다중 고유얼굴 기반의 키 생성 기법 연구

김애영° 이상호
이화여자대학교 컴퓨터학과
kay@ewhain.net, shlee@ewha.ac.kr

Study on Key Generation Using Multi-Eigenfaces

Ae-Young Kim° Sang-Ho Lee
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

인터넷과 같은 개방된 공간에서 중요한 정보는 상당한 발전을 이룩한 암호화 기술에 의해 보호된다. 그러나 컴퓨터의 급속한 발전은 암호화의 근간이 되는 키에 대하여 더욱 길고 안전한 키를 요구한다. 이는 기억해야할 또는 안전하게 소지해야할 정보가 더 많아짐을 의미한다. 이러한 상황에서 개인의 생체정보를 기반으로 하는 키의 이용은 일정 수준의 보안성을 만족하기위한 키의 길이가 증가됨을 억제하고, 외우거나 소지해야하는 불편함도 해소해준다. 그러나 기존의 생체인식 기반의 키 생성 기법 연구는 여러 종류의 생체인식을 동원한 특징점 및 매개변수 정보를 기반으로 하고 있어 실제 활용함에 제한이 있다. 따라서 본 논문에서는 적용할 단 하나의 생체인식으로 얼굴인식을 채택하였고, 이 얼굴인식의 다중 고유얼굴을 이용하여 특징점 및 매개변수 집합을 형성하고, 이 집합으로부터 더욱 안전하고 편리한 키를 생성하는 기법을 연구하였다.

1. 서 론

현대 사회는 인터넷을 통하여 데이터를 안전하게 주고받거나, 저장 시스템에 정보를 안전하게 저장하거나, 자신의 중요 정보를 보호하기 위하여 암호화 기술을 이용한다. 암호 시스템의 안전성은 암호 알고리즘의 강도, 키의 길이, 키의 관리 문제 등으로 평가한다.

특히 키와 관련하여, 컴퓨터의 급속적인 발달은 더욱더 긴 키를 요구하며, 패스워드, 스마트카드 등과 같이 키 관련 정보를 기억해야하거나 소지해야하는 등으로 불편한 키의 관리가 요구되는 문제점이 있다. 이러한 문제점을 해결하기 위하여 키의 생성 및 관리에 생체인식의 적용해 볼 수 있다.

생체정보 기반의 키를 생성하여 암호화에 이용하면 키와 관련된 값을 기억하거나 소지할 필요가 없는 편리성과 동일한 키 길이로 더 높은 안전성을 확보한다는 보안성을 장점으로 갖는다. 그러나 개개인의 생체정보인 특징점에서 키를 추출하는 것은 쉽지 않다. 생체인식에서 사용자 인증은 정확히 동일한 값의 비교가 아니라 기준 정보와 입력된 정보 사이의 유사도 측정으로 이뤄지므로, 매번 추출되는 생체정보는 매번 동일한 정보로 추출되기가 어렵다는 사실이 키 추출의 어려움이며 부동성의 확보가 요구된다.

이러한 요구사항들을 충족하기 위한 기법으로 지문, 얼굴, 홍채, 음성, 장문 등 각각에 대하여 특징점 및 관련 매개변수들을 모아서 하나의 키로 사용하는 개념이 연구되어왔다. 그러나 이 특징점 및 매개변수 집합을 이용한 키 생성 기법은 이전의 생체인식 기반의 키 생성 기법들의 문제를 해결하고는 있으나, 일정 수준의 안전성을 확보하기 위해서는 너무 많은 종류의 생체인식이 필요하다는 단점을 가지고 있다.

따라서 본 논문에서는 이러한 단점을 보완하기 위하여 여러 종류의 생체인식 기법이 아닌 얼굴인식 기법 하나만으로 대칭키 암호 시스템에 적합한 편리하고 안전한 키를 생성하는 기법을 연구하고자 한다. 다중 고유얼굴 기반의 특징점 및 매개변수 집합을 이용한 키의 생성은 단지 한 종류의 생체인식으로도 더욱 안전하고 편리한 생체정보 기반의 암호화 시스템을 구현하는데 효과가 있다.

2. 생체인식 기반의 암호화 시스템

2.1 생체인식 기반의 키에 대한 요구사항

비밀키 암호화 알고리즘을 위한 키 생성 기법이 유용하기 위해서는 다음과 같은 사항들을 고려해야 한다.

