情報保護學會論文誌
第 21 卷 第 3 號, 2011. 6

수신단에서 에러 전파 특성을 이용한 MPEG 암호화*

정 서 현,[1] 이 성 주,[1] 정 용 화,[1†] 김 상 춘,[2‡] 민 병 기[3]
[1]고려대학교, [2]강원대학교, [3](주)아스텔

Encryption of MPEG using Error Propagation by a Receiver*

Seo-hyun Jeong,[1] Sung-ju Lee,[1] Youngwha Chung,[1†] Sang-chun Kim,[2‡] Byoung-ki Min[3]
[1]Korea University, [2]Kangwon National University, [3]ASTEL

요 약

모바일 응용에서 MPEG 비디오 스트림 등 대용량 데이터의 이용이 증가함에 따라, 전송되는 대용량 데이터의 정보 보호가 중요한 문제로 부각되고 있다. 대용량 데이터의 효과적인 보호를 위한 부분 암호화 방법으로 SECMPEG이 존재한다. 그러나 SECMPEG의 보안 레벨 3은 B- 나 P-프레임에 비해 상대적으로 용량이 큰 I-프레임을 모두 암호화하기 때문에, 모바일 응용에 적용하기에는 암호화 오버헤드가 크다는 문제가 있다. 그러므로 MPEG2 표준의 압축 특성을 분석하여 I-프레임에서의 부분 암호화를 효과적으로 적용할 필요가 있다. 본 논문에서는 수신단에서 I-프레임 내의 에러 전파 특성을 이용하는, 슬라이스 레벨에서의 부분 암호화 방법을 제안한다. 실험 결과를 통하여 SECMPEG 보안 레벨 3과 비교하여 제안 방법은 보안 성능의 저하없이 수행 시간을 약 30배 이상 단축함을 확인하였다.

ABSTRACT

According to increased multimedia data(i.e., MPEG video stream) in mobile application, protecting data becomes an important problem in the multimedia data delivery. SECMPEG is a selective encryption approach for protecting multimedia data. However, the computational overhead of SECMPEG's security level 3 is quite large because it encrypts the whole I-frames whose size is relatively larger than P/B-frames. Therefore, we need to analyze the characteristics of MPEG2 standard and derive an effective encryption of the I-frames. In this paper, we propose a slice-level, selective encryption approach by using the error-propagation characteristics of I-frames by a receiver. Our experimental results show that the proposed approach can reduce the execution time of SECMPEG's security level 3 by a factor of 30 without degradation of the security.

Keywords: selective encryption, error propagation, MPEG2

I. 서 론

멀티미디어 기술의 발전으로, 대량의 멀티미디어 콘텐츠가 모바일과 같은 휴대기기에서 송/수신되고 있다. 멀티미디어 데이터의 수요가 증가하면서, 멀티미디어 데이터의 송/수신 시 데이터의 정보 보호가 중요한 문제로 부각되고 있다[1,2]. 대부분의 멀티미디어 데이터는 대용량 데이터이기 때문에, 멀티미디어 암호화가 실시간으로 이루어지기 위한 효과적인 암호화 알고리즘이 필요하다[5].

최근에는 암호와 압축을 병합한 비디오 암호-압축 방법인 SECMPEG(Secure MPEG)이 암호화 오버헤드를 줄여주는 방법으로 제안되고 있다[1,3,5]. 그러나 대부분의 멀티미디어 암호화 알고리즘은 모바일 환경에서 임베디드 시스템이 실시간으로 동작시키기에는 여전히 계산량이 많다. 본 논문에서는 SECM-

접수일(2010년 11월 8일), 게재확정일(2010년 12월 29일)
* 본 연구는 교육과학기술부와 한국산업기술재단의 지역혁신 인력양성사업으로 수행된 연구결과임.
† 주저자, ychungy@korea.ac.kr
‡ 교신저자, kimsc@kangwon.ac.kr

PEG 보다 적은 작업 오버헤드로 비디오 데이터를 안전하게 보장하기 위한 슬라이스 레벨의 부분 암호화 방법을 제안한다. MPEG의 프레임간의 데이터 비율을 확인한 결과, SECMPEG의 보안 레벨 3일 경우 전체 데이터의 30%(비디오 한 개의 전체 I-프레임 비율)가 암호화되어야 한다. 따라서 본 논문에서는 효과적인 I-프레임의 암호화 처리를 위하여 MPEG2 표준의 에러 전파 특성을 이용하여 I-프레임의 슬라이스 시작 데이터를 부분적으로 암호화하였다. 즉, 송신단에서는 I-프레임의 일부를 암호화하지만 수신단에서 정당하지 않은 사용자가 디코딩하는 경우 에러가 전파되는 특성을 이용함으로써, 대부분의 I-프레임에서 효과적인 암호화 효과를 얻어낼 수 있다.

