워터마킹 기법을 이용한 데이터의 은닉에 의한 인증 기법

°강 석* 아오끼 요시나오* 김 용기**
* 일본북해도대학대학원공학연구과
** 충북대학교전기전자컴퓨터공학부
* {°kssrh, aoki}@media.eng.hokudai.ac.jp
** courage super@hotmail.com

An Authentication Technique by Data Hiding Using Watermarking Technique

°Seok Kang* Yoshinao Aoki* Yong-Gi Kim**
* Graduate School of Engineering, Hokkaido University
** School of Electrical & Computer Engineering, Chungbuk National University

요 약

네트워크 상에서 특정의 시스템 또는 컴퓨터에 접속하려고 하는 사람이 정당한 사용자인지를 판단, 그 결과에 근거하여 접근을 제어하는 일련의 프로그램 또는 하드웨어 장치들을 인증 시스템이라 하며, 최근에 들어 정보보호 측면에 있어서 그 중요성이 커지고 있다. 본 논문에서는 인증 데이터를 암호화 또는 부호화 시켜서 전송하는 종래의 인증 알고리즘과는 달리, 인증 데이터를 이미지와 같은 제3의 미디어에 은닉시켜서 전송함으로써 인증을 실시하는 새로운 인증 기법을 제안함과 아울러 시뮬레이션 결과를 제시함으로써 제안된 방법의 유효성을 나타내고 있다.

1. 서 론

최근 개방된 네트워크 환경을 기반으로 전자상거래나 정보시스템 구축 등이 활발히 전개되고 있으며 정보화가 가속화되면서 사이버공간은 지리적 공간 못지않은 생활 공간으로서 그 영역을 확장해가고 있다. 반면 해킹, 바이러스나 음란물 유포 등의 각종 컴퓨터 관련 범죄가 갈수록 증가되고 있어 이에 따른 정보보호의 중요성도 크게 부각되고 있는 실정이다. 정보보호 기술은 차단기술과 암호화 기술, 인증 기술로 구분되며, 이중 인증 기술은 네트워크 접근자의 신원을 확인하고 사용권한을 결정하는 기술로 해커 등 불법 사용자의 무분별한 침입을 막아 정보를 보호하고 신뢰와 안정성을 확보하기 수단으로 사용된다.

인터넷 사용의 증가와 함께 점점 확대되는 인트라넷 및 익스트라넷 환경에서 사용자 인증과정은 필수적인 요소이다. 이런 환경에서의 인증 과정에 있어 현재 사용자 편의와 보안을 위한 단일 인증 시스템이 널리 사용되고 있다.

고전적인 인증 방식에 있어서는 단순히 아이디와 패스워드만을 전송함으로써 서버 측에서는 미리 등록되어 있는 데이터와의 일치성을 판단하여 그 결과에 근거하여 접근의 가부를 판단하며, 인증 데이터의 암호화의 견고성이 유일한 공격에 대한 안전성을 판단하는 기준이었다. 다양한 공격방법들의 등장으로 인해, 최근에 들어서는 인증 방식 자체를 바꾸는 새로운 인증 프로토콜들의 개발과 제3의 데이터를 사용하는 인증 방식들이 제안되어지고 사용되어지고 있다. 인터넷상에서 일반적으로 사용되어지고 있는 최근의 방식으로는 RSA알고리즘을 기반으로 하는 PKI인증 기법이 있으며, OTP(One-Time Password)라고 불리는 일회용 패스워드 방식과 지문, 홍채와 같은 생체정보를 이용하는 인증 방식 또한 사용되어지고 있다.

이러한 새로운 인증 프로토콜 또는 생체정보와 같은 제3의 데이터를 이용하는 방식과 달리, 인증 데이터를 이미지와 같은 제3의 미디어에 은닉시켜 전송함으로써 인증을 행함과 동시에 인증 데이터를 보호하는 방법이 생각되어질 수 있다. 본 논문에서는 워터마킹 기법을 이용해서 인증 데이터를 은닉시켜 전송함으로써 인증을 실시하는 새로운 인증 기법을 제안한다.

2. 워터마킹을 이용한 인증 시스템

워터마킹은 전자 문서, 이미지, 음악, 영상과 같은 멀티미디어 컨텐츠에 저작권에 관련된 데이터를 은밀히 삽입해서 소유권에 관한 권리를 주장하고자 기획된 방식으로서, 부정 복제에 의한 저작권의 침해에 대한 검증 수단으로서 기대를 받고 있다. 워터마킹에서는 저작권에 관한 정보로 사용되어지는 워터마크 데이터를 인증정보로서 이용하는 인증 시스템의 응용 예를 그림 1에 나타내고 있다. 본 논문에서 제안하고 있는 워터마크 데이터를 이용한 인증 알고리즘은 다음과 같이 4단계로 구성되어진다.

