안전한 스트리밍 서비스를 위한 지문인식기반 인증시스템

Authentication System based on Fingerprint Scan for Safety Streaming Service

조제경, 서종원, 이형우
한신대학교

Jo Je-Gyeong, Seo Jong-Won, Lee Hyung-Woo
Hanshin Univ.

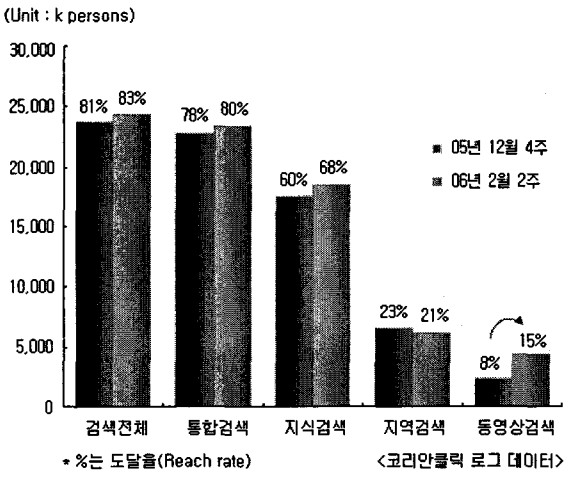
요약

현재 인터넷 상에서 수많은 멀티미디어들이 쏟아져 나오고 있다. 그로 인해 멀티미디어 서비스의 기술이 점점 발전해가며 그에 따라 멀티미디어의 불법 복제 또한 발달하였다. 기존의 ID와 Password를 입력하여 로그인 하던 시스템에서 수많은 해킹이 이루어졌으며 자신도 모르는 사이 자신의 아이디로 가입이 되고 결제가 되어 멀티미디어를 이용하고 있는 경우가 많아지고 있다. 이러한 많은 해킹의 위험으로부터 멀티미디어를 보호해야 할 필요가 있으며 그로 인해 현재 수많은 발달과 관심이 쏟아지는 바이오 인식을 이용하여 멀티미디어 서비스를 한 차원 더 발전시키고자 한다.

I. 서 론

인터넷 기술의 발달로 수많은 콘텐츠들이 인터넷을 통해 전파 되고 있다. 예전에는 상상도 못했던 인터넷을 통해 음악을 감상하고 영화나 뉴스를 실시간으로 인터넷을 통해 본다는 것이 가능해진 것이다. 이렇게 인터넷을 통해 음악이나 동영상의 재생 서비스가 가능해진 것은 인터넷의 발달이 그 기반이 되었다고 할 수가 있다. 예전에는 너무나 느린 인터넷의 속도로 인하여 동영상이나 음악의 데이터를 실시간으로 전송하기가 너무나 어려웠던 것이다. 하지만 이제는 공중파로 방송하는 뉴스조차도 실시간으로 볼 수 있을 정도로 빨라진 것이다. 여러 방송국에서 뉴스뿐만 아니라 채널의 대부분을 실시간으로 제공을 하고 있으며 지나간 채널도 다시 볼 수 있도록 서비스를 하고 있다. 그리고 방송국뿐만 아니라 몇몇 대형 포털 사이트에서도 웹서비스의 첫 화면에 동영상 서비스를 집어넣어 하루의 이슈가 되는 동영상이 올라오고 있다. 하지만 이것 큰 비중이라고 하기에는 부족하다고 말할 수 있다. 국내 교육의 비중이 큰 것은 누구라도 다들 알 것이다. 국내 교육에서 이제는 E-Learning이 차지하는 비율이 증가하면서 인터넷을 통한 동영상을 서비스하여 동영상을 통한 학습에 중점을 두고 있다. 대부분의 E-Learnig 서비스업체에서 동영상을 서비스하고 있으며 동영상의 기술이나 자금의 부족의 경우 그림과 음성을 통한 서비스로 국내 교육의 발달에 이바지 하고 있는 것이다. 특히 PMP라고 하는 Potable Media Player가 등장하면서 동영상은 어디서든 언제든 볼 수 있게 되었다. 그로 말미암아 동영상의 수요가 엄청난 속도로 증가하였으며 인터넷 및 컴퓨터 사용에 엄청난 비중을 차지하고 있다.

1) 본 연구는 2006년 정보통신부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음.



