

보안성이 향상된 화상회의 시스템 구축을 위한

영상 암호화에 관한 연구

김형균^{*} · 김단환^{*} · 오무송^{*}

^{*}조선대학교 컴퓨터공학부

A Study on the Image Encryption

for Video Conference System Construction that Security Improves

Hyeong-Gyun Kim^{*}, Dan-Hwan Kim^{*}, Moo-Song Oh^{*}

^{*}Dept of Computer Engineering, Chosun University

E-mail : multikim87@hanmail.net

요 약

화상회의를 실행함에 있어서 중요한 회의 내용의 유출, 도용 등이 발생할 수 있기 때문에 보안성이 확보된 화상회의 시스템에 관한 연구가 계속되고 있다. 본 연구에서는 화상회의 시스템의 보안성에 대한 문제점을 해결하기 위하여 현재 사용되고 있는 사용자 인증과 같은 일반적인 암호화 기법 이외에 화상정보의 변조와 유출, 도용 등을 방지하기 위하여 영상을 암호화 하는 기법에 대하여 연구하였다. 영상 정보를 암호화하기 위해서 개선된 Vernam의 암호화 기법을 이용하였으며, 보다 안전한 화상회의 시스템을 구축하기 위하여 영상 분할 통신 기법을 이용하여 화상을 여러 개의 모듈로 분할한 후 각각의 모듈별로 암호를 합성하는 방법을 제안하였다.

ABSTRACT

Video conference system has guided swiftness of information transmission and business processing taking away time and manufacturing drug of space that is happened that long-distance people gather and talk. But, leakage of important meeting contents, speculation etc.. in that execute video-conferences can happen. Therefore, research about video conference system of safety is progressing under secure superhigh speed information communication fetters. This treatise studied about techniques to encipher videotex to prevent variation and outward flow of burn information, speculation etc.. except general encryption notation such as user certification to have drawn problem about stability of general video conference system, and is used present as countermeasure about here. Used improved Vernam's encryption techniques to encrypt videotex.

키워드

Video conference system, encrypt videotex, Vernam's encryption

1. 서 론

화상회의 시스템은 원격리에 있는 사람들이 한자리에 모여서 이야기함으로써 발생할 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 보호

방법이 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 연산량이 필요하게 되어 암호를 처리함에 있어 속도 상에서 큰 문제가 되었다.[2]

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

II. 화상회의 시스템의 보안성 향상

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

화상회의 시스템의 보안성 향상을 위한 필수 기능을 살펴보면 다음과 같다.[8,9]

첫째, 기밀성을 보장해야 한다.

기밀성이란 소극적 공격으로부터 화상전송 자료를 보호하는 것을 말한다. 화상 및 메시지 내용 공개에 관한 여러 단계의 보호를 구분할 수 있다. 가장 개괄적인 서비스는 화상회의 참석자간에 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.

기밀성의 또 다른 면은 트래픽 흐름분석에 대한 보호로서 전송자료의 출처와 목적지, 횟수, 길이 또는 화상 전송로상의 트래픽 특성에 대하여 공격자가 알지 못하게 하는 것이다. 기밀성은 비인가자와 불법 침입자의 접근을 제어하고 비밀자료의 비밀성이 노출되지 않도록 인가된 자에게만 접근 가능하도록 해야 한다.

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 기조 조작 미숙 또는 대리 참석자의 서명 등에 대한 보안대책을 강구하여야만 정상적인 회의 시스템 운영이 가능하다.

셋째, 무결성을 보장해야 한다.

무결성이란 인가된 자만 시스템을 사용함으로써 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 장비 설치 장소에는 인가된 사용자가 회망할 때 즉시 효과적으로 이용되도록 해야 한다. 즉, 인가된 사용자에게 효과적으로 이용되도록 신원확인, 증명체제 구비, 화상전송 데이터의 백업, 중복성 유지, 물리적 위협으로부터 보안을 유지시킴으로써 가용성을 보장할 수 있는 기능이 제공되어야 한다.