- 작성된 워터마크 데이터를 전송하고자 하는 이미지에 삽입
- 아이디와 패스워드와 같이 워터마크가 삽입된 이미지

를 전송

- 전송된 이미지로부터 워터마크 데이터를 추출해서 등록된 데이터와의 일치성 검사
- 일치성 결과의 근거하여 접근 허가 여부를 판단

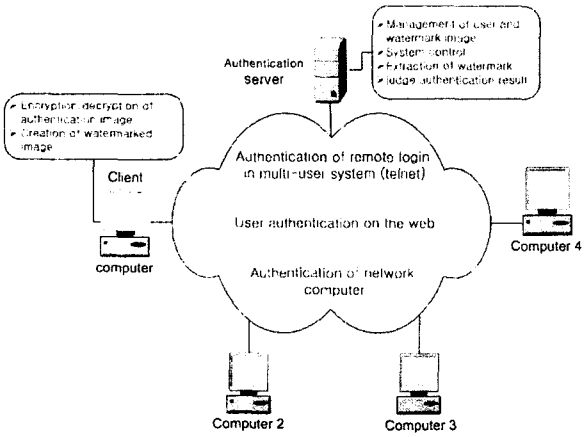

그림 1 워터마킹 기법을 이용한 인증 시스템의 응용 예

다음의 그림 2는 인증 시스템의 구성 요소를 나타내고 있다.

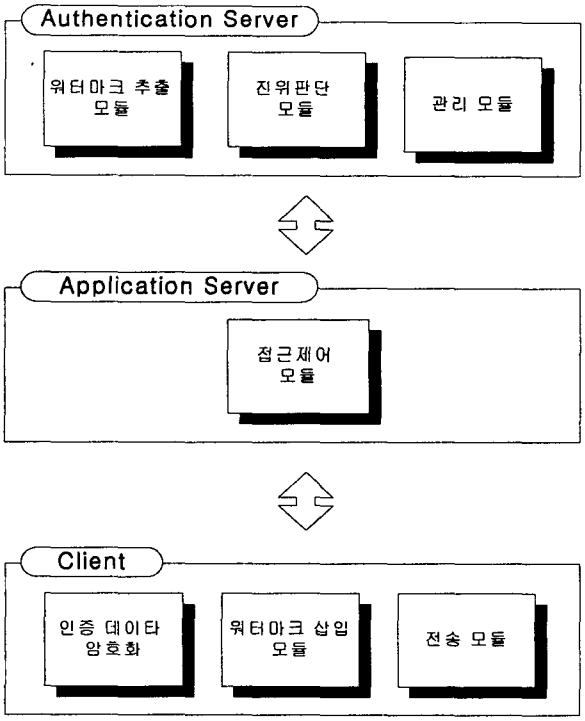

그림 2 인증 시스템의 주요 구성 요소

3. Fresnel 변환을 이용한 워터마킹 기법

워터마크 이미지를 Fresnel 변환시켜 얻은 패턴의 값들을 원 이미지에 삽입시키는 워터마킹 기법이 제안되어져 있다[1]. Fresnel 변환은 파동의 Fresnel 회절의 기술에 도입되어진 변환으로서, 그림 3에서 보이고 있는 것처럼 물체면과 관측면 사이의 거리를 이용해서 정변환과 역변환의 패턴을 계산하는 것이 가능하며[2], 거리가 멀어짐에 따라 얻어지는 패턴은 원래의 형태가 확산되어짐을 알 수 있다.

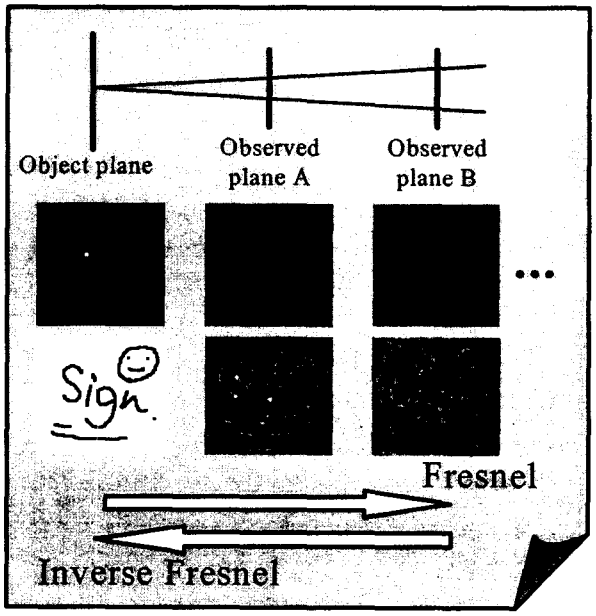

그림 3 거리 파라미터와 Fresnel 변환과의 관계

문헌[1]기법에서는 삽입 강도 파라미터와 Fresnel 변환의 거리 파라미터라는 두 가지가 사용되어지며, 역변환시 틀린 파라미터 값을 이용하면 명확한 재생상을 얻는 것이 불가능하다는 사실로부터, 워터마크 데이터를 삽입시 파라미터 값들을 동적으로 변하게 함으로써 인증 데이터의 안정성을 높일 수 있다.

