Journal of The Korea Society of Computer and Information
Vol. 23 No. 4, pp. 33-39, April 2018
www.ksci.re.kr
https://doi.org/10.9708/jksci.2018.23.04.033

Fake Iris Image Detection based on Watermark

Man-Ki Kim*, Samuel Lee**, Gye-Young Kim***

Abstract

In this paper, we propose a describes how to detect a false iris image by inserting watermark into a iris image. The existing method, which inserts the watermark into the entire iris image to detect a fake iris, has a problem that can evade it by segmenting iris region of an iris image. The purpose of overcoming the problem, this paper proposes a new fake iris detection technique based on digital watermark. It first searches a central point of an iris image, divide the image into blocks with respect to the point. executes Discrete Cosine Transform, inserts watermark into the blocks, and then verifies an iris image using NC(Normalized Correlation). In the experiments, we confirm the robustness for attacks - crop and JPEG.

▸Keyword: Discrete Cosine Transform, Iris Image, Digital Watermarking, Fake Biometric Discrimination

I. Introduction

최근 생체인식 기술의 발전으로 송금, 결제 등의 다양한 분야에서 신원확인용으로 활용되고 있다. 생체인식 기술은 만인부동의 특징을 가지고 있어 각 사람마다 고유하여 변하지 않고, 변화 시킬 수도 없다. 그 중 홍채인식 기술은 근적외선 카메라로 촬영한 홍채를 인식하며, 현재 많이 사용되고 있는 지문인식 기술에 비하여 더욱 많은 특징점을 내포하고 있어 위조나 중복 가능성이 매우 적다. 홍채 인식기는 홍채영상 획득, 홍채영상 저장, 홍채영역 분할, 특징점 추출, 특징점 비교로 크게 5가지로 분류할 수 있다. 이 때, 홍채 영상 데이터베이스가 유출되어 복제 및 악용 될 경우 변화시킬 수 없는 생채정보의 특징에 따라 단순히 시스템의 보안 침해뿐만 아니라, 해당 생체 정보의 재사용 불능까지 이루어질 수 있는 문제점이 있다. 이러한 문제를 방지하기 위해 생체정보 유출방지와 유출 시 위조판별 방법에 대해 많은 연구들이 꾸준히 수행되어 왔다[1-5]. Connell 등은 소형 프로젝터와 별도의 카메라를 사용하여 눈 영역의 굴절률로 콘택트 렌즈판별을 수행한다[3]. 이 방법은 위조 홍채뿐만 아니라 시력 교정용 투명 콘텍트 렌즈도 검출하기 때문에 위조판별에서 정상적인 사용자도 위조 홍채라고 판별하는 문제점이 있다. Costa 등의 방법은 근적외선의 광량을 조절하여 동공반사에 따른 생채 정보 위조 판별을 한다[4]. 이 방법은 동영상이 입력으로 사용되어 다소 많은 연산시간을 요구하며, 동공반사가 이루어질 때 까지 인식이 이루어져야 하는 불편함이 있다. Fouad 등은 생채영상을 이산 웨이블릿 변환(Discrete Wavelet Transform :DWT)을 수행하여, 그 결과를 생체영상과 무관한 영상에 워터마크로 삽입하는 방법을 제안했다[5]. 이 방법은 공격자가 생체영상 데이터베이스에 접근했을 때, 해당 영상이 생채영상인지 식별 할 수 없는 장점이 있다. 이와 같은 다양한 연구가 진행되었지만 유출된 영상이 누구의 생체정보인지, 어떤 홍채영상 데이터베이스에서 유출되었는지 확인할 수 없는 문제가 있다. Abdullah 등은 홍채영상 전체를 8x8블록으로 나눠 이산 코사인 변환 수행 후, DC 계수가 큰 위치에 워터마크를 삽입하여 잡음에 강건한 방법을 개발했다[6]. 하지만, 홍채 인식기는 획득한 영상에서 홍채영역을 따로 분할하여 처리하므로 홍채영역이 아닌 위치에 삽입된 워터마크 정보가 손실될 가능성이 높다. 즉, 홍채 부분만 분할하여 다른

