이중 워터마킹 기술을 이용한 지문정보 보호

김태해*, 정승환*, 정용화*, 문대성**
*고려대학교 컴퓨터정보학과
**한국전자통신연구원 생체인식연구팀
e-mail:taegar@korea.ac.kr

Protecting Fingerprint Information using a Dual Watermarking Technique

T. Kim*, S. Chung*, Y. Chung*, D. Moon**
*Dept of Computer & Information Science, Korea University
**Biometrics Research Team, ETRI

요 약

최근 지문인식 시스템에서 인식 성능과 인식 시간뿐만 아니라, 지문정보 자체를 외부 공격자로부터 보호하기 위한 연구가 활발히 진행되고 있다. 본 논문에서는 지문정보의 전송 경로에서 발생할 수 있는 Replay 공격과 지문 데이터베이스의 유출로 인한 사후 처리 방안으로 강인성(Robustness)과 약한 성질(Fragileness)을 동시에 만족시킬 수 있는 이중 워터마킹(Dual Watermarking) 알고리즘을 제안한다. 특히, 두 가지의 워터마킹 알고리즘을 동시에 사용할 때 발생할 수 있는 워터마크 삽입 위치에 의한 간섭을 최소화하기 위하여 약한 워터마크를 삽입할 때 융선의 윤곽선 정보를 이용하였다. 실험을 통하여 제안한 방법이 삽입된 워터마크의 추출에 영향을 주지 않음과, 여러 가지 공격에 강인함을 확인하였다.

1. 서론

일반적으로 사용자 인증수단을 PIN(Personal Identification Number) 또는 패스워드 방식을 사용하지만, 유출 및 망각의 위험이 상존하다. 따라서 이에 따른 보안상의 문제가 최근 들어 크게 부각되고 있다. 이러한 단점을 해결할 수 있는 개인 인증기술로서 생체인식이 등장하였다.

본 논문에서는 생체정보 중 가용성, 정확도, 경제적인 면에서 가장 일반적으로 사용되어지고 있는 지문을 선택하였다.[1] 현재 지문인증 시스템은 도어락과 같은 단순한 출입통제 시스템에서 인터넷뱅킹, 전자정부 등의 원격응용 시스템으로 발전하고 있다. 이러한 원격응용 시스템에서는 안전하지 않은 전송 채널을 통해 전송되는 사용자의 지문영상을 공격자가 가로채어 재사용할 경우 심각한 문제를 야기할 수 있다. 따라서, 암호, 워터마킹, 스테가노그래피 등의 기술을 이용하여 사용자의 중요한 지문정보를 보호하기 위한 연구가 활발히 진행되고 있으며, 본 논문에서는 멀티미디어 데이터의 저작권을 보호하기 위해 사용되는 워터마킹 기술을 지문영상을 보호하는데 사용한다. 워터마킹 기술은 적용되어지는 응용에 따라 강인한 워터마킹(Robust Watermarking)과 약한 워터마킹(Fragile Watermarking)으로 구분할 수 있다. 강인한 워터마킹 기술은 영상 압축이나 영상 처리와 같은 공격에도 삽입된 정보가 손실되지 않지만, 약한 워터마킹 기술은 단순한 공격에도 삽입된 정보가 쉽게 손실된다. 이런 특성을 이용하여 약한 워터마킹으로는 무결성을 검증하고, 강인한 워터마킹은 중요 데이터의 은닉에 사용될 수 있다.

본 논문에서는 지문영상에 대하여 강인한 워터마킹 기술과 약한 워터마킹 기술을 동시에 적용하기 위한 방법을 제안한다. 지문영상에 사용자의 중요한 정보를 삽입하거나 지문영상이 외부에 유출되었을 경우에 유출자의 정보를 확인하기 위하여 강인한 워터마킹 기술이 사용될 수 있으며, 지문영상이 공격자에 의하여 도용되었을 때 재사용을 방지하기 위하여 약한 워터마킹 기술을 사용할 수 있다. 본 논문

에서는 강인한 워터마킹 알고리즘으로 Dugad 방법[2]을 사용하며, 약한 워터마킹 알고리즘으로 Jain 방법[3]을 사용하였다. 그러나 강인한 워터마킹 기술이 적용된 지문영상에 약한 워터마킹 알고리즘을 수행하기 때문에 강인한 워터마크의 정확한 추출에 영향을 줄 수 있다.

즉, 두 가지 워터마킹 알고리즘을 단순 융합하면 삽입 정보 사이의 충돌이 발생하여 삽입 정보의 추출율이 감소할 수 있다. 본 논문에서는 약한 워터마킹 기술을 적용할 때 두 가지 워터마크가 서로 간섭을 주지 않는 이중 워터마킹(Dual Watermarking) 기법을 제안한다. 또한 두가지 워터마킹 알고리즘에 대하여 삽입된 워터마크가 정확하게 추출된다.