4. 시뮬레이션 및 결과

제안된 수법의 유효성을 검증하기 위한 인증 시뮬레이션을 그림 4와 5의 이미지를 각각 원이미지와 워터마크 이미지로 사용해서 서버와 클라이언트 간의 인증 시뮬레이션을 실시했다.

본 시뮬레이션에서는 아이디와 패스워드에 의해서 두 가지 파라미터의 값들이 동적으로 변하게끔 했으며, 삽입 강도 파라미터의 값들의 법위는 0.01에서 0.1사이이며, 거리 파라미터의 경우는 0.01에서 1.0이다.

그림 4 원 이미지

그림 5 워터마크 이미지

서버 측과 클라이언트 측에서 발생되는 소켓 이벤트는 다음과 같으며, 그림 6에 인증 절차의 시간흐름도를 나타내고 있다.

- Accept : 클라이언트로부터의 소켓을 accept & bind
- Connect : 클라이언트 소켓을 생성시켜 서버와의 연결
- Listen : 다음 소켓이 연결되는 것을 기다림
- Receive : 패킷을 받음
- Send : 패킷을 전송

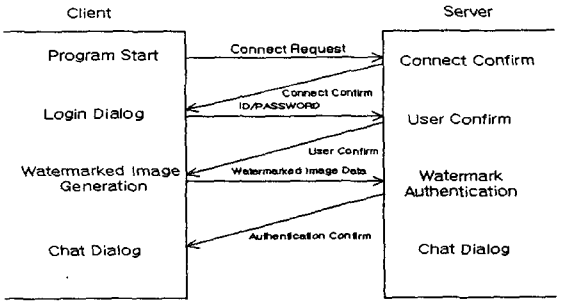

그림 6 인증 절차의 흐름도

그림 7과 8에 각각 채팅 프로그램에 있어서 클라이언트 측과 서버 측에서 인증 결과의 화면을 보여주고 있다.

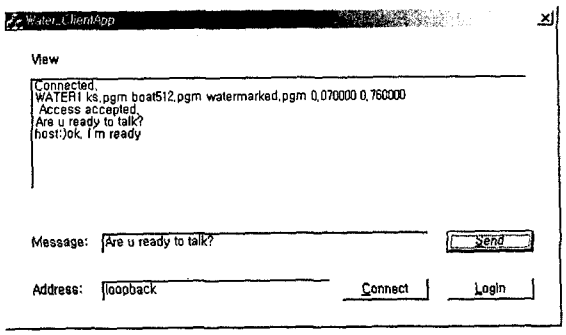

그림 7 클라이언트 측의 인증 결과 화면

5. 결론

인증 데이터를 제3의 미디어에 은닉시켜서 전송함으로써 인증을 행하는 새로운 수법이 제안되어졌으며, 제시된 시뮬레이션 결과로부터 그 유효성이 입증되었다고 할 수 있다. 기존의 아이디와 패스워드 방식에 비해 사전공

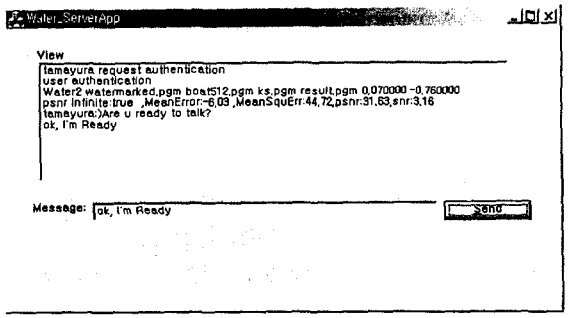

그림 8 서버 측의 인증 결과 화면

격이 불가능하며, 인증서 기반 방식에 대해서는 키 관리 및 키 분배를 필요로 하지 않으며 별도의 인증기관을 필요로 하지 않다는 점, 생체 인증 방식에서처럼 별도의 하드웨어 장치를 필요로 하지 않는다는 면과 프로토콜이 아닌 순수하게 프로그램만으로 구현이 가능한 것들이 제안된 인증 기법의 장점이라 할 수 있다.

다양한 공격에 대한 제안된 수법의 안정성을 검토하는 것이 앞으로의 과제로 남아 있다.

참 고 문 헌

[1] Seok Kang, Yoshinao Aoki, "Image-data Watermarking by Embedding a Fresnel-Transformed Pattern," trans. of ITE, Vol.54, No.5, pp.709-716, 2000.
[2] Y. Aoki, "Wave signal processing," Morikita publisher(Tokyo), 1986.