• First Author: Man-Ki Kim, Corresponding Author: Gye-Young Kim
*Man-Ki Kim (mainkey92@soongsil.ac.kr), Computer Vision Laboratory, Soongsil University
**Samuel Lee (lsme@ssu.ac.kr), Computer Vision Laboratory, Soongsil University
***Gye-Young Kim (gykim11@ssu.ac.kr), Dept. of Software, Soongsil University
• Received: 2018. 03. 27, Revised: 2018. 04. 03, Accepted: 2018. 04. 10.
• This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP: Ministry of Science, ICT & Future Planning) (No. NRF-2016K1A3A1A19945935).

영상에 덮어씌워 인식할 경우 워터마크 식별이 어려운 문제점이 있다. 이와 같은 문제를 해결하기 위해 본 논문에서는 홍채영상에 워터마크를 삽입하여 홍채영상의 유출된 경우, 위조를 판별하는 방법을 제안한다. 제안하는 생채영상의 위조판별 절차는 Fig. 1과 같이 동공의 중심점을 기준으로 $N\times N$블록으로 나눠 DCT변환 수행 후 워터마크 삽입하며, 이전에 저장된 워터마크 삽입위치로 워터마크 추출 후 NC(Normalized Correlation) 임계값을 이용하여 생채영상의 위조를 식별한다.

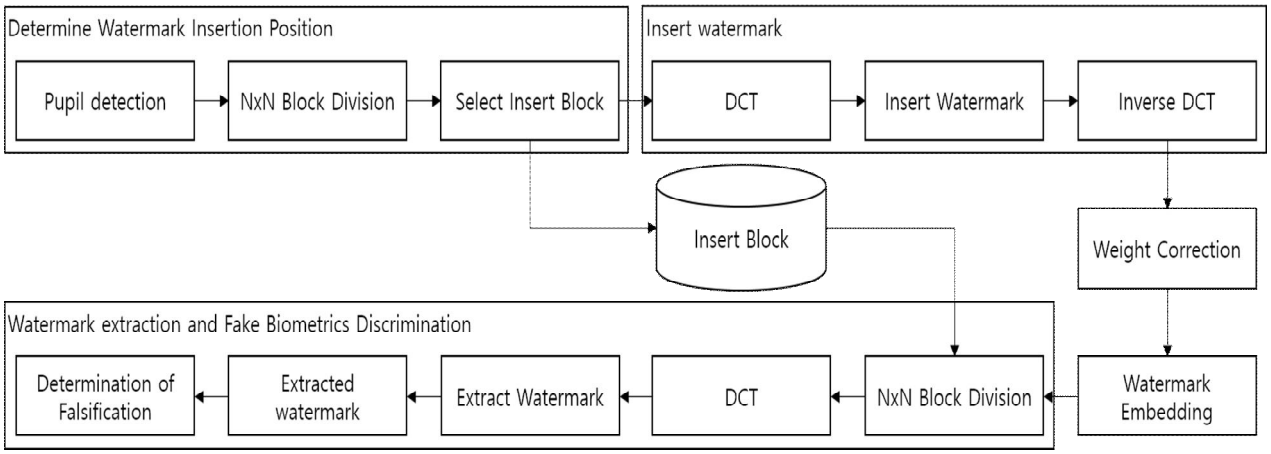


Fig. 1. Overview of the proposed technique for detecting a fake iris image

본 논문의 구성은 다음과 같다. 2절에서는 동공중심으로부터 워터마크 삽입위치 결정 및 워터마크 삽입 방법을, 3절에서 워터마크 추출 방법과 위조판별 방법에 대해 설명한다. 4절에서 실험결과를 보이고, 마지막으로 5절에서 결론 및 향후연구에 대하여 논술한다.

