워터마크 기술을 이용한 생체정보의 비교 분석

이현지 *문정은 **서영호
광운대학교
lhjblackjack@gmail.com, wjd77dma98@gmail.com

Analysis of biometric information using watermarking technology

Hyeon-ji Lee *jeong-eun Moon **Young-ho Seo
Kwangwoon University

요약

최근 스마트폰과 어플리케이션의 기술 발전으로 일상생활에서 은행의 주거래 혹은 보안인증으로 생체정보를 이용하는 것이 급격히 확대되고 있다. 이러한 생체정보 보호를 위해 디지털 콘텐츠 내에 저작권자의 정보를 삽입하여 정보를 보호하는 기술인 워터마킹 기술을 도입하여 생체정보의 복제 혹은 도용 시에 발생할 수 있는 문제를 예방하는 것이 본 연구의 목적이다. 본 논문에서는 홍채 이미지에 DWT를 적용한후 QIM 방식을 이용해 임의의 QR코드로 워터마크를 삽입하여 홍채 코드를 추출한후 워터마크를 삽입하기 전의 홍채코드와 삽입 후의 홍채코드를 PSNR 통해 비교 분석하고 Stirmark 에서 제공하는 강인성 테스트를 이용해 강인성의 정도를 알아본다

1. 서론

최근 스마트폰 및 정보통신 기술의 발전으로 일상생활에서 단순한 메일 업무이외에 주식거래, 금융 등 개인의 신원파악과 본인인증을 필수로 하는 업무 역시 스마트폰을 이용하고 있다. 이에 보안은 현재 사용되고 있는 모바일뱅킹과 관련하여 빼놓을 수 없는 문제 중 하나이다[1]. 현재까지 국내 은행들이 제공하는 스마트뱅킹 어플리케이션은 공인인증서 방식을 채택하고 있지만 최근 공인인증서 의무 사용에 대한 폐지 법안이 발의 되는 등 본인인증을 위한 다양한 방식에 대한 논의가 지속되고 있으며 홍채인증을 비롯한 다양한 생체정보 기술이 그 중 하나가 될 것으로 전망하고 있다.

현재까지 디지털 콘텐츠에 대한 저작권 보호를 위한 방법으로는 워터마크가 가장 많이 연구되어 왔으며 워터마크 기술은 크게 두 가지의 사항을 우선적으로 고려하는데 워터마크가 눈에 보이지 않는 비가시성과 전송 등의 공격에 워터마크가 손상이 일어나지 않아야 하는 강인성이다. 또한 방식으로는 DCT[2], DWT[3], SVD[4] 등이 있으며 이에 대한 많은 연구들이 진행되어 왔다.

홍채는 각 개인마다 구별되는 고유한 특징을 갖는 패턴을 가지고 있으며, 개인의 양쪽 눈도 같지 않은 유전적 특징과 시간에 관계없이 홍채의 특징이 지속적으로 유지되는 특징을 갖는 다[5]. 따라서 서로 다른 홍채를 구별하기는 어렵지 않아 생체 보안 분야에 많이 이용되고 있지만, 만약 홍채정보가 복제 또는 도용당할 시에는 홍채정보를 변경하기란 어렵기 때문에 큰 문제를 야기할 수 있다. 따라서 홍채인식에 사용되는 홍채 정보를 보호할 필요가 있으며 이 보호방법으로 워터마크를 이용한다.

본 논문에서는 홍채 이미지를 DWT로 변환 후 마이크로 QR코드를 이용한 워터마크를 다양한 위치에 QIM방식으로 삽입하여 워터마크가 삽입된 홍채이미지를 만든 후, 원본 홍채 이미지와 워터마크가 삽입된 홍채이미지에서 홍채코드를 추출하고 PSNR을 이용해 비교 및 분석한다. 또한 공격이 가해 졌을 때와 가해 지지 않았을 때의 이미지를 이용하여 강인성 및 가시성 정도에 대해 알아본다.

