Method 1A [9]	Method 1B [9]	Proposed method
Perceptual invisibility	O	O	O
Robustness	Normal	Normal	High
Clarity	High	High	High
Security	High	High	High
Extraction without original copy	O	O	O
Number of inserted watermark	1	2	16
Inverse transform	X	X	O
Speed	Fast	Fast	Slow

transform domain-based techniques have been proposed, which transform the spatial domain signal of digital watermark into the frequency domain signal and insert the watermark into a visually less sensitive area among the frequency domains [3].

3.1. Proposed Method. This study intends to restore the modified image to one close to the original through the process of image reverse conversion and then extract the watermark image by recombining undamaged image pieces among overlapped watermark pieces, whereby enhancing the robustness of watermark.

3.1.1. Watermark Insertion. The proposed watermark insertion process is explained in Figures 3 and 4.

(1) With the watermark text, a random number is generated using a watermark seed, and a watermark image is produced in the form of bits. This watermark image is separately stored as it is used during watermark extraction.

(2) The watermark image applied a 4×4 DCT. The JPEG image compression standard will be used when the DCT is applied; to reduce the data size, a quantization process is went through, and to rearrange from 1-dimensional to 2-dimensional, zigzag scan is applied.

(3) The original image applied 8×8 DCT. As with the watermark image, the original image also goes through the process of quantization and zigzag scan.

(4) A watermark image is embedded into the original image which has been transformed by DCT. A random number is generated using an embedding seed and the watermark image is embedded redundantly and dispersively. The insertion part is explained in detail in Figure 4.

(5) The watermark insertion image is obtained through IDCT.

As shown in Figure 4, watermark image pieces are embedded in the original image pieces redundantly and dispersively. Up to 16 pieces can be redundantly embedded in the shape of a diamond in order to increase the watermark extraction rate, avoiding the frequency domain where there is a concentration of image information and each of the edges which is more likely to suffer damage from a partial cutting attack.

3.1.2. Watermark Extraction. The proposed watermark extraction process is described in Figures 5 and 6.

(1) 8×8 DCT is applied to the watermark insertion image.

(2) From the frequency domain which has been transformed by DCT, frequency information is extracted from the location where the watermark image has been embedded with an embedding seed. The extraction part is explained in detail in Figure 8.

(3) The extracted frequency information is subjected to zigzag scanning, quantization, and IDCT.

(4) Using a watermark seed, the frequency information is rearranged and then a watermark image is generated.

(5) The generated watermark image and the stored watermark image are compared in terms of the PSNR value to assess their similarity. For the PSNR value, 9 db is used as the reference.

(6) If true, the text is extracted from the watermark image.

(7) If false, the watermark insertion image is restored via inverse transform by referring to the geometrical transform list, and the process is repeated from step (1).

In conclusion, watermark image pieces which were redundantly embedded are compared with matching pieces of the stored watermark image, and undamaged pieces are rearranged to increase the extraction success rate.

3.2. System Implementation. JAVA AWT was used to implement the GUI, while DCT-watermark [13], which is an open-source library from Google Code, was used for DCT, watermark generation, insertion, and extraction. Also, for inverse transform of the watermark insertion image, JAI (Java Advanced Imaging) [14], a Java imaging processing library, was used. The implementation environment is shown in Table 2.

As shown in Figure 7, the original image is partitioned into 8×8 and the spatial domain is transformed to a frequency domain based on DCT.

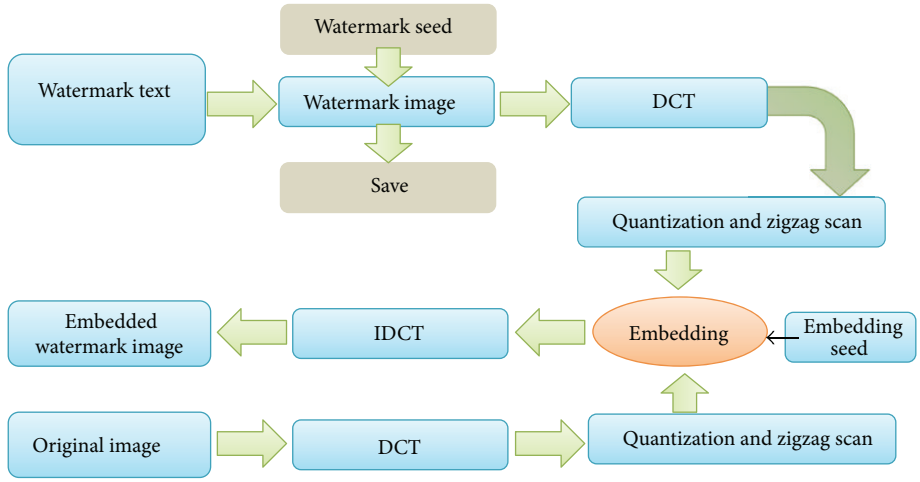


Figure 3: Insertion process of watermark.