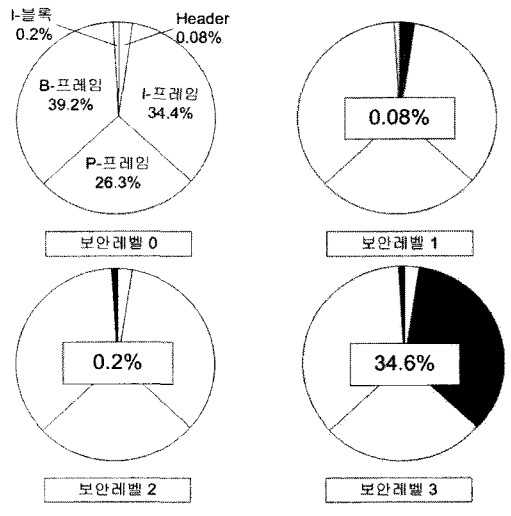
본 논문의 구성은 다음과 같다. 2장에서는 MPEG2의 특성과 SECMPEG의 부분 암호화에 대하여 설명한다. 3장에서는 MPEG2의 에러 전파 특성을 이용한 제안 방법을 설명하고, 4장과 5장에서는 각각 실험 환경 및 결과를 기술한다.

II. Selective Encryption(SECMPEG)

MPEG2[4]는 동영상 손실 압축의 표준으로, 비디오 스트림은 I-프레임, B-프레임, P-프레임으로 구성되어 있다. MPEG 비디오 압축 방법은 GOP(Group Of Picture)의 반복을 이용한 비디오 시퀀스로 구성되며, 각 GOP는 I-, P-, B-프레임의 집합으로 이루어진다. I-프레임은 다른 프레임의 참조 없이 정지영상 압축 표준인 JPEG의 방식으로 압축된다. 그리고 P-프레임은 I-또는 다른 P-프레임의 데이터를 참조하는 모션벡터(motion vector)를 가지고 있어 I-프레임에 비해 데이터의 크기가 작다. B-프레임은 I-와 P-프레임 또는 P-와 P-프레임 간의 움직임의 차를 보간하여 데이터를 구성한다. 또한, 프레임 간의 움직임 보상 시 맞는 블록을 찾지 못하면, 그 블록을 인트라-코드(intra-code) 상태로 압축하며, 그 매크로 블록을 I-블록이라고 한다. 또한, 각 프레임은 데이터열의 최소 단위인 슬라이스로 구성되어있다. 일반적으로 한 개의 슬라이스로 동영상의 한 행을 구성하고 매 행마다 새로운 슬라이스가 구성된다. MPEG2에서는 각 매크로 블록이 이전의 매크로 블록 값을 참조하게 되는 계산 특성에 따라, 하나의 슬라이스 처음 부분에서 일부 에러가 발생하면 해당 슬라이스의 행이 모두 에러가 나타나는 특성이 있다.

SECMPEG[5]는 MPEG과 부분 암호화 알고리즘을 병합한 방법으로, 보안 레벨 4는 전체 암호화를 한 경우이고 보안 레벨 0은 암호화를 하지 않은 경우로, 총 5단계의 보안 레벨을 제공한다. 보안 레벨 1일 경우, 비디오 시퀀스의 헤더만을 암호화 한다. 보안 레벨 2일 경우는 보안 레벨 1과 I-블록의 일부분을 암호화 한다. 보안 레벨 3일 경우에는 I-프레임과 모든 I-블록을 암호화 한다. SECMPEG의 보안 레벨 1에서 암호화하는 헤더 정보는 고정된 크기를 갖고 알려진 정보이기 때문에, 보안 레벨 2와 3 보다 상대적으로 보안성이 낮다. 또한, I-프레임은 I-블록 보다 원영상의 중요한 정보를 더 많이 갖기 때문에 보안 레벨 3은 보안 레벨 2 보다 보안성이 높다. 그러나 보안 레벨이 높아질수록 암호화 하는 데이터 량도 증가한다.

