안전한 화상회의를 위한 영상암호화에 관한 연구

*김형균, *민혜란, **이상범
*조선대학교 컴퓨터공학과 **조선이공대학 컴퓨터정보과

A Study on the Image Cryptography for Secure Video Conference

Hyeong gyun Kim*, Hye Lan Min*, Sang Beom Lee**
*Dept. of Computer , Chosun University, **Chosun College of Science & Technology
E-mail : hr7sun@hanmail.net

요 약

본 연구에서는 화상회의 시스템의 안정성에 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. 영상 정보를 암호화하기 위해서 개선된 Vernam의 암호화 기법을 이용하였으며, 보다 안전하고 신속한 화상회의 시스템을 구축하기 위하여 영상 분할 통신 기법을 이용하여 화상을 여러 개의 모듈로 분할한 후 각각의 모듈별로 합성하는 방법을 제안하였다.

키워드

Cryptography ,Security, Video Conference

I. 서 론

화상회의 시스템은 원거리에 있는 사람들이 한 자리에 모여서 이야기함으로 발생될 수 있는 시간적, 공간적 제약을 제거함으로써 정보전달과 업무처리의 신속성을 이끌어 낼 수 있지만, 중요한 회의 내용의 유출, 도용 등이 발생할 수 있기 때문에 안전성이 확보된 화상회의 시스템에 관한 연구가 계속되고 있다.[1]

이러한 연구는 암호화를 이용한 정보의 보호방법이 일반적으로 많이 사용되어 왔으며, 특히, 화상통신 분야의 암호화 방법은 일반적으로 화상을 Scramble하거나, DCT 등을 적용해 화상에 가장 영향을 많이 미치는 부분만을 암호화하는 알고리즘이 많이 사용되었다. 이러한 기존의 암호화 방식은 화상 자체를 암호화함으로써 수많은 연산양이 필요하게 되어 암호를 처리함에 있어 속도 상에서 큰 문제가 되었다. 최근에는 화상의 효율적인 암호화 방법으로 화소정보를 비밀리에 화상에 혼합하는 합성 알고리즘이 제시되고 있다. 즉, 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 것이다.[3]

본 연구에서는 안전한 화상회의 시스템을 구축하기 위하여 공개키 암호화 알고리즘과 비밀키 암호화 알고리즘을 함께 사용하였다. 특히, 영상 정보를 암호화하기 위해서 개선된 Vernam의 암호화 기법을 이용하였으며, 보다 안전하고 신속한 화상회의 시스템을 구축하기 위하여 영상 분할 통신 기법을 이용하여 화상을 여러 개의 모듈로 분할한 후 각각의 모듈별로 합성하는 방법을 제안하였다.

II. 관련연구

화상회의의 개념은 1927년 미국의 Bell Lab.에서 음성과 영상 시스템을 상호·연동하는 기술로 처음 등장한 후, 1964년 AT&T가 비디오가 추가된 데스크탑 전화장치인 Picture-Phone을 개발하여 1970년 이를 4개 도시의 공공 회의실에 설치하여 Picture-Phone Meeting Service를 실시하여

구체화되었다.

화상회의 시스템에 대한 정의는 사람이나 기구에 따라 조금씩 다르게 정의가 되고 있는데, KINTI (Korea Institute of Industry & Technology Information)에서는 "멀리 떨어진 지점의 회의실을 통신회선으로 영상과 음성을 연결하여 상대를 텔레비전 화면으로 보면서 전원이 동일한 회의실에 있는 것 같은 분위기에서 회의를 할 수 있도록 하는 서비스이다"라고 정의하고 있으며, Elliot Gold는 "화상회의란 시간과 장소에 구애받지 않고 교환이 필요한 화상, 음성, 문자, 그래픽 등의 모든 정보원을 컴퓨터, 비디오, 오디오 등의 장비로 동일시간, 동일 장소에서 회의하는 것과 같은 효과를 갖도록 하는 첨단 회의 방식이다."라고 정의하고 있다.

