실시간 동영상 암호화 기법을 적용한 화상회의 시스템 구축

최우진* · 김형균* · 오무송**

Video Conference System Construction that Apply Real Time Video Encryption Techniques

Woo-Jin Choi* · Hyeng-Gyun Kim* · Moo-Song Oh**

요 약

본 연구에서는 동영상정보의 암호화에 중점을 두어 보안성을 향상함으로써, 기존의 사용자 인증 기법에 의존한 화상회의 시스템에 비해 기밀성과 무결성 측면이 강조된 실시간 동영상 암호화 기법을 적용한 화상회의 시스템을 구축하였다.

송신자의 영상은 Vernam의 암호화 과정을 패킷 단위로 수신자에게 전송한다. 수신자는 전송되어진 영상을 받아서 합친 후 영상의 복호화과정과 압축 복원을 통해 영상을 출력할 수 있다. 이때, 암호화 및 복호화 속도가 빠른 Vernam의 알고리즘을 사용함으로써 동영상의 실시간 암호화에 따른 전송속도 지연 문제를 해결하였다. Vernam 알고리즘의 단순성 문제는 암호화 및 복호화에 사용되는 보안Key를 Client와 Server간의 채널에서 이용할 Session Key를 RSA 알고리즘을 이용함으로써 해결하고자 하였다.

ABSTRACT

By emphasize and enhance security in encryption of same viewdata in this research, constructed video conference system that apply real time video encryption techniques that confidentiality and integrity aspect are emphasized than video conference system that depend on existent user certification techniques. Sender's image transmits Vernam's encryption process to listener by packet. Listener can display image through image's decipher process and uncompress after unite receiving transmited image. This time, solved transmission speed delay problem by video's real time encryption using Vernam's algorithm that encryption and the decipher speed are fast. Simplification problem of Vernam algorithm wished to solve Session Key that use security Key that is used encipherment and decipher in channel between Client and Server using RSA algorithm.

키워드

Real time video encryption, Vernam's encryption, Video conference system

* 조선대학교 대학원 컴퓨터공학과

** 조선대학교 전자정보공과대학 컴퓨터공학부

접수일자 : 2002. 10. 18

Ⅰ. 서 론

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[1].

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[2,3].

본 연구에서는 실시간 동영상 암호화 기법을 화상회의 시스템에 적용하여 보안성을 향상시키고자 한다. 동영상 정보의 암호화에서 가장 큰 문제점인 전송속도의 지연문제를 해결하기 위하여, 영상을 압축한 후 패킷 단위로 분할하고, 암호화 및 복호화 속도가 빠른 Vernam의 알고리즘을 영상의 암호화에 사용하고자 한다.

Vernam 알고리즘의 단순성 문제는 암호화 및 복호화시에 사용되는 보안Key를 Client와 Server간의 채널에서 이용할 Session Key를 RSA 알고리즘을 이용하여 암호화한 후 사용하도록 이중으로 암호화함으로써 해결하고자 한다.

Ⅱ. 실시간 동영상 암호화 기법을 적용한 화상회의 시스템의 설계

그림 1은 본 연구에서 설계하고자 하는 실시간 동영상 암호화 기법을 적용한 화상회의 시스템의 순서도를 보여 주고 있다. 먼저, 인증된 사용자에 한하여 클라이언트와 서버 간에 Session Key를 생성해 주고, RSA알고리즘을 이용하여 Session Key를 암호화하여 클라이언트에 전송함으로써 보안 Key를 공유하게 된다.

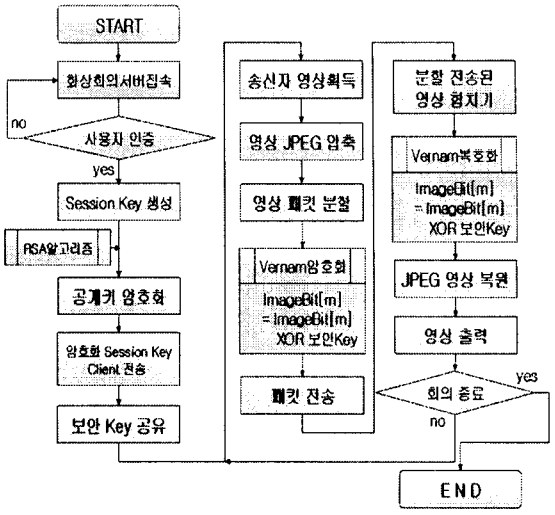

그림 1. System Flow Chart

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.

1. Session Key 생성

화상회의 Server에 접속된 Client는 Session Key를 생성하고 RSA 암호화 과정을 거쳐 보안 Key를 공유하게 된다.

