홍채코드의 보안 취약성에 대한 연구

윤성조*, B.V.S Anusha**, 김계영***
*숭실대학교 융합소프트웨어학과
**Indian Institute of Technology Bombay 전기공학과
***숭실대학교 소프트웨어학과
e-mail:sungjo90@ssu.ac.kr

A Study of Security Vulnerability of Iriscode

Soung-Jo Youn*, B.V.S Anusha**, Gye-Young Kim***
*Dept of Convergence Software, Soongsil University
**Dept of Electrical Engineering, Indian Institute of Technology Bombay
***Dept of Software, Soongsil University

요 약

홍채코드는 홍채의 정보를 이진코드로 표현함으로써 홍채정보를 보호하는 방법이다. 이러한 방법은 현재 홍채인식 시스템에서 표준으로 채택된 기술이다. 본 논문에서는 1-D 가버 필터를 사용하여 홍채코드로부터 역공학적 방법을 사용하여 홍채영상을 복원하고, 복원된 홍채 영상과 기존의 홍채영상의 인식 결과를 통해 홍채 인식에 대한 취약성을 연구한다.

1. 서론

생체인식은 개인마다 다른 지문, 홍채, 얼굴 등 개인의 독특한 생체 정보를 추출하여 정보화시키는 인증 방식이다. 이러한 생체 정보들은 변경되거나 분실할 위험성이 없어 보안 분야에서 많이 활용된다. 이러한 생체인식 특성 중에서 홍채는 높은 신뢰성과 정확성을 보인다[1]. 또한 홍채는 각 개인 간에 상당히 고유한 정보를 갖는 것으로 입증되었다[2]. 홍채인식기술은 현재 출입통제, 근태관리, 빌딩통합시스템, 금융자동화기기, 컴퓨터보안 분야, 전자상거래 인증, 공항정보 시스템 등 여러 보안 시스템에 적용되고 있다.

홍채코드는 각 사람의 홍채 정보의 차별적인 특성을 매우 효율적이고 간결하게 표현하기 때문에 홍채 인식시스템에서 표준으로 채택되었다. 그리고 이러한 홍채코드는 원래의 홍채 이미지로 재구성할 수 있는 충분한 정보를 가지고 있지 않다고 여겨졌다[3]. 홍채코드는 눈 영상에서 홍채를 분할 후에 일정한 크기를 갖는 직사각형 모양으로 정규화 한 후, 어떠한 유형의 필터링(ex, 가버 필터링)을 수행하고, 양자화 하여 이진 코드(홍채코드)형태로 생성된다.

본 논문에서는 1-D 가버 필터로 형성된 홍채코드를 역공학적 방법을 통해 복원하여 원본 홍채영상과 인식여부를 실험하여 홍채 인식기술의 취약성을 연구하고자 한다.

2. 가버 필터

본 논문에서는 홍채영상에서 홍채 특징을 추출하는 방법으로 1-D 가버 필터를 사용하였다. 아래 식1,2와 같다.

$$G(x;\sigma,p)=\frac{1}{\sqrt{2\pi}\,\sigma}exp\left(\frac{-x^2}{2\sigma^2}\right)\cos(2\pi px) \qquad 식\ (1)$$

$$G(x;\sigma,p)=\frac{1}{\sqrt{2\pi}\,\sigma}exp\left(\frac{-x^2}{2\sigma^2}\right)\sin(2\pi px) \qquad 식\ (2)$$

식1은 영상의 실수 값의 특징을 나타내는 필터식이고 식2는 허수 값의 특징을 나타내는 필터식이다. 필터를 거치고 나온 실수 값을 가지는 영상과 허수 값을 가지는 영상은 양자화 하여 0또는 1값으로 변환 후 두 영상을 교차로 붙여 하나의 홍채코드 영상으로 만든다.

