안전한 화상회의 시스템을 위한 영상암호화

고석만* · 오무송**

Image Cryptography for Secure Video Conference System

Suk-Man Koh* · Moo-Song Oh**

요 약

화상회의 시스템은 원거리에 있는 사람들이 한자리에 모여서 이야기함으로 발생될 수 있는 시간적, 공간적 제약을 제거함으로써 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 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 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, peculation 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, peculation 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

* 조선대학교 대학원 컴퓨터공학과

** 조선대학교 전자정보공과대학 컴퓨터공학부

접수일자: 2002. 2. 15

Ⅰ. 서 론

최근 인터넷을 통한 멀티미디어 통신 기술과 이를 이용한 정보통신의 발달은 우리 생활 전 분야에 걸쳐 많은 기여를 하였다. 그중에서 화상회의 시스템은 원거리에 있는 사람들이 한자리에 모여서 이야기함으로 발생될 수 있는 시간적, 공간적 제약을 제거함으로써 정보전달과 업무처리의 신속성을 이끌어 낼 수 있었다. 그러나 화상회의를 실행함에 있어서 중요한 회의 내용의 유출, 도용 등이 발생할 수 있기 때문에 안전성이 확보된 화상회의 시스템에 관한 연구가 계속되고 있다.

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 속도상에서 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 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 안전한 화상회의 시스템을 구축하기 위하여 영상 분할 통신 기법을 이용하여 화상을 여러 개의 모듈로 분할한 후 각각의 모듈별로 암호를 합성하는 방법을 제안하였다.

Ⅱ. 화상회의 시스템의 통신 설계

화상회의의 개념은 1927년 미국의 Bell Lab.에서 음성과 영상 시스템을 상호·연동하는 기술로 처음 등장한 후, 1964년 AT&T가 비디오가 추가된 데스크탑 전화 장치인 Picture-Phone을 개발하여 1970년 이를 4개 도시의 공공 회의실에 설치하여 Picture-Phone Meeting Service를 실시하여 구체화되었다. PC를 기반으로 한 최초의 데스크탑 화상회의 시스템은 CLI(Compression Labs Inc.)의 Cameo 퍼스널 비디오 시스템이었다. 데스크탑 화상회의 시스템은 특수한 하드웨어가 필요 없이 이미 각자의 책상위에 있는 PC를 이용하므로 별도의 전용공간이 필요 없을뿐더러 가격이 훨씬 저렴했다.[1] 데스크탑 화상회의를 업무에 도입함으로써 얻을 수 있는 효과는 다양했다. 회의를 위해 각지에서부터 모일 필요가 없이 화상회의 시스템을 통해 각자의 근거지에서 회의를 할 수 있으므로 이동비용이 절감되고 이동시간의 소모가 없어지게 된다.

1. 화상회의 시스템의 통신 설계

일반적인 컴퓨터 통신시스템은 통신 방식에 따라 두 가지로 나누어진다. 먼저, 양방향 통신은 일반적인 동영상 전송 기법에서 채택하고 있는 방법으로 사용자 간에 정보를 주고받는 통신이고, 다른 하나는 방송처럼 특정 사용자로부터 전송되어 오는 정보를 단순히 받아 보기만 하는 단방향 통신이다.

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.

2. 영상 분할 전송

본 연구에서는 과거 방송망에서 영상전송의 불규칙한 시간의 보완 및 영상재생의 품질을 높이기 위하여 사용된 Buffering 기법을 기반으로 한 영상 분할 전송 기법을 사용하였다.

현재 사용되고 있는 동영상의 전송은 먼저 사용자가 접속할 경우 Server로부터 자료 전송이 이루어지면 바로 사용자에게 재생되는 것이 아니라 일정시간 Buffer에 보관하여 Buffer의 내용이 100%가 되었을 때 재생을 시작한다. 이러한 동영상 전송 기법은 화상회의와 같은 실시간 통신에는 적용하기 어렵다. 실시간 통신이라 함은 사용자 간에 정보를 주고받는 것을 기본으로 하며, 서로간의 응답 속도가 주된 관점이 된다. 그러므로 동영상 통신 기법에서 사용하는 Buffering의 개념을 사용할 경우 Buffering에 사용되는 시간만큼의 지연이 발생하게 되며 지연시간을 1T라 하였을 경우 실제 사용자들 사이에서 정보의 지연은 2T가 되어 대화가 원활하지 못하게 된다.[2]

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.