▶▶ Fig 1.1 동영상 사용의 증대

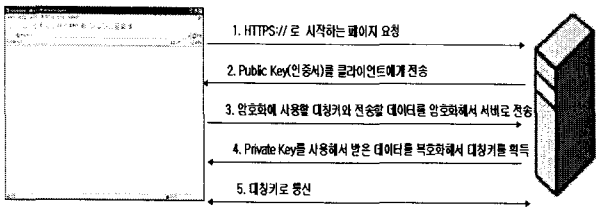
하지만 동영상 서비스의 증대로 인해 결제 시스템이 필요해지고 동영상의 결제를 위해 다른 사람의 아이디 도용이나 불법 결제자들이 늘어나고 있다. 동영상 서비스의 양은 늘었지만 거기에 대한 기술은 제자리를 돌고 있는 것이다. 그렇기에 동영상 서비스와 같은 결제를 요구하는 서비스에서 조금 더 보안에 강한 기술이 나와야 하는 것이다.

II. 관련연구

2.1 HTTPS

현재 HTTPS는 수많은 사이트에서 결제용으로 사용되고 있다. HTTPS는 월드 와이드 웹통신 프로토콜인 HTTP의 보안

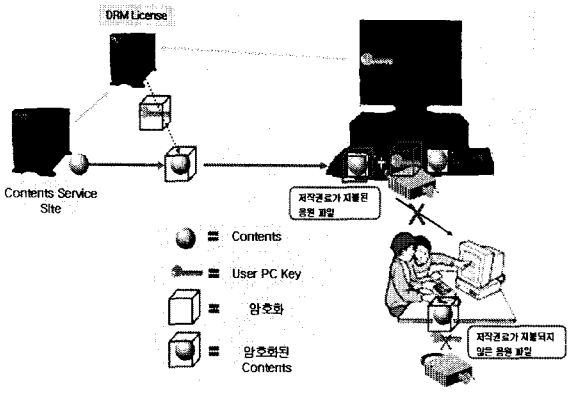
이 강화된 버전이다. HTTPS는 통신에서의 인증과 암호화를 위해 넷스케이프 커뮤니케이션즈 코퍼레이션이 개발했으며 전자 상거래에서 널리 쓰인다. HTTPS는 소켓 통신에서 일반 텍스트를 이용하는 대신에 SSL이나 TLS 프로토콜을 통해 세션 데이터를 암호화한다. 여기서 SSL은 RC4 스트림 암호 알고리즘으로 40비트 키 크기를 사용한다. 하지만 웹에서 신용카드를 사용하는 사람들 사이의 흔한 오해 중 하나는, HTTPS를 이용할 때 HTTPS가 완벽한 보호를 제공해준다고 생각하는 점이다. 그러나 실제로 이것은 웹서버와 브라우저 간에 전송되는 카드 정보만이 암호화될 뿐이다. 카드 정보는 보통 데이터베이스에 저장되며 대개의 정보 유출은 내부 인력에 의해 이루어진다. 그렇기에 단순히 HTTPS를 사용한 결제시스템이라고 해서 믿기는 힘들다. 이제는 HTTPS만 믿고 사용하는 것이 아니라 새로운 인증 기술이 필요하다. 자세한 내용은 IETF의 RFC2660에서 알수가 있다.



▶▶ Fig 2.1 HTTPS의 작동 순서

2.2 DRM(digital rights management)

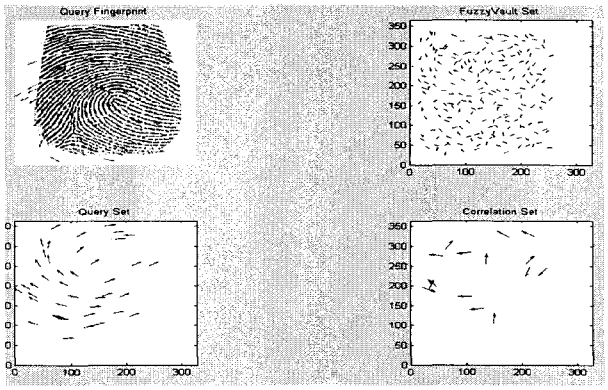
단순히 인증만이 아닌 콘텐츠의 이용을 위해 결제 한 컨테츠에 한해 제한을 두기 위해 DRM이라는 기술이 나오기 시작하였다. DRM은 네트워크에서 다양한 컨텐츠 제공자로부터 유통되는 각종 디지털 콘텐츠의 안전한 분배와 불법 복제 방지를 위한 보호방식을 말한다. 파일 교환 프로그램을 통해 전파되는 상업적 자료의 온라인 불법 복제로부터 디지털 콘텐츠를 보호하기 위한 것으로, 관련 법령이나 위반자 단속으로는 예방이 어렵기 때문에 사후 단속 보다 사전에 문제점을 파악해 첫 단계에서 내용 복제 자체를 못하도록 한 것이다.



