지문 퍼지볼트의 상관공격에 강인한 거짓 특징점 삽입 방법

최한나*, 이성주*, 정용화*, 최우용**, 문대성**, 문기영**
*고려대학교 컴퓨터정보학과
**한국전자통신연구원 생체인식연구팀
e-mail:seracle7@korea.ac.kr

Inserting Chaff Points into Fuzzy Fingerprint Vault for Protecting Correlation Attack

Hanna Choi*, Sungju Lee*, Yongwha Chung*, Woo-yong Choi**, Daesung Moon**, Kiyoung Moon**
*Dept of Computer and Information Science, Korea University
**Biometrics Technology Research Team, ETRI

요 약

지문 템플릿(Fingerprint Template)을 보호하기 위해 암호학적 기법인 퍼지볼트(Fuzzy Vault)가 적용되었다. 퍼지볼트 기법은 지문으로 부터 추출되는 특징점을 은닉하기 위하여 지문 템플릿에 다수의 거짓 특징점을 "임의"로 삽입하는 방법이다. 그러나 최근 이러한 지문 퍼지볼트를 효과적으로 크래킹 할 수 있는 상관공격(Correlation Attack)에 관한 연구가 발표되었는데, 이것은 동일한 지문으로 부터 생성되는 두 개의 지문 템플릿을 획득함으로써 진짜와 거짓 특징점을 쉽게 구별하는 방법이다. 본 논문에서는 상관공격에 강인도록 지문 퍼지볼트를 생성하는 방법을 제안한다. 제안한 방법은 특징점의 각도 정보를 이용하여 거짓선분(Chaff Line)을 생성한 후 "규칙적"으로 거짓특징점을 삽입함으로써, 두 개 지문 템플릿을 획득하더라도 동일한 지문에 대해 삽입된 거짓 특징점의 위치와 각도가 유사하기 때문에 진짜와 거짓 특징점을 구별하기 어려워 상관공격을 피할 수 있다. 실험을 통하여 거짓 특징점을 규칙적으로 저장하는 방법을 적용함으로써 기존 방법의 인식 성능을 유지하면서, 상관 공격에 강인함을 확인하였다.

1. 서론

바이오 인식 기술은 패스워드 또는 PIN 방식에 비해서 타인에 의해 도용될 우려가 적고 사용자가 암기하지 않아도 되는 장점이 있다. 그러나 사용자 인증을 위해 저장된 바이오 정보가 타인에게 도용된다면 패스워드나 PIN과 달리 변경이 불가능하거나 제한적이기 때문에 심각한 문제를 일으킬 수 있다. 따라서 바이오 정보를 안전하게 전송/저장하는 방법이 필요하다[1].

2002년 Juels[2]가 퍼지볼트 이론을 제안하면서부터 퍼지볼트를 지문에 적용하는 연구가 활발히 진행되고 있다. 지문 퍼지볼트[3] 방법은 다수의 거짓 특징점(chaff minutiae)을 "임의"로 생성하여 진짜 특징점(real minutiae)과 함께 데이터베이스에 지문 템플릿으로 등록함으로써 지문 정보를 보호한다.

또한, 퍼지볼트 이론을 지문에 적용하였을 때 발생하는 지문정렬 문제(Fingerprint Alignment Problem)를 해결하기 위하여 여러 가지 연구가 진행되는데, 그 중에서 Chung은 기하학적 해싱(Geometric Hashing)[4]을 이용하여 지문 퍼지볼트에 추가 정보 없이 자동 정렬을 수행하였다[5].

그러나 최근, 이러한 지문 퍼지볼트를 효과적으로 크래킹 할 수 있는 상관공격(Correlation Attack)에 관한 연구가 발표되었다[6,7]. 이것은 동일한 지문으로 부터 생성되는 두 개 이상의 지문 템플릿을 획득하여 진짜 특징점과 거짓 특징점을 쉽게 구별하는 방법이다.

본 논문에서는 지문 퍼지볼트에 대한 상관공격의 특징을 살펴보고, 진짜 특징점의 정보를 이용하여 "규칙적"으로 생성된 거짓 특징점을 삽입함으로써, 생성되는 두개의 지문 템플릿을 동시에 취득하도라도 진짜와 거짓 특징점을 구분할 수 없는 방법을 제안한다.