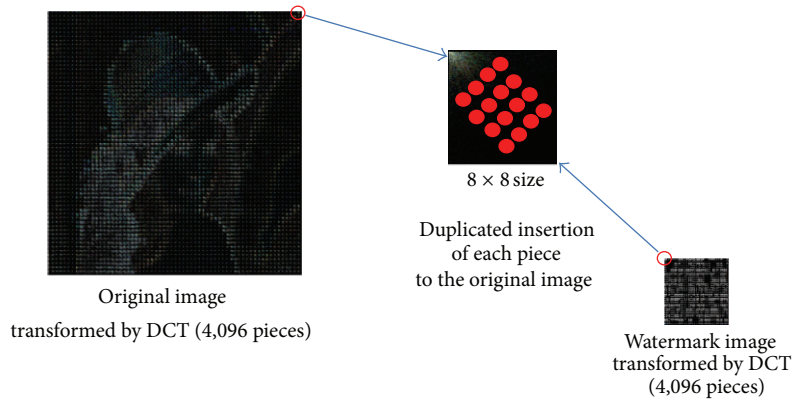


Figure 4: Detailed insertion process of watermark.

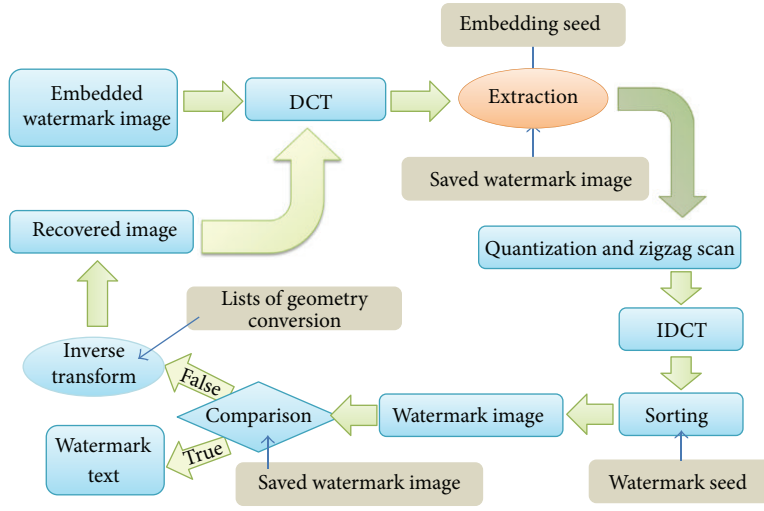


Figure 5: Extraction process of watermark.

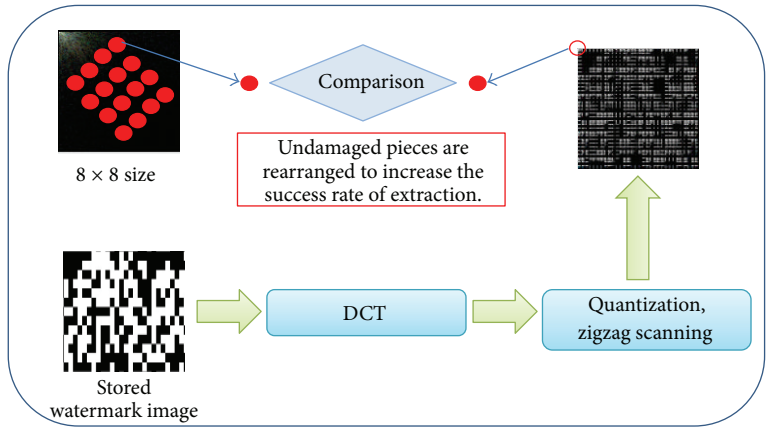
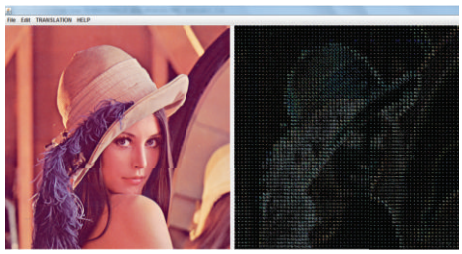


Figure 6: Detailed extraction process of watermark.



