개선된 Vernam의 암호화 기법을 적용한 화상회의 시스템 구축

이은정, 김형균, 정기봉*, 김단환*, 김충원*, 오무송*
조선대학교 컴퓨터공학과

Video conference system construction that apply improved Vernam's encryption technique

*Eun-Jeong Lee, Hyeong-Gyun Kim, Ki-Bong Jeong, Dan-Hwan Kim, Choong-Won Kim, Moo-Song Oh
Dept. of Computer Science, Chosun University

요 약

화상회의 시스템은 원격지간 실제회의가 가능하도록 환경을 제공해주는 화상통신 시스템으로써 정보전달과 업무처리의 신속성을 이끌어 낼 수 있다. 그러나 화상회의를 실행함에 있어서 중요한 회의 내용의 유출, 도용 등이 발생할 수 있기 때문에 안전성이 확보된 화상회의 시스템에 관한 연구가 계속되고 있다. 본 연구에서는 화상회의 시스템의 안전성에 대한 문제점을 해결하기 위하여 현재 사용되고 있는 사용자 인증과 같은 일반적인 암호화 기법 이외에 화상정보의 변조와 유출, 도용 등을 방지하기 위하여 영상 정보를 암호화 하는 기법에 대하여 연구하였다. 화상정보를 암호화하기 위해서 개선된 Vernam의 암호화 기법을 이용하였다.

1. 서론

인터넷은 언제 어디서나 누구나 사용할 수 있을 정도로 지난 몇년동안 급속도로 발전하였다. 인터넷을 통한 멀티미디어 통신 기술과 이를 이용한 정보통신의 발달로 우리 생활 깊숙이 차지하게 되었다. 그중 화상회의는 시간과 장소에 구애받지 않고 교환이 필요한 화상, 음성, 문자, 그래픽 등의 모든 정보원을 컴퓨터, 비디오, 오디오 등의 장비로 동일시간, 동일장소에서 회의하는 것 같은 효과를 갖도록 하였다. 하지만 화상회의를 실행함에 있어서 중요한 회의 내용의 유출, 도용 등이 발생할 수 있기 때문에 보안성이 확보된 화상회의 시스템에 관한 연구가 계속되고 있다.

특히, 화상통신 분야의 암호화 방법은 일반적으로 화상을 Scramble하거나, DCT 등을 적용해 화상에 가장 영향을 많이 미치는 부분만을 암호화 하는 알고리즘이 많이 사용되었지만 화상 자체를 암호화함으로써 수많은 연산양이 필요하게 되어 암호를 처리함에 있어 속도문제가 크게 대두되었다.

최근엔 화상에서 Runlength나 Distance의 차를 이용해 합성된 화상의 보안 전송여부를 제 3자가 판독할 수 없게 하여 1차적으로 암호화 여부의 시각적 확인에 따른 공격 대상으로서의 가능성을 줄인다. 2차적으로는 해독자가 전송된 화상에 대하여 공격을 가한다 해도 합성 알고리즘 자체의 안전도에 의해 해독이 용이하지 않도록 방어하는 화상의 효율적인 암호화 방법으로 화소정보를 비밀리에 화상에 혼합하는 합성 알고리즘이 제시되고 있다.

본 연구에서는 화상회의 시스템의 보안성을 향상하기 위하여 사용자 인증을 통한 보안 Key를 공유한 후, 화상정보의 변조와 유출, 도용 등을 방지하기 위하여 보안 Key를 통해 화상 정보를 암호화하기 위하여 기존 text 기반의 암호화 알고리즘에 사용되었던 Vernam의 암호화 기법을 개선하여 사용하고자 한다.

2. 화상회의 시스템의 보안

화상회의 시스템의 근간을 이루고 있는 인터넷은 정보에 대한 공유를 기본으로 하고 있기 때문에 화상회의 시스템이 제공하는 중요한 정보의 전송을 위해서는 보호를 위한 서비스 제공이 절대적으로 필요하다.

화상회의 시스템의 보안성 향상을 위한 필수 기능을 살펴보면 다음과 같다.

첫째, 기밀성을 보장해야 한다.

기밀성이란 소극적 공격으로부터 화상 전송자료를

보호하는 것을 말한다. 화상 및 메시지 내용 공개에 관한 여러 단계의 보호를 구분할 수 있다. 가장 개괄적인 서비스는 화상회의 참석자 간에 모든 화상 전송 자료를 일정기간 보호하는 것이다. 예를 들어 두개소의 화상회의 시스템 사이에 가상 회로가 개설되었다면 이 개괄적 보호 서비스는 그 가상 회로 상에 전송된 모든 사용자 자료를 공개되지 않도록 보호하는 것이다.