[그림 1]은 MPEG의 비디오 데이터에서 SECMPEG의 보안 레벨에 따라 암호화 되는 데이터량의 비교를 보여준다. GOP 설정에 따라 I-/P-/B-프레임 구성이 달라질 수는 있지만, I-프레임의 크기는 P-와 B-프레임보다 크다. 이는 I-프레임이 한 장의 원 영상을 압축한 데이터이고, P-와 B-프레임은 움직임 예측에 의한 차 영상 등으로 구성되어 있기 때문이다[2]. 특히, 보안 레벨 3에서 I-프레임은 P-와 B-프레임보다 데이터가 크기 때문에 부분 암호화를 적용하더라도 전체 데이터의 30% 이상을 암호화해야 한다[6]. 따라서 임베디드 시스템 등 자원제약적인 환경에서는 보다 효율적으로 I-프레임을 암호화하는 방법의 개발이 필요하다[7].

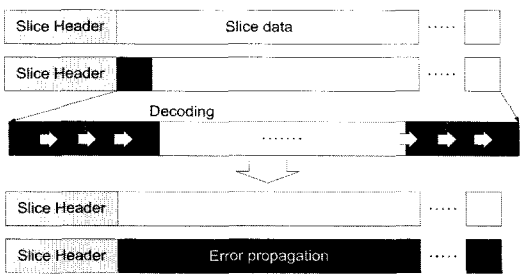


[그림 1] SECMPEG[5] 보안 레벨에 따른 데이터 암호화 크기

III. 제 안 방 법

제안 방법은 MPEG2의 특성에 따른 에러 전파를 이용하여 I-프레임 암호화의 작업 부하를 최소화하는 것이다. 전체 데이터 중 비디오 재생을 위한 헤더 데이터들을 제외한 비디오데이터는 프레임 내에서 슬라이스 단위로 구성되어 있다. 따라서 압축 후 슬라이스의 시작 부분을 부분적으로 암호화를 시키게 되면 디코딩 시 암호화된 데이터와 기존의 정상적인 데이터들이 함께 계산되어 암호화하지 않은 데이터에도 암호를 한 것과 같은 시각적인 왜곡이 전파된다(〔그림 2〕 참조). 즉, 정상적인 사용자는 암호화된 비디오 데이터를 허용된 서버에서 암호화한 부분을 복호화하여 원래의 데이터를 확인하게 된다. 이와 같은 MPEG2의 에러 전파 특성을 이용하여 적은 양을 암호화하여 슬라이스 전체를 암호화하는 효과를 얻을 수 있다.

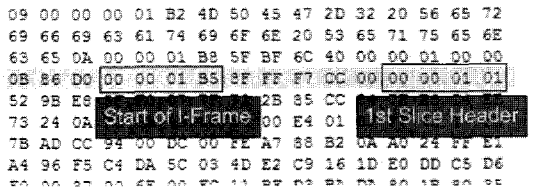
〔그림 3〕은 슬라이스 데이터에 부분 암호화를 적용하였을 경우 암호화 효과가 전파되는 예를 보여준다. 〔그림 3〕의 (a)는 슬라이스 헤더 뒤의 첫 데이터를 암호화 시켰을 경우 나타나는 현상이며, (b)는 슬라이스 중간에 위치하는 데이터를 암호화 시켰을 경우 나타나는 현상이다. 즉, MPEG의 에러 복구(error concealment) 기능에 의하여 암호화 효과(MPEG 변환 후의 데이터 변경에 의하여 MPEG에서는 에러로 처리)가 해당 슬라이스에만 미친다는 것을 확인할



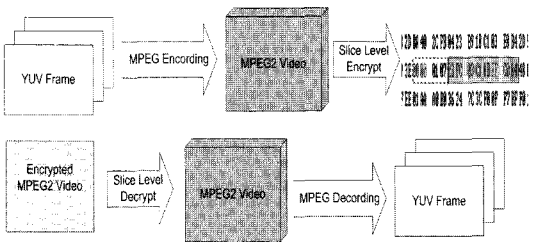
〔그림 2〕 슬라이스 내 에러 전파 과정

(a) 슬라이스 데이터 처음 (b) 슬라이스 데이터 중간

〔그림 3〕 슬라이스 데이터의 에러 전파의 예



〔그림 4〕 슬라이스 헥사 코드



〔그림 5〕 암호화 및 복호화 동작 순서

수 있다. 이러한 에러 복구 기능을 극복하기 위해서는, 각 슬라이스별로 부분 암호화를 적용할 필요가 있음을 확인할 수 있다.