(a) (b)

Figure 7: Screen for original image (a) and 8 × 8 DCT image (b).

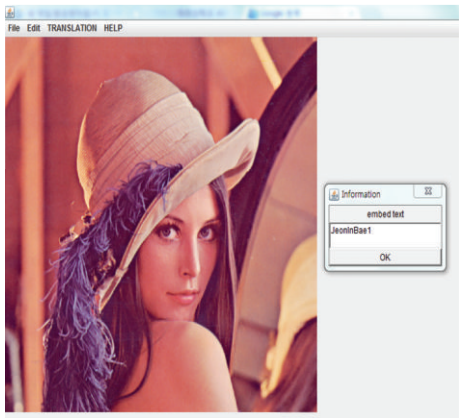
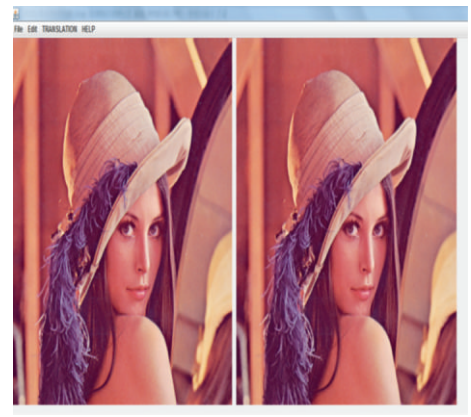


Figure 8: Screen for insertion of watermark text.

Table 2: Implementation environment.

Platform	Intel(R) Core(TM) 2 Duo CPU 2.53 GHz/2 GB RAM
OS	Microsoft Windows 7 (32 bit)
Language	JAVA (SDK 1.7)

3.2.1. Watermark Insertion. When the original image is loaded and the watermark text is inserted, the embedded watermark image is generated as shown in Figure 9.



(a) (b)

Figure 9: Screen for original copy image (a) and embedded watermark image (b).

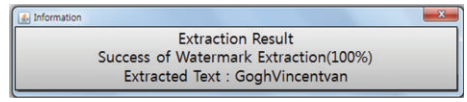


Figure 10: Screen for extraction result of watermark.

3.2.2. Watermark Extraction. When watermark extraction is successfully extracted from the embedded watermark image, the extracted text can be checked, as shown in Figure 10.

4. Experiments

Saeed's Method 1A, Method 1B, and the proposed method were compared and analyzed. The experimental units to be assessed in the test are shown in Table 3.

4.1. Experimental Method. A watermark is embedded in the original image, and partial cutting, size change, quality change, compression, rotation, and noise are applied to the

Table 3: Experimental units.

Extraction rate	(no. of successfully extracted texts/total no. of texts inserted) ∗ 100
PSNR	Shows the difference in image or voice using a numerical value.
Insertion speed	The time taken to embed a watermark.
Extraction speed	The time taken to extract a watermark.

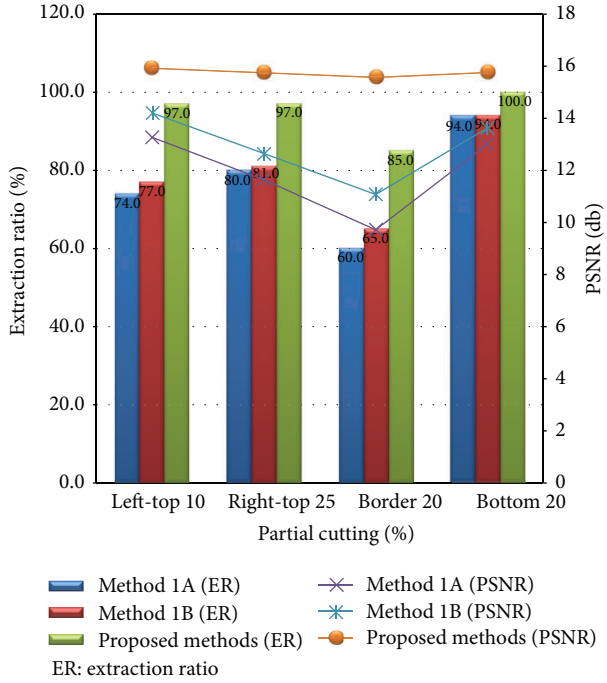


Figure 11: Extraction ratio and PSNR of partial cutting.

