Journal of Korea Multimedia Society Vol. 11, No. 11, November 2008(pp. 1555-1565)

전자신분증용 바이오 영상을 위한 비인지 워터마킹 설계

신용녀[†], 이용준[††], 김원겸[†††]

요 약

얼굴, 지문 등의 바이오 정보는 사용자의 유일성과 편리성을 제공하는 인증 방식으로 전자신분증에 보편적으로 활용되고 있다. 전자신분증에 사용되는 바이오 정보는 강화된 부인봉쇄를 제공하지만 기존의 인증 방식에서 제공하는 폐지 후 재발급 절차가 없기 때문에 악의적으로 도용되는 경우는 심각한 개인 개인정보 침해가 발생한다. 본 논문에서는 전자신분증용 바이오 영상의 무결성과 책임 추적성을 검증할 수 있는 비인지 워터마킹을 제안한다. 삽입되는 워터마크는 바이오 영상을 획득하는 일자와 CRC(Cyclic Redundancy Checks)와 같이 조합되어 삽입된다. 얼굴, 지문은 JPEG, WSQ의 압축 형식으로 저장되는데 제안한 워터마킹 알고리즘은 영상 압축에 강인하며 바이오인식 성능을 저하시키지 않도록 설계하였다. 획득 단계에 삽입된 워터마크는 통신, 저장, 전자신분증 발급, 판독 단계에서 추출되어 바이오 영상의 개인 개인정보를 제공한다.

Design of Invisible Watermarking for Biometric Image of Electronic ID Card

Yong Nyuo Shin[†], Yong Jun Lee[††], Won Gyum Kim[†††]

ABSTRACT

Biometric information such as face and fingerprint information is highlighted in many security areas, including authentication, due to its uniqueness and convenience factors. However, if exploited maliciously, it can cause more serious damage than traditional security measures, like passwords. This paper reviews the watermarking method that is able to verify the integrity of this biometric information. The watermark to be inserted is the date of the biometric information acquisition. It is combined with 16-bit Cyclic Redundancy Checks prior to insertion. In particular, face and fingerprint images are saved in a specific compressed format. The proposed watermarking algorithm will be designed in such a way as to remain resilient against compression. The watermark inserted at the acquisition stage will be extracted at each storage and deployment stage, so that the integrity of the biometric information can be verified.

Key words: Biometrics(바이오인식), Watermarking(워터마킹), Privacy(개인정보)

1. 서 론

현재 인터넷에서는 개인의 중요한 정보가 타인에 의해 쉽게 도용되거나 노출되는 심각한 문제가 제기되고 있다. 이로 인해 개인의 정보만이 손실되는 것이 아니라 국가의 중요 정보와 전자상거래 등의 경제활동에 필요한 정보도 동시에 손실되는 현상이 발생되고 있다. 따라서 현재 많이 사용되고 있는 패스워드 또는 PIN(Personal Identification Number)만을 이용한 사용자 인증 방법으로는 개인, 산업, 그리고

※ 교신저자(Corresponding Author) : 신용녀, 주소 : 서울시 송파구 중대로 135 IT벤처타워(138-950), 전화 : 02)405-5237, FAX : 02)405-5219, E-mail : ynshin@kisa.or.kr
접수일 : 2008년 5월 26일, 완료일 : 2008년 9월 16일
[†] 정회원, 한국정보보호진흥원 주임연구원
[††] 정회원, LG CNS 책임연구원 (E-mail : bigman@lgcns.com)
[†††] 정회원, 마크애니 수석연구원 (E-mail : wgkim@markany.com)
※ 본 연구는 한국정보통신기술협회의 "정보보호기반 및 바이오인식 표준개발(2008-P1-27-06J40)" 사업의 연구결과로 수행되었음

국가의 중요 정보를 안전하게 보관할 수 없는 실정이다. 이러한 문제를 해결하기 위해 최근 들어 개인의 고유한 생체정보인 신체적 또는 행동학적 특징에 따라 사람들의 신원을 확인하는 바이오 인식 기술이 대두되고 있다. 바이오 정보는 개인의 고유 정보인 지문, 홍채, 음성, 얼굴 모양, 손의 형태, 서명, 손등의 정맥 분포 등 아주 다양하다. 이것은 신체의 일부이거나 개개인의 행동 특성을 반영하여 잊어버리거나 타인에게 대여 또는 도난당하지 않기 때문에 정보 보안을 위한 새로운 분야로 활성화되고 있다[1-4].

그러나 바이오 정보 역시 개인의 주요 정보이면서 개인 정보와 관련이 있기 때문에 사용자 인증 혹은 인식을 위하여 저장된 바이오 정보가 타인에게 도용이 된다면 패스워드나 PIN과 달리 변경이 불가능하여 심각한 문제를 야기할 수 있다. 특히 지문이나 얼굴과 같은 정보는 유출되었을 때 심각한 개인정보 침해 문제를 야기할 수 있다. 이러한 문제를 해결하는 여러 방법 중 하나가 워터마킹 기술을 사용하는 것이다. 이는 바이오 정보에 부가정보를 삽입함으로써 해당 바이오 정보에 대한 인증 및 위, 변조를 검출할 수 있다. 또한 저작권 보호 기술을 사용하게 되면 바이오 정보가 불법적으로 유출되었을 때 생길 수 있는 치명적인 개인정보 문제의 책임여부를 가리는 일과 유출 경로를 파악하는 데 도움을 줄 수 있다[5-7].

얼굴, 사진의 바이오영상에 대한 개인 개인정보 보호 기술로써 최근에는 바이오정보를 보호표준에 맞게 암호화 기법과 바이오정보 특징점을 변환 가능하도록 하는 방법, 원타임 바이오템플릿 기법 등의 다양한 보호 기술이 제안되고 있다.

워터마킹은 영상, 오디오, 비디오 같은 멀티미디어 데이터에 부가정보를 인지적 혹은 비인지적으로 삽입하고 추출하는 기술이다. 삽입하려는 데이터의 형태와 부가정보에 따라 구현하는 기술이 조금씩 차이가 난다. 이러한 워터마킹 기술을 바이오정보에 적용한다면 바이오정보가 타인에게 도용되었을 경우 삽입된 워터마크의 추출 여부 자체로 1차 인증을 하고 2차로 추출된 워터마크로 바이오 인식 시스템에 인증을 요구하여 요구한 바이오 정보에 대해 수용 및 거부를 결정할 수 있다. 또한 바이오정보의 배포처 정보를 워터마크로 삽입한다면 후에 불법 유출된 바이오정보에 대해 유출 점을 역 추적할 수 있다[8-10].