2. 설계 알고리즘

본 논문의 구현 환경은 Visual studio와 matlab이고, 사용한 PC는 Intel(R) Core(™) i7-9750H CPU @ 2.60 GHz, 8GB RAM을 갖고 있으며, 운영체제는 64-bit Windows, 그리고 GPU는 intel(R) UHD Graphics 630/NVIDIA GeForce GTX 1650을 사용하였다. 홍채를 이용한 워터마크 실험을 위하여 CASIA Iris image Database (ver. 1.0)을 이용하였으며, 입력홍채영상의 형식은 320*280 픽셀크기에 8비트 그레이 영상이며, 워터마크로는 52*52 픽셀크기에 8bit 마이크로 QR코드를 사용하였다.

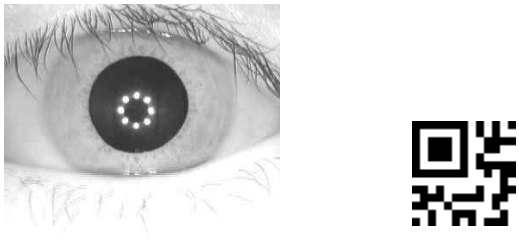


그림1. 홍채입력영상과 워터마크

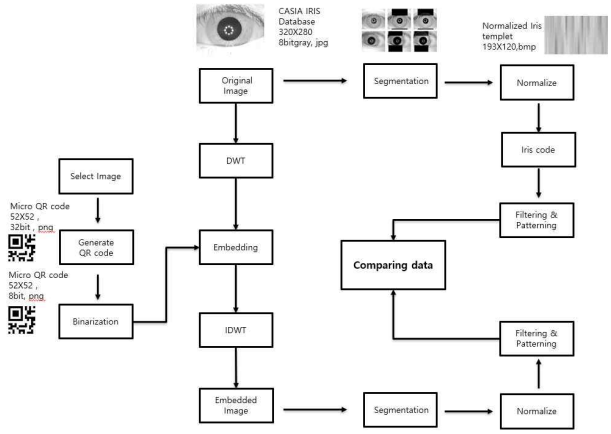
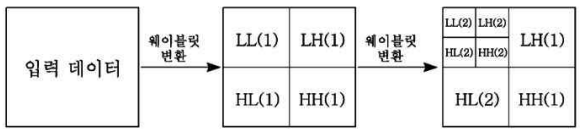


그림2. 설계 알고리즘

2-1. 워터마킹 기술

워터마킹 기술은 영상 및 음악등의 디지털 콘텐츠에 일정 형태의 정보를 제 3자가 알 수 없도록 숨겨놓는 기술이다. 이 기술은 저작권 보호 차원에서 개발이 진행된 것으로 콘텐츠에 저작권자에 관한 ID정보 등을 삽입해 두면 부정으로 사용할 경우 저작권 침해를 주장할 수 있는 강력한 수단이 되기 때문이다. 워터마크 기술은 크게 공간 영역(spatial domain)에서의 워터마크 삽입 기술과 주파수 영역 (frequency domain)에서의 워터마크 삽입 기술로 나눌 수가 있는 데 두 방법 중 주파수영역에서의 마킹 기술이 제 3자로 하여금 영상의 왜곡이나 변형에 보다 강력하기 때문에 이 방법을 주로 사용한다.

만약 2차원 신호의 웨이블릿 변환을 하게 되면, 1개의 근사값과 3개의 세부값(수평 세부값, 수직 세부값, 대각 세부값)으로 분해가 가능하다. 멀티 스케일로 분해하면 근사값이 또 1개의 근사값과 3개의 세부값으로 분해된다. 예를 들면 400x400 이미지를 2개의 스케일로 분해한다면 첫 단계에서 200x200사이즈의 근사값과 3개의 세부값을 얻게 되고, 두 번째 단계에서는 200x200 근사값 이미지가 다시 한번 분해되어 100x100 사이즈의 근사값 이미지와 3개의 세부값 이미지로 분해된다.