▶▶ Fig 2.2 DRM 구조

2.3 Fuzzy Vault

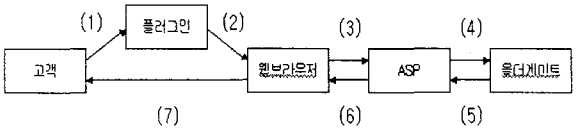
지금 현재 수많은 생체 인식 기술들이 개발되고 있다. 지문, 홍채, 음성, 안명, 체취 등 많은 종류의 생체 인식 기술들이 개발되고 있다. 일반적으로 지문은 스캔된 지문 데이터를 그대로 보관하게 된다. 이것은 노출의 위험이 상당히 높다. 지문의 인증시 아무런 암호화 과정도 없이 비교한다. 이것은 지문의 이미지를 스니핑 하는 것만으로도 충분히 재사용이 가능하다. 그리고 지문의 단점은 한번 누출시 지문의 변경은 사실상 어려우며 등록된 지문을 다른 손가락으로 변경함으로 인하여 10번의 지문 변경만이 가능하게 된다는 단점을 안고 있다. 그렇다면 이 스캔 이미지를 어떻게 보호할 것인가가 중요한 문제점이다. 현재 운영체제인 유닉스시스템에서는 암호를 Hash화하여 저장함으로써 시스템에 침투를 하더라도 암호를 볼 수 없게 하고 있다. 그렇다면 지문을 Hash화 한다면 어떠할 것인가? 이 질문에 대답하여 주는 것이 바로 Fuzzy Vault이다. 퍼지 볼트는 Hash화 된 암호처럼 가짜 특징점을 입력한 지문을 저장하여 시스템에 침투하더라도 Hash화된 암호처럼 보호할 수 있게 된다.



▶▶ Fig 2.3 Fuzzy Vault 구조

2.4 기존 시스템

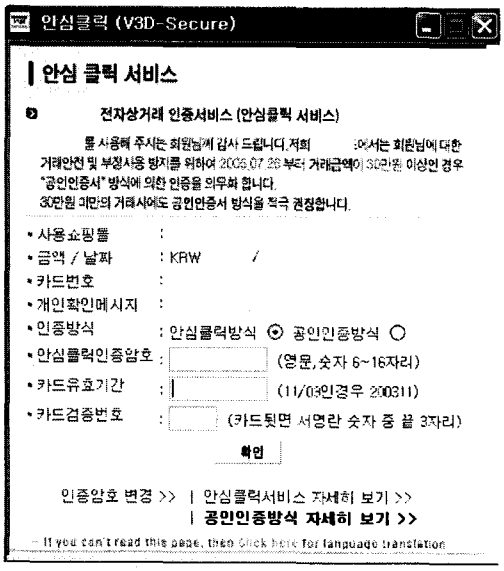
기존 결제 시스템중 H사의 A모델의 구조를 보도록 하겠다. 현재 구조를 보면 고객이 플러그인을 설치한다음 웹브라우저를 통해 결제회사에 해당 정보를 보내고 결제에 대한 정보를 다시 사용자에게 보여준다.



▶▶ Fig 2.4 결제 시스템의 구조

여기서 전송되는 정보는 카드 번호와 카드 유효 기간, 카드의 승인 번호들이다. 하지만 이것만 가지고는 결제하는 사람이 본인인지 아닌지 알수가 없다. 카드 도용의 문제점이 생길수

있는 것이다. 분실된 카드만 가지고도 충분히 결제가 가능한 것이다.

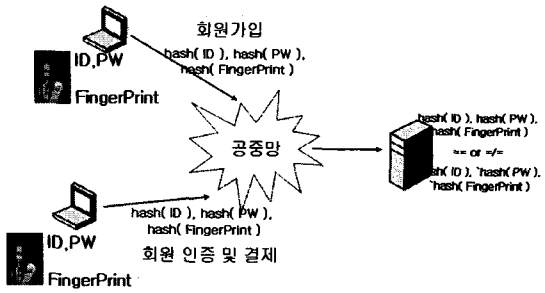


▶▶ Fig 2.5 결제 요청시 입력화면

이러한 본인의 확인 유무가 부족하기에 본인 인증을 위한 지문의 기술이 결제에 필요하게 되는 것이다.