본 논문에서는 바이오정보에 대한 워터마킹 기술을 제안한다. 얼굴과 지문 데이터는 일반적으로 스캐너나 디지털 카메라 등으로 획득되며 사이즈가 작고 특정 압축 형식 형태로 저장된다. 본 제안 알고리즘은 얼굴 및 지문 파일에 대해 워터마크 정보를 삽입, 추출하여 위변조 여부를 판별할 수 있다. 본 논문이 제안하는 바이오영상 워터마킹 기술은 소유기관의 책임추적성과 원본 영상의 무결성을 보장하는 기술로 활용이 가능하다. 특히 최근에 전자여권, 전자주민증에 지문, 얼굴 정보를 저장하여 바이오인식을 활용하는 기술이 보편화됨에 따라서 제안하는 워터마킹 기술은 바이오정보 획득기관의 안전성을 높이는 방법이 될 것으로 예상된다.

본 논문은 II장에서는 바이오인식에서 디지털 워터마킹에 대한 기존연구를 제시하고, III장에서는 전자신분증용 바이오인식 기술에서 요구되는 보안 요구사항을 정의한다. IV장에서는 제안하는 워터마킹 시스템에 대한 설계를 기술하고 V장에서는 실험결과를 제시하고 VI장에서는 결론을 맺는다.

2. 바이오인식에서 디지털 워터마킹

바이오인식에서의 워터마킹 기술은 아직까지 많은 연구가 진행되고 있지 않다. 대표적인 바이오인식에서의 워터마킹은 일종의 데이터 은닉의 개념에서 출발한다. 얼굴의 특징점 정보를 지문영상에 워터마크로 삽입한 연구가 있다. 지문의 특징점을 지문영상에 숨기는 방법도 제시하였다. 해당 연구에서는 사용자의 2가지 이상의 바이오정보를 상호 워터마킹 처리를 함으로써 해당 사용자에 대한 부인봉쇄 기능을 증가시켰다. 일반적으로 공개되어 있는 사진영상에 민감한 정보인 지문정보를 은닉시키는 의미 있는 연구였다.[11]

그보다 앞서 지문인식에서는 연성 워터마킹 기법을 이용하여 검증을 구현한 연구도 있다. 연성 워터마킹을 지문인식에 도입시켰을 때 인식률에 최소한의 영향을 미치도록 가능한 약하게 워터마킹을 삽입시키는 연구를 수행하였다.[12] 또한 얼굴에서 저작권 보호를 위한 강인한 워터마크를 제안하여 다양한 필터링과 JPEG 압축, 회전, 스케일링, 영상 훼손, 영상 절삭 등의 공격에서 강인한 결과를 보이는 알고리즘도 있다.[13] 최근에는 웨이블릿 기반의 워터마킹

방법을 이용하여 지문의 특징점 정보를 지문에 삽입하여 통신 채널에서 지문정보를 보호하는 알고리즘도 제안되었다. 웨이블릿을 이용하여 정보는 은닉하는 방법 중 이진영상의 은닉 및 복원을 위한 워터마킹 기법을 제안하고 바이오 정보의 은닉 및 복원을 위한 워터마킹 기법이 제안되었다.[14]

저작권 보호를 위해 멀티미디어 영상에 지문정보를 은닉시키기 위한 알고리즘의 연구가 진행되었다. 지문과 얼굴에서 워터마크 키를 이용하여 워터마킹된 영상에서의 추출한 키와 실제 삽입한 키와의 비교를 통한 개인의 인증 여부를 판단하는 알고리즘의 연구가 수행되었다. 네트워크 환경에서 얼굴 영상의 인증을 위해서 개인의 신원정보를 워터마크에 삽입하여 전송함으로써 보안을 강화하고 통신부하를 줄이기 위한 연구가 수행되었다. 얼굴, 지문 등 다양한 바이오인식을 위하여 워터마킹의 기법을 시도하는 연구가 제안되었다.[15-19]

3. 요구사항

본 논문에서 제안하는 워터마킹 기술은 얼굴과 지문영상을 대상으로 한다. 얼굴과 지문 영상의 개인을 구별하는 가장 대표적인 바이오정보로 주민등록증이나 여권, ID, 출입통제, 범죄기록조회 등 아주 다양한 분야에서 응용되고 있다. 제안하는 워터마킹 기술에 대한 응용 시나리오는 그림1과 같다.

시나리오의 첫 번째로 바이오정보의 획득은 다음과 같다. 얼굴정보는 신청자로부터 사진을 제출 받아 디지털스캐너를 통해 영상으로 획득되며 지문정보는 포터블 지문센서를 이용해 직접 획득된다. 획득된 바이오정보는 획득 일자가 워터마크 정보로 바로 삽입된 후 디지털 형식으로 압축, 저장된다. 얼굴영상의 경우 JPEG, 지문영상의 경우 WSQ 형식이다. 저장된 바이오 정보는 바이오 DB로 전송되어 저장된다. 저장된 바이오 정보는 여권이나 신용카드 등의 스마트카드DB로 전송되어지고 이는 다시 여권이나 신용카드가 사용될 때 바이오정보 DB와 비교되어 위, 변조를 감별해 낸다. 또한 바이오정보DB에 얼굴, 지문영상이 등록되고 배포될 때 워터마크를 추출하여 그 검출여부로 무결성을 검증한다. 같은 원리로 스마트카드 DB에 저장되어 있는 얼굴 및 지문영상도 워터마크를 검출하여 무결성을 검증할 수 있다.

제시되는 시나리오에 적용할 수 있도록 얼굴 및 지문영상에 대한 워터마킹 기술 개발 시 요구되는 사항을 정리하면 다음과 같다.

3.1 영상품질(Image Quality)

영상에 대한 워터마크 신호는 일종의 잡음이다. 따라서 워터마크가 삽입된 영상의 잡음이 삽입된 영상이라 말할 수 있다. 즉, 워터마크 삽입 후 원 영상의 왜곡 정도가 영상품질이다. 일반적으로 사람의 눈으로 잘 인지할 수 없는 정도라고 말할 수 있는데 평가척도로 PSNR(Peak Signal-to-Noise Ratio)를 사용하는데 일반적으로 워터마크 삽입 후 38dB 이상이면 품질을 만족한다고 판별한다. 하지만 원 영상의 형태가 JPEG이나 WSQ 같은 압축 형태라면 품질 평가 기준이 달라진다. 이는 압축 자체가 영상의 품질을 많이 손상시키기 때문이다.