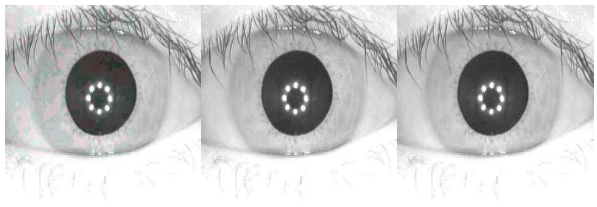
본 논문에서는 2레벨 웨이블릿 변환을 이용하여 생체정보를 보다 안전하게 은닉하고 추출할 수 있는 기법을 제안한다.

2-2. 홍채코드 추출

홍채영역 추출은 동공과 홍채의 경계에 해당하는 동공 경계와 공막과 홍채 경계에 해당하는 홍채 외부 경계를 추출하고 추출된 경계를 기준으로 극좌표 변환하는 두 과정을 거치게 된다. 일반적으로 동공과 홍채의 경계를 원으로 가정하고 동공 경계와 홍채 사이의 영상의 명암 값이 급격히 변화하는 성질을 이용하여 영역을 홍채영역을 추출한다[6]. 이처럼 입력 영상에서 홍채 영역이 추출되면 이 영역으로 부터 홍채 코드를 검출하게 된다. 홍채 정보를 효과적으로 찾아내기 위한 방법으로는 가버(Gabor) 필터가 널리 쓰이고 있다. 가버 필터를 통해 각 개인당 256 바이트 (2048 비트) 크기의 홍채 코드를 생성하게 되며 이러한 홍채코드와 해밍거리(hamming distance)를 통해 본인여부를 판단하게 된다[7].

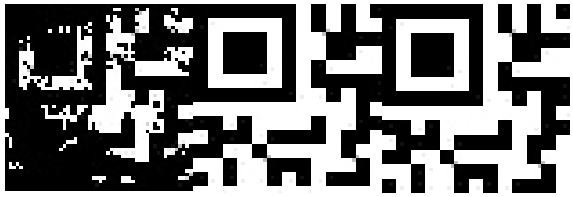
3. 결론

우선적으로 각각 LL2, HH2, HH1 영역에 워터마크가 삽입된 후의 이미지와 원본의 이미지를 비교하고 추출한 워터마크와 원래의 워터마크를 비교하여 표로 정리하였다. 이미지 비교에는 인간의 시각적 화질 차이를 평가하는 도구인 SSIM을 이용하였고 워터마크(본 논문에서의 micro QR)는 영상의 화질에 대한 손실정도를 평가하는 PSNR을 이용하였다. PSNR은 손실이 적을수록 높은 값을 가지며, 손실이 없을 경우 정의되지 않으며, 30dB가 넘을 경우 두 영상의 차이를 눈으로 구분할 수 없다.



0.9331 0.9590 0.9599

그림3 LL2, HH2, HH1 에서의 워터마크 삽입 이미지



30.0783 52.0686 52.0686

그림3 LL2, HH2, HH1 에서의 추출된 워터마크 이미지

위와 같이 워터마크 추출의 복원성과 워터마크가 삽입 되었을시 비가시성 면에 있어서 HH1 영역이 가장 뛰어남을 알 수 있었다. 그러나 HH1영역은 회전이나 노이즈 등의 공격에 굉장히 취약하다. 따라서 워터마크를 삽입할때는 중간영역인 HH2영역에 삽입하여 워터마크의 강인성과 비가시성을 모두 충족시킬 수 있다.

또한 홍채 영역 추출에서 동공경계와 홍채사이의 급격한 명함 변화를 이용하여 홍채 코드를 추출하기 때문에 고주파수 영역에서의 데이터가 굉장히 중요하다고 할 수 있다. 따라서 HH1 영역에서 워터마크를 삽입할 시에 홍채코드가 손상되어 나올 가능성이 매우 높으며 이는 곧 개인의 생체 정보가 손상됨을 의미한다. 따라서 생체정보 보안을 위한 워

터마크 삽입 형식에는 HH2와 같은 중간영역이 워터마크를 삽입하기에 적절함을 유추해 볼 수 있는 바이다.