다섯째, 부인 봉쇄(non-repudiation)

부인봉쇄란 회의 시스템에 있어서 단방향성 화상 전송을 할 경우 수신측에서 거부하지 못하도록 막는 것을 의미한다. 따라서 화상이 송신되었을 때 수신자는 그 화상이 실제로 송신자에 의해서 송신되었음을 확인할 수 있게 된다. 마찬가지로 화상이 수신되었을 때 송신자는 그 화상이 실제로 수신자에 의해 수신되었음을 확인할 수 있다.

III. 안전한 화상회의 시스템의 설계

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

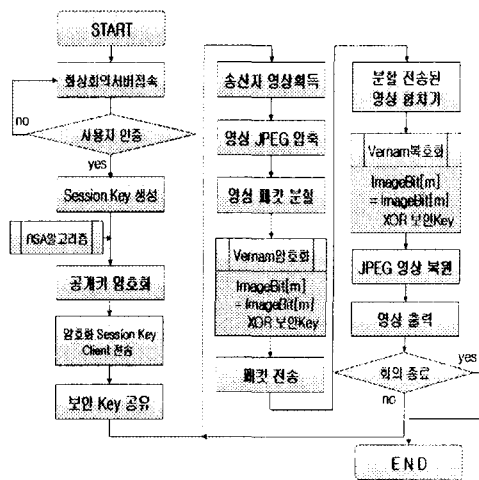


그림 1. System Flow Chart

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.

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

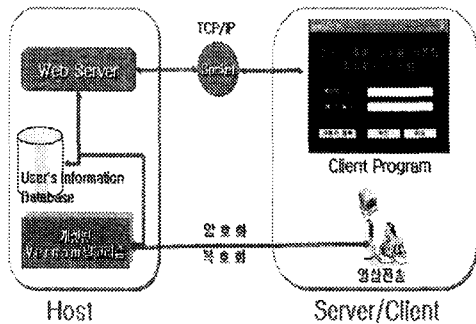


그림 2. 안전한 화상회의 시스템 구성도

Host는 화상회의 시스템에서 Server의 역할은 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.

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 개설

할 수 있다.

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.

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.

본 연구에서는 패킷 단위로 분할된 영상 정보를 Byte 단위로 추출하여 앞서 Server와 Client간에 공유된 보안 Key와 Exclusive-OR 연산을 수행하였다.

3. 일대일 화상회의



그림 3. 일대일 화상회의 화면

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

4. 다자간 화상회의

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

으로 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.

5. 권한이 없는 참석자의 영상 출력

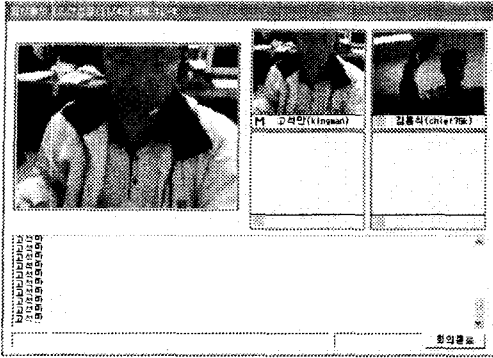


그림 4. 다자간 화상회의

그림 5를 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 5. 권한이 없는 참석자의 영상 출력 화면

IV. 결 론

화상회의 시스템의 근간을 이루고 있는 인터넷은 정보에 대한 공유를 기본으로 하고 있어서 다른 대부분의 인터넷 응용 프로그램과 마찬가지로 보안성이 문제가 되기 때문에 화상회의 시스템이 제공하는 중요한 정보의 전송을 위해서는 보호를 위한 서비스 제공이 절대적으로 필요하다 따라서 본 연구에서는 영상암호화를 이용해 화상회의 시스템의 보안성을 향상하고자 했다.

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.
- [7] NIST, "Internet Security Policy : A Technical Guide", 1997, 7
- [8] B. Chapman and E. Zwicky, "Building Internet Firewalls", O'Reilly and Associates, Sebastopol, CA, 1995.
- [9] Chaim Ziegler & Gerald Weiss, "Multimedia Conferencing on Local Area Networks", IEEE, 1990
- [10] C.P. Schnorr, Efficient identification and signature for smart cards, Advances in Cryptology-CRYPTO'89, LNCS 435, Springer -Verlag, pp. 239- 251, 1989.
- [11] Elliot Gold, "PC-Based Videoconferencing Arrives", Data Communications, 1994