II. Insert watermark on DCT blocks

1. Selecting Watermark Insertion Positions

사람의 동공은 식 (1)과 같은 원의 방정식으로 근사할 수 있으며, 영상에서 동공영역은 원의 중심(x_0, y_0)와 반지름 r로 표현 할 수 있다[7].

$$(x-x_0)^2+(y-y_0)^2=r^2 \quad (1)$$

동공 중심점을 검출하기 위해 영상의 고주파 성분을 유지하면서, 잡음제거를 위해 중간값 필터(Median Filter)를 적용한다. 그 후 동공의 경계만 남기기 위해 캐니 에지(Canny Edge) 검출을 통해 에지맵을 만든 후, 허프변환(Hough Transform)을 통하여 원을 검출한다. 동공은 홍채와 색상의 대비가 크기 때문에 동공검출이 용이하고, 주변 잡음에 강인하여 허프변환으로 중심점을 찾을 수 있다. 즉, 에지를 검출한 후 Fig. 2(c)와 같이 허프변환을 수행하여 원으로 추정되는 후보들을 생성한 다음, 허프공간에서 누적수가 가장 큰 위치를 중심점으로 선택한다. Fig. 2(d)는 동공과 동공의 중심점을 분할한 예이다.

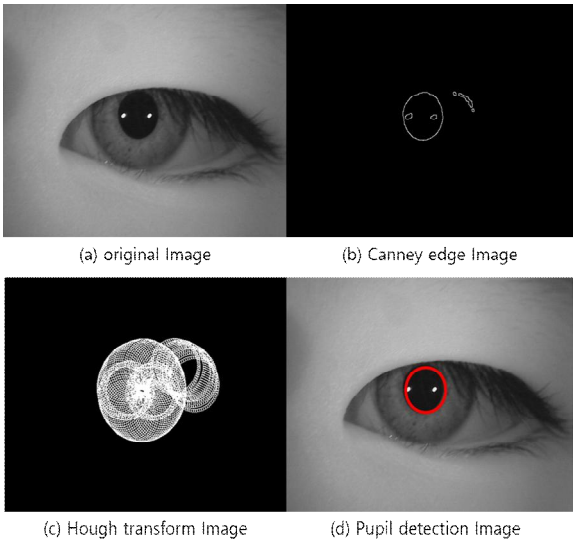
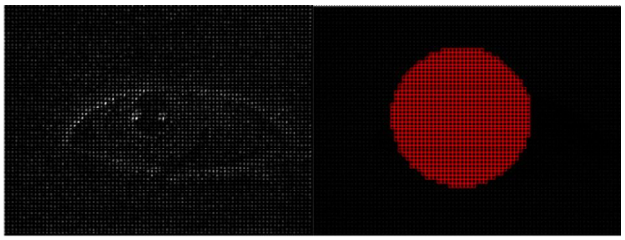


Fig. 2. Pupil detection using Hough transform

대부분의 홍채인식기의 경우 홍채영역을 따로 분할하여 사용하기 때문에 홍채의 중심으로부터 가까운 블록에 워터마크를 삽입할수록 워터마크가 보존될 가능성이 높다. 식 (2)와 같이 유클리디언 거리(Euclidean Distance)를 이용하여 동공 중심점과 영상 블록간의 거리 d를 측정하여 중심점으로부터 가까운 거리순으로 블록을 선택한다.

$$d=\sqrt{(x_0-x_{coef})^2+(y_0-y_{coef})^2} \quad (2)$$

여기서 (x_0,y_0)은 동공 중심점이며 (x_{coef}, y_{coef})는 DCT 블록의 DC 위치를 의미한다. 동공 중심점에서 홍채영역까지를 포함하며, 사용자 식별이 가능한 워터마크를 위해 32x32 워터마크 영상을 사용하여 Fig. 3과 같이 중심점에서 가까운 순서대로 1024개의 DCT 블록들을 선택하여 워터마크를 삽입한다.