다음으로는 LL2, HH2, HH1 영역에 워터마크를 삽입한 홍채 이미지에서 홍채 코드를 추출하여 원본 이미지의 홍채 코드와 비교하였다. 원본 이미지 및 각각 LL2, HH2, HH1 영역에 워터마크를 삽입한 홍채 이미지를 segmentation와 normalization한 다음 PSNR을 이용하여 손실정도를 알아보았다.

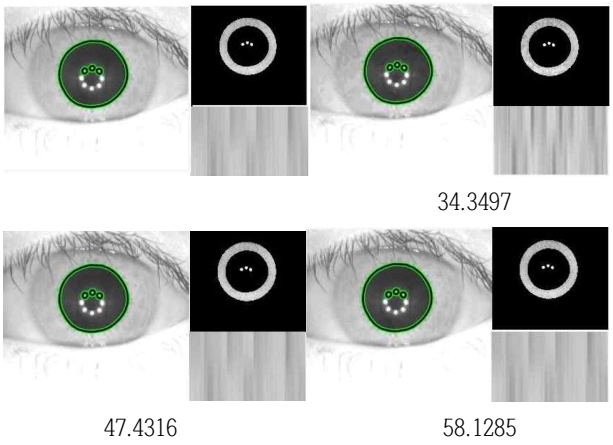
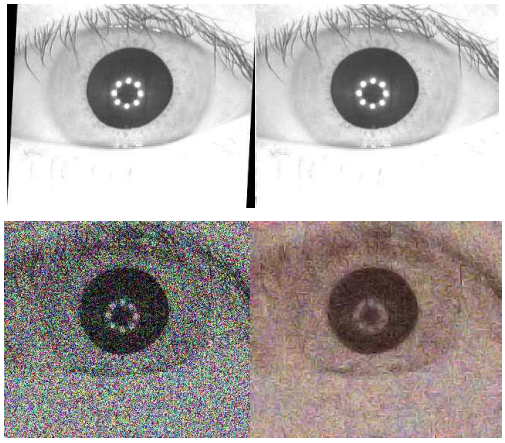


그림4 원본이미지, LL2, HH2, HH1 에서의 홍채 추출 이미지

위와 같이 각 영역에 워터마크를 삽입한 후, 홍채 이미지를 추출하여 PSNR을 이용해 normalization된 홍채를 원본 이미지와 비교했을 때, LL2영역에 워터마크를 삽입시 홍채에 가장 많은 손실이 일어났음을 알 수 있다. 그리고 HH1영역에 워터마크를 삽입시 가장 손실이 적은 것을 알 수 있다.

다음으로는 Stirmark로 HH1과 HH2영역에 워터마크를 삽입한 이미지에 공격을 가한 후의 홍채 추출 이미지와 복원한 이미지의 홍채 추출 이미지를 공격받기 전 홍채 추출 이미지와 비교하였다. 가한 공격은 AFFINE, NOISE, ROT 3가지이며 각 복원한 이미지는 320*280 픽셀크기에 24비트 BMP 영상이며, 공격받은 이미지는 각각의 픽셀크기는 다르지만, 24비트 BMP 영상이다.



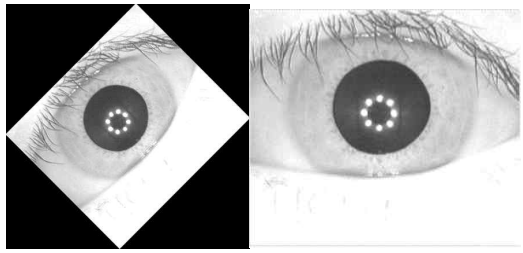


그림5 AFFINE, NOISE, ROT 공격 후 이미지와 복원한 이미지

PSNR	HH2 공격	HH2공격후 복원	HH1 공격	HH1 공격후 복원
AFFINE_4	29.4126	28.4789	29.8411	27.6115
NOISE_20	X	22.0897	X	21.7251
ROT_10	28.9526	29.6810	28.9254	30.6337
ROT_45	X	29.3197	X	31.3398
ROT_90	28.7653	31.5785	28.8330	31.6771