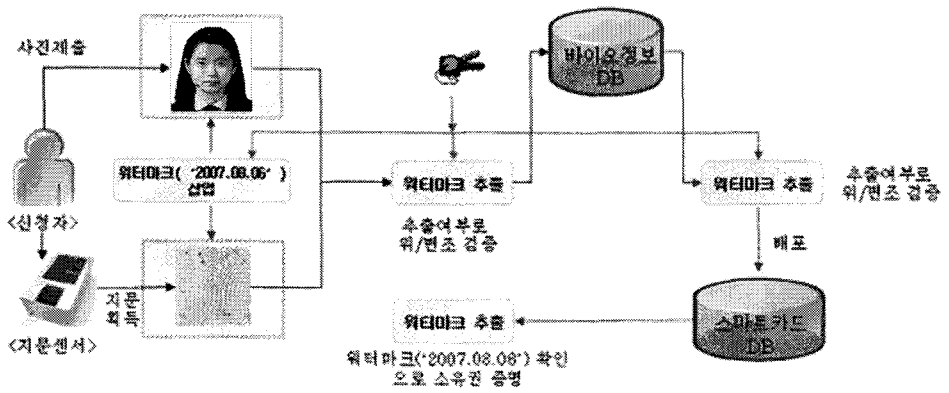


그림 1. 바이오정보 워터마킹 적용 시나리오

3.2 강인성(Robustness)

강인성은 워터마크가 삽입 된 영상이 노이즈 환경에 노출 된 후 워터마크가 검출될 확률이며 검출률이라고도 한다. 본 논문에서 요구되는 워터마크의 강인성은 압축에 대한 강인성이다. 얼굴이나 지문에 사용되는 압축방법인 JPEG, WSQ는 손실압축(Lossy compression)이기 때문에 그 자체가 삽입된 워터마크를 제거하려는 시도가 된다. 개발될 워터마크는 시나리오에서 요구하는 압축비(compression ratio)에 강인하도록 설계되어야 한다.

3.3 삽입량(Payload)

삽입량은 얼굴이나 지문영상 당 얼마의 워터마크 정보를 수용할 수 있는가를 나타내다. 제안된 시나리오에서는 영상이 획득된 날짜(년/월/일)가 워터마크로 삽입되어야 한다.

3.4 검출률(False negative alarm)

검출률은 삽입 된 워터마크에 대해 얼마나 정확히 검출해 낼 수 있느냐를 나타내는 비율로 워터마크를 삽입한 총 영상에 대해 검출이 성공한 영상의 수를 백분율로 나타낸 것이다. 본 시나리오에서는 100% 검출률을 지원하는 것을 가정으로 한다.

3.5 오검출류(False positive alarm)

오검출률은 워터마크가 삽입되지 않은 영상에 대해 워터마크가 있다고 판별할 확률이다. 시나리오상 위, 변조 된 바이오정보를 제대로 검출하기 위해서는 오검출률이 10^{-12}% 이하로 매우 낮아야 한다.

제약조건으로 얼굴영상의 형식은 320×240, Color, 24 bits, JPEG압축(15KB 이하)이고 지문영상의 형식은 400×450, Gray, 8 bits, WSQ압축(15KB 이하)로 한정한다. 워터마크 삽입 후의 영상의 크기는 공통으로 15KByte 이하로 유지되어야 하며 이에 따른 평균 압축비는 각각 15:1(226K/15K), 11.8:1(177K/15K)이다. 강인성은 압축만 고려한다. 워터마킹 삽입 모듈은 워터마크를 삽입 한 후 15Kbyte 이하로 압축한 후 저장해야 한다. 다음 장에서는 제약조건 하에서 위에서 제시한 요구사항을 만족하는 워터마킹 시스템에 대해 설명한다.

4. 워터마킹 시스템

제안하는 워터마킹 시스템은 전자신분증용 지문, 얼굴 영상을 획득한 이후, 품질 확인을 거쳐서 보정 불가인 바이오정보는 재획득하며 보정 가능한 영상은 보정을 하여 정상 영상을 획득한다.

그림 2와 같이 정상적인 지문, 얼굴영상에 소유기관을 명시하기 위해 워터마킹을 수행하고 지문은 WSQ와 얼굴은 JPEG 압축을 수행한다. 압축된 영상으로부터 워터마크 추출을 한 후 추출된 바이오영상에 대하여 전자신분증으로 발급된다.

워터마킹 시스템은 크게 삽입 모듈과 추출 모듈로 구성된다. 삽입모듈에 대한 블록다이어그램이 그림 3에 나타나 있다. 삽입과정은 크게 영상의 휘도(Luminance)부분을 취하는 부분과 영상의 HVS(Human Visual System)를 계산하는 부분, 날짜 형태의 워터마크를 휘도 영역에 삽입 가능한 랜덤시퀀스(Random Sequence)신호로 바꿔주는 메시지 변환 부분으로 구성된다. 메시지 변환에 사용되는 키(Key)는 유일한랜덤시퀀스를 발생시켜주도록 하는 시드(seed)이며 추출 시에도 사용된다. 워터마크 신호가 같더라도 이 시드 값이 다르면 실제 다른 워터마크가 삽입된다. 키에 의해 생성된 랜덤시퀀스는 단위블록 형태가 되고 이 블록이 영상의 크기에 맞게 반복되어 삽입된다. 320×240의 얼굴 영상의 경우 워

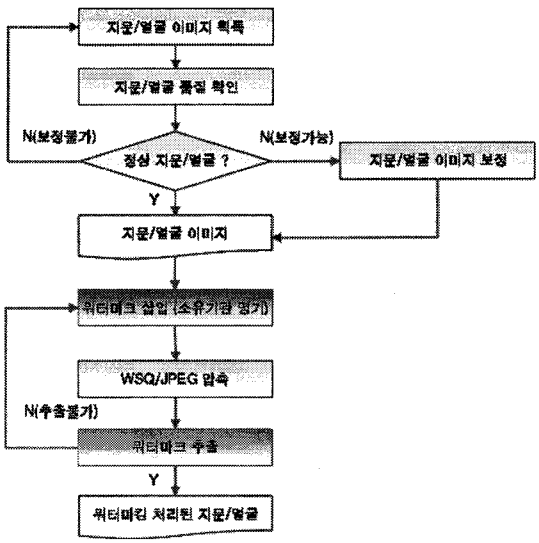


그림 2. 바인지 워터마킹 수행과정

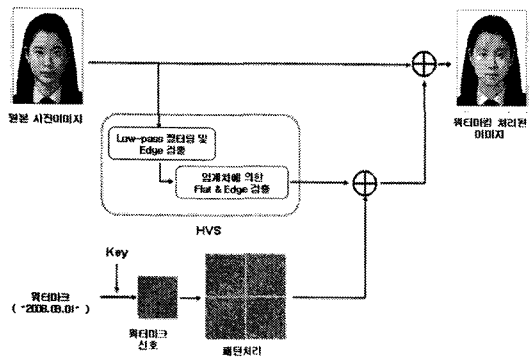


그림 3. 워터마킹 삽입

터마크 신호에 대한 단위블록의 크기는 120×160이며 이 블록이 4번 반복 삽입된다. 지문영상의 경우 같은 원리로 단위블록의 크기는 200×225이다.