본 논문의 구성은 2장에서 기존의 워터마크를 이용한 생체정보 보호연구를 기술하고, 3장에서는 제안하는 이중 워터마킹 알고리즘을 설명한다. 4장에서는 제안한 알고리즘에 대한 실험결과를 설명하며, 마지막으로 5장에서 결론을 내린다.

2. 워터마킹 기술을 이용한 생체정보 보호연구

Yeung과 Pankanti[4]는 지문영상에서 보이지 않는(Invisible) 약한 워터마킹 기법을 사용하여 영상의 무결성을 보장하였으며, 워터마킹 정보가 삽입되는 위치는 공유한 키를 통해 결정되며 전송 전후에 사용된다. 이에 반하여 Uludag과 Tekalp[5]는 강인한 워터마킹 기법을 사용하였으며 영상의 강한 왜곡에도 삽입된 정보가 탐지된다. 따라서 강인한 성격의 정보를 삽입할 수 있다.

이와 같이, 지문영상을 보호하기 위하여 워터마킹 기술을 이용하는 연구는 사용될 응용에 따라 워터마크를 삽입하는 강도를 조절하여 약한 워터마킹이거나 강인한 워터마킹을 제안하였다. 그러나, 지문영상을 더욱 안전하게 보호하기 위해서는 무결성 검증과 중요 정보의 저장을 동시에 보장할 수 있는 방법이 필요하며, 본 논문에서는 강인한 워터마킹 알고리즘을 수행한 결과로 나온 지문영상에 약한 워터마킹 알고리즘을 적용하는 이중 워터마킹 알고리즘을 제안한다. 특히, 지문인식 시스템에 적합한 블라인드 워터마킹 기술을 적용하여 구현하였다.

3. 이중 워터마킹 알고리즘

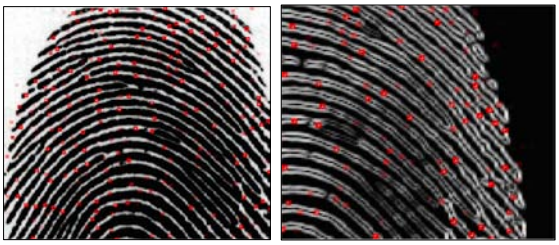
본 장에서는 지문영상의 안전한 전송을 위해 이중 워터마킹 기법을 제안한다. 지문영상의 무결성을 검증하고 중요정보를 동시에 삽입하기 위해 다음 조건을 만족 시켜야 한다.

- 강인한 정보, 약한 정보 순서로 삽입한다.
- 삽입 정보 간에 간섭이 없어야 한다.
- 정합단에 미치는 영향을 최소화 한다.

두 워터마킹 방법은 삽입된 워터마크 정보를 원본 영상 없이 추출 할 수 있는 블라인드 워터마킹 방법으로 지문인식 시스템에 적합하다. 왜냐하면, 워터마크의 추출에 사용하기 위하여 원본 지문영상을 전송하는 과정을 생략할 수 있기 때문이다.

그러나, Jain의 워터마킹 기법이 Dugad의 알고리즘에 영향을 주기 때문에, 두 알고리즘을 단순 결합하여 이중 워터마킹 기술을 구현할 경우 Dugad의 워터마크 추출율이 떨어진다는 문제점이 있다. 본 논문에서는 Jain의 워터마킹 알고리즘을 개선하여 Dugad의 워터마킹 알고리즘에 영향을 주지 않는 이중 워터마킹 알고리즘을 제안한다.

Dugad의 방법은 워터마크가 융선 내/외에 삽입되며, Jain이 사용한 방법은 지문영상 전체 영역에 분산된다. 그림 1은 삽입영역의 차영상을 이용하여 워터마크의 간섭이 발생하는 부분을 원본 지문영상에 표현한 것이다. 실험 결과 원본영상에서 지문 융선의 경계영역에 충돌이 발생하는 것을 확인할 수 있으며, 이를 보완하기 위해 Jain의 워터마크 삽입 영역에서 경계부분을 제거하였다.



(그림 1) 충돌이 발생하는 영역

제안하는 워터마킹 기법은 지문영상을 보호하기위해 두 번 워터마킹하며, 지문영상의 무결성을 측정하고 강인한 정보를 삽입하기 위하여 다음과 같이 동작한다.