① Client는 Server에 연결을 요청한다.
② Server는 Client에서 연결요청이 있으면 Session Key를 생성한다.
③ 생성한 Session Key를 RSA 알고리즘을 이용하여 Client의 공개키로 암호화한다.
④ 암호화된 SessionKey를 Client에 전송한다.
⑤ Client는 수신된 Session Key를 RSA 알고리즘을 이용하여 복호화한다.

위의 과정들을 마치면 연결설정이 이루어지고 Client와 Server는 암호화된 채널에서 이용할 Session Key를 보안 Key로 공유하게 된다.

2. 송신자 영상 획득

개설된 회의룸에 다른 접속자가 참여하게 되면 개설자의 프로그램은 Server로 변경되어 실행되며, 일반 접속자는 Client로 실행된다. Client와 Server는 암호화된 채널에서 이용할 Session Key를 보안 Key로 공유하는 과정을 거친 후 송신자의 영상을 수신자에게 전송하게 되는데 먼저 송신자의 영상을 클립보드를 통해 얻게 된다.

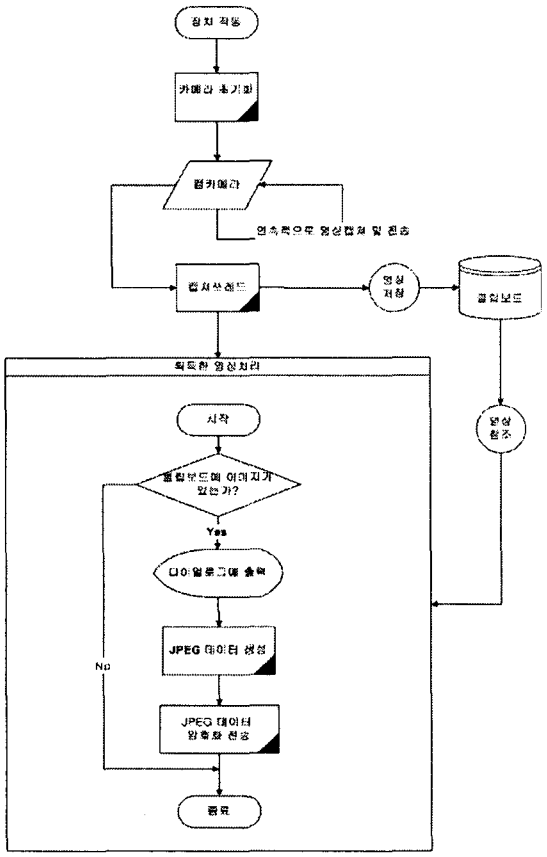

그림 2. 송신자 영상 획득 과정 흐름도

그림 2는 송신자 영상을 획득하기 위한 과정을 흐름도로 표시하고 있다. 접속된 사용자의 영상을 캠 카메라를 통하여 연속적으로 캡쳐 및 전송을 실시하고, 캡쳐쓰레드 과정을 거쳐 클립보드에 영상을 저장한다. 이렇게 클립보도를 통해 영상을 획득한 후 JPEG 압축을 위한 기본 데이터를 생성하게 된다.

3. 송신자 영상 압축

획득한 송신자의 영상은 원활한 전송을 위하여 JPEG압축 과정을 거친다. 본 연구에서는 무손실 JPEG 압축 기법을 이용하여 초당 10장의 영상을 압축·전송할 수 있도록 설계하였다. 먼저, JPEG Codec 구조체를 생성하고 압축될 영상의 크기, 색상정보 등을 설정한 후 압축 결과를 저장하기 위한 버퍼를 생성한다. 획득한 영상의 GrayScale 여부에 따라 영상을 적정한 형태의 자료로 버퍼에 저장한 후 압축을 수행한다. 압축이 완료되면 JPEG Codec 구조체를 삭제한다.

4. 송신자 영상의 암호화

압축된 송신자의 영상은 패킷 단위로 분할하여 암호화된다. 영상 정보의 특성상 많은 양의 자료를 연산해야 하므로 암호화 및 복호화 속도가 빠른 Vernam의 알고리즘을 동영상의 실시간 암호화에 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 그림 3과 같이 패킷 단위로 분할된 영상 정보를 바이트 단위로 추출하여 서버와 클라이언트 간에 공유된 보안 키와 Exclusive-OR 연산을 수행하였다.