화상회의 시스템의 근간을 이루고 있는 인터넷은 정보에 대한 공유를 기본으로 하고 있어서 다른 대부분의 인터넷 응용 프로그램과 마찬가지로 보안 문제를 고려하지 않아, 보안이 요구되는 민감한 분야에 사용하기는 적합하지 않다. 따라서 화상회의 시스템이 제공하는 중요한 정보의 전송을 위해서는 보호를 위한 서비스 제공이 절대적으로 필요하다.

초고속정보통신기반하에서 규정하고 있는 안전성 서비스를 바탕으로 화상회의 시스템에서 제공되어야 할 보안 필수 기능을 살펴보면 다음과 같다[2].

첫째, 기밀성을 보장해야 한다. 기밀성이란 소극적 공격으로부터 화상 전송자료를 보호하는 것을 말한다.

둘째, 인증성을 제공해야 한다. 사용자만이 아니라 시스템의 각 기기 및 각종 프로그램 등이 대상이 되어 실체를 가장해서 화상회의 시스템에 침입하는 경우를 대비하여 정확하게 인증 대상을 확인하는 기능이 제공되어야 한다.

셋째, 무결성을 보장해야 한다. 무결성이란 인가된 자만 시스템을 사용함으로서 비인가자의 접근으로부터 보안을 보장하는 것이다.

넷째, 가용성을 보장해야 한다. 화상회의 시스템에 구비된 각종의 기기나 장비설치 장소에는 인가된 사용자가 희망할 때 즉시 효과적으로 이용되도록 해야 한다.

다섯째, 부인봉쇄(non-repudiation). 부인봉쇄란 회의 시스템에 있어서 단방향성 화상 전송을 할 경우 수신측에서 거부하지 못하도록 막는 것을 의미한다.

III. 안전한 화상회의 시스템의 설계

본 연구에서 설계하고자 하는 안전한 화상회의 시스템의 보안 프로토콜은 공개키 암호화 알고리즘과 비밀키 암호화 알고리즘을 함께 사용하여 안전한 화상회의를 제공하고자 한다.

세션키 분배를 위해 RSA알고리즘을 사용하였고, 클라이언트와 서버 간에 공유한 세션키를 개선된 Vernam의 알고리즘을 이용하여 영상 정보의 암호화 및 복호화를 수행하였다.

본 시스템의 동작 개념은 통신하고자 하는 응용 실체 사이에 특별히 설계된 소켓 루틴들을 사용하여 먼저 안전한 통신채널을 확립한 다음, 이 채널을 통하여 정보를 교환할 수 있도록 하는 것이다. 안전한 채널을 확립하기 위해 소켓 루틴은 RSA공개키 암호화 알고리즘을 이용하여 인증과 세션키 교환 과정을 수행하며[6], 키 교환과정을 통해 공유되는 세션키를 이용하여 개선된 Vernam의 알고리즘을 사용한 대칭키 암호를 통해 안전한 화상회의가 이루어지게 된다.

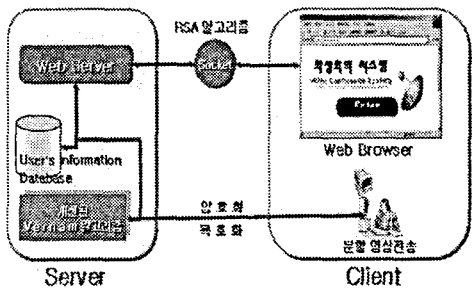

그림 1. 안전한 화상회의 시스템

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.

1. 화상회의 시스템의 통신망 설계

본 논문에서 설계된 화상회의 시스템은 양방향 통신을 기본으로 하여 많은 사용자들의 원활한 접속을 위하여 인터넷상에서 기본 Protocol로 채택하여 사용하는 TCP/IP를 이용하여 설계되었다.

전반적인 시스템의 구성은 자료 전송에 따른 부하의 감소와 원활한 영상의 전송을 위하여 Host, Server, Client로 구분하여 설계하였다. 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 Master에게 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 하였다.