먼저 MPEG2의 헥사 코드를 분석해 보면, 각 프레임과 슬라이스의 헤더가 〔그림 4〕와 같이 "00 00 01 0X"으로 동일한 패턴이 반복되는 것을 알 수 있다. 따라서, 슬라이스 헤더부터 암호화를 하게 되면 알려진 평문 공격(Known Plaintext Attack)의 위험이 있고, 암호화된 동영상을 복호화할 때 암호화된 위치를 파악할 수 없는 문제가 생기기 때문에, 슬라이스 헤더는 암호화 하지 않는다.

〔그림 5〕는 본 논문에서 제안하는 암호화 및 복호화의 전체적인 동작 순서를 보여준다. 먼저, YUV로 구성된 프레임들은 MPEG2 인코더에 의해 인코딩되어 압축 데이터를 생성하고, 이러한 압축 데이터에서 "00 00 01 0X"와 같은 헤더의 시작 부분을 분석하여 슬라이스 데이터의 처음 나타나는 16Byte를 암호화 한다. 또한 복호화는 마찬가지로 "00 00 01 0X" 헤더의 시작 부분을 해석한 후, 슬라이스 데이터의 처음 나타나는 16Byte를 복호화 하며, 마지막으로 복호화된 압축 데이터는 MPEG2에 의해 디코딩 되어 프레임들을 재생성 한다.

IV. 실 험

본 논문에서의 실험 환경은 2-코어 프로세서(인텔 코어2듀오, 3.99GHz, RAM 2.0GB)이고, 실험 비디오 영상은 foreman과 hall monitor 영상으로 프

레임 사이즈는 352×288이고 초당 25프레임으로 동작한다[9]. 헤더를 제외한 프레임의 크기는 610KB이고, 1개의 I-프레임 크기는 43KB이다. P-와 B-프레임은 동작에 따라서 모션 벡터의 양은 달라지지만, 평균적인 수치로 P-프레임의 크기는 33KB, B-프레임의 크기는 17KB이다.

먼저 제안 방법의 수행 성능을 확인하기 위하여 전체 암호, SECMPEG, 그리고 제안 방법의 수행시간을 측정하였다. [표 1]은 SECMPEG의 I-block을 암호화하는 것과 P-, B-프레임의 슬라이스 데이터 16Byte 씩 암호화 하는 것이 비슷하다고 가정하고 I-프레임의 슬라이스 레벨 암호의 성능을 보여준다. 실험에 사용한 암호화 방법은 AES이고, 에러 전파의 특성을 이용한 슬라이스 레벨에서의 부분 암호화 방법이 SECMPEG의 암호화 시간보다 매우 빠르게 수행됨을 확인하였다.

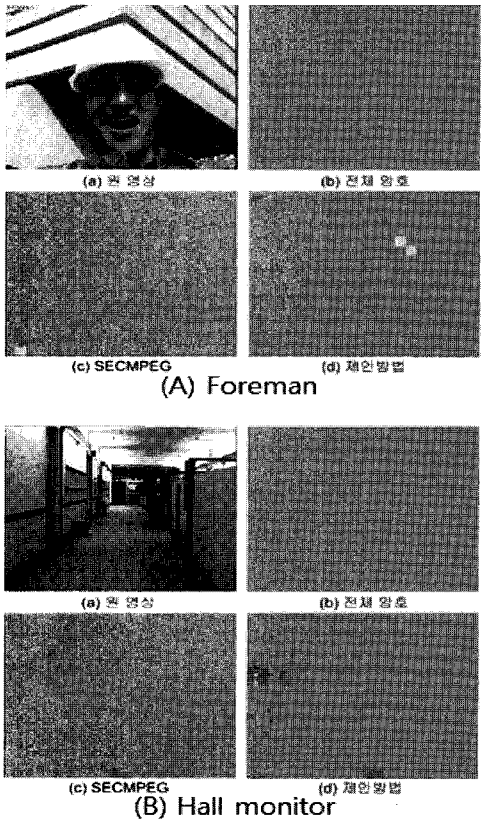
또한, 제안 방법의 보안성을 검증하기 위하여 슬라이스 레벨에서 부분 암호화된 데이터를 디코딩한 영상을 확인하였다. [그림 6]은 각각의 암호화 방식을 적용한 MPEG2의 결과이다. 제안 방법과 SECMPEG은 입력된 비디오가 감시 카메라 환경 등의 모바일 응용에 적용시키기 충분할 정도로 변형된다. 따라서 복호화 키가 없을 경우에는 제안 방법으로 부분 암호화된 데이터를 디코딩 할 경우, MPEG2의 에러 전파 특성에 의해 대부분의 영상을 은닉 할 수 있다.