III. 제안모델

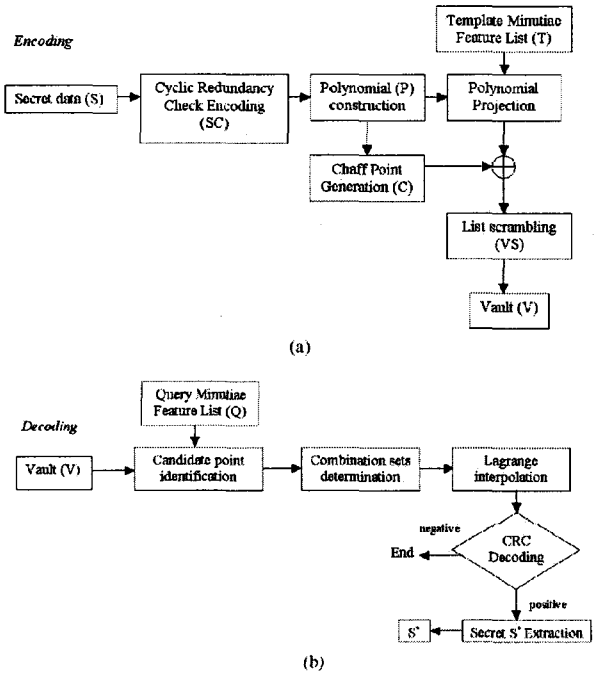
현재 구현이 되는 시스템의 경우 아래와 같은 구조로 이루어지게 되며 각 부분별 기능은 크게 차이가 없으며 구현 환경에서나 가능하다.



▶▶ Fig 3.1 시스템 구조

3.1 지문 입력 시스템

로그인이나 결제시 사용자의 지문을 입력을 받아야 하기 때문에 지문의 입력 프로그램이 필요하다. 하지만 단순히 지문을 입력받는 하드웨어로 끝낼수는 없다. 이 지문을 비교하기 위해 전송이 되어야 하며 전송하기 위해서는 Fuzzy Vault 과정을 거쳐야 하기 때문이다. 이 실험에서는 Fuzzy Vault 과정을 Matlab을 통해 구현한다. 이 시스템은 로그인과 결제뿐만 아니라 회원 가입에서도 사용하게 되며 중요 시스템중 하나가 되는 것이다.



▶▶ Fig 3.2 Fuzzy Encoding & Decoding

3.2 지문 저장 시스템

지문의 비교를 위해서는 비교대상인 지문이 저장이 되어 이 있어야 한다. 지문의 저장 및 사용자 아이디와 비밀번호 및 스크리밍 서비스를 이용하는 사용자들의 정보가 들어가는 시스템으로 일반적으로 알고 있는 계정 데이터베이스 서버와 동일하다. 하지만 이 시스템에서는 계정 정보외에 지문의 정보 또한 입력되기에 상당히 중요한 시스템이다. 이 시스템은 방화벽 안에 있어야 함은 기본이며 타 통신의 이용을 절제하도록 하여야 한다.

3.3 로그인 시스템

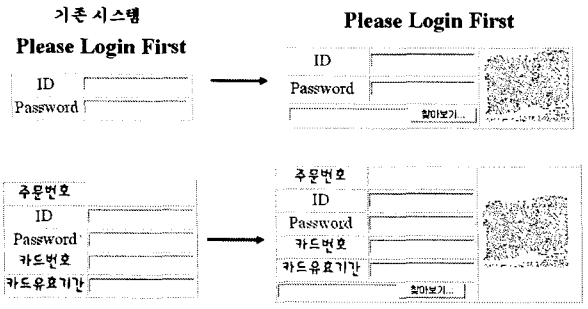
일반적으로 스트리밍 서비스 사이트의 경우 회원제로 운영이 된다. 누구나 볼수 있기 보다는 회원을 대상으로 서비스를 하기 때문이다. 그리고 익명의 결제를 통한 보안상의 취약점을 막기 위해서이다. 보통의 서비스 사이트의 경우에는 ID와 Password를 입력받게 되며 입력받은 ID와 Password를 비교하여 로그인에 대해 인정을 하게 되는 것이다. 이 시스템에서는 기존의 로그인 방법에서 ID와 Password 뿐만이 아닌 지문의 입력도 같이 보여주게 된다. 입력된 지문을 Fuzzy Vault화 시켜 전송 하여야 하기 때문이다. 이 시스템에서는 상품화의 목적이 아닌 실험의 목적이 있기에 단순히 ID와 Password 입력창, 그리고 지문의 입력창만을 보여준다.