2. 상관공격에 강인한 지문 퍼지볼트

2.1. 지문 퍼지볼트 상관공격

지문 퍼지볼트의 상관공격[6,7]은 동일한 지문으로 부터 생성되는 두개의 지문 템플릿을 취득함으로써 진짜 특징점과 거짓 특징점을 쉽게 구별하는 방법이다. 따라서 두 지문 템플릿을 정렬하여 가장 많이 매칭되는 특징점을 획득하면, 매칭되는 특징점들 중에는 진짜 특징점 다수와 거짓 특징점 소수가 추출된다. 즉, 동일한 지문으로 부터 생성된 각각의 지문 템플릿을 매칭하였을 때, 진짜 특징점을 쉽게 추출 할 수 있다.

지문 퍼지볼트에서 상관공격을 피하기 위한 방법은 서로 다른 응용간 특징점을 패스워드와 같은 추가정보를 이용하여 강제 변형하는 방법이 있다[8,9]. 따라서 만약, 공격자가 강제로 변형된 두 지문 템플릿을 이용하여 매칭시킨다면 변형된 특징점 때문에 다항식을 풀 수 있을 만큼의 충분한 진짜 특징점을 획득할 수 없다.

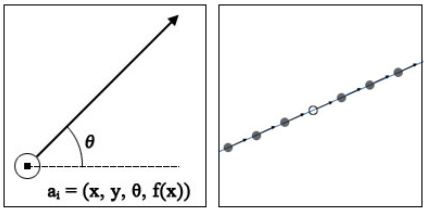
그러나, 패스워드를 이용하여 특징점을 강제변환 하는 방법은 지문정보를 활용하는 기본 이유인 편리성을 크게 훼손하게 된다. 따라서 패스워드와 같은 추가적인 정보 없이 상관공격에 강인하도록 지문 퍼지볼트 기법을 개선할 필요가 있다.

2.2 제안 알고리즘

본 논문에서는 상관공격에 강인한 지문 퍼지볼트를 생성하기 위하여 진짜 특징점의 정보를 이용하여 거짓 특징점을 삽입한다. 기본적인 방법으로는 지문 특징점 좌표 및 각도 정보를 이

용하여 거짓 선분을 생성하고 진짜 특징점으로부터 일정한 간격으로 거짓 특징점을 거짓 선분 위에 위치시킨다. 이 때, 거짓 특징점은 지문 특징점과 동일한 각도 정보를 갖게 된다.

그림 1은 거짓 특징점을 삽입하는 과정을 나타낸다. 진짜 특징점은 그림 1.(a)에서와 같이 좌표 및 각도 정보를 갖는다. 본 논문에서는 특징점 정보를 이용하여 거짓 선분을 생성 한 후, 계산된 좌표 변화량과 거짓 특징점의 간격을 이용하여 거짓 특징점을 삽입한다. 이와 같은 방법으로 그림 1.(b)같이 거짓 특징점을 삽입할 수 있다. 이 때, 삽입되는 거짓 특징점 간격은 인식 성능에 영향을 주기 때문에 인식 성능이 저하되지 않는 범위에서 고려해야한다.



(a) (b)

(그림 1) 제안한 거짓 특징점 삽입 방법

따라서, 공격자는 상관공격에 의하여 지문 특징점을 획득하여도 다량의 거짓 특징점을 동시에 획득하기 때문에 추가적으로 상관공격 결과에서 진짜 특징점과 거짓 특징점을 구별하는 작업이 필요하게 된다.

또한, 많은 양의 거짓 특징점을 삽입하기 위하여, 다수의 거짓 선을 생성함으로써 문제를 해결한다. 즉, 앞에서 생성된 거짓 선분의 평행이동 값을 이용하여 다수의 거짓 선분을 생성하여 동일한 방법으로 거짓 특징점을 삽입한다. 그림 2는 실제 지문 이미지에서 추출한 특징점 정보로 거짓 특징점을 삽입한 퍼지볼트의 그림이다.

(a) (b)

(그림 2) 제안한 거짓 특징점 삽입 방법을 적용한 그림 (a) : 실제 이미지로부터 추출한 특징점 (b) : 제안한 거짓 특징점 삽입 방법을 적용한 퍼지볼트

마지막으로, 제안한 알고리즘을 적용하기 위해서는 인식 성능에 영향을 주는 거짓 특징점의 간격과 생성되는 거짓 선분 사이의 간격을 기존 방법에서의 인식 성능을 유지할 수 있는 수준에서 결정하여야 한다.

