# 생체정보보호를 위한 워터마킹 기법

김여진° 안정호 변혜란
연세대학교 컴퓨터과학과
{naiad6°, jungho, hrbyun}@cs.yonsei.ac.kr

# Watermarking for Bio Information Security

Yeojin Kim° Jungho Ahn H.K. Hyeran Byun
Dept. of Computer Science, Yonsei University

**요 약**

생체 정보를 도용하기 어렵다는 장점에도 불구하고 생체 인증시스템이 그 자체로 안전한 것은 아니다. 생체정보를 위조하기는 어렵지만 손상되기는 쉽기 때문이다. 본 논문은 생체 정보로부터 생성된 초기값을 이용하여 생체정보의 무결성을 보장하는 생체 인증시스템을 제안한다. 실험 결과 카드 소유자를 소유자로 인식한 확률은 최적 파라미터 하에서 약 96%정도였으며, 비소유자를 소유자로 오인한 확률은 0%였다. 학습에 참여한 비소유자 뿐만 아니라, 학습에 참여하지 않은 비소유자도 100% 기각을 하여 소유자 검증에 높은 신뢰도를 보였다.

## 1. 서 론

현재 생체 인식 연구 분야에서는 생체 인식률을 높이기 위해 수많은 연구가 이루어지고 있다. 그러나 생체 인식 정보 보호에 대한 연구는 미비한 실정이다. 워터마킹 기법은 멀티미디어 데이터의 저작권 및 소유권을 보장하기 위해 주로 사용되었다. 최근 생체 정보 보호를 위하여 워터마킹을 적용하는 시도가 이루어지고 있으며 Jain과 Uludag[1]은 얼굴 이미지와 지문 이미지를 보호하는 워터마킹 기법을 소개하였다. 또한 Wu와 Kuo[2]는 음성 신호의 무결성을 보장하는 워터마킹 연구를 수행하였다. 워터마킹에서 비가시성 및 비가청성은 데이터의 최종 사용자가 인간이라는 측면에서 매우 중요하다. 그러나 우리는 워터마킹된 데이터의 최종 사용자로서 하나의 시스템을 고려할 수 있다. 시스템은 워터마크된 데이터의 비가시성이나 비가청성 대신 실행가능성을 요구한다.

일반적인 생체인증시스템은 중앙 데이터베이스에 인식정보를 저장한다. 만약 데이터베이스의 보안이 비밀번호나 개인인증번호와 같은 어떤 보안키에 의존한다면 그 정보가 유출될 가능성이 있다. 이러한 키들이 어떤 방식으로든 도난당할 경우 데이터베이스를 변경해야만 한다. 이러한 취약점을 극복하기 위해서 우리는 생체인증시스템을 위한 공간 워터마킹 기법을 제안한다. 이 기법이 적용된 생체 데이터베이스는 도난당하더라도 불법 사용자가 정확한 인식 정보를 획득하는 것은 불가능에 가깝다.

## 2. 생체 인증 시스템 모델

제안된 인증 시스템은 시드 생성, 생체 데이터베이스 구성, 검증의 세단계로 이루어진다. 우리는 일반적인 모델로 멀티 모달 인증 시스템을 다룬다.

### 2.1 시드 생성

워터마크 키 생성을 위한 시드는 이중시드구조를 통해 생성된다. 일반적인 모델은 다음과 같다. 우선, 저작권 및 소유권에 기반 한 두 개의 PN-시퀀스를 생성한다[3]. 우리는 생체 정보로부터 적절한 특징추출 기법을 이용하여 특징을 추출하고 d-차원의 생체인식정보를 얻는다. 각 차원에 대한 특징의 평균 및 분산을 이용하여 100%에 가까운 신뢰구간을 찾는다. 각 차원에서 하나의 특징 값이 해당 신뢰구간에 속하면 정확한 시드를 얻을 수 있다. 그림 1과 같은 방법으로 미리 생성된 두 개의 PN-시퀀스를 결합하여 시드를 생성한다.

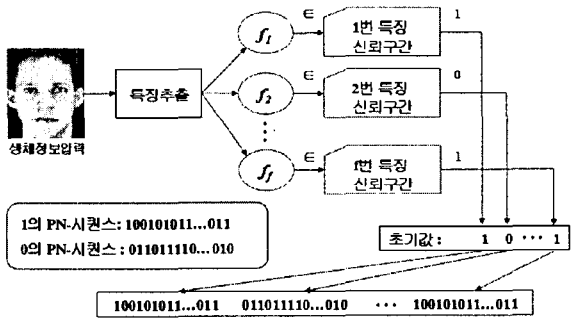


그림 1. 워터마크 키 생성을 위한 시드 생성

### 2.2 생체 데이터베이스의 구성

일반적으로 멀터 모달 인증시스템을 구축하기 위해서, 두 개의 다른 생체정보로부터 특징을 추출하고 학습하여 각각의 생체인식기를 생성한다. 이 두 생체인식기정보는 앞서 소유자의 저작권 및 소유권을 바탕으로 구한 시드를 이용하여 결합된다. 즉, 하나의 생체 인식기 정보에 다른 생체 인식기정보가 워터마크로 삽입된다. 유니 모달 인증시스템의 경우, 다른 하나의 생체인식기정보 대신 랜덤 데이터를 이용하여 워터마킹한다. 그림 2는 데이터베이스 구성을 보여준다.