(a) DCT coefficient blocks (b) DCT blocks near the pupil center

Fig. 3. 1,024 DCT blocks selected from the pupil center

2. Inserting Watermark into a DCT block

앞서 선택한 각 DCT 블록별 2차원 이산 코사인 변환(2D-DCT)을 통해 주파수 공간으로 변환한다. 주파수 공간은 Fig. 4와 같이 $C(0,0)$의 DC 성분과 나머지 AC 성분으로 구성되며, DC 성분에 가까울수록 영상 내 많은 정보가 포함되는 특징을 가지고 있다.

$$DCT(i,j) = C(i)C(j)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y) \cos\left[\frac{(2x+1)i\pi}{2N}\right]\cos\left[\frac{(2y+1)j\pi}{2N}\right] \quad (3)$$

$$where \quad C(i), C(j) = \begin{cases} \sqrt{\frac{1}{N}} & \text{for } i,j = 0 \\ \sqrt{\frac{2}{N}} & \text{for } i,j \neq 0 \end{cases}$$

여기서 i, j는 해당 블록의 DC공간에서의 좌표를 의미하며, x, y는 생체 영상에서의 좌표를 의미하고, N은 사용자가 설정한 DCT 블록의 크기를 의미한다. 각 $N \times N$블록 별로 식 (3)과 같이 2D-DCT를 수행한다. 기존 Langelaar방법은 이산 코사인 변환수행 후 영상 내 중요한 정보가 덜 포함되어 있는 AC성분인 $C(0,3)$, $C(1,2)$, $C(2,1)$, $C(3,0)$에 삽입한다[8]. 이 방법은 워터마크가 삽입된 영상의 손실을 최소화하기 위해 AC성분에 워터마크를 삽입하지만 본 논문에서는 영상 자르기 공격(crop) , JPEG압축 공격에 강건성을 위해 Fig. 4와 같이 DC계수에 가까운 $C(0,2)$, $C(1,1)$, $C(2,0)$ 부분 중 한 곳에 워터마크를 삽입한다. 하지만, Fig. 5(a)와 같이 DC성분에 가깝게 워터마크 삽입 시, 화질 열화를 해결하기 위해 후처리 과정으로 가중치를 사용하여 보정한다.

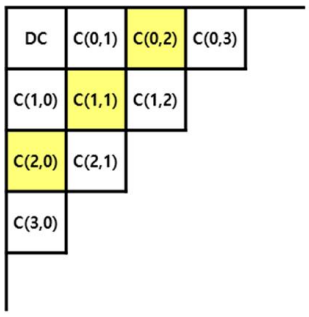
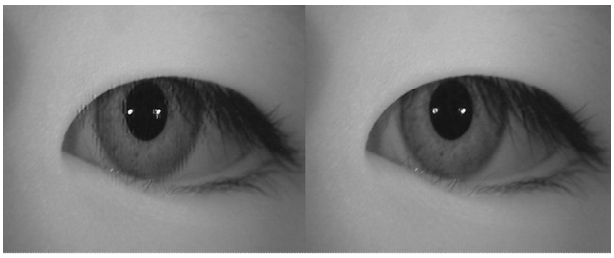


Fig. 4. Watermark insertion position on a DCT block



(a) $C(1,1)$ coefficient Insert (b) $C(3,0)$ coefficient Insert

Fig. 5. DC Coefficient and AC Coefficient Watermark Insert

워터마크의 삽입위치를 결정한 후, 각 블록에 대하여 Fig. 6과 같은 생체영상 식별코드를 포함하는 0과 1로 이루어진 이진영상을 각 비트별로 순회하면서 식 (4)로 선택된 DCT 계수에 워터마크를 삽입한다.