① 키의 강도
부루트포스 공격에 대항하기 위하여 키의 길이를 길게 하기보다는 동일한 키의 길이에 대하여, 이 공격에 더 강한 키를 형성하도록 한다.

② 생체정보의 유일성
생체정보 기반 키의 유일성은 개개인의 생체정보가 유일하다는 성질을 바탕으로 한다.

③ 키의 부동성
제한된 키 공간에서 유효한 사용자를 찾기 위해 특징점의 다양성을 적당한 크기로 줄인다.

④ 계산량 감소
생체정보를 비밀키로 이용하는 과정에서 계산량이 많지 않도록 한다.

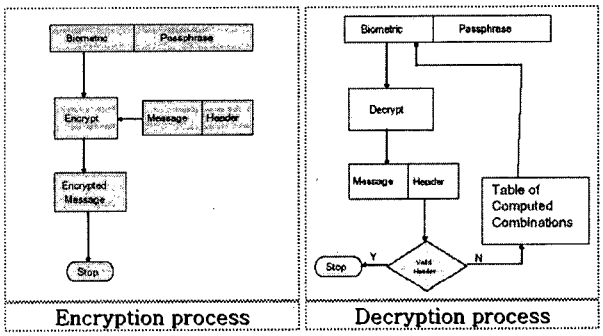
⑤ 암호화 시스템의 단순화
생체정보 기반의 키 생성으로 인하여 암호화 시스템이 복잡해지지 않도록 한다.

2.2 생체정보 암호화 시스템의 기존 연구 사례

1998년에 제안된 키 분배 알고리즘에서 암호화 키는 사용자의 DB에 저장, 판별을 위한 생체정보에의 접근, 그리고 사용자의 인증과 키의 분배에 대한 완전한 분리를 요구된다. 이 방법은 키를 생성할 신뢰자의 확보가 어렵고, DB에 저장해야하는 약점이 있으며, 스푸핑을 통한 정보의 노출이 발생하는 문제점을 가지고 있다[1].

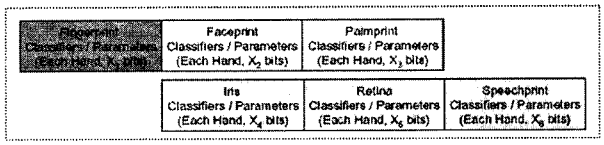
그 이후 1999년에 생체정보 암호를 위하여 Bioscrypt가 제안되었다[2]. 이 시스템은 암호키 접근을 위하여 패스워드를 입력하는 대신에 생체인증으로 키를 보호하는 생체정보 암호 시스템이다. 이 시스템에서 키는 등록과정에서 생체정보와 연결되고, 인증과정에서 반환되는 방법이며, 이때 반환되는 결과값은 예/아니오의 정보가 아니라 생체이미지에서 추출되는 값이다.

이 시스템에서 키는 생체 정보와 관계가 없으므로 해킹이 되어도 쉽게 변경이 가능하고 생체 인증 한 번으로 암호화를 할 수 있는 편리함을 제공한다. 하지만 처리 과정에 대한 계산량이 크고 시스템이 복잡한 문제점을 가지고 있다.



[그림 1] Biometric Cryptography, CSPRI-2004-09

2004년에는 비밀키 암호 시스템을 위한 키 생성 알고리즘이 제안되었으며, 전체 흐름은 [그림 1]과 같다[3]. 이 시스템에서는 생체정보를 비밀키로 사용하며, 상대적으로 이전의 생체정보 기반의 암호 시스템보다 덜 복잡하고 계산량도 많지 않다.



[그림 2] 생체정보 기반 키

[그림 1]에서 비밀키로 사용하는 생체정보 키의 구성은 [그림 2]와 같이 여러 종류의 생체인식을 동원하여 그 조합의 경우의 수를 크게 하였으며, 이는 브루트포스 공격에 강하도록 했다. 하지만 이는 동시에 여러 생체인식을 수행해야하는 문제점을 가지고 있다.

3. 다중 고유얼굴 기반 얼굴인식 모듈

3.1 고유얼굴

주성분 분석 기반의 고유얼굴을 획득은 다음과 같은 흐름을 통해 이루어진다.