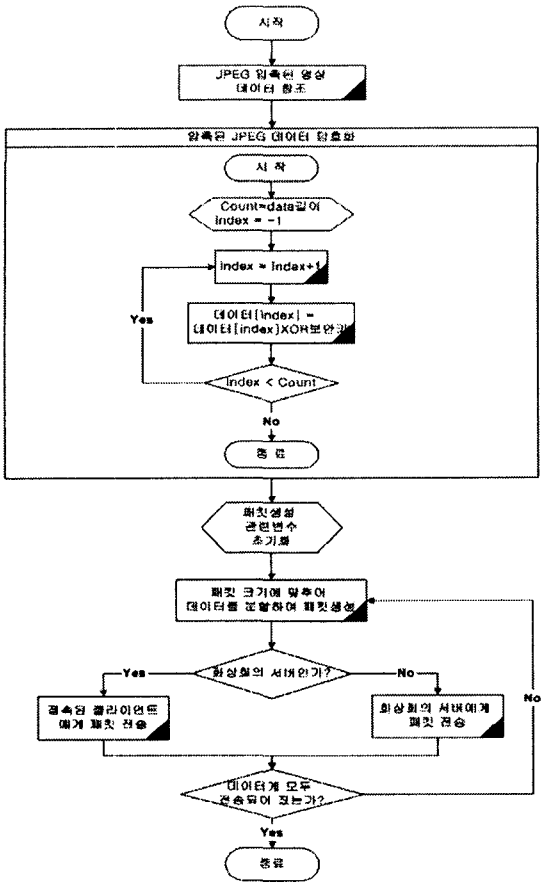

그림 3. 압축영상의 패킷단위 실시간 암호화 과정 흐름도

III. 시스템의 구현

본 연구에서 구현한 화상회의 시스템은 자료 전송에 따른 부하의 감소와 원활한 영상의 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 프로그램으로 구성되어 있으며, 회의를 하고자 하는 당사자간에 모두 설치하여 사용하는 프로그램으로 회의룸의 개설 권한을 가진 사용자가 작동할 경우 Server로 변경되어 실행되며, 일반 사용자의 경우 Client로 실행된다.

1. 회의룸 개설

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

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

2. 다자간 화상회의

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

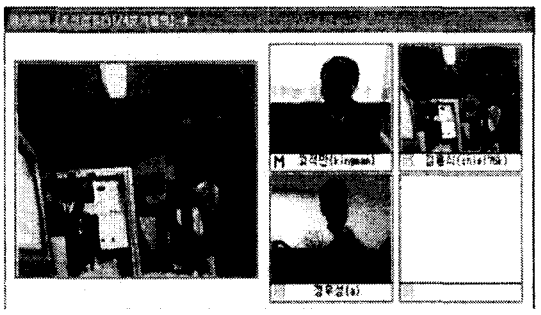

그림 5. 다자간 화상회의

그림 5는 다자간 화상회의를 위한 회의룸의 경우로, 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.

3. 권한이 없는 참석자의 영상 출력

화상회의의 구현 시 전송되는 데이터는 크게 문자, 영상, 음성으로 구분된다. 본 연구에서는 이중에서 동영상정보의 실시간 암호화에 중점을 두어 보안성을 향상함으로써, 기존의 사용자 인증 기법에 의존한 화상회의 시스템에 비해 기밀성과 무결성 측면이 강조된 안전한 화상회의 시스템을 구현하였다.

그림 6. 권한이 없는 클라이언트의 영상 출력

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

IV. 실험 및 고찰

본 논문에서 구현한 화상회의 시스템이 전체 네트워크 트래픽에 미치는 영향을 알아보기 위하여 조선대학교와 Kornet망 사용자간에 클라이언트 프로그램을 각각 설치하여 각각의 기능에 대한 트래픽을 측정해 보고, 기존의 화상회의 시스템과의 트래픽을 비교해 보았다.

트래픽 측정을 위해 'DU meter' 측정 툴을 이용하였으며[5], Server측 프로그램은 Windows 2000서버 시스템 환경에 웹과의 연동을 위한 IIS Web Server와 사용자 정보의 관리를 위한 MS-SQL Server를 설치하였다.

표 2는 본 연구에서 구현한 안전한 화상회의 시스템(SVS)의 트래픽량과 기존의 인스턴트 메신저의 트래픽량을 비교하기 위하여 대표적인 인스턴트 메신저인 MSN 메신저의 트래픽을 측정해 본 결과이다.