3.4 결제 시스템

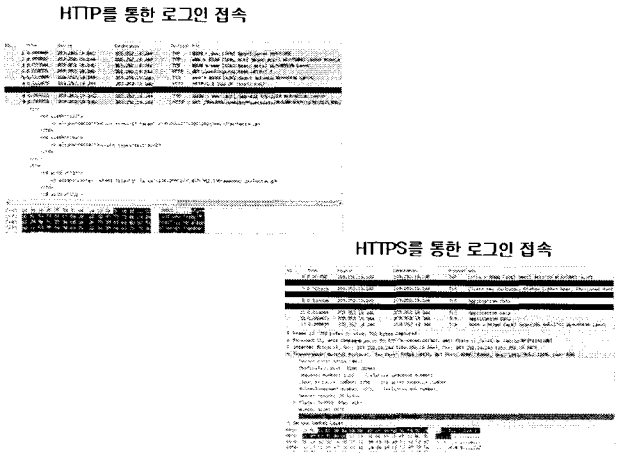
현재 대부분의 결제 시스템에서 사용하는 ActiveX 프로그램을 사용하지는 않는다. 실제적으로 ActiveX 프로그램은 결제 회사와의 연동을 위해 필요한 것일 뿐 이 시스템에서는 실험의 목적이 있기에 단순히 텍스트를 통해 카드번호와 기타 정보들 그리고 지문의 입력을 받는 구조로 생성이 된다. 실제 상품화의 경우 각자의 시스템에 지문의 입력 창이 늘어나는 것으로 충분히 호환이 가능하다.

IV. 실 험

지문의 정보를 Fuzzy Vault화 시키는 작업은 MATLAB을 통해 일정 포인트내의 가짜 특징점을 생성하며 기존의 Steaming service 페이지처럼 일반 HTTP의 경우와 HTTPS의 경우를 스니핑을 통해 데이터 보호 정도를 알아 본다. 이 실험으로 기존의 시스템과의 비교를 할수 있게 된다.



▶▶ Fig 4.1 실 시스템의 로그인 및 결제 시스템



▶▶ Fig 4.2 패킷 스니핑을 통한 보안 테스트

V. 결 론

현재 많은 인터넷 사용자들이 음악이나 영화 서비스를 오프라인 상에서가 아닌 온라인을 통해 접하고 있다. 예전에는 직접 공연장에 가서 표를 예매하고 음악이나 영화, 연극을 접했으나 기술의 발달로 인터넷을 통한 예매를 거쳐 이제는 직접 공연장을 갈필요도 없이 인터넷이 되는 곳이라면 진짜 공연장에 있는 것처럼 느낄수 있을 만큼 많은 기술이 발달 되었다. 하지만 현재 많은 공연 정보들이 무료가 아닌 유료 서비스를 하고 있으며 이로 인해 결제 시스템을 이용하고 있다. 하지만 이 결제 시스템은 안전하다고 말할수 없으며 단순한 과정으로도 본인이 아님에도 결제가 가능하다. 본인이 아님에도 카드의 습득이나 다른 방법을 통해 쉽게 결제를 할 수 있으며 그런 부분에 대해 많은 방안이 나와야 한다. 그렇기에 이 시스템을 생각하게 된 것이다. 이 시스템 역시 완벽하다고 말할 수 있는 것은 아니지만 기존의 시스템에 비하여 조금 더 안전한 서비스를 할 수 있다. 지문은 사람이 가지고 있는 고유의 정보이기에 지문을 빌려 준다는 것은 실질적으로 불가능에 가깝다. 현재 많은 회사나 연구 기관에서 생체인식을 준비하고 있다. 하지만 개인 단체로부터 사생활 침해라는 이유로 환영받지 못하고 있는 것이다. 이 시스템은 지문의 암호화 과정을 한번더 거치게 되기에 안전하게 사용할 수 있다는 장점을 가지게 된다. 하지만 이 시스템도 역시 사람이 만든 것으로 단점이 나올 수 있다고 생각하며 앞으로도 계속적으로 증가할 스트리밍 서비스에 대비해 안전하게 사용할 수 있도록 많은 기술들이 연구되어야 한다.

▌참 고 문 헌 ▐

[1] Forouzan, Behrouz A., "Data Communications and Networking", McGraw-Hill
[2] 윤종호, "무선 LAN 보안 프로토콜", 교학사
[3] Kaufman, Charlie., "Network Security Private Communication in a Public World", Prentice-Hall
[4] Austerberry, David, "The Technology Of Video And Audio Streaming", Butterworth-Heinemann
[5] 이필규, "영상처리 및 생체인식", 홍릉과학출판사
[6] Hearn, "Computer Graphics with OpenGL", Prentice Hall
[7] Gonzalez, "Digital Image Processing", Prentice-Hall