① 영상을 고차원상의 포인트로 취급
② 얼굴 분포에 대한 PC(Principal Components, 주성분)를 각 얼굴 영상간 구별을 위한 특징정보로 사용, 즉 얼굴 영상의 covariance matrix의 eigenvector를 특징정보로 사용 = 고유얼굴
③ 주요한 M개의 eigenface가 부여된 공간을 Facespace로 여김
④ 입력된 얼굴 영상을 Facespace 상에 투영
⑤ 투영된 영상값을 패턴인식 처리

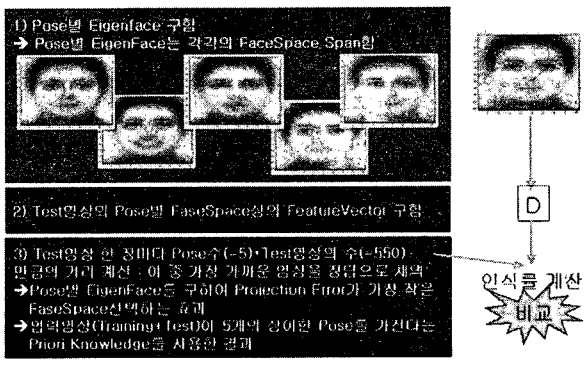
본 논문의 실험을 위해 위의 흐름을 매트랩으로 구현한 코드는 [그림 3]과 같다.

M : average image of training set
A=[I_1-M I_2-M I_3-M... I_N-M], I : training set
C=A' A
[W_{PCA} L_{PCA}]=eigs(C,ComponentNo)
W_{PCA}=A*W_{PCA}
W_{PCA}(:,i) = W_{PCA}(:,i) ./ norm(W_{PCA}(:,i)) : Eigenface normalization
FeatureVector= W_{PCA}'* (TestImage –M)

[그림 3] 고유얼굴 확보를 위한 매트랩 코드

3.2 포즈별 다중 고유얼굴

1) 포즈별 고유얼굴 획득 및 인식 기법



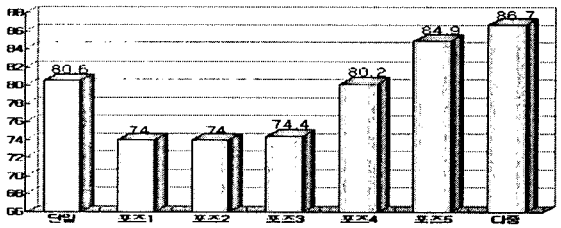
[그림 4] 다중 고유얼굴 획득 및 얼굴인식

데이터가 포즈별로 확실하게 구분되어있다는 사실을 인지하

고 [그림 4]와 같은 세 단계에 걸쳐 포즈별 고유얼굴을 형성하고 얼굴인식을 수행한다. 이러한 인식 과정에서 인식 대상의 영상은 다중 고유얼굴과 각각 유사도를 측정하고, 그 측정값들 중에서 가장 유사도가 높은, 즉 가장 적은 거리 값을 갖는 영상과 같은 영상이라고 최종 인식된다. 이는 웃는 얼굴은 웃는 고유얼굴을 기준으로 하여야 최적의 인식률을 갖는다는 생각을 기반으로 한다.

2) 구현결과

[그림 5]와 같이 단일 고유얼굴(80.6%)에 비해 포즈별로 고유얼굴을 형성해 다중(86.7%)으로 인식에 참여시킨 결과가 인식률이 높다. 이는 포즈별 고유얼굴이 유효한 기준임을 나타낸다.



[그림 5] 단일 고유얼굴과 다중 고유얼굴의 적용 비교

4. 다중 고유얼굴 기반 키 생성

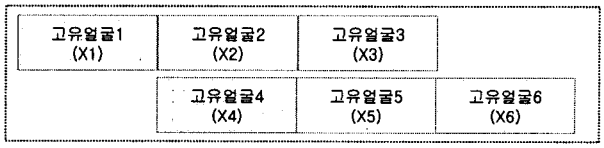
4.1 생체정보 기반 암호 시스템

본 논문에서 적용하고자 하는 생체정보 기반의 암호 시스템은 [그림 1]과 같이 복잡하지 않은 비밀키 암호 시스템이다. 생체정보로 구성된 값을 비밀키로 이용하여 메시지를 암호화하며, 마찬가지로 같은 정보를 비밀키로 이용하여 암호문을 복호화한다.