HVS(Human Visual System) 함수는 워터마크가 삽입된 영상의 품질과 동시에 강인성을 결정하는 중요한 부분으로 랜덤시퀀스 형태의 워터마크 신호를 영상의 특성을 고려하여 스케일링(scaling)하는 역할을 한다.

4.1 워터마크 설계

워터마크의 구조는 그림 4와 같으며, 본 알고리즘에서는 날짜 정보를 입력으로 받아 들여 4 bytes 워터마크 신호를 생성한다. 년, 월, 일 정보는 아래와 같은 매핑테이블을 이용하여 2 byte 의 공간 안으로 재배치된다. 나머지 2 byte는 년, 월, 일의 2byte 워터마크에 대한 16 bits CRC 값이다.

최종적으로 생성되는 4 bytes 워터마크 정보는 아래와 같다.

4.2 메시지 변환(Message Modulation)

메시지 변환은 얼굴, 지문 영상의 크기를 고려할 때 많은 정보의 워터마크를 삽입하기 어렵기 때문에 4 bytes로 한정하였으며 상위 2 byte는 생성일자를 7 bits, 월은 4 bits, 일자는 5 bits로 표현하였다. 하위 2 bytes는 워터마크 추출하는 경우 생성일자의 정합

표 1. 워터마크 매핑테이블

년도	비트값
2007	0000000
2008	0000001
2009	0000010
2010	0000011
2011	0000100
2012	0000101
:	:
2135	1111111

월	비트값
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	1010
11	1011
12	1100

일	비트값	일	비트값
1	00001	17	10001
2	00010	18	10010
3	00011	19	10011
4	00100	20	10100
5	00101	21	10101
6	00110	22	10110
7	00111	23	10111
8	01000	24	11000
9	01001	25	11001
10	01010	26	11010
11	01011	27	11011
12	01100	28	11100
13	01101	29	11101
14	01110	30	11110
15	01111	31	11111
16	10000		

을 검증하기 위해 CRC(Cyclic Redundancy Checking)로 사용하게 된다. 본 메시지 변환과정은 4 bytes를 얼굴, 지문영상에 삽입이전에 수행한다.

생성된 4 bytes 워터마크는 실제 영상에 잡음의 형태로 더해져야 하는데 이를 위해 랜덤시퀀스로 변환하는 과정이 필요하다. 이 과정이 메시지 변환과정으로 주어진 키를 사용하여 4 byte 워터마크 신호를 단위블록 크기의 2차원 랜덤시퀀스로 바꾸어 준다. 첫째로 4 byte를 표현하기 위해 +1, -1로 구성된 4개의 서로 직교하는 2차원 랜덤시퀀스가 생성된다. 각각의 시퀀스는 주어진 키에 의해 4개의 서브키가 만들어지고 각각의 서브키로부터 단위블록 길이로 생성된다. 다음으로 생성된 랜덤시퀀스는 각 byte의 값에 따라 환상 쉬프트 된다.

각 바이트의 표현 범위가 0부터 255까지이므로 단위블록 길이의 2차원 랜덤시퀀스는 표 1과 같이 16×16의 서브블록으로 논리적 분할이 이루어진다. 그 후 해당 서브 블록의 위치로 시퀀스가 환상쉬프트 된다. 바이트의 값이 블록의 위치로 표현되는 것이다. 이렇게

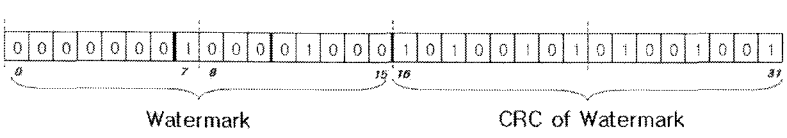


그림 4. 워터마크 구조

표현된 4장의 2차원 랜덤시퀀스는 최종적으로 합해져 그 사인(sign)값만 다시 취해진다. 최종적으로 4개의 신호를 포함한 1개의 2차원 랜덤시퀀스가 생성된다.

4.3 키 정의

랜덤 시퀀스를 발생시키는 키(Key)는 램덤 넘버 생성기의 입력으로 시드(Seed) 넘버로 이용된다. 시드 넘버는 32bits로 그 범위는 0 부터 4294967295 까지 이다. 삽입 시 사용했던 키를 추출 시에 같이 사용해야만 추출이 가능하다. 기본적으로 워터마크 입력이 같더라도 할당된 키가 다르면 다른 정보가 워터마크로 삽입된다.

4.4 육안 인지 시스템(HVS : Human Visual System)

HVS는 워터마크를 삽입하는 데 있어 강하게 삽입하면서 비가성(im-perceptibility)을 유지하는 기술이다. 영상의 품질만을 우선시 한다면 영상 전반에 아주 약하게 삽입하는 방법이 사용되지만 어느 정도 왜곡에 대한 강인성을 고려한다면 가능한 한 강하게 삽입해야 한다. HVS는 영상의 어느 부분에 강하게 삽입해도 되는지를 알려 주는 함수이다. HVS의 기본 원리는 베버의 법칙(weber's law)을 근거로 한다. 베버의 법칙은 자극이 약할 때에는 다음의 자극이 조금만 강해도 자극의 변화를 느낄 수 있으나, 처음의 자극이 강한 경우에는 약할 때의 증가율에 비례하여 상당히 큰 자극이 가해져야 자극의 크기 변화를 느낄 수 있다는 것이다. 영상에서 베버의 법칙을 살펴보면, 사람의 눈이 지각할 수 있는 영상상의 작은 변화량은 주변픽셀에 따라 달라진다는 법칙으로 같은 변화량이라도 주변 값에 따라 눈에 띄지 않을 수 있다는 것을 내포한다. 일반적인 HVS 모델은 주변 값들에 대한 관계로 나타내어 질 수 있는데 통계적 계산치인 주변 값과의 표준편차를 주로 이용하며, 그림5와 같다. 즉, 주변 픽셀과의 편차가 작은 평면(flat) 영역에는 편차 값에 비례하여 작고 약하게 삽입되는 반면 편차 값이 큰 edge 또는 texture영역에는 강하게 삽입된다.