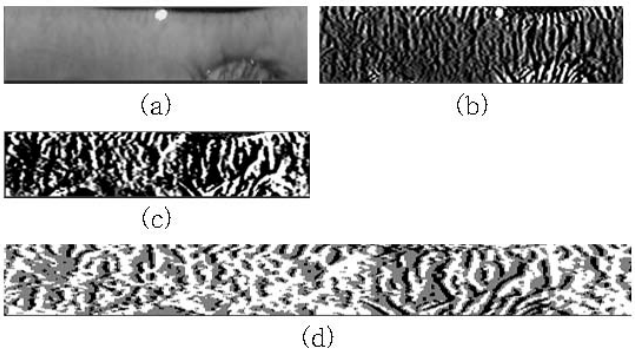


그림 1 (a) 정규화된 원본 홍채 영상, (b) 실수 값 특징, (c) 허수 값 특징, (d) 홍채코드

2. 복원 방법

홍채코드를 만드는데 쓰이는 가버 필터의 매개변수는 알고 있다고 가정하고 역공학적 방법을 통해 복원을 하였다. 홍채코드를 원본 영상을 복원하기 위해 $A*X=B$식을 사용하였다. 여기서 A, X, B는 각각 가버 필터, 원본 영상, 홍채코드를 의미한다. 홍채코드는 이진형태로 양수는 1, 음수는 0으로 표현되는데, 이를 양수는 1, 음수는 -1로 변환하고 그림 2와 같은 행렬식을 통해 원본 영상을 추정한다.

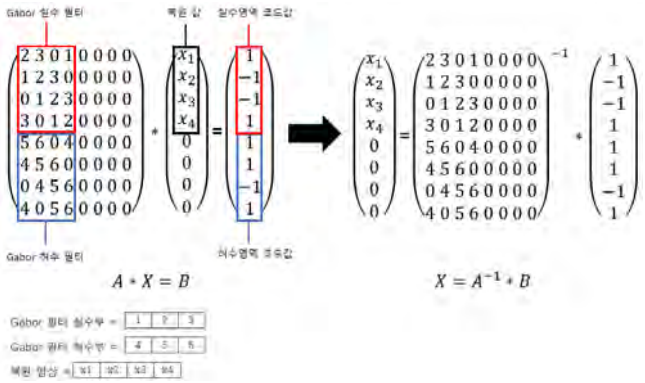
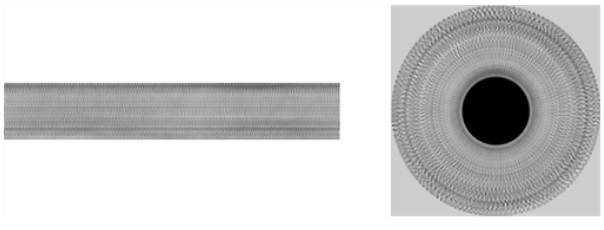


그림 2 역 공학적 행렬식 예시

복원된 홍채영상 육안으로 봤을 때는 원본영상과 다른 형태의 모습으로 보이지만, 동일한 인식기에서 원본 홍채코드와 비교한 결과 약 90%이상의 일치율을 보였다. 하지만 인식기의 영상취득 단계에서는 정규화 된 직사각형 영상이 아닌 눈 모양의 영상을 취급하기 때문에 아래 그림 3과 같이 직교 좌표계 변환을 통하여 가짜 홍채영상을 생성하였다.



(a) (b)

그림 3 (a)복원된 홍채 영상 (b)좌표계 변환된 홍채 영상

3. 실험 및 결과

제안한 방법의 성능을 평가하기 위해 홍채 인식기를 만들어 실험하였다. 해당 인식기는 홍채 분할, 정규화, 홍채 특징 추출, 인식으로 구성하였다. 홍채 분할 및 정규화는 도그만 알고리즘을 사용하였고[4], 홍채 특징 추출은 1-D 가버 필터를 사용하여 홍채코드인 이진코드를 생성하였다. 그리고 마지막 인식단계에서는 비교하는 홍채코드의 해밍거리를 비교하여 인식여부를 정하였다. 해당 인식기의 성능을 평가하기 위해 CASIA Database에서 100명의 사람의 홍채를 사용 하여 아래의 그림 4,5와 같이 같은 사람의 홍채 간의 비교와 다른 사람 홍채 간의 비교를 실험하였다.

