지문영상을 이용한 전자서명 키의 실시간 생성 및 인증 시스템 설계 및 구현

김재호° 한형구
한국외국어대학교 컴퓨터공학과
{highkey, hghan}@san.hufs.ac.kr

A Key Creation System for Digital Signature and Authentication using Fingerprint Feature

Jaeho Kim° Hyungoo Han
Dept. of Computer Science & Engineering, Hankuk University of Foreign Studies

요 약

현실세계에서 사이버 세계로의 전환은 우리에게 많은 생활의 변화를 가져옴과 동시에 혼란을 동반 하고 있다. 이러한 상황에서 암호기술은 사이버 세계의 질서를 잡는 핵심기술로 발전하고 있다. 본 논문에서는 기존의 공개키 기반 구조의 단점들을 보안 하는 방법으로 생체인증 기술인 지문 인식시스템과 RSA암호 알고리즘을 결합한 새로운 인증 시스템을 제안한다.

1. 서론

현실세계에서 사이버 세계로의 전환은 우리에게 많은 생활의 변화를 가져 다 주었다. 그 중 전자상거래의 발달은 직접대면 방식의 상거래가 비대면 방식의 상거래로 바뀜에 따라 지금까지 개인의 신분을 증명하기위해 사용되어 오던 기존의 방식들을 대신할 새로운 방식들이 필요하게 되었다.

사이버 세계에서의 신분 증명을 위해서 지금까지 공개키 기반 구조의 전자서명을 이용한 방법을 이용해 왔으며 세계의 각 국가들은 이를 법적으로 인정하는 추세이다. 공개키 기반 구조에서 전자서명을 위해 발급 받은 개인키는 안전한 보관이 필수 적이다. 이를 위하여 스마트 카드 등을 이용하기도 한다. 이러한 방법은 키 관리에 대한 대책을 요구하며 무엇보다도 개인키가 실제로 상존함에 따라 분실 및 도용의 위험이 항상 존재 하게 된다.

본 논문에서는 이러한 공개키 기반구조의 단점을 해결하기 위하여 개인의 신분확인을 위해서 사용되는 생체 인증 기술 중 하나인 지문 인식을 이용하여 전자 서명을 위한 실시간 키 생성 방법을 제시한다.

2. 관련연구

지문특징 추출 알고리즘은 현재 많은 연구가 진행되어 왔으며 일부 기업에서는 상용화를 시작하였다. 본 논문에서 이용된 지문영상 특징 추출 알고리즘인 "블록 FFT를 이용한 실시간 지문 인식 알고리즘"[3]은 8x8 화소 크기의 작은 블록에 대하여 2차원 고속 퓨리에 변환(FFT)을 적용한 후, 퓨리에 스펙트럼으로부터 나타나는 방향성을 이용하여 각 블록의 특징을 추출 한다. 이 방법은 2차원 FFT를 수행하기 때문에 일반 적으로 거치는 여러 전처리 과정이 생략되어 실시간 처리를 가능하게 한다.

공개키 암호 방식은 1976년 Stanford 대학의 Diffie와 Hellman이 발표한 "New Direction in Cryptography"[1]에서 처음 개념을 발표한 이후 1978년 MIT의 Riverst, Shamir와 Adleman이 제안한 RSA는[2] 현재 가장 널리 사용되어 지고 있는 암호 알고리즘이다. 본 논문에서 사용한 RSA공개키 암호 알고리즘은 충분히 큰 수 n에 대하여 두개의 소수 p, q가 $n = p \cdot q$인 관계가 성립할 때 n을 알고 있는 사람이 p, q를 찾는 소인수 분해의 어려움에 이론적 기반을 두고 있다.