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.

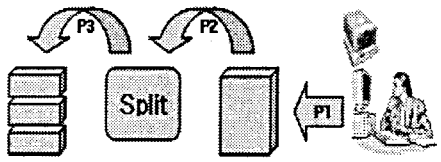

그림 2. 전송될 영상의 분할

본 연구에서 제안한 영상분할 통신은 영상의 불규칙한 전송을 보완하기 위하여 1초당 10장의 이미지를 화상 카메라을 이용하여 작성하고 작성된 각각의 이미지는 상,중,하 세 단계로 분할된다.

분할된 이미지는 각각 압축 과정을 통하여 전송이 이루어지며, 전송된 이미지는 각 영상의 위치에 따른 자료 공간에 저장되어 진다. 저장된 이미지는 Client의 프로그램에 의하여 지정된 위치에서 재생되며, 저장된 영상이 재생되는 동안 다음 영상이 도착하게 된다.

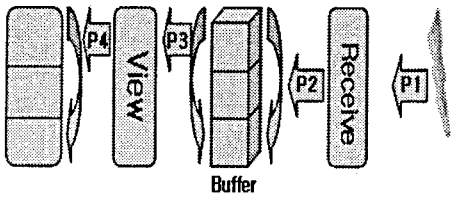

그림 3. 분할 전송된 영상의 재생

2. 영상 암호화

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

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.

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

본 연구에서는 JPEG형태로 압축된 송신자의 영상을 패킷 단위로 분할한 영상 정보를 Byte 단위로 추출하여 앞서 Server 와 Client 간에 공유된 보안 Key와 Exclusive-OR 연산을 수행하였다.

영상의 암호화를 위해 개선된 Vernam의 알고리즘을 그림 4와 같이 제안하였다.

앞에서 제시한 바와 같이 RSA공개키 암호화 알고리즘을 이용하여 인증과 Session_key 교환 과정을 수행하며, 키 교환과정을 통해 공유되는 Session_ key는 전송 화상에 개선된 Vernam의 알고리즘을 이용하여 합성된다. 이 때 영상분할을 통해 화상의 전송이 이루어지므로 상,중,하의 단계로 분할된 영상에 합성하게 된다.

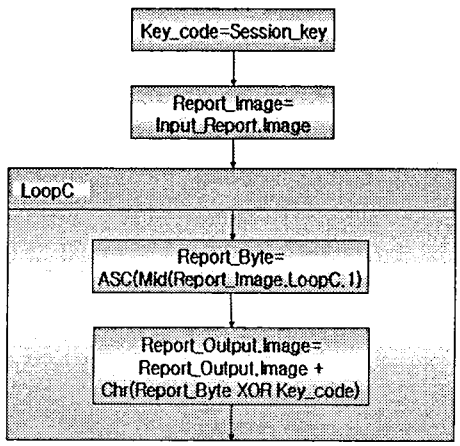

그림 4. 개선된 Vernam의 암호화 알고리즘

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

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

3. 안전한 화상회의 시스템 구현

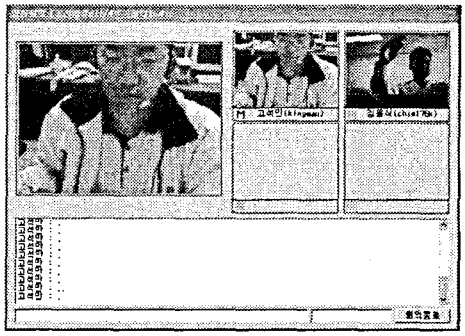

그림 5. 다자간 화상회의

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.

Ⅳ. 결론

본 연구에서는 화상회의 시스템의 안정성에 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.

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

회의에는 참석했지만 권한이 부여되지 않아 보안 Key를 공유하지 못한 참석자는 암호화된 영상을 복호화할 수 없기 때문에 영상을 출력할 수 없게 된다.

참고문헌

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

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

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

[4] "SSL Protocol", http://www.netscape.com /eng/ security/SSL_2.html

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

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