### 2.3 검증 단계

검증은 다음의 순서로 이루어진다. 1) 소유자의 생체정보 입력 2) 전처리된 데이터로부터 특징 추출 3) 지정된 생체정보로부터 생성된 시드를 기반으로 보안키 생성 4) 보안키를 이용하여 메모리에 저장된 데이터에서 두 개의 생체정보인식기 분리 5) 분리된 인식기를 이용하여 소유자 검증. 그림 3은 실시간으로 입력된 생체정보를 이용하여 인식기를 분리한 뒤 검증하는 단계를 보여준다.

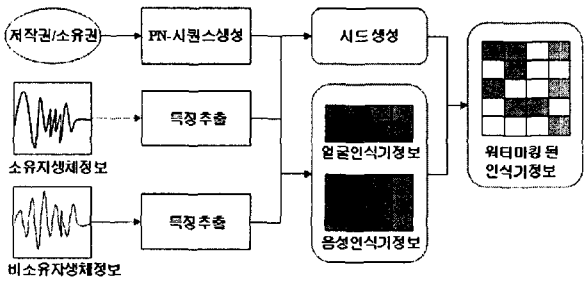


그림 2. 생체 인식기의 결합

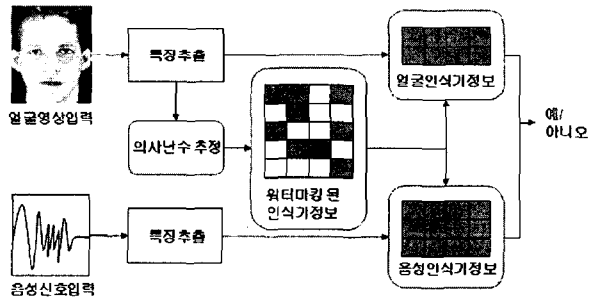


그림 3. 생체 인식기의 분리

## 3. 생체인식 시스템의 응용

### 3.1 학습과 데이터베이스 구성

우리는 최적 결정함수를 생성하는 방법으로 SVM을 선택하였다. 그러나 대량의 음성신호를 대상으로 SVM을 실행하면 학습시간이 매우 오래 걸리므로, GMM을 이용하여 M개의 코드북을 생성한 뒤 각 가우시안 모델에 대해 SVM을 학습하는 방법을 제안한다.

#### 3.1.1 얼굴 시드를 위한 신뢰구간

얼굴 특징 추출법으로 직접선형판별법을 사용한다. 만약 얼굴 특징 차원이 $d_f$이면, 우리는 $d_f$개의 축을 갖는다. 소유자의 학습데이터를 각 축에 투영시키고 그 분포를 포함하는 하한과 상한을 찾는다. i번째 차원의 값에 대한 평균이 $m_i$이고 표준편차가 $s_i$라면, 하한은 '$m_i - K_i \times s_i$', 상한이 '$m + K_i \times s_i$'이다. 이 신뢰구간은 테스트 시 시드를 추정하기 위해 사용된다.

#### 3.1.2 생체인식의 구축

얼굴 시드 생성 단계에서 직접선형판별분석을 사용하여 특징을 추출한다. 소유자를 양의 클래스로 설정하고, 비소유자를 음의 클래스로 설정한 뒤, SVM을 학습시킨다. 이 결정함수가 소유자의 얼굴 인식기가 된다. 음성 인식기의 경우, MFCC를 이용하여 $d_v$ 차원의 음성 특징을 추출하고, 각 클래스에 대해 균형 있게 분포하는 M개의 가우시안 모델들을 찾는다. 마지막으로 각 가우시안 모델에서 소유자를 비소유자로부터 분리하도록 SVM을 학습시킨다. 즉, 각 사람은 $M$개의 SVM을 가지며, 이 $M$개의 결정함수가 바로 그 사람의 음성 인식기 정보가 된다.