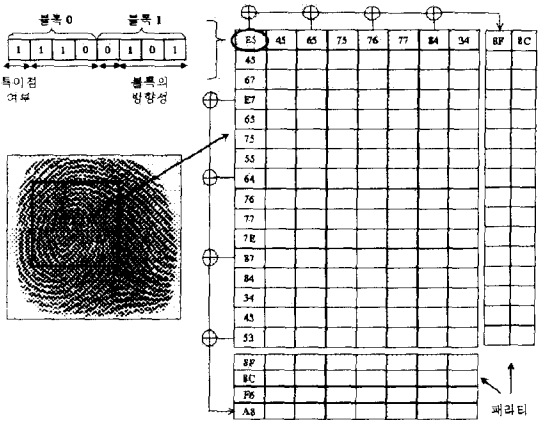
3. 지문영상 특징을 이용한 공개키 암호알고리즘 키 생성

전자서명에 사용되는 서명키는 공개키 암호알고리즘의 개인키를 이용한다. 따라서 본 논문에서는 입력 지문영상으로부터 추출된 지문영상 특징을 이용하여 공개키 암호알고리즘의 개인키를 실시간 생성하는 방법을 제시한다.

3.1 지문영상 특징의 표현과 오차 교정

본 논문에서는 입력 지문영상을 256x256화소, 256그레이 레벨의 화상으로 하였으며, 8x8화소의 단위 블록으로 분할하여 1024(32x32)개의 블록을 얻었다. 단위블록에 대한

방향성을 8-방향중의 하나로 결정하며, 방향이 정의 되지 않는 블록 등은 특이점으로 구분한다. 이렇게 얻어진 방향성을 이용하여 실제로 지문인식을 위한 중심점을 선정하고 중심점을 기준으로 하여 유용한 블록 영역만을 선택한다[3]. 본 연구에서는 최종적으로 256(16 x 16)개의 블록을 유용한 블록으로 선택 하였다. 방향성과 특이점 여부를 나타내고 있는 추출된 지문영상의 특징은 각각 블록에 나타난 특징을 4비트의 정형화된 표현 형식으로 나타낼 수 있다. [그림 1]은 추출된 지문 특징을 정형화 하여 표현 하는 방법을 보여주고 있다.



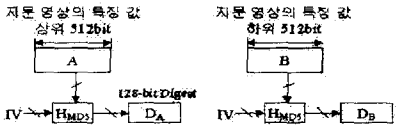
[그림 1]블록에 나타난 지문영상 특징의 표현

여기서 두개 블록의 지문영상 특징 정보는 한 바이트에 나타낼 수 있으며 전체 16 x 16블록은 8 x 16바이트로 표현가능 하다. 지문영상은 채취 되는 때의 조건에 따라 동일인의 지문이라 하더라도 약간의 오차를 가진다. 이러한 오차로 인해 전혀 다른 키가 생성되는 오류를 방지하기 위하여 최초 지문 등록시에 수평/수직 패리티를 두었다. 최초 등록시에 기록된 패리티는 추후에 입력되는 지문의 오류를 교정해주는 역할을 하여 약간의 오차로부터 동일한 결과값을 유도해 낼 수가 있다. 본 연구에서는 16개의 블록을 하나의 단위로 하여 그 중에 한 개 블록에 대한 오류에 대해서는 동일인의 지문으로 간주하여 오류를 교정한다. 여기서 지문영상의 입력 오류의 특성상 인접한 블록들에 오류가 같이 존재할 가능성이 높기 때문에 16개의 블록을 한 단위로 묶을 때 전체에서 고르게 선택되어지도록 하였다.

3.2 해시함수를 통한 지문영상 특징에 대한 다이제스트의 산출

지문입력으로부터 얻은 1024비트의 입력정보는 상위 512비트 A와 하위 512비트 B로 두 부분으로 나누고 나누어진 두 부분은 각각 해시함수를 통해서 두개의 128비트의 다이제스트(Digest) D_A, D_B를 얻게된다. 본 연구에서 해시함수로서는 MD5를 이용하였다.

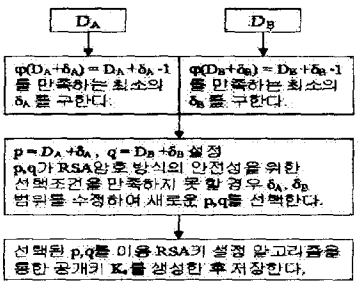
[그림 2]는 지문영상 특징으로부터 D_A, D_B를 얻는 과정을 보여주고 있다[4]. 여기서 IV는 버퍼의 초기값을 나타내다.