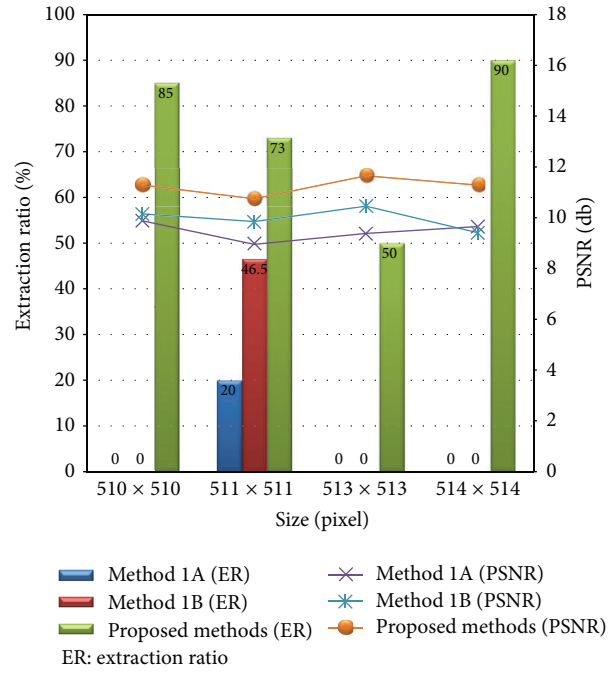


Figure 12: Extraction ratio and PSNR in each size.

embedded watermark image, after which watermark extraction is attempted. If the watermark extraction fails, inverse transform is done according to the geometrical transform list, and watermark extraction is attempted again. Experimental results show that proposed algorithm can be robust against many different types of geometric image attacks such as partial cutting, resizing, rotating, and so forth.

4.2. Experimental Results

4.2.1. Partial Cutting. Partial cutting was applied to parts that are different from one another in the embedded watermark image and then watermark extraction was attempted. The results of partial cutting attacks are shown in Figure 11 for all the three watermarking schemes and it can be seen that, on average, extraction rate and PSNR are high for the proposed method, Method 1A, and Method 1B, in that order.

4.2.2. Size. Watermark extraction was attempted on two embedded watermark images which were reduced in size, and two embedded watermark images which were increased in size. Figure 12 shows that, on average, extraction rate and PSNR are high for the proposed method, Method 1B, and Method 1A, in that order. For the proposed method, the watermark was extracted after an image inverse transform.

4.2.3. Quality. Watermark extraction was attempted on the four embedded watermark images which were obtained by lowering the image quality from 100% in steps of 2%. Figure 13 shows that, on average, extraction rate and PSNR are high for the proposed method, Method 1B, and Method 1A, in that order.

4.2.4. Compression Format. An embedded watermark image was changed to four images of different compression formats and watermark extraction was attempted. Figure 14 shows that, on average, extraction rate and PSNR are high for the proposed method, Method 1B, and Method 1A, in that order. For the GIF format for the proposed method, image inverse transform was done before extracting the watermark.

4.2.5. Rotation. The embedded watermark image was rotated and watermark extraction was attempted on it. Figure 15 shows that, for extraction rate, for Method 1A and Method 1B it is 0%, and for the proposed method, it is 100% after image inverse transform. For PSNR, it was the highest for the

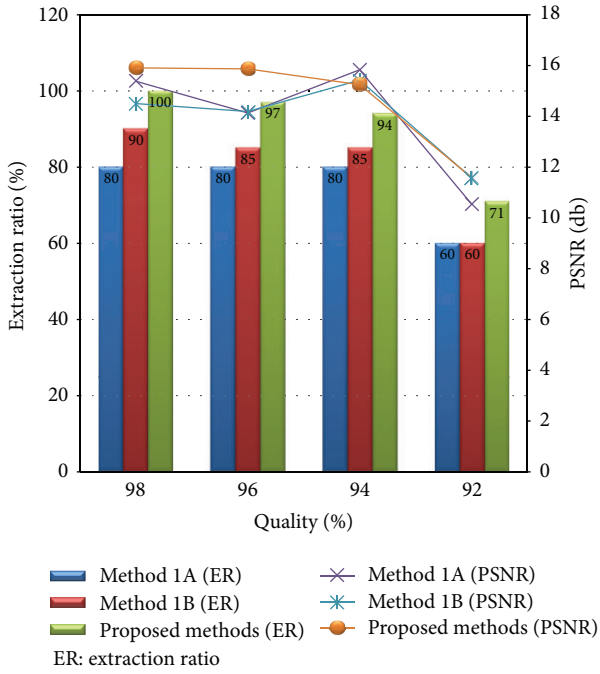


Figure 13: Extraction ratio and PSNR in each quality.