둘째, 인증성을 제공해야 한다.

화상회의 시스템을 사용할 시에는 여러 가지 방법으로 사용자들을 확인할 필요성이 대두된다. 인증성에는 반드시 사용자만이 인증 대상이 되는 것이 아니고 화상회의 시스템의 각 기기 및 각종 프로그램 등도 포함될 수 있다. 이런 대상들이 실체를 가장해서 화상회의 시스템에 침입하는 경우를 대비하여 정확하게 인증 대상을 확인하는 기능이 제공되어야 한다. 특히, 회의 대상자의 위장, 회의 중 비인가자 참석, 주요 사안 찬반 결정시 기기조작 미숙 또는 대리 참석자의 서명 등에 대한 보안대책을 강구하여야만 정상적인 회의 시스템 운영이 가능하다.

셋째, 무결성을 보장해야 한다.

무결성이란 인가된 자만 시스템을 사용함으로서 비인가자의 접근으로부터 보안을 보장하는 것이다. 즉, 비인가자에게는 회의 시스템에 대한 접근을 엄격히 제한하는 것이다. 특히, 인가자라 할지라도 시스템의 사용범위, 사용시간 등의 권한 등을 통제할 수 있는 기능이 제공되어야 한다. 이러한 통제방법은 암호화를 이용한 회의 시스템 비밀 유지 서비스의 자동효과로써 실현할 수 있다.

넷째, 가용성을 보장해야 한다.

화상회의 시스템에 구비된 각종의 기기나 장비설치 장소에는 인가된 사용자가 희망할 때 즉시 효과적으로 이용되도록 해야 한다. 즉, 인가된 사용자에게 효과적으로 이용되도록 신원확인, 중명체제 구비, 화상 전송 데이터의 백업, 중복성 유지, 물리적 위협으로부터 보안을 유지시킴으로써 가용성을 보장할 수 있는 기능이 제공되어야 한다.

3. 화상회의시스템의 설계

본 연구에서 설계하고자 하는 안전한 화상회의 시스템은 인증된 사용자에 한하여 클라이언트와 서버간에 Session Key를 생성해 주고, RSA암호화기법을 이용하여 Session Key를 암호화하여 클라이언트에 전송함으로써 보안 Key를 공유하게 된다.

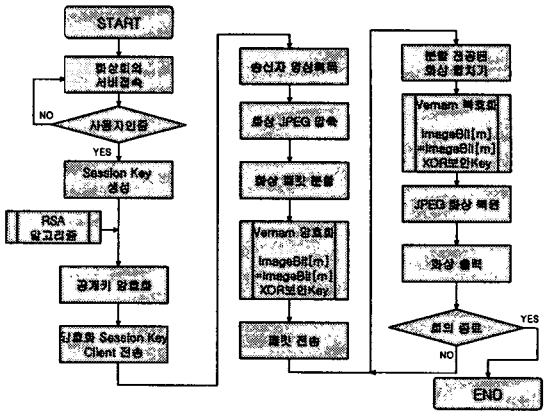

그림 1 System Flow Chart

송신자의 화상은 클립보드를 통하여 이미지를 획득하고 이 화상은 JPEG 압축 과정을 거쳐 패킷단위로 분할된다. Vernam의 암호화 과정을 거쳐 화상을 암호화한 후 패킷을 수신자에게 전송한다. 수신자는 패킷 단위로 전송되어진 화상을 받아서 합친 후 화상의 복호화과정과 압축 복원을 통해 영상을 출력할 수 있다.

전반적인 시스템의 구성은 자료 전송에 따른 부하의 감소와 원활한 화상의 전송을 위하여 Host, Server, Client로 구분하였다.

Host는 화상회의 시스템에서 Server의 역할을 담당하고 있는 것으로 현재 접속된 사용자의 기본 정보와 현재 개설된 화상회의 룸의 정보를 보관 및 관리하는 기능을 가진다.

Server는 사용자의 입출과 통제 권한을 가지는 기능으로 회의룸의 개설자에게 주어지며 Group 내부에서의 정보 교류를 담당하고 회의룸의 개설 권한을 가진 사용자가 신규 룸을 개설할 경우 생성된다.

Client는 전형적인 사용자 중심으로 설계되어 사용자 정보를 다른 사용자에게 전송 및 수신 기능을 담당하도록 설계하였다.

Server와 Client는 하나의 Program으로 구성되어 있으며, 회의를 하고자 하는 당사자간에 모두 설치하여 사용하는 program으로 회의룸의 개설 권한을 가진 사용자가 작동할 경우 Server로 변경되어 실행되며, 일반 사용자의 경우 Client로 실행된다.