[그림 2] MD5 해시를 통한 Digest의 산출

3.3 지문등록을 통한 RSA 공개키의 생성

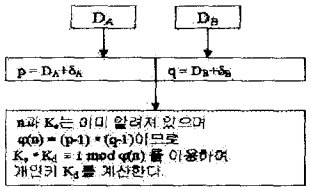
MD5 해시함수를 통해서 얻어진 두개의 128비트의 다이제스트 D_A, D_B는 RSA 공개키 암호 알고리즘의 두 소수 p, q를 계산하는데 사용 된다. D_A, D_B로부터 가장 근접해서 존재하는 소수를 각각 p, q로 선택한다. 단 p, q는 RSA암호 방식의 안전성의 보장 조건에 만족되는 소수 이어야 한다. 여기서 소수여부의 판정은 Euler의 함수(φ)에서 어떤 수 n이 소수 일 때 φ(n)이 n-1인 특성을 이용하였다. 그리고 D_A와 p의 차를 δ_A, D_B와 q의 차를 δ_B로 둔다. δ_A, δ_B는 저장해 두었다가 이후의 소수 생성시에 소수를 찾아내는 과정 없이 D_A, D_B로부터 바로 소수 p, q를 찾아 실시간 키 생성이 가능 하도록 한다. 다음으로 선택된 두 소수 p, q를 이용하여 RSA 암호 알고리즘을 이용 공개키를 생성한다. 다음은 소수 p, q의 생성과 생성된 소수를 이용한 공개키 생성의 절차이다.



소수 p, q의 생성 및 공개키 생성

3.4 개인키의 생성

개인키 생성을 위해서 지문영상이 입력되면 앞에서 제시된 해시함수를 통해서 지문영상특징에 대한 다이제스트 D_A, D_B를 얻는다. 먼저 지문 검증 과정을 거친후 본인 지문으로 확인이 되면 D_A, D_B와 가지고 있던 δ_A, δ_B 를 이용하여 간단히 p, q 계산해 낸다. 이미 알고있는 공개키 K_e와 p, q를 이용 개인키를 생성한다.

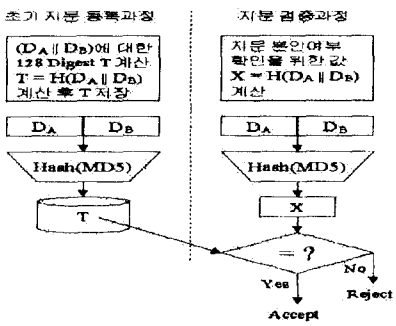


개인키 생성 과정

3.5 지문 검증

초기 지문등록과정에서 입력 지문영상 특징으로부터 해시함수를 통해 얻어진 D_A, D_B를 다시 해시함수를 (MD5) 적용해서 새로운 128비트 다이제스트 T를 계산하여 저장한다. 이렇게 생성된 T는 지문영상의 본인여부를 확인 하는데 사용된다. 비록 디바이스에 저장된 T가 노출이 되어도 이는 일방향 해시함수를 거친 결과이므로 T를 통해 D_A, D_B를 얻어 내는 것이 사실상 불가능하다. 따라서 지문특징이나 p, q 를 찾아낼 수 없으므로 개인키를 생성할 수 가 없다.

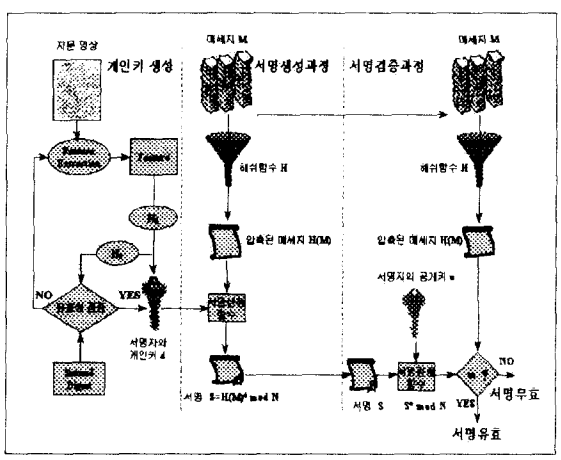
지문 검증과정에서 지문영상이 입력되고 지문영상 특징에 대한 다이제스트 D_A, D_B가 얻어지면 D_A, D_B에 대한 해시함수를 적용한 값 X가 디바이스에 저장되어있는 T와 일치하는지 비교 한다. 일치하면 본인의 지문으로 검증되며 본인의 비밀키를 생성할 수 있다.