#### 3.1.3 생체 워터마크 삽입

소유자는 저작권 및 소유권에 근거한 랜덤 시드를 가진다. 이 랜덤 시드는 모든 직접선형 판별 값이 각 차원의 신뢰구간 내에 포함될 때 올바르게 생성된다. 얼굴 인식 데이터의 수가 $N$인 경우, $N$개의 수를 선택한 뒤 0-1 PN-시퀀스를 생성한다. 이 시퀀스의 길이는 음성 인식기 정보의 총 길이와 동일하다. 생성된 0-1 PN-시퀀스에서 음성 정보는 0의 자리에, 얼굴 정보는 워터마크를 의미하는 1의 자리에 위치한다.

### 3.2 검증 테스트

#### 3.2.1 얼굴 시드 추정

테스트되는 사람의 생체 정보로부터 시드를 추정한다. 직접선형판별분석을 이용하여 테스트되는 얼굴 데이터에서 $d_f$ 차원의 특징을 추출한다. 각 차원의 값이 연관된 차원의 신뢰구간에 속하면 우리는 정확한 시드 초기값을 얻을 수 있다. 이 시드 초기값에서 2.1과 같은 방법으로 얼굴 시드를 추정한다.

#### 3.2.2 생체 워터마크 추출

앞서 구한 시드로 워터마크 키를 생성하고, 워터마크 된 인식기정보를 분리하여 얼굴 인식기와 음성 인식기를 얻는다. 만약 시드가 조금이라도 잘못 추정된다면 인식기 정보가 왜곡되므로 불법적인 사용자가 소유자로 승인될 확률은 거의 0에 가깝다. 시드가 정확하게 추정되면 두 개의 생체인식기가 조금은 손실도 없이 복구 될 수 있다. 복구된 생체인식기는 다음 단계인 얼굴인식 및 음성인식에 사용된다. 반면에 기각되면 다음 단계는 수행되지 않는다.

#### 3.2.3 얼굴 인식

시드 추정 단계에서 추출된 $d_f$ 차원의 얼굴 특징을 재사용한다. 각 특징은 하나의 특징 벡터로 이전 단계에서 분리된 얼굴 인식기에 입력된다. 소유자 검증 결과가 참이면, 다음 단계로 넘어가고, 거짓이면 기각된다.

#### 3.2.4 음성 인식

YOHO 데이터베이스의 음성 샘플 파일은 하나 당 약 200개의 프레임으로 구성된다. 우리는 MFCC를 사용하여 테스트 데이터의 각 프레임으로부터 $d_v$ 차원의 특징을 추출한다. $M$개의 GMM을 사용하여 이 특징들을 클러스터링하고, 각 가우시안 모델의 SVM으로부터 마진을 구한다. 임계값을 가지는 마진의 중앙값을 비교하여 만약 중앙값이 임계값보다 크거나 같으면 1을, 작으면 0을 리턴한다. 결과 값의 평균이 실험을 통해 결정된 음성 승인률보다 높으면 테

스트한 사람을 소유자로 승인하고, 그렇지 않은 경우에는 기각한다.

## 4. 실 험

본 연구에서 ORL 얼굴 데이터베이스와 YOHO 음성 데이터베이스를 사용했다. ORL 데이터베이스는 40명의 사람에 대해 10장씩의 데이터가 할당되어 있다. 우리는 YOHO 데이터베이스에서 40명을 임의로 선정한 후, 각 사람에 대해 24개의 음성 파일을 할당했다. 학습 시에는 20명의 사람만 참여시켰다. 테스트를 위해, 임의로 선정한 카드 소유자 한 명, 학습에 참여한 나머지 19명중 한 명과 학습에 참여하지 않은 나머지 20명중 임의로 한명을 선택하여 한 번의 실험에 총 세 명이 참여한다. 각 사람은 1개의 얼굴영상과 4개의 음성데이터 갖는다.
시드 생성 및 얼굴 인식을 위해 직접선형판별분석과 서포트벡터 머신을 이용하고 음성 인식을 위해 MFCC, GMM, SVM을 이용한다. 우리는 앞서 얼굴 시드 추정을 위한 신뢰구간을 찾았다. 구간의 하한은 '$m-K_1 \times s$' 이고, 상한은 '$m+K_1 \times s$'이다. 표1은 $K_1$ 을 5부터 8까지 변화시킬 때의 시드 추정율을 나타낸다. 최적 파라미터 $K_1$은 8이다.

**표 1. 시드 추정율(%)**

| $K_1$ | 5 | 6 | 7 | 8 |
|---|---|---|---|---|
| 소유자 | 90 | 95 | 98 | 100 |
| 비소유자(학습) | 0 | 7 | 6 | 12 |
| 비소유자(미학습) | 4 | 6 | 18 | 22 |

실험적으로 얼굴인식을 위한 SVM의 최적 파라미터는 C=1, d=2이다. 표2는 $K_2$를 5에서 8까지 변화시키며 얼굴 인식률을 테스트한 결과이다. 최적 값은 7이다.

