생체정보 인증을 위한 위·변조 검출 가역 워터마킹 알고리즘

*이효빈, **김성완, **임재혁, **이상윤
연세대학교 *생체인식연구센터, **전기전자공학부
e-mail : {leehb00, knauer, jhlim, syleee}@yonsei.ac.kr

Watermarking Algorithm for Biometric image authentication

*Hyobin Lee, **Seongwan Kim, **Jaehyuck Lim, **Sangyoun Lee
Biometric Engineering Research Center(BERC),
*Graduate Program in Biometrics,
**Department of Electrical and Electronic Engineering, Yonsei University

Abstract

In this paper, we propose an invertible biometric image watermarking algorithm which can detect block-wise malicious manipulations. The proposed method embeds two types of watermark. The first type can completely remove distortion due to authentication if the data is deemed authentic. The second type can detect block-wise malicious manipulation by applying the parity bits concept to biometric image blocks.

I. 서론

생체인식 기술의 폭넓은 활용을 위해서는 생체 영상의 보안성을 높일 필요가 있다. 그 방법으로 암호화와 디지털 워터마킹 기술 두 가지가 있다. 암호화는 정보를 기호화하여 권한이 없는 자에게는 의미 없는 정보로 만드는 방법이며, 디지털 워터마킹 기술은 소유정보를 생체 영상에 삽입하여 정당한 지적 소유권을 보호하거나 또는 그 영상을 인증한다. 암호화의 경우는 복호키를 이용하여 복호화 된 이후의 데이터에 대해서는 어떠한 보안성도 가지지 않는다. 따라서 복호화 된 데이터가 가로채질 수 있기 때문에 복호화 이후에도 보안성을 유지하려 한다면 암호화는 생체영상의 보안성을 끝까지 보장할 수 없다. 암호화-복호화 과정이 없는 워터마킹은 생체영상의 불법적인 사용에서 또 다른 방어가 가능하다.

본 논문에서는 생체영상의 보안성을 높이기 위하여 워터마킹을 사용하였으며, 워터마킹을 이용하여 원본영상의 인증을 하였다. 그리고 원본영상으로 완벽한 복원이 가능하며 기존의 인증을 위한 워터마킹과는 달리 더 나아가 인증이 되지 않았을 경우, 즉 원본 생체영상이 조작되었음을 확인하면 그 위치까지 찾을 수 있도록 구현되었다.

II. 본론

2.1 Embedding

알고리즘은 그림 1에서와 같은 방법으로 삽입될 워터마크를 생성한다. 영상을 블록 단위로 나누어 각 블록에 심볼 결정 함수를 적용R, S의 블록으로 이름 짓는다. 모든 블록에 이처럼 적용하면 R, S로 이름 지어진 0과 1의 비트스트림을 얻을 수 있다. 이 비트스트림을 이용하여 비손실 영상압축을 하게 되면, 원본영상의 정보를 그대로 가지고 있으며 부가적인 정보, 즉 워터마크를 삽입할 수 있는 공간을 만들 수 있다.

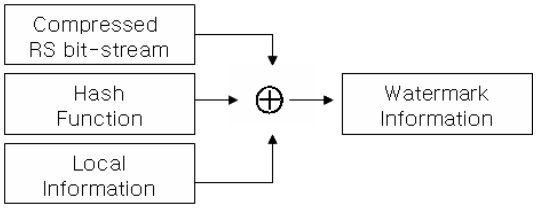


그림 1 워터마크 정보 생성 개념도

영상에 인증 여부를 결정짓기 위해 원본 영상에 해쉬(Hash) 함수를 적용하여 128 비트의 고유 정보를 생성한다. 해쉬 함수의 특성상 모든 영상은 다른 해쉬 값을 가지게 되면 이 경우 다른 두 영상이 같은 해쉬를 가질 확률은 $1/2^{18}$ 이 된다.