3.1. 지문정보 송신측에서의 동작과정

먼저 Dugad의 방법을 이용하여 워터마크를 강인하게 삽입한다. 강인한 워터마킹에 사용될 워터마크 정보는 특정응용을 명시하기 위한 정보, 역추적(Traceback)을 위한 지문센서정보, “Replay Attack”을 방어하기 위한 시간정보(Time Stamp) 및 난수정보(Nonce) 등이 가능하다. 강인한 워터마킹 알고리즘의 결과로 나온 지문영상에 무결성 검증을 위해 Jain 방법을 개선한 약한 워터마킹 방법을 적용한다. 약한 워터마킹 알고리즘은 <식 1>[3]을 이용하여 무결성 검증을 위한 워터마크 정보를 삽입하게 된다.

$$P_{wm}(i,j) = P(i,j) + \{(2s-1)P_{AV}(i,j)q(1+\frac{P_{SD}(i,j)}{A})\times (1+\frac{P_{GM}(i,j)}{B})\beta(i,j)\} \quad <식1>$$

<식 1>에서 β은 공유된 키를 통해서 생성된 삽입될 위치를 의미한다. 앞서 언급한 것처럼 약한 워터마킹 알고리즘이 강인한 워터마킹 알고리즘에 영향을 주지 않기 위해서는 워터마크가 삽입될 위치 정보인 β에서 융선의 경계부분을 제외하여야 한다. 왜냐하면 강인한 워터마킹 알고리즘인 Dugad의 방법은 주로 융선의 경계부분에 워터마크 정보를 삽입하기 때문이다. 그러나, 원영상에서 소벨(Sobel) 연산을 이용하여 윤곽선 정보를 계산한 후 해당하는 위치를 삽입 영역 β에서 제외시킬 경우, 워터마크 삽입으로 인한 영상의 왜곡으로 인하여 수신측에서 삽입된 워터마크를 추출할 때 송신측과 동일한 삽입영역 β를 생성하지 못한다. 따라서, 본 논문에서는 삽입영역 β를 결정하기 위하여 워터마크를 추출할 때 사용되어지는 근사영상을 <식 2>와 같이 먼저 생성하고, <식 2>의 결과로부터 융선의 윤곽선 정보를 <식 3>과 같이 계산한다. <식 3>의 결과가 실험에 의하여 미리 정의된 임계값 t보다 클 경우 초기에 생성된 β에서 제외시킨다.

$$\hat{P}(i,j) = \frac{1}{8}\left(\sum_{k=-2}^{2} P(i+k,j) + \sum_{k=-2}^{2} P(i,j+k) - 2P(i,j)\right) \quad <식2>$$

$$\beta\{(i,j):\ i \in x,\ \ j \in y,\ \ P_{GM}(\hat{P}(i,j)) \le t\} \quad <식3>$$

3.2. 지문정보 수신측에서의 동작과정

수신측의 워터마크 추출과정은 송신측 워터마크 삽입과정의 역순으로 진행된다. 먼저, 전송된 지문영상의 무결성 여부를 테스트 한다. 무결성이 검증되면 강인한 워터마킹 알고리즘의 워터마크 추출 방법을 적용하여 해당 응용에 적합한 지문인지를 판별한다. 만약 적합하지 않은 정보가 발견되면 즉시 파기되거나 불법 행위에 대한 대응절차가 실행된다. 또한 강인한 워터마킹 정보를 통해 방치된 지문 정보의 출처를 알 수 있으며, 이를 이용하여 인증 시스템을 보완할 수 있다.

4. 구현 및 성능 분석

본 논문에서 제안한 워터마킹 방법의 타당성을 검증하기 위하여 다음 두 가지의 관점으로 실험을 수행하였다. 먼저, 강인한 워터마킹 알고리즘에 대하여 여러 가지 시그널 공격을 가한 후 삽입된 워터마크의 존재여부를 확인함으로써 워터마킹 알고리즘의 강인성을 검증하였다(실험 1). 또한, 제안한 이중 워터마킹 방법에서 무결성 검증을 위하여 사용된 약한 워터마킹 알고리즘이 강인한 워터마킹 알고리즘의 워터마크 추출에 영향을 주지 않는지 여부를 확인하는 실험을 수행하였다(실험 2).

본 논문에서는 니트젠 센서를[6] 통해 입력된 지문영상을 이용하였다. 실험 1에서 삽입될 워터마크의 길이는 200bit 이며, 사용되는 파라미터 T1과 T2는 각각 40, 50으로 설정하였다. 여기서 파라미터는 워터마크가 삽입되는 계수의 순서를 말하며, 삽입 시 T1보다 큰 계수에 삽입이 되며 워터마크 검증에 사용된 T2는 T1 보다 커야 한다[2].

a) 원본 b) 삽입 후 c) 삽입된 영역

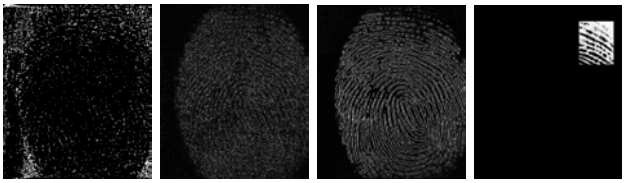
(그림 2) 강인한 워터마킹 방법에 의한 지문영상

그림 2 c)는 원본 지문영상 a)와 워터마크가 삽입된 지문영상 b)의 차영상이며, 워터마크 정보가 삽

입되어지는 위치를 나타낸다.