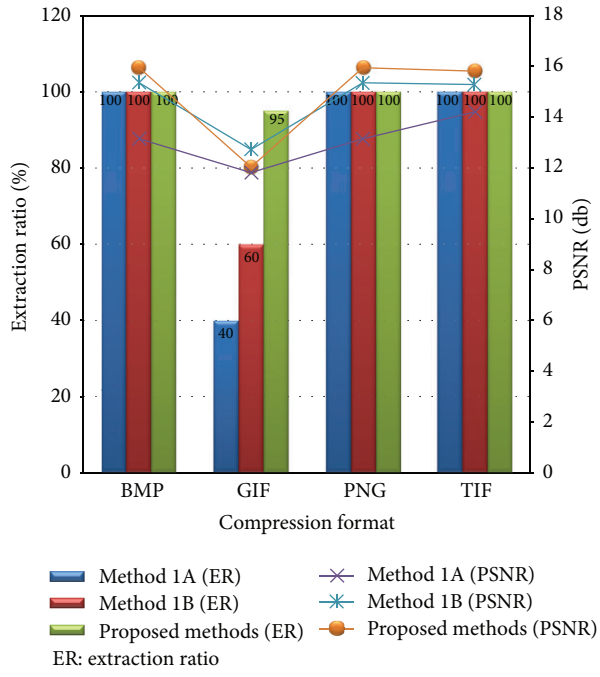


Figure 14: Extraction ratio and PSNR in compression format.

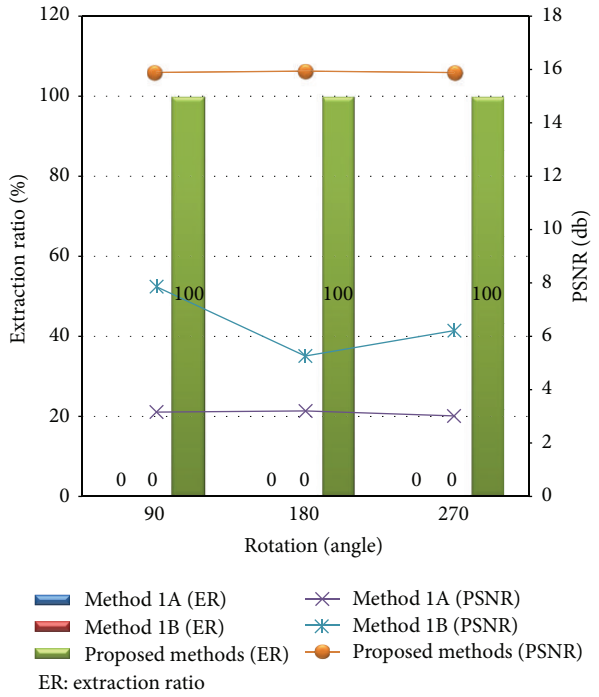


Figure 15: Extraction ratio and PSNR in each rotation.

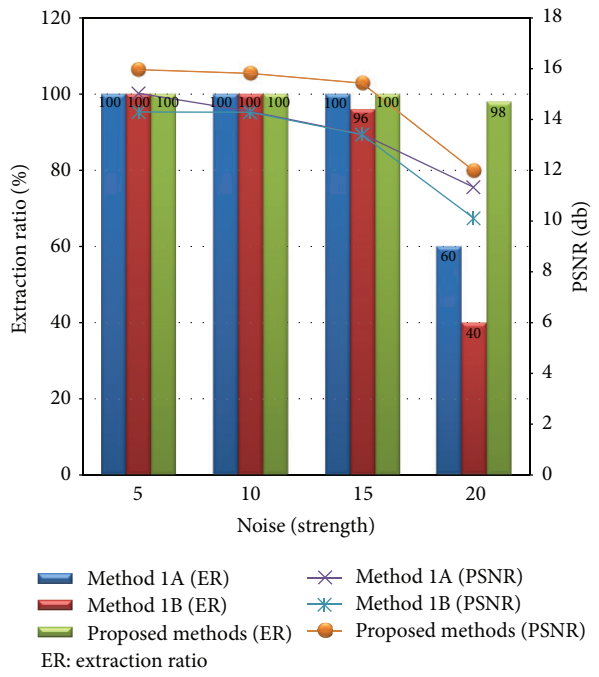


Figure 16: Extraction ratio and PSNR in each noise.

proposed method, followed by Method 1B and then Method 1A.