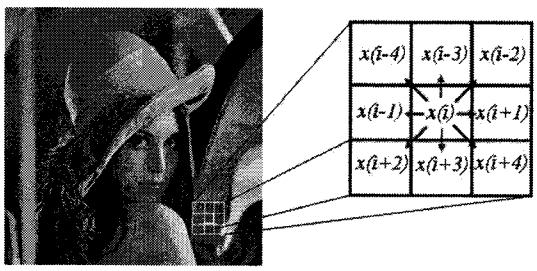


그림 5. 주변값에 대한 평균과 분산

HVS를 계산하기 위해서는 첫 번째로 주변 값들과의 평균과 표준편차를 계산하여야 한다. 위의 그림은 3×3 마스크를 이용하여 평균과 표준편차를 계산하는 과정을 보여주고 있다. 그 계산식은 아래와 같다.

$$Aver(i,\ j) = \frac{1}{9}\sum_{+4}^{i=-4} x(i)$$

$$StD(i,\ j) = \frac{1}{8}\sum_{+4}^{k=-4} |x(i)-x(i-k)| \qquad (1)$$

Aver(i,j)는 mask내의 평균값이고 StD(i,j)는 주변 값들과의 차를 평균한 것이다. 여기서 계산된 StD(i,j)가 본 기술에서 사용하는 HVS의 기본 값으로 사용된다. 두 번째는 영상을 flat 영역과 strong edge 영역, texture 영역으로 구별하여야 한다.

$$x(i,j)\begin{cases}\text{Flat} & \text{If StD}(i,\ j)\le 2\\ \text{Strong edge} & \text{If Edge}(i,\ j)>\text{Aver}(E)+2*\text{StD}(E)\\ \text{Texture} & \text{If StD}(i,\ j)>2\end{cases} \qquad (2)$$

구별 조건은 위와 같으며, strong edge의 구별 조건은 prewitt 필터의 결과 값을 Edge(i,j)라 할 때 Edge(i,j)값이 정해진 threshold값을 넘으면 strong edge라 정의하였다. Threshold는 위의 식과 같으며 Aver(E)는 Edge(i,j)의 평균, StD(E)는 Edge(i,j)의 표준편차를 나타낸다. 위와 같이 영상을 구분하는 이유는 각각 삽입강도를 다르게 하기 위함이다. 마지막으로 본 HVS기술에서는 어두운 영역과 아주 밝은 영역에 삽입의 가중치를 두기 위하여 가중함수(Weighted function)를 아래와 같이 사용한다. 일반적으로 아주 어둡거나 아주 밝은 영역은 시각이 덜 민감한 것으로 알려져 있다. 가중함수, WF(Aver(i, j))는 다음과 같다.

$$WF(Aver(i,\ j)) = 2 - \tanh(i/25),\ i = [0i \mid 255] \qquad (3)$$

위에서 정의된 가중함수는 픽셀의 평균값, Aver(i,j)에 의해 결정된다. 즉, Aver(i,j)가 작은 값이면 어두운 영역이므로 1과 2사이의 가중치를 적용한

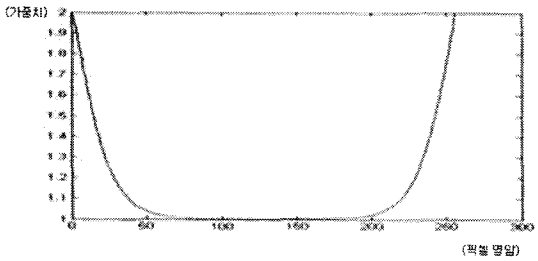


그림 6. 가중함수

다. 반대로 큰 경우에도 1과 2사이의 가중치를 같게 적용한다.

가중함수의 응답은 그림 6과 같다. 가중치의 범위는 1과 2사이이고 Aver(i,j)가 0이나 255로 가까이 갈수록 2값에 가까운 가중치를 출력한다. 본 논문에서 사용하는 HVS는 아래와 같다.

$$HVS(i,j)\begin{cases} k & \text{If } x(i,j) \text{ is Flator Strong edge} \\ StD(i,j)*WF(Aver(i,j)) & \text{Otherwise} \end{cases} \quad (4)$$

k는 상수이며 2로 정의되어 있다. k는 HVS의 최소치로 삽입강도나 영상의 종류에 따라 달리 정의될 수 있다. 그림 7은 본 논문에서 사용한 HVS 모델로 삽입강도를 계산한 그림이다. 회색부분은 k로 계산된 부분이고 흰색 부분이 StD(i,j)에 따라 강하게 삽입되는 부분이다.

4.5 최적삽입강도 추정

본 시나리오의 요구 조건 중 검출률의 조건은 100%이었다. 즉 워터마크가 삽입 된 영상에서는 모두 검출해야 한다. 이를 만족시키기 위해 삽입 시 미리 검출을 시도해 검출이 성공하는 삽입 강도를 선택하는 방법을 사용하였다. 제안한 워터마크 삽입 알고리즘은 워터마크 삽입 강도를 조절할 수 있는 삽입 강도가 입력으로 주어지며 그 범위는 1부터 10까지이다. 강도 1은 약하게 삽입한다는 의미로 비인지적인 특성을 포함하고 있다. 반대로 강도 10은 강하게 삽입하는 경우로 왜곡의 정도가 사람의 눈에 인지할 정도이지만 여러 가지 워터마크를 제거하려는 공격에 강인하게 된다. 따라서 삽입강도가 높을수록 검출될 확률이 높아진다. 하지만, 강도가 높으면 영상의 품질이 문제될 수 있고 또한 시나리오의 요구 사항인 위, 변조를 검증함에 있어 어느 정도의 위, 변조에도 삽입된 워터마크가 검출될 확률이 있다. 따라서 단순히 압축에 대해서만 강인성을 가지며 100% 검출을 보장하는 최소 삽입강도를 추정해야 한다. 본 알고리즘은 이 추정 과정을 삽입 시에 진행한다. 본 논문에서는 제안하는 방식은 다음과 같다. 삽입 시 최소 삽입 강도 1에서 삽입하고 바로 워터마크를 검출해 본다. 검출이 성공하면 강도 1로 워터마크가 삽입된 영상을 저장한다. 검출이 실패하면 삽입 강도를 하나 증가시켜 삽입하고 다시 추출을 시도한다. 검출이 성공하면 영상을 저장하고 실패하면 이 과정을 반복한다. 위와 같은 삽입 과정으로 워터마크가 삽입된 얼굴 및 지문 영상에 대해 검출률 100%의 결과를 얻을 수 있었다.