또한, 그림 3에서와 같이 네 가지의 외부 공격을 가정하고, 워터마크가 삽입된 지문영상에 공격을 가한 후 본 논문에서 제안한 이중 워터마킹 알고리즘의 강인성을 검증하였다.

표 1은 지문영상을 공격하여 삽입된 워터마크의 추출률을 측정하였으며, 충분한 수준의 추출률을 보여주고 있다.



a) median b) jpeg(30%) c) blur d) cut

(그림 3) 공격에 의한 원본영상의 차영상

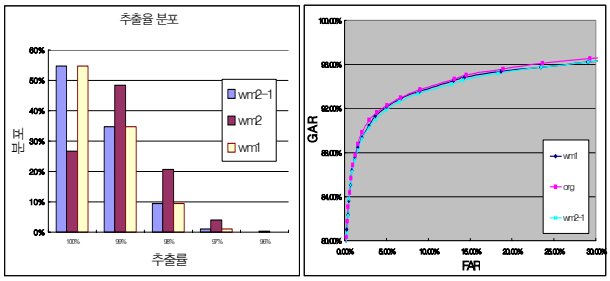
〈표 1〉 공격에 대한 측정값

Attack	PSNR	Measured value
Median filter	60.161461 dB	1.000000
Jpeg compression (30%)	25.241369 dB	0.777778
Blur filter	27.950458 dB	1.000000
Cut	15.169233 dB	0.888889

다음은 약한 워터마킹 방법이 강인한 워터마킹 방법의 워터마크 추출률에 어떤 영향을 주는지를 확인하기 위해 추출율 분포 그림 4 a)를 측정하였으며, 약한 워터마킹 방법 삽입 시 융선의 윤곽선을 제외하는 방법이 강인한 워터마킹 방법에 영향을 주지 않음을 확인 하였다. 즉, 그림 4 a)에서와 같이 융선의 윤곽선을 고려하지 않은 이중 워터마킹 방법(wm2)은 강인한 워터마킹 방법(wm1)의 워터마크 추출률에 영향을 주고 있지만, 본 논문에서 제안한 수정한 알고리즘(wm2-1)은 강인한 워터마킹 방법의 워터마크 추출률에 영향을 주지 않는 것을 확인 할 수 있었다.

또한, 지문영상에 워터마크를 삽입하여 영상이 훼손되었을 경우 지문인식 성능에 얼마나 영향을 주는지 실험하였다. 지문 인식 성능의 측정을 위해 총 4,200개, 248×292 크기의 gray scale 지문영상을 사용하였다. Genuine 정합에서는 12,000번의 횟수를 테스트 하였으며, Impostor 정합에서는 20,000번의 정합테스트를 수행 하였다.

그림 4 b)에서 나타낸바와 같이 워터마크를 삽입했을 경우에도 원본 영상의 지문인식 성능과 아주 유사한 인식성능을 확인할 수 있었다.



a) 추출율 분포 b) 정합 ROC

(그림 4) 제안한 이중 워터마크 실험 결과

5. 결론

본 논문에서는 이중 워터마킹 방법을 이용하여 지문영상이 유출되었을 때 재사용이 불가능하게 하고, 무결성을 보장하기 위한 방법을 제안하였다. 특히, 두 가지의 워터마킹 알고리즘을 동시에 사용할 때 발생할 수 있는 간섭을 최소화하기 위하여 약한 워터마크를 삽입할 때 융선의 윤곽선 정보를 이용하였다. 향후 본 논문에서 제안한 지문 워터마킹 방법을 확장하여 얼굴, 정맥, 홍체 등 다른 생체 정보 데이터에 적합한 이중 워터마킹 알고리즘을 개발하는 것도 흥미로운 연구 분야가 될 것으로 기대된다.

참고문헌

[1] D. Maltoni, et al., Handbook of Fingerprint Recognition, *Springer*, 2003.

[2] R. Dugad, K. Ratakonda, and N. Ahuja, “A New Wavelet-based Scheme for Watermarking Images,” *Proc. of the ICIP*, 1998.

[3] A. Jain, U. Uludag, and R. Hsu, "Hiding a Face in a Fingerprint Image," *Proc. of ICPR*, pp. 756-759, 2002.

[4] M. Yeung and S. Pankanti, “Verification Watermarks on Fingerprint Recognition and Retrieval,” *Journal of Electronic Imaging*, Vol. 9, No. 4, pp. 468 - 476, 2000.

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

[6] NiGen, http://www.nitgen.com