화상회의 Client Program을 실행해서 Server에 접속한 후 사용자 인증 과정을 거쳐 화상회의에 참여할 수 있다.

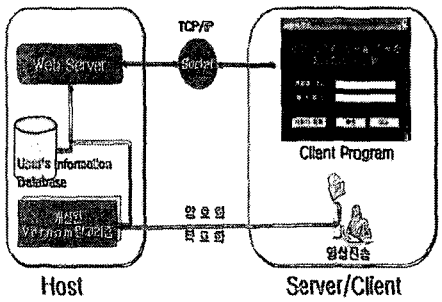

그림 2. 안전한 화상회의 시스템 구성도

본 시스템의 동작 과정은 다음과 같다.

첫째, 화상회의를 실행하고자 하는 웹 브라우저는 프록시 서버에 서비스를 요청한다.

둘째, 프록시 서버는 서버게이트웨이에 연결을 요청한다.

셋째, 서버게이트웨이의 RSA암호 모듈은 키를 생성하여 프록시 서버에 전송한다.

넷째, 서버 게이트웨이는 화상회의 서버에 서비스를 요청한다.

다섯째, 화상회의 서버는 분할된 영상의 이미지를 제공한다.

여섯째, 개선된 Vernam의 암호 모듈은 해당 이미지를 암호화하여 전송한다.

일곱째, 프록시 서버는 송신된 이미지를 복호화하여 웹 브라우저에 전송한다.

표 1. 일반적인 Vernam 알고리즘의 예

보통문	C(010011)	O(100110)	D(010100)	E(010101)
Key	N(100101)	A(010001)	M(100100)	E(010101)
Exclusive-OR 연산				
암호문	110110	110111	110000	000000

이것은 1917년 Major Joseph Mauborgne과 AT&T의 Gilbert Vernam이 개발한 것으로 일반적인 Vernam의 암호화 방식은 BCD표를 이용하여 보통문과 키를 이진수로 변환하고 논리연산인 Exclusive-OR 연산을 실시하여 암호화 문자로 대치한다.

화상의 암호화를 위해 개선된 Vernam의 암호화 기법을 그림3과 같이 제안하였다. 여기서 제시한 바와 같이 RSA공개키 암호화 알고리즘을 이용하여 인증과 Session_key 교환 과정을 수행하며, Key 교환과정을 통해 공유되는 Session_ key는 전송 화상에 개선된 Vernam의 암호화 기법을 이용하여 합성된다. 이 때 화상분할을 통해 화상의 전송이 이루어지므로 상,중,하의 단계로 분할된 화상에 합성하게 된다.

송신 측에서는 이러한 단계를 거쳐서 암호화된 화상을 전송하며, 수신 측 클라이언트의 프록시 서버는 송신된 이미지를 복호화하여 웹 브라우저에 전송하게 된다.

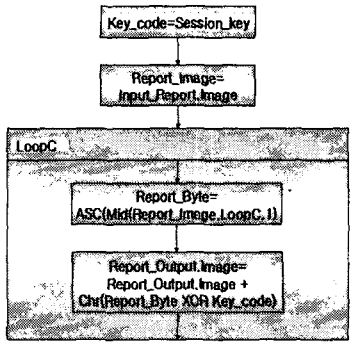

그림 3 개선된 Vernam의 암호화기법

4. 실험 및 고찰

4.1 회의룸 개설

인증된 접속자는 부여된 권한에 따라 회의룸의 개설 권한을 가지게 된다. 권한을 가진 접속자는 접속자 현황 화면의 [회의 개설] 버튼을 클릭하여 회의룸을 개설할 수 있다.

[회의 개설]창이 열리면 회의에 참석하는 인원수와 회의 공개여부를 선택하여 회의룸을 개설할 수 있다.

4.2 송신자 영상의 암호화

JPEG 압축된 송신자의 영상은 패킷 단위로 분할하여 암호화된다.

영상 정보의 특성상 많은 양의 자료를 연산해야 하므로 암호화 및 복호화 속도가 빠른 Vernam의 알고리즘을 개선하여 사용함으로써 시스템의 전송속도 지연 문제를 해결하였다.

본 연구에서는 패킷 단위로 분할된 영상 정보를 Byte 단위로 추출하여 앞서 Server 와 Client 간에 공유된 보안 Key와 Exclusive-OR 연산을 수행하였다.

4.3 일대일 화상회의

[회의 개설]창에서 참여 인원을 "2인"으로 선택하면 일대일 화상회의를 실행할 수 있다.