Fig. 6. 32x32 watermark Image with user information

$$\begin{aligned} &\text{if} \quad watermark\,bit = 1 \\ &\quad C(i,j) = -C(i,j) \,(\text{if} \quad C(i,j) < 0) \end{aligned} \quad (4)$$

$$\begin{aligned} &\text{if} \quad watermark\,bit = 0 \\ &\quad C(i,j) = -C(i,j) \,(\text{if} \quad C(i,j) > 0) \end{aligned}$$

여기서, $C(i,j)$는 DCT 계수를 의미하고, 워터마크의 비트가 1일 때 DCT 계수는 양수로, 0일 때 DCT 계수를 음수로 바꾼다. 워터마크 삽입으로 변경된 DCT 계수를 식 5와 같이 역 이산 코사인 변환(IDCT)으로 워터마크가 삽입된 영상을 획득한다.

$$f(x,y) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} C(i)C(j)DCT(i,j) \cos\left(\frac{(2x+1)i\pi}{2N}\right)\cos\left(\frac{(2y+1)j\pi}{2N}\right) \quad (5)$$

$$where \quad C(i), C(j) = \begin{cases} \sqrt{\frac{1}{N}} & \text{for } i,j = 0 \\ \sqrt{\frac{2}{N}} & \text{for } i,j \neq 0 \end{cases}$$

여기서 x, y는 출력될 영상의 좌표를 나타내고, i, j는 DCT공간에서의 좌표를 의미한다. 역 이산 코사인 변환을 이용하여 워터마크가 삽입된 영상을 획득한다. 워터마크가 삽입된 영상의 경우 Fig. 7(b)와 같이 동공의 빛 반사점 부분에 시각적으로 두드러지는 화질 열화가 발생한다. 이것은 워터마크 강인성을 위하여 DC성분에 가까운 위치에 워터마크 삽입 시 발생하는 문제점으로 이를 해결하기 위하여 가중치 보정 절차를 거쳐 최종적인 생체영상 I를 획득할 수 있다.

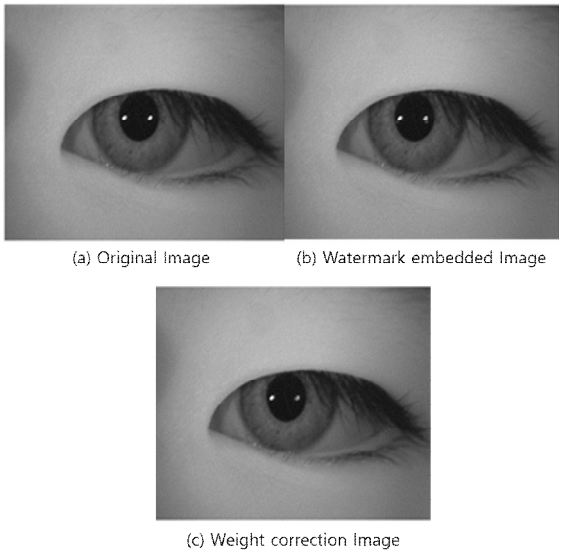


Fig. 7. Image Correction using a weight

$$I = I_e + f \times (I_o - I_e) \quad (6)$$
$$where \;\; 0 < f < 1$$

여기서, I_e는 워터마크가 삽입된 영상이고, I_o는 원본영상이다. 가중치 계수 f의 값이 크면 원본과 가깝게 표현되어 시각적 품질이 향상 되지만, 워터마크 추출 시 품질이 떨어진다. 가중치 계수 f값은 수집된 생채영상별 실험적으로 적절한 값을 설정한다. 본 논문에서는 가중치 계수 f를 0.43으로 설정하였다.

III. Watermark Extraction and Fake Image Discrimination

워터마크 추출 단계에서는 삽입한 블록위치, 블록의 크기 N, 블록 내 삽입위치가 필요함으로써 워터마크 존재여부를 알 수 없는 공격자가 워터마크의 유무를 확인 할 수 없도록 구성된다. 이전에 저장된 삽입위치를 확인하기 위해 워터마크 삽입 단계에서 동공의 중심좌표를 검출 후, 중심에서부터 미리 저장된 삽입위치에 대하여 해당 $N \times N$ 블록만 식 (3)을 이용하여 이산코사인 변환을 수행 후 각 블록의 DCT 계수 $C(i,j)$에 따라 아래와 같이 워터마크를 추출한다.