3. 세부 구현 및 실험 결과

본 논문에서는 실험을 위해 FVC2002[10]의 DB1 Set A를 사용하였다. 지문 이미지의 크기는 388×374이다. 또한 본 논문에서 제안한 방법을 적용하여 평균 390개를 생성하였고, 지문 정렬을 위하여 기하학적 해싱 기법[8]을 적용하였다. 모든 실험은 2.66GHz CPU에 2GB RAM이 탑재된 PC에서 수행하였다.

본 논문에서는 제안한 방법을 적용하기 위하여 기존 방법에서의 인식 성능이 저하되지 않는 범위에서 거짓 특징점의 간격과 거짓 선분 간격을 정하기 위하여 실험을 전개하였다. 따라서, 제안한 방법 중 FRR이 6.0%, FAR이 0.5%의 인식 성능을 보이는 경우로, 거짓 특징점 간격은 100, 거짓 선분 간격을 50으로 결정하였다.

본 논문에서 제안한 방법이 상관공격에 강인한지를 확인하기 위해 기존방법과 제안한 방법에서 두 개의 지문 템플릿을 매칭하여 상관공격을 수행한 후, 보안성을 분석하였다. 즉, 두 개의 지문 템플릿의 상관공격을 통하여 진짜 특징점을 구별할 때 필요한 전수조사에 진짜 특징점을 구별할 수 있는 확률로 나눔으로써, 보안성을 계산하였다. 표 1은 기존 방법과 제안한 방법에서의 보안성을 나타낸다. 수행 결과에 따르면, 제안한 방법이 기존 방법보다 인식성능이 저하되지 않고 상관공격에 대한 보안성이 30배 향상되었음을 확인 할 수 있었다.

<표 1> 기존 방법과 제안 방법에서의 보안성 및 인식성능

Chaff 360	전수조사	상관공격에서 보안성	인식성능	
			FRR	FAR
기존 방법	2.93×10^7	1.74×10^4	7%	0.2%
제안한 방법		5.25×10^5	6%	0.5%

4. 결 론

본 논문에서는 지문의 특징점 정보를 이용하여 거짓 특징점을 규칙적으로 삽입함으로써 상관공격에 강인한 지문 퍼지볼트 기법을 제안하였다. 제안한 방법은 동일한 지문으로 부터 생성된 두개의 지문 템플릿을 동시에 획득하더라도 상관공격으로부터 획득한 지문 특징점으로부터 진짜와 거짓 특징점을 구분하기 어렵다. 실험을 통하여, 제안한 방법은 인식성능의 저하없이 기존방법에 비해 상관공격에 30배 높은 보안성을 제공하는 것을 확인하였다.

감사의 말

본 연구는 지식경제부 및 정보통신연구진흥원의 IT성장동력기술개발사업[2007-S-020-02, 프라이버시 보호형 바이오인식 시스템 개발]과 대학IT연구센터(홈네트워크연구센터) 육성, 지원사업의 연구결과로 수행되었음.

참고문헌

[1] U. Uludag, *et al.*, "Biometric Cryptosystems: Issues and Challenges," *Proc. of IEEE,* 2004.

[2] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," *Proc. of ISIT*, 2002.

[3] U. Uludag, *et al.*, "Fuzzy Vault for Fingerprints," *LNCS 3546*, 2005.

[4] H. Wolfson and I. Rigoutsos, "Geometric Hashing: an Overview," *IEEE CSE*, 1997.

[5] Y. Chung, *et al.*, "Automatic Alignment of Fingerprint Features for Fuzzy Fingerprint Vault," *LNCS 3822*, 2005.

[6] W. Scheirer and T. Boult, "Cracking Fuzzy Vaults and Biometric Encryption," 2007.

[7] A. Kholmatov and B. Yanikoglu, "Realization of Correlation Attack against the Fuzzy Vault Scheme," *Proc. of SPIE*, 2008.

[8] N. Ratha, *et al.*, "Generating Cancelable Fingerprint Templates," 2007.

[9] K. Nandakumar, *et al.*, "Hardening Fingerprint Fuzzy Vault using Password," 2007.

[10] http://bias.csr.unibo.it/fvc2002/databases.asp.