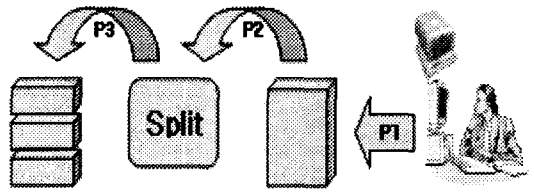

그림 1. 전송될 영상의 분할
Fig. 1 Segment of image that is transmited

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.

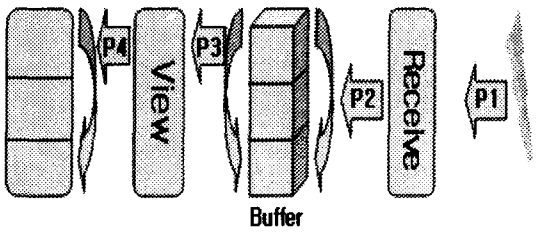

그림 2. 분할 전송된 영상의 재생
Fig. 2 Refreshing of image that is segmentalized and is transmited

Ⅲ. 안전한 화상회의 시스템 구축

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.

이러한 용도에 따른 보안 요구 사항을 살펴보면 다음과 같다.

첫째, 폐쇄그룹 구성원간에 정보공유를 위한 응용이 이루어 져야 한다.

이러한 응용은 특정 그룹 구성원들 간에만 민감한 정보를 공유하는 형태로, 서버의 정보에 접근하는 클라이언트를 제어하기 위해 클라이언트에 대한 인증 서비스가 요구된다. 또한, 민감한 정보에 대한 접근에 대해서 구성원별로 차등을 둘 수 있다.

둘째, 중요한 정보를 안전한 채널을 통해 교환하기 위한 응용이 필요하다.

구매 주문서나 공문서 같은 중요한 정보를 교환하고자 할 때, 클라이언트와 서버는 상호 인증 서비스를 제공해야 하며, 교환되는 메시지 또는 문서자체에 대한 인증도 요구된다.

셋째, 기밀성이 보장된 서비스의 응용이 필요하다.

인터넷을 이용하여 교환되는 각종 정보가 타인에게 노출되지 않도록 통신 내용의 비밀 보장 서비스가 요구된다.

1. 인터넷 기반의 보안

인터넷에 기반을 둔 화상회의 시스템의 보안 기술은 HTTP에 암호 기술을 어떻게 적용하느냐에 따라 3가지로 분류할 수 있다.[4]

HTTP는 특정 정보에 대한 접근 프로토콜 (Access Protocol)과 메시지 교환을 위한 구문 (syntax)제공이라는 두 가지 특성을 가지고 있다. SMTP(Simple Mail Trans fer Protocol), Telnet, RPC(Remote Procedure Call)등과 같이 정보에 대한 접근 프로토콜이라는 측면에서는 세션에 대한 채널 보호가 요구되어 지는 채널보안(Channel Security), MIME(Multi-purpose Internet Mail Extensions)이나 WAIS/Z39.50과 같은 구문(syntax) 측면에서는 메시지 보안(Message Security)이 필요하다. 세 번째로 내용보안(Content Security)은 HTTP상에서 외부 응용인 PGP 또는 PEM(Privacy Enhanced Mail)에 의해 암호화된 문서 형태로 안전하게 데이터를 전송하는 접근 방법이다.[5]

2. 암호화 알고리즘

암호화 알고리즘은 암호화 및 복호화에 사용되는 키의 특성에 따라 대칭키 알고리즘과 공개키 암호알고리즘으로 나누어 볼 수 있으며, 대칭키 알고리즘은 메시지의 처리 형식에 따라 스트림 암호알고리즘과 블록 암호알고리즘으로 나눌 수 있다. 블록 암호알고리즘은 전자 데이터의 기밀성 기능을 제공하기 위한 핵심기술이다. 따라서 국내 전자상거래에서 활용 가능한 블록 암호알고리즘 개발을 목적으로 많은 연구가 이루어졌고, 안전성과 효율성을 고려하여 SEED를 비롯한 많은 블록 암호알고리즘이 개발되었다. SEED는 128비트의 안전도를 제공하며, 효율성은 3중 DES 이상의 암호화 및 복호화 속도를 보인다.