$$\text{if} \quad C(i,j) \geq 0 \quad (7)$$
$$watermark\,bit = 1$$

$$\text{if} \quad C(i,j) < 0$$
$$watermark\,bit = 0$$

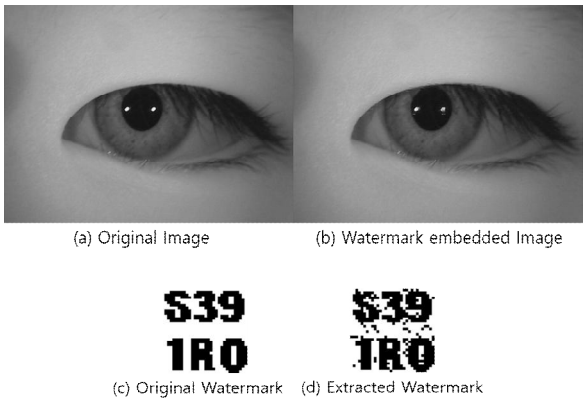


Fig. 8. an example of watermark extraction

Fig. 9. extracted watermark from the original image(Fig. 8(a))

Fig. 8은 워터마크가 삽입된 영상과 추출된 워터마크 영상이다. Fig. 8(d)에서 원본 워터마크에 비해 화질 열화가 발생한 이유는 워터마크 삽입 시, 시각적 품질 향상을 위하여 가중치 보정 절차를 때문에 워터마크가 손상된다. Fig. 9는 유출된 생채영상과의 비교를 위해 워터마크가 삽입되지 않은 홍채영상에 대한 워터마크 추출 결과다.

추출된 워터마크와 원본 워터마크의 유사도를 식 8의 NC(Normalized Correlation)를 산출하고, NC를 이용하여 홍채영상의 유출을 여부를 판단한다.

$$NC = \frac{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} W(i,j) \times W^*(i,j)}{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} [W(i,j)]^2} \quad (8)$$

$$\text{if}(NC \geq T)$$
$$Accept$$
$$else$$
$$Deny$$

$$where \;\; 0 < T \leq 1$$

여기서 W는 원본 워터마크 영상이며, W^*은 추출된 워터마크 영상이고, T는 임계값을 의미한다. NC는 원본과 유사할수록 1에 가까운 값으로 표시되며, 일정 임계값을 기준으로 위조 생채영상을 식별한다. 본 논문에서는 Fig. 8(d)와 같이 추출된 워터마크와 Fig. 9처럼 추출된 워터마크의 NC는 각각 0.87과 0.51로 측정되었다. 이 결과 워터마크 추출 후 0.7의 임계값 T로 생채영상의 유출 여부를 판단하여 인식 거부를 수행한다.

IV. Experiment Result

홍채영상의 위조를 판별을 실험하기 위하여 CASIA Iris image

Database ver 4.0을 이용하였다[9]. CASIA 홍채 데이터베이스는 Chinese Academy of Sciences Institute of Automation (CASIA)에서 근적외선 카메라로 촬영한 1,800종류의 홍채로 추출된 총 54,601장의 홍채영상으로 구성되어 있으며, 640x480의 해상도의 8비트 명암영상이다. 실험에서는 3,183개의 홍채영상을 무작위로 선택하여 사용했다. 영상의 시각적 품질을 객관적으로 비교하기 위하여 원본영상과 워터마크가 삽입된 영상간의 신호 대비 잡음비(Peak Signal to Noise Ratio :PSNR)을 기준으로 평가하고, 원본 워터마크와 추출된 워터마크간의 유사도 측정을 위해 앞에서 위조된 생채영상을 식별하기 위해 사용한 식(8)의 NC를 기준으로 평가한다.

$$PSNR(dB) = 10\log_{10}\frac{E_{\max}^2 \times I_w \times I_h}{\sum(I_{x,y} - I_{x,y}^*)^2} \quad (9)$$

여기서 $E_{\max}$는 영상에서 최대 화소 값이며, I는 원본 영상이고, I^*은 워터마크가 삽입된 영상을 의미한다. 신호 대비 잡음비는 dB로 표현되며, 원본과 유사할수록 높은 값을 가지는 특징이 있으며, Chen이 제안한 방법에 따르면 보통 30dB이상일 때 사람의 눈으로 시각적 품질 차이를 느끼기 힘들다[10].