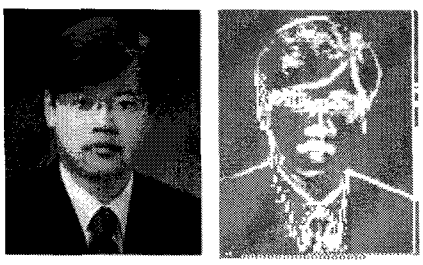


그림 7. HVS에 의한 삽입

4.6 워터마크 추출

본 장에서는 삽입된 워터마크를 추출하는 과정을 그림 8과 같이 설명한다. 본 기술은 원본 없이 워터마킹 된 영상에서 바로 추출할 수 있는 기술을 제공하며 추출 과정은 크게 원본추정 과정과 역 변환의 2가지 요소기술로 구분할 수 있다.

4.7 원본예측(Original Estimation)

원본예측기술은 노이즈와 같은 워터마크 신호를 영상에서 분리하는 기술로 일반적으로 노이즈 제거 필터를 사용한다. 노이즈 제거 필터에 의해 제거된

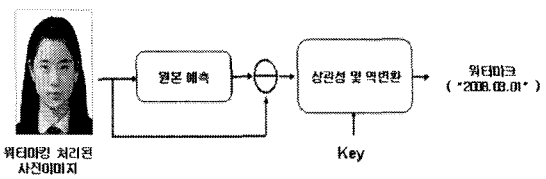


그림 8. 워터마크 추출

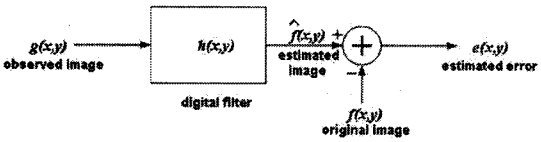


그림 9. 위너필터링

노이즈에는 삽입한 핑거프린트 신호가 많이 포함되어 있다고 가정한다. 본 기술에서는 그림 9와 같이 적응 위너(Adaptive Wiener) 필터를 사용하였다.

위너필터는 입력을 원하는 출력과 가능한 한 매우 근사하게 변환시켜주는 필터로써, 여기서 '가능한 한 매우 근사하게'의 의미는 필터 출력과 원하는 결과의 차의 제곱의 합이 최소가 된다는 의미이다. 위의 그림에서 e(x,y)가 최소가 되는 h(x,y)를 위너 필터라 한다. 본 기술에서 사용하는 위너필터의 수식은 아래와 같다. 아래의 수식은 Lee필터라고도 하며 픽셀의 지역적인 특성을 이용하여 노이즈를 제거한다.

$$\therefore f'(n_1,n_2) = \hat{m}_f(n_1,n_2) + \frac{\hat{\sigma}_f^2(n_1,n_2)}{\hat{\sigma}_f^2(n_1,n_2)+\sigma_v^2}(g(n_1,n_2)-\hat{m}_f(n_1,n_2)) \tag{5}$$

$$\hat{m}_f = \frac{1}{(2M+1)^2}\sum_{k_1=n_1-M}^{n_1+M}\sum_{k_2=n_2-M}^{n_2+M} g(k_1,k_2), \tag{6}$$

$$\hat{\sigma}_f^2 = \frac{1}{(2M+1)^2}\sum_{k_1=n_1-M}^{n_1+M}\sum_{k_2=n_2-M}^{n_2+M}(g(k_1,k_2)-\hat{m}_f(n_1,n_2))^2 \tag{7}$$

m_f는 주변 값들과의 평균을 나타내고 σ_f^2는 주변 값들과의 분산, σ_v^2은 noise의 분산을 나타낸다. 위너필터의 성능은 m_f, σ_f^2, σ_v^2 값을 어떻게 추정하느냐에 달려 있다. 본 논문에서는 m_f, σ_f^2값을 추정하기 위하여 3×3 마스크를 이용하였으며 noise의 분산은 3×3 마스크내의 지역분산들의 평균을 사용하였다.

그림 10은 위너필터를 이용하여 워터마크를 추출한 예이다. 좌측그림은 워터마크가 삽입된 그림이며, 우측 그림은 위너필터를 사용하여 원본을 예측한 후, 실제 삽입한 워터마크와 비교하여 같으면 흑색으로, 틀리면 백색으로 표시한 그림이다. 본 필터에서 사용한 노이즈 차이는 93.7이었으며 원래 삽입한 워터마크 신호, {+1, -1}와의 일치율은 72%를 나타내었다.

그림 10. 위너필터를 이용한 원본예측

4.8 상호상관도와 메시지 역변환

상호상관도(cross correlation)는 두 신호간의 유사한 정도를 추정하는 표준 방법이다. $x(i), y(i)$라는 두 1차원 신호가 있다고 가정할 때 delay d에서의 유사도 r은 다음과 같은 식에 의해 계산된다.

$$r(d) = \frac{\sum_i[(x(i)-mx)*(y(i-d)-my)]}{\sqrt{\sum_i(x(i)-mx)^2}\sqrt{\sum_i(y(i-d)-my)^2}} \tag{8}$$

여기서 mx와 my는 각 신호의 평균을 의미한다. 신호 $x(i)$에 대해 신호 $y(i)$를 $d=0,1,2,\cdots,N-1$ 만큼씩 이동해 가면서 각 d 거리에서의 두 신호의 유사도를 계산할 수 있다.

간단한 예로 그림 11에서 신호 $x(i)$와 신호 $y(i)$의 delay에 따른 유사도를 살펴보면, $y(i)$가 3만큼 delay 되었을 경우에 두 신호의 유사도가 정확히 1이 되어 일치함을 알 수 있다.

2차원 영상에서 마스크를 이용해서 원 영상과의 상호상관도를 계산하는 방법을 아래 그림 12에 나타내었다. 마스크를 (0, 0) 위치에서부터 한 픽셀씩 오른쪽으로 이동해 가면서 마스크 상의 영상과의 유사도를 측정할 수 있다. 이러한 방법은 워터마킹에서 메시지 추출 시 사용되는 방법이기도 하다.