4.2 다중 고유얼굴 기반 키 생성

비밀키 암호화 시스템에 사용되어질 키를 [그림 2]와 같이 구성한다면, 하나의 키는 6 종류의 생체인식을 수행함으로 얻을 수 있다. 또는 하나의 키 블록은 몇 종류의 생체인식으로부터 6개의 값만큼을 조합해 같은 종류의 생체정보에 대한 중복을 허용하여 키를 생성 할 수도 있다. 이는 어떤 종류의 생체정보로부터 특징 값을 추출해내어 키를 구성시키느냐의 조합의 문제가 된다. 즉 6비트가 한 라운드에 적용되는 하나의 키 블록이라고 한다면, 이 하나의 키를 생성하기 위한 경우의 수는 전체 생체정보의 종류의 수에서 6가지를 골라내는 경우의 수와 동일하다. 이 경우의 수는 키의 길이가 길어질수록 지수 승으로 커진다. 이와 같이 키 스페이스가 커지는 것은 부루트포스 공격으로부터 안전함을 의미한다. 그러나 여러 종류의 생체인식을 통해 해당 측정값들을 확보하는 것은 쉬운 작업이 아니거나 비효율적이다.

본 논문에서는 여러 종류의 생체인식을 수행해야하는 불편함을 해결하기 위하여 [그림 6]과 같이 여러 종류의 고유얼굴을 기반으로 하는 키의 생성을 제안해보았다. 키를 형성하는 조합의 수는 고유얼굴의 수에 따라 달라질 수 있다. 가능한 키 생성의 수는 고유얼굴의 전체 수에서 키를 형성하기 위해 참여시킬 고유얼굴을 선택하는 경우의 수이다. 그리고 사용하고자 하는 키의 길이에 따라 경우의 수는 상당히 달라진다. 즉 키 길이의 확보에 의해서만이 아니라, 고유얼굴 수에 의해서도 높은 수준의 보안성 유지에 필요한 키 스페이스를 확보할 수 있다.



[그림 6] 다중 고유얼굴 기반 비밀키

따라서 여러 종류의 생체인식 정보를 기반으로 하는 키 구성법을 대신하여, [그림 6]과 같이 여러 종류의 고유얼굴을 기반으로 하는 키의 구성은 길지 않은 키로도 훨씬 더 효율적이고 유용한 생체인식 기반 암호화 시스템을 구현하는데 효과적이다.

5. 결론 및 향후 연구과제

본 논문에서는 여러 종류의 생체인식을 기반으로 하는 키 생성 기법과 얼굴인식에서 유효한 여러 종류의 고유얼굴을 생성하는 기법을 고려하여, 비밀키 암호 알고리즘에 적용할 키를 구성해보았다. 본 키의 구성은 얼굴인식 기법의 하나인 다중 고유얼굴을 기반으로 키를 생성하기 때문에 여러 생체인식을 수행하는 불편함을 해소하였으며, 키 생성에 참여할 생체정보의 수를 여전히 여러 가지 고유얼굴의 수로 확보하고 있기 때문에 키 생성을 위한 경우의 수, 즉 키 스페이스는 여전히 확보된다. 이러한 키의 생성 기법은 유용한 생체인식 기반 암호 시스템을 구현할 것이다.

향후 연구과제로는 제안된 키 생성법을 실제 상황에 적용할 때 보안상의 문제점은 없는지를 연구해보는 것과 다중 고유얼굴과 다른 생체인식과의 조합은 어떠한 결과를 나타내는지를 연구하는 것이다.

참고문헌

[1] Soutar, C., D.Roberge, S.A.Stojanov, R.Gilroy, and B.V.K.Vijaya Kumar, "Biometric encryption using image processing." Proceedings of the SPIE OSCDT II, 178-188, 1998

[2] Soutar, C., D.Roberge, "Biometric Encryption", 1999

[3] Christopher Ralph Costanzo, "Biometric Cryptography: Key Generatioin Using Feature and Parameteric Aggregation", CSPRI, 2004

[4] 송영기, 강환일, "생체인식의 길," 인터비전, 2004