4.2.6. Noise. Watermark extraction was attempted on four embedded watermark images which had different degrees of noise applied. Figure 16 shows that, on average, extraction and PSNR are high for the proposed method, Method 1A, and Method 1B, in that order.

5. Conclusion

With the rapid development of the medium as image and video, digital watermarking is to use the digital embedding

method to protect information [15], and copyright authentication based on watermarking becomes more and more urgent with wide spread of multimedia content over the Internet [15].

This study suggested an image integrity verification system utilizing DCT domain watermark, which is one of the transform domain based methods. The suggested method is strong against partial cutting, filtering and noise by diffusing and overlapping the watermark image, which includes copyright information, onto the original image. By reassembling those undamaged and fully intact image pieces during extraction, watermark extraction rate can be increased even further.

After a watermark is extracted, its similarity to the watermark image being stored is compared. If the similarity is lower than some threshold, then the extracted image is deemed to be damaged and it is inverse transformed from the extractor to restore it; then, the watermark extraction process is done again. Watermark extraction rate could be increased over that in existing studies via redundant embedding of watermarks, reassembly of intact watermark image pieces, and image inverse transform process.

But as a stage-by-stage computational process is involved, there is the shortcoming that the proposed method has longer computational time than existing methods. Thus, some better features for reducing computational process will be considered to reduce the computational time in future work.

Acknowledgment

This research was supported by Technology Innovation Program of the Knowledge Economy (no. 10041834) funded by the Ministry of Knowledge Economy (MKE, Korea).

References

[1] J. Jo, H. Kang, H. Kim, and S. Kim, *Multimedia Signal Processing: Fundamentals and Practice*, Sayitek Media, Seoul, Republic of Korea, 2nd edition, 2011.

[2] S.-W. Han, *DCT based watermarking using block indexing [M.S. thesis]*, Department of Computer Science, Pukyong National University, 2005.

[3] D. Lee, *DCT Zerotree-based digital watermarking using modification of threshold and embedding level [M.S. thesis]*, Inhwa University, 2005.

[4] W. R. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," in *Storage and Retrieval for Image and Video Databases III*, vol. 2420 of *Proceeding of the SPIE*, pp. 164–173, February 1995.

[5] I. Pitas and T. H. Kaskalis, "Applying signatures on digital images," in *Proceedings of the IEEE Workshop on Nonlinear Signal and Image Processing*, pp. 460–463, Neos Marmaras, Greece, June 1995.

[6] J. J. K. O. Ruanaidch, W. J. Dowling, and F. M. Boland, "Watermarking digital images for copyright protection," *IEE Proceedings—Vision, Image and Signal Processing*, vol. 143, no. 4, pp. 250–256, 1996.

[7] E. Koch and J. Zhao, "Towards robust and hidden image copyright labeling," in *Proceedings of the IEEE Workshop on Nonlinear Signal and Image Processing*, pp. 452–455, Halkidiki, Greece, June 1995.

[8] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[9] S. Al-Mansoori and A. Kunhu, "Robust watermarking technique based on DCT to protect the ownership of DubaiSat-1 images against attacks," *International Journal of Computer Science and Network Security*, vol. 12, no. 6, pp. 1–9, 2012.

[10] J. Bang, *Binary watermark image in the DCT domain watermarking method for insertion [M.S. thesis]*, Chunnam University, 2003.

[11] S. Jung and M. Lee, "Pure java based image processing with imageGS API," JungIkSa, Seoul, Republic of Korea, 2005.

[12] W. Choi, *A DCT based fragile watermarking for JPEG image authentication [M.S. thesis]*, Sejong University, 2011.

[13] https://code.google.com/p/dct-watermark/.

[14] https://java.net/projects/jai.

[15] J. Mei, S. Li, and X. Tan, "A digital watermarking algorithm based on DCT and DWT," in *Proceedings of the International Symposium on Web Information Systems and Applications (WISA '09)*, pp. 104–107, 2009.