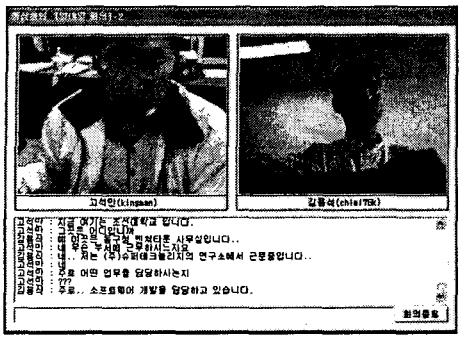

그림 4. 일대일 화상회의 화면

4.4 다자간 화상회의

본 연구에서는 일대일 화상회의와 다자간 화상회의를 분리하여 선택할 수 있게 하였으며, 다자간 화상회의의 경우 최대 참여 인원수를 4인으로 한정하였다.

다자간 화상회의를 위한 회의룸의 경우, 좌측 상단의 화면은 확대 화면으로 원하는 회의 참석자의 영상을 확대해 볼 수 있도록 하였고, 우측 상단의 4개로 구성되어 있는 화면은 참석자의 영상과 이름을 확인할 수 있다.

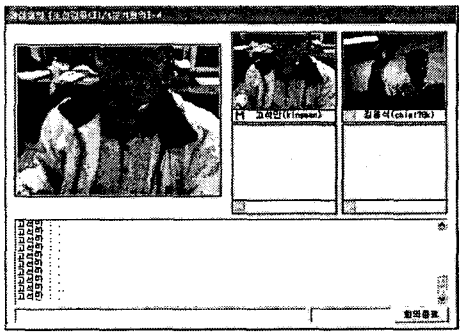

그림 5. 다자간 화상회의

4.5 권한이 없는 참석자의 영상 출력

그림 6를 보면 "김평수" 참석자의 경우 영상을 볼 수가 없는데, 이것은 회의에는 참석했지만 권한이 부여되지 않아 보안 Key를 공유하지 못해서 암호화된 영상을 복호화할 수 없기 때문이다.

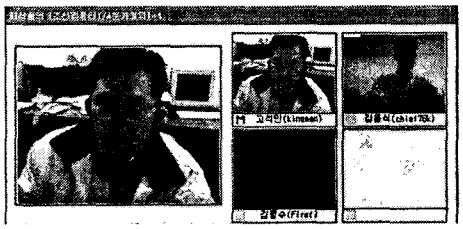

그림 6. 권한이 없는 참석자의 영상 출력 화면

5. 결론

본 연구에서는 인터넷상의 정보 공유로 인한 화상회의 시스템의 안전성에 관한 문제점을 해결하기 위해서 현재 사용되고 있는 사용자 인증과 같은 일반적인 암호화 기법 이외에 화상정보의 변조와 유출, 도용 등을 방지하기 위하여 화상 정보를 암호화 하는 기법에 대하여 연구하였다.

화상회의에 접속한 인증된 사용자에 한하여 클라이언트와 서버 간에 Session Key를 생성해 주고, RSA 암호화 기법을 이용하여 Session Key를 암호화하여 클라이언트에 전송함으로써 보안 Key를 공유하게 된다. 송신자의 화상은 클립보드를 통하여 이미지를 획득하고 이 화상은 JPEG 압축 과정을 거쳐 패킷단위로 분할된다. Vernam의 암호화 과정을 거쳐 화상을 암호화한 후 패킷을 수신자에게 전송한다. 수신자는 패킷 단위로 전송되어진 화상을 받아서 합친 후 화상의 복호화 과정과 압축 복원을 통해 화상을 출력할 수 있다. 이때, 암호화 및 복호화 속도가 빠른 Vernam의 암호화 기법을 개선하여 사용함으로써 시스템의 전송속도 지연 문제를 해결하였다.

[참고문헌]

[1] R.Jain and K.Wakimoto, "Multiple Perspective Interactive Video", in Proc.of Intl.Conf on Multimedia Computing and Systems, 1995, pp201-211

[2] "전산망간 상호접속시 보안대책에 관한 연구" 한국전산원 최종 보고서, 1996. 11.

[3] "웹 환경 구축 및 운영을 위한 보안 기술 연구" ,한국전산원 최종 보고서, 1997.12.

[4] A. Freier, P.Karlton, and P.Kocher, "The SSL Protocol Version3.0", Internet Draft, 1996. 3.

[5] 이인수, "RSA 공개키 암호시스템 현황 ,한국정보보호센터, 1998. 5.