인증 이후 영상에 조작이 가해졌다고 판단이 되면 그 위치를 찾을 수 있도록 하기 위해 원본영상의 지역 정보를 삽입한다. 즉, 8x8 블록 단위로 블록 내부의 RS 심볼의 개수를 이용하여 Parity bit를 생성한다. 생성된 Parity bit를 이용하여 Parity bit의 사용 개수에 따라 1비트를 사용했을 경우 그림2 에서와 같이 1/2의 확률로 조작위치 여부를 판단할 수 있다.

2.2 Decoding

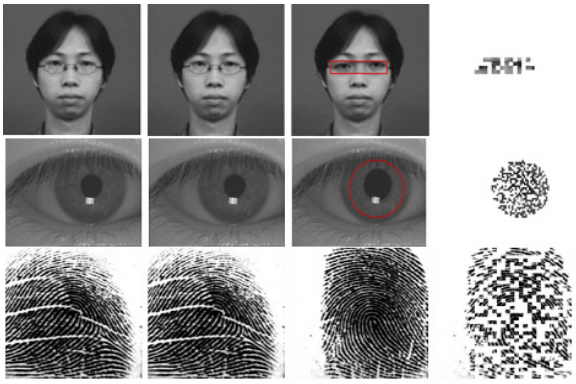
워터마크를 추출하는 과정은 삽입하는 과정과 동일하다. 블록단위로 RS 비트스트림을 뽑아낸 후 비손실 영상압축 기술로 복원한다. 복원된 원본 영상과 입력된 영상의 해쉬 값 비교를 통하여 영상의 인증여부를 판단한다. 물론 인증이 되지 않는다면 영상에서 지역 정보를 추출하여 조작된 위치를 파악할 수 있다.

Ⅲ. 실험결과

그림2는 제안된 알고리즘을 얼굴, 홍채, 지문 등의 생체 영상에 적용하여 실험한 결과이다. 원본영상과 워터마크가 삽입된 영상을 비교해 보면 두 영상의 차이를 알 수 있다. 즉, 워터마크는 LSB를 이용하여 삽입하기 때문에 영상에서 차이를 느낄 수가 없다. 이것은 워터마크의 비가시성을 잘 가지고 있음을 확인할 수 있다. 그림2(c)의 경우 얼굴은 눈 부분을, 홍채는 홍채의 패턴영역을, 지문은 전체적인 바꿔치기를 가해보았다. 그 결과 모두 인증이 되지 않았으며, 그림2(d)에서와 같이 조작된 위치를 찾을 수 있었다.

Ⅳ. 결론 및 향후 연구 방향

생체영상에서 영상의 무결성을 판단하기 위하여 워터마킹 인증을 적용하였다. 기존의 인증 알고리즘과는 달리 원본영상으로 완벽히 복원이 가능하며, 또한 조작의 위치를 파악할 수 있도록 구현하였다. 본 논문에서는 최근에 이슈화 되고 있는 생체인식에서의 정보보안의 한 가지 해결 방안으로 본 알고리즘을 제안하며 나아가 워터마킹의 또 다른 분야인 저작권 보호의 측면에서 접근하여 생체정보의 저작권 보호를 위한 알고리즘 연구를 할 예정이다.



좌측에서부터 (a)원본영상 (b)워터마크된 영상
(c)공격 받은 영상 (d)공격 위치 검출
그림 2 실험 결과 영상

Acknowledgement

본 연구 결과는 한국과학재단 지정 생체인식연구센터의 지원을 받아 이루어졌습니다.

참고문헌

[1]. J. S. Coron, "What Is Cryptography?" IEEE Security & Privacy Magazine, Vol. 4, Jan. pp. 70-73, 2006.

[2]. J. Fridrich, M. Goljan, and R. Du, "Invertible authentication watermark for JPEG images, " Proc. IEEE Int. Conf. on Information Technology, Las Vegas, NV, USA, pp. 223-227, April 2001.

[3]. C. T. Li, D. C. Lou, and T. H. Chen, "Image authenticity and integrity verification via content-based watermarks and a public key cryptosystem, " Proc. IEEE Int. Conf. on Image Processing, vol. III, pp. 694-697, September 2000.

[4]. J. Fridrich, M. Goljan, R. Du, "Lossless data embedding for all image formats," Proc. SPIE Photonics West, Vol. 4675, , 572-583, January, 2002.