그림6 공격과 복원 후 홍채 이미지의 PSNR을 나타낸 표

그림6에서 볼 수 있듯, 홍채가 추출되지 않았던 NOISE 공격 이미지의 경우 복원 후에는 추출이 가능해졌으며, ROT 공격 이미지의 경우에도 복원 시 추출되지 않던 홍채가 추출이 가능해지고, PSNR 값이 증가함을 볼 수 있다. 하지만 AFFINE 공격 이미지의 경우 오히려 복원시 값이 떨어졌음을 볼 수 있다.

또한, 전체적으로 봤을 때 가장 손실이 적은 것은 HH1 영역에 워터마크를 삽입 및 공격한 후 복원한 이미지이며, 가장 손실이 높은 것은 HH2 영역에 워터마크를 삽입하고 공격한 이미지임을 알 수 있다. 이는 이론적으로 봤을 때 상대적으로 HH2 영역에 워터마크를 삽입하는 것이 HH1 영역에 워터마크를 삽입할 때보다 정보의 손실이 더 많이 일어나기 때문에 적절한 실험결과라고 볼 수 있다. 그뿐 아니라, NOISE 공격을 가할 경우 HH1, HH2 상관없이 PSNR 값이 낮기 때문에 어느 영역에서든 NOISE 공격에 가장 취약함을 알 수 있다.

4. 작품의 기대효과

홍채인식이나 지문인식과 같은 생체 정보를 이용한 보안방식의 경우에는 PIN이나 패스워드와 같은 방식과 비교하면 상대적으로 높은 보안력을 가져 정보가 유출될 확률이 적다는 장점을 가진다. 하지만 PIN이나 패스워드방식의 경우에는 한번 정보가 유출될 경우 쉽게 변경할 수 있으나, 생체 정보를 이용한 보안방식의 경우에는 생체정보를 변경하기란 어렵기 때문에 도난이나 복제당할 경우 큰 문제를 야기할 수 있다. 따라서 워터마크를 삽입함으로써 생체 정보의 유출을 방지하고 보호하여 생체 정보가 유출될 시 발생하는 심각한 문제들을 어느 정도 줄일 수 있을 것으로 예상된다. 또한 지금까지 가지고 있던 생체 정보 시스템의 단점을 보완할 수 있기 때문에 편리성과 같은 다양한 장점을 갖는 생체 정보시스템을 다양한 분야에 적극적으로 적용할 수 있어 더 높은 보안력을 갖는 정보 보안이 가능할 것으로 예상된다.

5. 참고문헌

[1] Institute for Information & communications Technology Promotion: “Technology Development Trend and Market Forecast of VR/AR,” Weekly Technology Trends, Vol. 1803,

July, 2017.
[2]성준헌, 유송현, 정제창. (2018). DCT를 이용한 디지털 이미지 워터마킹. 대한전자공학회 학술대회, (), 459-461.
[3]이용석, 서영호, 김동욱. (2015). 디지털 영상을 위한 DWT 기반의 강인성 블라인드 워터마킹. 한국방송미디어공학회 학술발표대회 논문집, (), 69-72.
[4]박병수, 추형석, 안종구. (2009). SVD 및 트리플릿 기반의 디지털 워터마킹 기법. 전기학회논문지, 58(5), 1041-1046.
[5]김기진, 손병준, 이일병. (2004). 홍채인식을 위한 강건한 특징추출 방법. 한국정보과학회 학술발표논문집, 31(1B), 793-795.
[6]윤경록, 양우석. (2004). 홍채 인식을 위한 홍채 영역 추출. 대한전기학회 학술대회 논문집, (), 181-183.
[7]정대식, 박강령. (2005). 중간 주파수 영역에서의 디지털 워터마킹 기법에 의한 홍채 및 지문 데이터 보호 연구. 멀티미디어학회논문지, 8(9), 1227-1238.