Table 1은 3,183개의 홍채영상에 워터마크를 적용한 영상과 원본영상의 신호대비 잡음비, NC값과 워터마크를 삽입하지 않은 영상에서의 NC값(Negative NC)를 비교한 결과를 나타낸다. 따라서 NC 임계값으로 0.7을 설정하면 생채영상의 유출 여부를 식별할 수 있다.

Table 1. Averages of PSNR, NC and Negative NC for the selected iris images

PSNR	NC(Normalized Correlation)	Negative NC
49.18 dB	0.80	0.51

Table 2. the robustness of the proposed technique for attacks - crop and JPEG

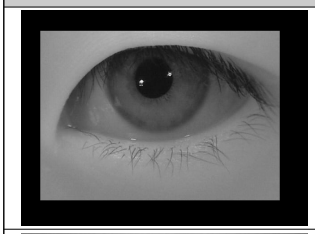
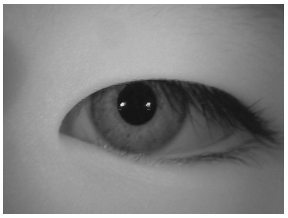
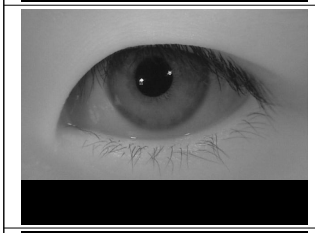
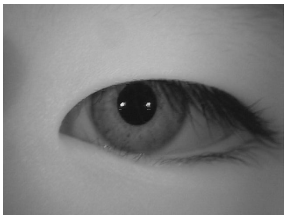
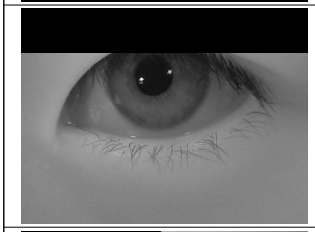
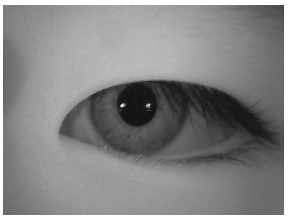
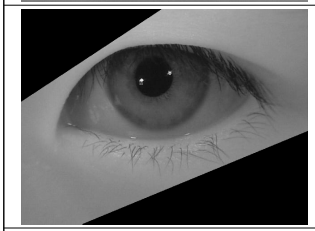
Crop Attack	Crop Ratio	Extracted Watermark	NC	JPEG Compression Attack	Quality	Extracted Watermark	NC
	36%		0.90		95		0.89
	22%		0.91		90		0.87
	22%		0.89		85		0.85
	28%		0.90		80		0.83
	75%		0.81		75		0.81

Table 2는 홍채영상의 위조 판별을 실험하기 위해 홍채영상 위·변조 공격을 실험하였다. Table 2는 위·변조 공격 중 홍채영상에서 가장 중요한 홍채 부분을 제외한 영상 자르기 공격 실험(Crop)과 JPEG압축 공격에 대해 분석한 결과다. 홍채 인식기에서 가장 중요한 홍채 부분을 직접 자르지 않는 이상 워터마크 정보의 손실이 거의 없다. 보편적으로 많이 사용되는 JPEG 90 품질 압축에서 우수한 결과를 나타냈으며, JPEG 80 품질 압축까지 워터마크 판별이 가능하다.