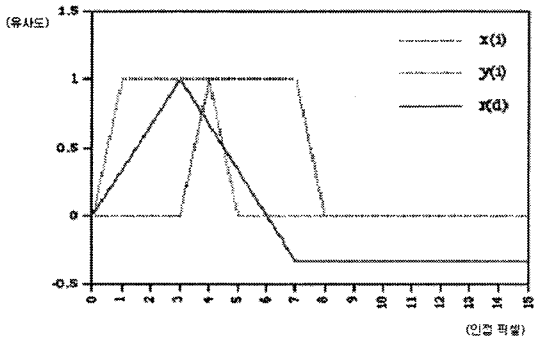


그림 11. 두 신호 간의 상호상관도

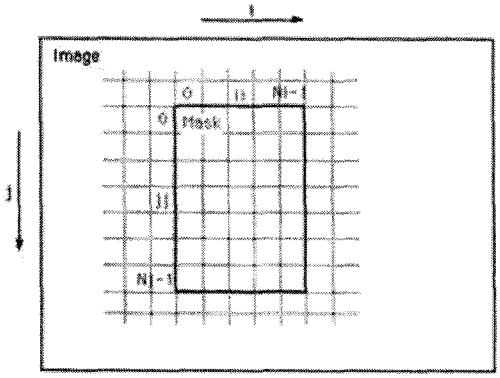


그림 12. 2차원 신호에서의 상호상관도

일반적으로 2차원 신호에 대한 상호상관도 함수는 상당한 계산 복잡도를 가지고 있다. 따라서 속도 개선을 위해 주파수 영역에서 아래의 식을 이용하여 계산한다.

$$f \otimes g = \frac{IFFT[FFT(f) \times FFT(g)^*]}{M \times N} \quad (9)$$

$\otimes : convolution, ^* : conjugate\ operation$

제안한 워터마킹 알고리즘에서는 위식을 이용해 상호상관계수를 구한 다음 계수들에서 최고값의 위치를 추출된 워터마크로 간주한다. 삽입 시 워터마크의 값에 따라 환상쉬프트가 이루어진 2차원 랜덤 시퀀스는 환상쉬프트가 이루어지지 않은 시퀀스와 상호상관계수를 구할 경우 그 피크의 위치가 쉬프트한 서브블록의 위치가 된다. 따라서 피크가 나타난 서브블록의 인덱스가 워터마크 신호이다. 이렇게 4 byte를 모두 추출한 후 처음 2 바이트의 16 bits CRC를 계산한다. 계산한 CRC 값은 뒤의 2 바이트와 일치했을 경우에만 최종 워터마크가 추출 된 것이라 간주한다.

5. 실 험

본 논문에서는 바이오영상에 대한 워터마킹 후 인식률 변화율에 대한 성능 실험을 수행하였다. 그림 13에 워터마크와 인식률에 대한 실험방법을 나타내었다. 지문, 사진영상을 40명을 대상으로 5회씩 획득하여 200개를 대상으로 바이오정보에 대하여 압축 이후 워터마크 삽입, 추출을 한 후 바이오인식률에 대한 변화율을 실험평가 하였다.

항목	영상 픽셀 크기	파일 크기	대상수	기타
얼굴	320*240	226K	200	사진정보
지문	400*450	176K	200	Live 스캐너

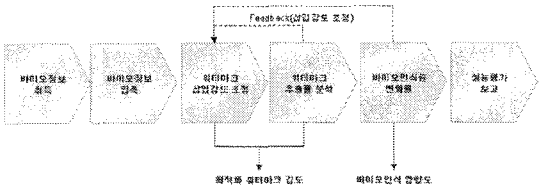


그림 13. 워터마크와 바이오인식률 성능평가

그림 14는 워터마크 처리된 얼굴영상의 인식률 변화량을 나타내었다. 본 실험은 인식률은 알고리즘에서 정의하는 임계치 수치로 0~2까지 조정이 가능하며 0으로 근접할수록 본인인식이 가능하다. Distance는 본 실험에서 사용된 얼굴인식 알고리즘은 두 얼굴영상의 차를 통해 인식률을 결정하게 되며 임계치가 0.8 이상인 경우 본인임에도 타인으로 인식하게 된다. 워터마크 처치된 총 200개의 얼굴영상 중 2%가 얼굴인식에 영향을 미쳤다. 본 실험결과를 볼 때 얼굴인식에서는 원본영상의 변화에 따라서 민감하게 반응하는 결과를 나타내었다.

그림 15와 워터마크 처리된 지문영상의 인식률 변화량을 나타내었다. 본 실험은 인식률은 알고리즘에서 정의하는 임계치 수치로 0~1까지 조정이 가능하며 1에 가까울수록 본인인식이 높아지게 되며 매칭값은 본 실험에서 사용된 지문인식 알고리즘은 임계치가 0.8 미만인 경우 본인임에도 타인으로 인식하게 된다.

본 실험을 통해 워터마킹 처리된 사진, 지문 영상이 원본 영상과 비교하여 인식률에 큰 차이가 나지

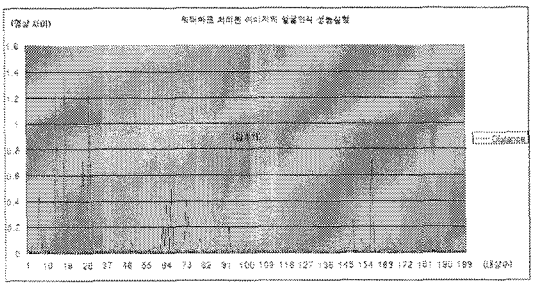


그림 14. 얼굴영상 성능실험

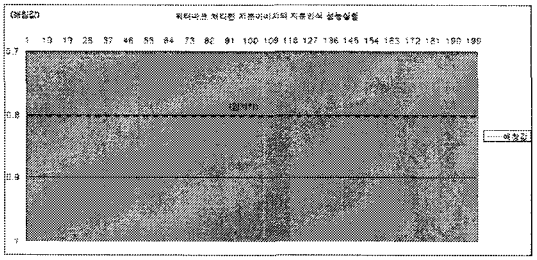


그림 15. 지문영상 성능실험

않았으며 지문의 경우는 인식률에 미치는 변화가 미비함을 나타내었다.