**표 2. 얼굴 인식률(%)**

| $K_2$ | 5 | 6 | 7 | 8 |
|---|---|---|---|---|
| 소유자 | 95 | 95 | 99 | 98 |
| 비소유자(학습) | 4 | 4 | 10 | 22 |
| 비소유자(미학습) | 3 | 8 | 21 | 26 |

표 3은 $K_3$=50이고 64개의 컴포넌트를 가진 GMM의 음성 인식률을 보여준다. SVM의 파라미터 C=1, d=3이다.

**표 3. 음성 인식률(%)**

| 승인율 (%) | 95 | 93 | 92 | 90 | 85 |
|---|---|---|---|---|---|
| 소유자 | 73.33 | 86.67 | 93.33 | 93.33 | 100 |
| 비소유자 | 0 | 0.70 | 2.81 | 3.16 | 9.12 |

GMM을 사용하지 않고 SVM을 학습할 경우 학습에 3시간이 소요되는 반면, GMM을 사용하면 10분 이내로 학습시간을 단축할 수 있다(펜티엄 4, 2.4 GHz 컴퓨터). 두 경우 모두 서포트벡터의 수는 비슷하므로 제안된 방식이 훨씬 효율적임을 알 수 있다. 표 4는 얼굴 시드 추정, 얼굴 인식, 음성 인식의 단계별 인증 성공률을 보여주고, 표 5는 전체 인식률을 보여준다.

**표 4. 단계별 인증 성공률 ($K_1$=8, $K_2$=7, $K_3$=7, C=1, d=2)**

| | ① 키 추정 | ② 얼굴인식 | ③ 음성인식 |
|---|---|---|---|
| 소유자 | 100% | 96.67% | 96.67% |
| 비소유자(학습참여) | 20% | 3.34% | 0% |
| 비소유자(학습미참여) | 20% | 6.67% | 0% |

**표 5. 최종 인식률 (k1=8, k2=7, k3=7, C=1, d=2)**

| 음성승인율 | 진양성 | 진음성 | 위양성 | 위음성 |
|---|---|---|---|---|
| 90% | 87% | 100% | 0% | 13% |
| 87% | 96.67% | 100% | 0% | 3.33% |
| 85% | 96.67% | 100% | 0% | 3.33% |

## 5. 결 론

본 논문에서 제안하는 시스템은 생체정보로부터 워터마크키를 생성하고, 안전한 생체인식 데이터베이스를 구축한다. 실시간으로 입력되는 생체정보에서 시드를 추정한다는 점에서 보안성과 편리성을 획득할 수 있다. 또한 두 개의 약한 인식기를 결합하여 개별적으로 강한 인식기보다 더 높은 인식률을 얻었다. 본 실험에서 진양성 비율은 약 96%였으며, 위음성 비율은 0%였다. 학습에 참여한 비소유자뿐 아니라, 학습에 참여하지 않은 비소유자 또한 기각된 것으로 미루어 볼 때, 본 생체인식시스템이 높은 신뢰도를 갖는다는 것을 알 수 있다. 최적의 특징 추출법을 선택하기 위하여 추가적인 실험이 수행되면, 보다 나은 인식률을 얻을 수 있을 것으로 기대된다.

## 6. 참고문헌

[1] A. Jain, U. Uludag, Rein-Lien Hsu, "Hiding a Face in a Fingerprint Image", Proc. AutoID 2002, 3, Workshop on Automatic Identification Advanced Technologies, pp. 97-102, 2002.
[2] C. -P. Wu, C. -C. J. Kuo, "Fragile Speech Watermarking for Content Integrity Verification", 2002 IEEE, International Symposium on Circuits and Systems, (Phoenix, Arizona), May 2002.
[3] L. Boney, A. Tewfik, K, Hamdy, "Digital Watermarks for Audio Signals", EUSIPCO-96, VIII European Signal Proc. Conf., Trieste, Italy, September 1996.
[4] H. Yu, J. Yang, "A direct LDA algorithm for high-dimensional data with application to Face Recognition", Pattern Recognition, vol. 34, 2001.
[5] D. A. Reynolds, "Speaker identification and verification using Gaussian mixture speaker models", 1994.
[6] C. Cortes, V. Vapnik, "Support Vector Networks", Machine Learning, Vol. 20, pp 53- 60, 1995
[7] C. J. C. Burges and B. Scholkopf, "Improving the accuracy and speed of support vector machines", Neural Information Processing Systems, 9:7, 1997.
[8] C. J. C. Burges, "A Tutorial on support Vector Machines for Pattern Recognition", Data Mining and Knowledge Discovery, Vol. 2, No. 2, pp. 121-167, 1998.