표 2. 기능별 트래픽 비교표(단위: kbps)

횟수	문자전송		음성전송		화상전송		
	SVS	MSN	SVS	MSN	SVS (암호화)	SVS	MSN
1	2.4	1.6	32.8	12.8	280.3	261.2	250.4
2	2.4	2.4	32.9	14.4	281.2	266.3	285.6
3	2.3	2.6	32.4	12.8	278.5	270.4	172.8
4	2.2	1.6	33.6	15.2	283.3	253.4	311.2
5	2.0	2.4	32.8	14.4	279.5	261.0	164.0
6	1.8	2.4	33.6	14.4	283.4	266.3	256.6
7	2.4	2.4	32.9	13.6	286.5	250.2	187.2
8	2.6	4.0	33.4	14.4	287.5	260.4	319.2
9	2.5	2.4	33.1	12.8	270.5	256.8	285.6
10	2.8	3.6	34.3	13.6	286.3	260.3	320.0
평균	2.3	2.5	33.2	13.8	281.7	260.6	255.3

화상전송의 경우 비암호화시의 SVS의 평균 트래픽은 260.6kbps로 측정되었으며, MSN 메신저의 평균 트래픽은 255.3kbps로 측정되었다. 화상 전송기능에서 트래픽의 차이가 약간 나는 것을 볼 수 있는데, 이는 화면의 프레임률의 차이에서 오는 것으로 추측되며 무시할 수 있을 정도의 것으로 본다. 또한 암호화 시의 SVS의 평균 트래픽은 281.7kbps로 측정 되었다. 암호화와 비암호화시의 평균 트래픽의 차이는 21.1kbps로 나타났으며, 화상 전송의 지연 부분에 있어서 문제가 없는 정도로 측정되었다.

IV. 결 론

본 연구에서는 실시간 동영상 암호화 기법을 적용한 화상회의 시스템을 다음과 같이 구축하였다.

화상회의에 접속한 인증된 Client는 Server에 연결을 요청한다. Server는 Client에서 연결요청이 있으면 Session Key를 생성한다. 생성한 Session Key를 RSA 알고리즘을 이용하여 Client의 공개키로 암호화한다. 암호화된 Session Key를 Client에 전송한다. Client는 수신된 Session Key를 RSA 알고리즘을 이용하여 자신의 비밀키로 복호한다. 이러한 과정들을 마치면 연결설정이 이루어지고 Client와 Server는 암호화된 채널에서 이용할 Session Key를 보안 Key로 공유하게 된다.

송신자의 영상은 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 사용함으로써 동영상의 실시간 암호화에 따른 전송속도 지연 문제를 해결하였다. Vernam 알고리즘의 단순성 문제는 암호화 및 복호화에 사용되는 보안Key를 Client와 Server간의 채널에서 이용할 Session Key를 RSA 알고리즘을 이용하여 암호화한 후 사용하도록 이중으로 암호화함으로써 해결하였다.

참고문헌

[1] A. Freier, P. Karlton, and P. Kocher, The SSL Protocol Version 3.0, Internet Draft, 1996. 3.

[2] Andrew S. Tanenbaum, Computer Net works, 3rd ed, Prentice-Hall,New Jersey, 1996.

[3] B. Chapman and E. Zwicky, Building In ternet Firewalls, O'Reilly and Associates, Sebastopol, CA, 1995.

[4] Berners-Lee, T., Fielding, R., and H. Frystyk, Hypertext Transfer Protocol-HTTP /1.0, Request for Comments : 1945, May 1996.

[5] Charles Arehart, Nirmal Chidambaram, Shashirikan Guruprasad, Professional WAP, Wrox Press Inc., 2000. 7.

[6] Dave Kosiur,IP Multicasting: the complete guide to interactive corporate networks, John Wiley & Sons, New York, 1998.

[7] Douglas E.Comer, Computer Networks and Internets, Prentice-Hall, New Jersey, 1997.

저자소개

최우진(Woo-Jin Choi)

1993년 8월 조선대학교 대학원 컴퓨터공학과 공학석사

1999년 8월 조선대학교 대학원 컴퓨터공학과 박사과정 수료

1997년 3월-현재 순천청암대학 조교수

※관심분야: 멀티미디어, 영상처리, 영상통신

김형균(Hyeng-Gyun Kim)

1998년2월: 조선대학교 산업대학원 전자계산전공(공학석사)

2000년-현재: 조선대학교 대학원 컴퓨터공학과 박사과정

※관심분야: 멀티미디어, 영상처리, 영상통신

오무송(Moo-Song Oh)

1968년 9월 조선대학교 전기공학부 공학석사

2001년 2월 전남대학교 전기공학과 공학박사

1988.3-1990.1 조선대학교 컴퓨터공학과 학과장

1999.1-1999.4 조선대학교 컴퓨터공학부 학부장

1999.4-1999.11 조선대학교 산업대학원장

1988년-현재 조선대학교 컴퓨터공학부 교수

※관심분야: 멀티미디어, 영상처리, 영상통신