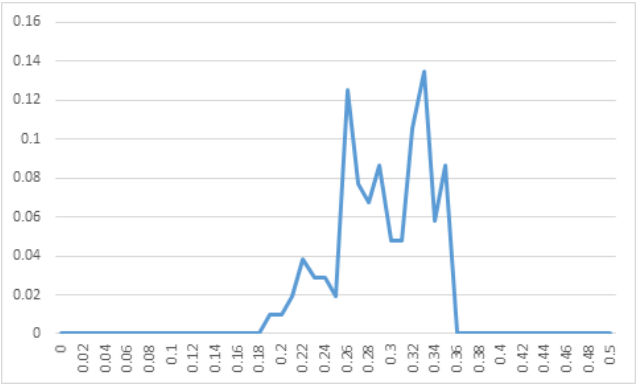


그림 4 같은 사람 홍채 간의 해밍거리 비교

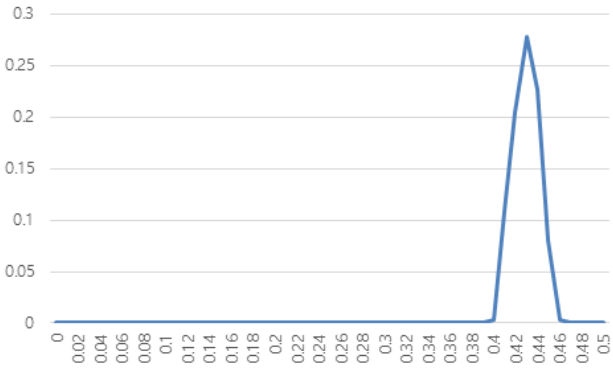


그림 5 다른 사람 홍채 간의 해밍거리 비교

같은 사람 홍채 간의 비교에서 해밍거리는 0.19~0.36사이로 평균 0.3의 해밍거리 값을 가졌고, 다른 사람 홍채 간의 비교에서 해밍거리는 0.39~0.46사이로 평균 0.43값을 가졌다. 위와 같은 결과를 토대로 해당 인식기의 홍채코드 간의 해밍거리 비교 인식 임계값은 0.38로 설정하였다.

원본 영상의 홍채코드를 복원하여 가짜 홍채 영상을 만들고 동일한 인식기에서 원본 영상과 복원 영상의 인식 비교를 통해 복원 결과를 실험하였다. 인식 결과는 아래 그림 6과 같다.

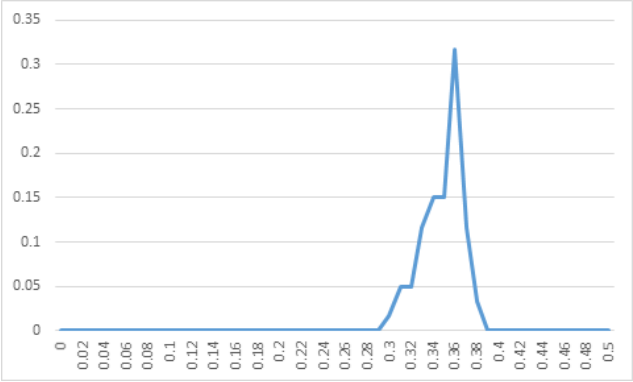


그림 6 원본 영상과 복원 영상 간의 해밍거리 비교

원본 영상과 복원 영상간의 해밍거리는 0.3~0.38사이로 평균 0.34의 값을 가졌다. 이는 인식 임계값 0.38으로 설정된 해당 인식기에서 97%인식률을 보인다.

4. 결론 및 향후 연구

본 논문에서는 역공학적 방법을 통해 홍채코드를 가짜 홍채 영상으로 복원하였다. 그리고 해당 영상과 원본영상의 비교를 통해 인식률을 실험하여 홍채코드로부터 홍채 영상의 복원이 충분함을 보여주었다. 사용되고 있는 홍채 코드 시스템은 홍채 정보를 보호하는데 있어 부족함이 있어 추가적인 보안 수단이 연구 되어야 한다.

Acknowledgement

본 연구는 한국연구재단의 연구비 지원을 받았습니다 (과학기술정보통신부).

참고문헌

[1] A. Jain, P. Flynn, A. Ross (Eds.), “Handbook of Biometrics”, Springer.

[2] John G. Daugman “Probing the uniqueness and randomness of iris codes: results from 200 billion iris pair comparisons”, Proceedings of the IEEE.

[3] International Biometric Group “Generating Images from Templates”, White paper.

[4] John G. Daugman “High Confidence Visual Recognition of Persons by a Test of Statistical Independence” , IEEE Transactions on Pattern Analysis and Machine Intelligence.