2 .1 RSA(Rivest Shamir & Adleman)

공개키 암호방식의 개념은 1976년 Diffie와 Hellman에 의해 제안된 이후 부분합 문제에 기반을 둔 Merkle-Hellman 의 Knapsack 암호시스템이 제안되었으나, 대부분의 Knapsack 암호 시스템이 안전하지 않다고 판정되었으며, 그 뒤를 이어 1977년 Rivest, Shamir와 Adleman에 의해 개발되고 1978년 공개된 RSA 공개키 암호시스템이 현재 가장 널리 사용되고 있다.[6]

RSA는 암호화와 전자서명 모두를 제공할 수 있으며, 소인수 분해의 어려움에 안전도의 근간을 두고 있다. 즉, 두 소수 p와 q의 곱은 계산하기 쉬우나, 주어진 곱 n = pq 로부터 p와 q를 추출하기는 어렵다는 사실에 근간을 두고 있다. 개발 이후, 많은 암호분석가들의 분석이 있었으나, 아직 RSA공개키 암호시스템의 안전도에 대한 어떠한 증명 또는 반증명도 존재하지 않는다. 즉, 아직 RSA의 안전도를 치명적으로 위협하는 어떠한 공격도 존재하지 않는다. RSA 암호시스템은 모듈러 지수 연산이 주를 이룬다. 실제 응용에 있어, 작은 암호화 지수를 사용함으로써 복호화보다는 암호화를 더 빠르게 수행할 수 있도록 설계되고 있으며, 마찬가지로 서명보다는 검증을 더 빠르게 수행할 수 있도록 설계되고 있다.

2.2 DES(Data Encryption Standard)

컴퓨터와 통신 기술의 발달로 통신망을 통한 정보의 전송이 급속히 늘어남에 따라 이들 정보의 보안 문제가 대두하게 되었다 .안전한 정보의 전송 및 보관을 위해 NBS(National Bureau of Standard) 는 암호화 알고리즘을 공모하였다. 이에 IBM이 Water Tuchman과 Carl Meyer가 만든 DES를 제안하였고, 안전성에 대한 평가를 거친 후에 1977년 1월 FIPS(Federal Information Processing Standard) Publication No.46으로 표준화되어 현재까지도 널리 사용되고 있다.

DES와 같은 현대 암호화 알고리즘의 원칙은 암호화 및 복호화 알고리즘은 공개하고 암호화 키나 복호화 키를 숨기는 것이다. 즉 키를 아는 자만이 암호를 해독할 수 있게 하는 것이다. 이런 암호화 방법은 크게 대칭형 (symmetric)암호 시스템과 비대칭형 (asymmetric) 암호 시스템으로 나뉘는데 DES 는 대칭형 암호 시스템의 대표적인 예이다. 대칭형 암호 시스템은 암호화 키와 복호화 키가 같은 시스템으로, 이 말은 암호를 할 때의 키로 복호화가 가능하다는 뜻이다. 비대칭형 암호 시스템의 대표적인 예로는 RSA가 있는데 비대칭형이라는 말 그대로 암호화할 때의 키와 복호화할 때의 키가 다르다는 뜻이다.

DES는 블럭암호시스템인데 이것은 평문 (plaintext) 64bit를 암호문(ciphertext) 64bit블럭으로 바꾸는 암호화를 한다. 이때 사용되는 키도 64bit 인데 여기서 8bit는 패리티 비트이므로 실제로 키의 길이는 56bit 이다.

3. 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 서버간에 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, 안전한 통신 채널을 통하여 정보를 교환할 수 있도록 하는 것이다. 안전한 채널을 확립하기 위해 소켓 루틴은 RSA공개키 암호화 알고리즘을 이용하여 인증과 세션키 교환 과정을 수행하며, 키 교환과정을 통해 공유되는 세션키를 이용하여 개선된 Vernam의 알고리즘을 사용한 대칭키 암호를 통해 안전한 화상회의가 이루어지게 된다.

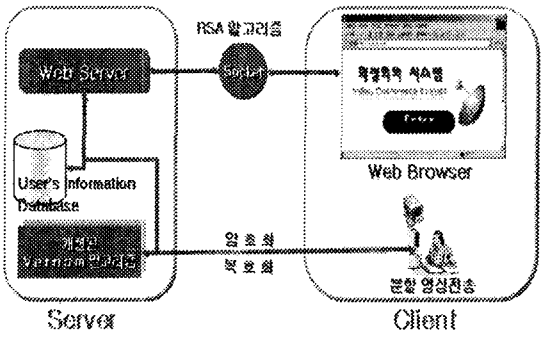

그림 3. 안전한 화상회의 시스템
Fig. 3 Secure Video Conference System

본 시스템의 동작 과정은 다음과 같다.

1) 화상회의를 실행하고자 하는 웹 브라우저는 프록시 서버에 서비스를 요청한다.
2) 프록시 서버는 서버게이트웨이에 연결을 요청한다.
3) 서버게이트웨이의 RSA암호 모듈은 키를 생성하여 프록시 서버에 전송한다.
4) 서버 게이트웨이는 화상회의 서버에 서비스를 요청한다.
5) 화상회의 서버는 분할된 영상의 이미지를 제공한다.
6) 개선된 Vernam의 암호 모듈은 해당 이미지를 암호화하여 전송한다.
7) 프록시 서버는 송신된 이미지를 복호화하여 웹 브라우저에 전송한다.