V. Conclusions

본 논문에서는 동공 중심점을 기준으로 블록을 나눠 2D-DCT를 수행한 다음 워터마크를 삽입하고, 추출 과정에서 NC(Normalized Correlation) 임계값으로 홍채영상의 위조를 판별하는 방법을 제안하였다. 홍채영상에서 가장 중요한 부분인 홍채만 건재하면 위조 판별이 가능하며, DCT공간에서 DC와 가까운 위치에 워터마크를 삽입하여 JPEG 압축공격에도 강인하다.

워터마크 추출 시, 가중치 계수 f의 값에 따라 워터마크 추출률이 변화 하는데, 향후에는 DC성분에 가깝고 별도의 가중치 계수 f 없이도 시각적 품질이 유지되는 방법과 홍채영상뿐만 아니라 얼굴영상, 지문영상에서도 적용 가능한 워터마킹 방법에 대한 연구가 필요하다.

REFERENCES

[1] Younghwan Kim, Jang-Hee Yoo, Kyoungho Choi, “A motion and similarity-based fake detection method for biometric face recognition systems”, IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, May 2011.

[2] Diego Gragnaniello, Giovanni Poggi, Carlo Sansone, Luisa Verdoliva, “An Investigation of Local Descriptors for Biometric Spoofing Detection”, IEEE Transactions on Information Forensics and Security, Vol. 10, No. 4, April 2015.

[3] Jonathan Connell, Nalini Ratha, James Gentile, Ruud Bolle, “Fake Iris Detection Using Structured Light”, Acoustics, Speech and Signal Processing (ICASSP), 8692-8696pp, May 2013.

[4] Ronaldo Martins da Costa, Adilson Gonzaga, “Dynamic Features for Iris Recognition”, IEEE Trans. on System, Man, and Cybernetics—Part B: Cybernetics, Vol. 42, No. 4, July 2012.

[5] Marwa Fouad, Abdulmotaleb EI Saddik, Emil Petriu, “Combining DWT And LSB Watermarking To Secure Revocable Iris Templates”, 10th International Conference on Information Science, Signal Processing and their Applications, 25-28pp, May 2010.

[6] M ohammed A. M. Abdullah, S. S. Dlay, W. L. Woo, “Securing Iris Images with a Robust Watermarking Algorithm based on Discrete Cosine Transform”, In Proceedings of the 10th International Conference on Computer Vision Theory and Applications, 108-114pp, March 2015.

[7] HK Yuen, J Princen, J Illingworth, J Kittler, “Comparative study of Hough Transform methods for circle finding”, Image and Vision Computing, Vol. 8, No. 1, 71-77pp, Feb. 1990.

[8] Langelaar, G.C, Setyawan, I, Lagendijk, R.L, “Watermarking digital image and video data. A state-of-the-art overview”, IEEE Signal Processing Magazine, Vol. 17, No. 5, Sep. 2000.

[9] CASIA Iris Image Database, http://biometrics.idealtest.org

[10] Tung Shou Chen, Chin Chen Chang, Min Shiang Hwang, “A virtual image cryptosystem based upon vector quantization”, IEEE Trans. on Image Processing, Vol. 7, No. 10, Oct. 1998.

Authors

Man Ki Kim received the B.S. degrees in Computer Science from Chungwoon University, Korea, in 2017He is currently a Student in the Computer Vision Laboratory, Soongsil University. He is interested in Computer vision, Image Processing and Pattern Recognition.

Samuel Lee received the B.S degrees in Computer & Information Engineering from Kunsan National University in 2017. He is currently a student in the Computer Vision Laboratory, Soongsil University. He is interested in Computer Vision, Image Processing, Pattern Recognition and Biometrics.

Gye Young Kim received the B.S., M.S. and Ph.D. degrees in Computer from Soongsil University, Korea, in 1990, 1992 and 1996, respectively. From March 1996 to February 1997, he served as a Post-Doctoral Fellow at Electronics and Telecommunication Research Institute (ETRI), Daejon, Korea. Dr. Kim joined the faculty of the Department of Software at Soongsil University, Seoul, Korea, in 2001. He is currently a Professor in the Department of Software, Soongsil University. He is research interests are in the field of computer vision, multimedia database, augmented reality and biometric