지문 검증과정

4 지문영상 특징을 이용한 전자 서명

지문영상 특징을 이용 최초 공개키를 인증기관에 등록 후 전자서명을 할 경우 지문 입력으로부터 개인키를 생성하여 전자 서명을 할 수 있다. [그림 3]은 기존의 전자서명 방식에 본 논문에서 제한한 방식을 적용한 전체 시스템 구성을 보여주고 있다.



[그림 3] 지문 특징 정보를 이용한 전자서명

5 제안된 시스템의 안전성

본 논문은 지문 인식을 기반으로 공개키 암호알고리즘인 RSA의 키를 생성하는 방법을 사용함에 따라 지문 자체 보안 특성에 의존한다. 본 논문에서 사용한 지문인식 알고리즘은 타인의 지문을 본인의 지문으로 잘못 인식하는 타인 접수율을 0%로 했을 때 자신의 지문을 타인의 지문으로 판단하는 본인 거부율이 2.2%로 실험결과 발표되었다.[3] 지문인식 알고리즘의 계속된 발달로 현재에는 본인 거부율이 0.1%미만 까지 줄일 수 있는 알고리즘이 개발된 상태이다.

다음으로 본 논문에서 제시된 MD5 해시함수는 입력의 크기가 128bit이상에 대해서는 안정성이 검증되어 있다. 즉 2차 다이제스트 T로부터 D_A, D_B를 알아내는 것이 거의 불가능 하다.[4]

6 지문 특징 정보를 이용한 전자 서명의 장점

제안된 시스템은 기존의 공개키 기반 전자서명의 개인키를 따로 보관하지 않고 개인의 지문영상의 특징을 통해서 개인키를 실시간 생성함으로 서 키 관리상에 발생할 수 있었던 보안상의 문제점을 해결 하였으며 또한 개인 지문 입력을 통한 일괄적인 전자서명 방식은 보안성 및 편리성을 향상시킬 수 있다. 이러한 특징은 관리상의 헛점과 분실의 우려가 높은 이동통신 단말기에 특히 효율적으로 적용 될 수 있을 것인다. 21세기 차세대 개인 휴대정보단말기로서 주목 받고 있는 PDA(Personal Digital Assistant)환경에 본 시스템을 적용한다면 기존의 전자 지불은 물론 은행창구와 ATM을 통한 은행업무를 대신할 수 있는 대안이 될 것 이다.

7. 결론 및 향후 연구과제

본 논문은 새로운 생체 인증 보안 솔루션으로 각광 받고있는 지문 인식시스템과 암호화 알고리즘의 장점을 결합하여 전자서명을 위한 키를 실시간 생성하는 방법을 제시하였다. 제안된 시스템은 수많은 응용분야를 가지고 있어 향후 보안 산업발전에 많은 기여를 할 수 있을 것이다.

향후 과제로 더욱더 효율적인 지문 인식시스템의 개발과 이동통신환경의 열악한 컴퓨팅능력에서 더욱더 효과적으로 적용될 수 있는 암호 알고리즘이 개발 되어야 할 것이다.

8. 참고 문헌

[1] W. Diffie, and M. E.Hellman, "New directions in cryptography", IEEE Trans. on Information Theory IT-22 No. 6, pp.644-654, 1976.

[2] R. L. Rivest, A. Shamir and L. Adleman, "A method of obtaining digital signature and public key cryptosystem", ACM Communication 21 No.2, pp.120-126, 1978.

[3] 안도성, 김학일, "블럭 FFT를 이용한 실시간 지문인식 알고리즘," 전자 공학회 논문지, 제32권, B편, 제6권, pp.89-101, 1995.

[4] 김철, 암호학의 이해, p.328, 영풍문고, 서울, 1996.