영상의 암호화를 위해 개선된 Vernam의 알고리즘을 다음과 같이 제안하였다.

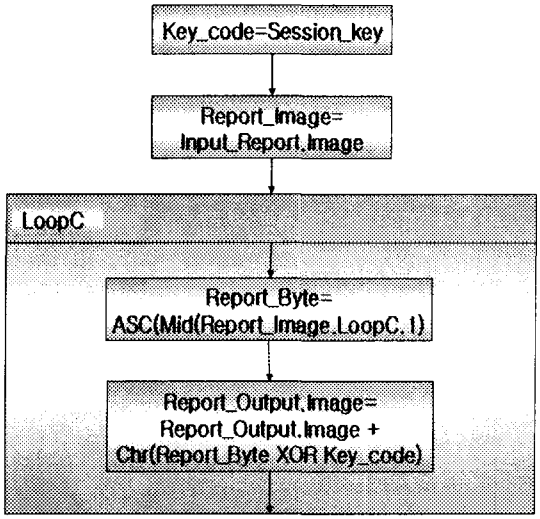

그림 4. 개선된 Vernam의 암호화 알고리즘
Fig. 4 Improved Vernam's encryption algorithm

표1. 안전한 화상회의 시스템의 전송속도 비교
Table 1 Transmission speed comparison Secure Video Conference System

	Text Data	Image Data
안전한 화상회의 시스템	1.4Mbps	0.9Mbps
일반 Web 시스템	1.6Mbps	1.1Mbps

개선된 Vernam의 암호 모듈은 이미지를 암호화할 때 이미 설명한 바와 같이 영상분할을 통해 화상의 전송이 이루어지므로 상,중,하의 단계로 분할된 이미지에 암호화를 실행하게 된다.

암호화 및 복호화 과정에 따른 성능분석으로 일반

웹 시스템과 본 연구에서 설계한 시스템의 전송속도를 분석하였다. 화상회의 시스템의 경우 채팅 창을 통한 텍스트의 전송을 위한 텍스트 데이터와 화상전송을 위한 대량의 이미지 데이터를 생성되므로 두 가지 측면에서 전송속도를 나누어 측정하였다.

암호모듈을 삽입했을 때와 그렇지 않을 때의 전송속도가 다소 차이가 있어, 이로 인해 웹 서비스 속도 면에서 영향을 줄 수 있으나, 외부 망의 경우 암호화 및 복호화 처리속도는 일정하므로, 100Kbps 정도의 웹 서비스 환경에서는 암호모듈의 처리시간이 전송시간에 비해 무시할 수 있을 정도로 작기 때문에 본 연구에서 설계한 안전한 화상회의 시스템을 통한 화상회의 구현 시 웹 서비스 속도 면에서 거의 영향을 미치지 않을 것으로 사료된다.

Ⅳ. 결 론

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.

안전한 화상회의 시스템의 구축을 위하여 보안 프로토콜은 공개키 암호화 알고리즘과 비밀키 암호화 알고리즘을 함께 사용하여 안전한 통신을 제공하고자 하였으며, 영상 정보를 암호화하기 위해서 개선된 Vernam의 암호화 기법을 이용하였고, 영상 분할기법을 이용하여 화상을 여러 개의 모듈로 분할한 후 각각의 모듈별로 암호를 합성하는 방법을 사용하여 보다 안전한 시스템을 구축하였다. 암호화 및 복호화 과정에 따른 성능분석으로 일반 웹 시스템과 본 연구에서 설계한 시스템의 전송속도를 분석한 결과, 100Kbps 정도의 웹 서비스 환경에서는 암호모듈의 처리시간이 전송시간에 비해 무시할 수 있을 정도로 작은 것을 확인할 수 있었다.

참고문헌

[1] J. Aggarwal and Q. Cai, "Human Motion Analysis: A Review, Computer Vision and Image Understanding", vol. 73, no. 3, March 1999, pp 428-440

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

[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.

저자소개

고석만(Suk-Man Koh)

1992년 2월 동국대학교 대학원 전자계산학과 이학석사

2001년 2월 조선대학교 대학원 컴퓨터공학과 박사과정 수료

1993년 3월 제주산업정보대학 전임강사

1998년 10월-현재 제주산업정보대학 조교수

※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

1999.4-1999.11조선대학교 산업대학원장

1988년-현재 조선대학교 컴퓨터공학부 교수

※관심분야 : 멀티미디어, 영상처리, 영상통신