6. 결 론

본 논문에서는 얼굴 및 지문영상에 대하여 비인지 워터마크를 삽입하고 추출하는 알고리즘을 제안했다. 워터마크는 바이오정보가 획득일자와 CRC와 함께 총 4 byte로 구성된다. 4 byte의 워터마크는 실제 영상에 더해지기 위해 랜덤시퀀스로 변환되며 각 바이트의 값에 비례하여 환상쉬프트 시킨 값 4개를 모두 더해 최종적으로 더해질 워터마크 신호를 얻는다. 추출은 위너필터를 이용하여 원본영상을 추정하는 단계와 상호상관함수를 이용하여 메시지를 디코딩하는 단계가 있다. 삽입 시 행했던 환상쉬프트 연산은 삽입하는 워터마크 값의 위치로 상호상관계수 중 최대값을 쉬프트 시키는 효과가 있다. 최대값의 위치가 삽입된 워터마크 값이다. 얼굴 및 지문 영상은 JPEG이나 WSQ 같은 압축 포맷으로 저장되기 때문에 워터마크 삽입 시 압축에 강인하면서 최소의 강도로 삽입할 수 있도록 제안하였다. 본 논문에서는 전자신분증용 바이오영상을 대상으로 삽입 모듈에서 추출 과정을 실시해 그 추출을 검증하는 과정을 이용하여 최적 강도를 추정하였으며 인식률에 영향이 미치지 않는 성능실험을 수행하였다.

본 논문에서 제안하는 바이오영상에 대한 비인지 워터마킹은 소유기관의 책임추적성과 원본 영상의 무결성을 제공함으로써 바이오정보의 개인 개인정보 보호를 위한 기술로 활용이 가능하다.

참 고 문 헌

[1] I.J. Cox, Joe Kilian, T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. on Image Processing*, Vol.6, No.12, pp. 1673-1687, 1997.

[2] C.Y Lin, M. Wu, J.A. Bloom, I. J. Cox, M. L. Miller and Y. M. Lui, "Rotation, scale, and translation resilient watermarking for images," *IEEE Trans. on Image Processing*, Vol.10, No.5, 2001.

[3] J.J.K., O R. and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Processing*, Vol.66. No.3, pp. 303-317, 1998.

[4] D.J. Fleet and D.J. Heeger, "Embedding invisible information in color images," *Proceeding of ICIP'97*, IEEE Int. Conf. Image Processing, Santa Barbara, CA, 1997.

[5] R.B. Wolfgang and E.J. Delp, "Fragile watermarking using the VW2D watermark," *Proceeding of Electronics Imaging'99*, Vol. 3657, San Jose, CA, 1999.

[6] M. kutter and F.A.P. Petitcolas, "A fair benchmark for image watermarking systems," *proceeding of Electronic Imageing'99*, Security and Watermarking of Multimedia Contents, Vol.3657, San Jose, CA, pp. 226-239, 1999.

[7] G. Depovere, T. Kalker and J.P. Linnartz, "Improved watermark detection using filtering before correlation," *Proceeding of IEEE ICIP'98*, Vol. I, Chicago, IL, pp. 430-434, 1988.

[8] R.G. van Schyndel., "A digital watermark," *Proceeding of ICIP'94*, Vol.2, Austin, TX, pp. 86-90, 1994.

[9] A. Hanjalic., "Image and video databases: restoration, watermarking and retrieval Advances in Image Communications," *New York"Elsevier Science*, Vol.8. 2000.

[10] C.E. Shannon and W.W. Weaver, *The Mathematical Theory of Communications*, Urbana, IL: Univ. of Illinoise Press, 1949.

[11] A. K. Jain, U. Uludag and R.L Hsu, "Hiding

a Face in a Fingerprint Imge," *International Conference on Pattern Recognition*, Vol.3, pp. 756-759, Quebec City, Quebec, Canada, 2002.

[12] S. Pankanti, M. and M. Yeung, "Verification Watermarks on Fingerprint Recognition and Retrieval," *Proc. SPIE*, Vol.3657, pp. 6-78, 1999.

[13] Tzouveli, P., Ntalianis, K. and Kollias, S., "Human face watermarking based on zernike moments," *Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology*, pp. 399-404, 2005.

[14] Zebbiche, K., Ghouti, L., Khelifi, F. and Bouridane, A., "Protecting Fingerprint Data Using Watermarking," *First NASA/ESA Conference on Adaptive Hardware and Systems*, pp. 451-456, 2006.

[15] B. Gunsel, U. Uludag, and A.M. Tekalp, "Robust Watermarking of Fingerprint Images," *Pattern Recognition*, Vol.35, No.12, pp. 2739-2747, 2002.

[16] S, Jain, "Digital Watermarking Techniques: A Case Study in Fingerprints and Faces," *Proc. Indian Conference of Computer Vision, Graphics, and Image Processing*, pp. 139-144, 2000.

[17] Shang-Lin Hsieh, Hsuan-Chieh Huang and Tsai, I.-J, "A Copyright Protection Scheme for Gray-Level Images Using Human Fingerprint," *The Third International Conference on Information Technology: New Generations*, pp. 482-489, 2006.

[18] Hashimoto, M. and Nakamura, O., "Personal identification based on both facial images and watermarking techniques in network environment," *Canadian Conference on Electrical and Computer Engineering*, Vol.2, pp. 1029-1033, 2005.

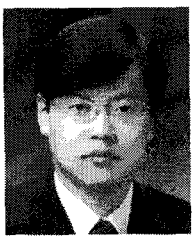
[19] Vatsa, M., Singh, R., Mitra, P. and Noore, A., "Digital watermarking based secure multimodal biometric system," *IEEE Conference on Systems, Man and Cybernetics*, Vol.3, pp. 2983-2987, 2004.

신 용 녀

1999년 2월 숭실대학교 컴퓨터학과 학사
2001년 9월 고려대학교 컴퓨터학과 석사
2008년 2월 고려대학교 컴퓨터학과 박사
2002년 1월~현재 한국정보보호진흥원 산업지원팀 주임연구원
2005년~현재 TTA PG505(바이오인식프로젝트 그룹) 간사
관심분야 : 프라이버시보호, 바이오인식, 정형기법

이 용 준

1999년 2월 강남대학교 전자계산학과 학사
2001년 2월숭실대학교 컴퓨터학과 석사
2005년 2월 숭실대학교 컴퓨터학과 박사
2006년 9월~현재 LG CNS 기술연구부문 부책임연구원
관심분야 : 정보보호, 바이오인식



김 원 겸

1992년 2월 충남대학교 전산학과(학사)
1994년 2월 충남대학교 전산학과(석사)
2001년 2월 충남대학교 컴퓨터과학과(박사)
1995년 2월~1997년 7월 LG반도체㈜ 생산기술연구소 주임연구원
2002년 2월~2007년 1월 한국전자통신연구원 디지털콘텐츠연구단 선임연구원
2007년 3월~현재 마크애니(주) 수석연구원
관심분야 : 이미지/오디오 신호처리, DRM, 디지털 워터마킹, 디지털 펑거프린팅