마지막으로 제안 방법의 보안성을 SECMPEG과 비교하기 위하여 부분 암호화 방법의 안전도를 계산하였다. 즉, 안전도가 높을수록 원 이미지 I 와 변형된 이미지 D를 비교하여 최대한 차이가 나야하며, 이때 데이터 분량의 차이를 측정하는 방식으로는 Mean-Square-Error(MSE)[8]를 이용하여 암호 시스템에서 암호문과 평문의 차이를 나타내는 Confusion Degree(CD)를 식 (1)과 같이 정의한다.

$$\mathrm{CD(MSE)} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j)-D(i,j)]^2 \qquad (1)$$

[표 1] 610KB 비디오 데이터의 암호화 시간

	전체 암호	SECMPEG [5]	제안 방법
전체 크기	610KB	610KB	610KB
암호화 크기	610KB	207KB	7KB
수행시간	0.73sec	0.25sec	0.008sec



[그림 6] 암호화된 데이터

또한, 전체 암호 이미지와 부분 암호 이미지의 상대적인 보안성을 측정하기 위해서, Relative Confusion Degree(RCD)를 식 (2)와 같이 정의한다.

$$\mathrm{RCD}(\%) = \frac{\textit{Selective encryption's MSE}}{\textit{Full encryption's MSE}} \times 100 \qquad (2)$$

식 (1)과 (2)에 따르면, SECMPEG의 RCD는 99.9%이고, 제안 방법의 RCD는 99.7%이다. 즉, SECMPEG은 전체 비디오의 33%를 암호화하고 제안 방법은 1%를 암호화하지만, RCD를 이용한 부분 암호화의 보안성 관점에서는 두 방법이 유사한 보안성을 제공함을 알 수 있다.

[표 2] MSE를 이용한 부분 암호화의 Relative Confusion Degree(RCD) 측정

보안성	SECMPEG[5]	제안 방법
RCD	99.9%	99.7%

V. 결 론

본 논문에서는 적은 작업 계산량으로 비디오 데이터를 보호하기 위한 효율적인 부분 암호화를 제안하였다. 먼저, 기존의 부분 암호 방법인 SECMPEG을 분석한 후, 암호화 시 안전한 보안을 위해서는 보안레벨 3 이상을 적용해야 하며 데이터의 30% 이상을 차지하는 I-프레임의 효과적인 암호화가 필요함을 확인하였다. 그리고 MPEG2의 에러 전파 특성을 이용하여 I-프레임에서 각 슬라이스의 시작 데이터만을 암호화함으로써 수행시간을 감소시키고, 디코딩 시 MPEG2의 에러 전파 특성에 의해 정당한 복호화 키가 없는 경우에는 영상을 제대로 복원하지 못하도록 하는 방법을 제안하였다. 실험을 통하여 제안 방법은 보안성의 저하없이 SECMPEG 보다 약 30배 이상의 수행 시간을 감소시킬 수 있음을 확인하였다.

마지막으로 비디오 데이터를 보호하기 위하여 비트 스트림 레벨 또는 코딩 레벨에서 부분 암호화를 수행하는 많은 연구가 발표되었으며, 각각은 서로 다른 장단점을 가지고 있다[10,11,12]. 코딩 레벨에서의 부분 암호화 방법에 비하여 본 논문에서 제안한 비트 스트림 방식의 방법은 압축 효율의 저하가 없고 표준 비디오 코덱과 부합하는 등의 장점이 있다. 특히, 대량의 멀티미디어 콘텐츠를 휴대기기 등의 임베디드 시스템에서 동작시키는 경우에 매우 효과적일 것으로 기대된다.

참고문헌

[1] B. Furht and D. Kirovski, Multimedia Security Handbook, CRC press, 2005.

[2] G. Jakimoski and K. Subbalakshmi, "Cryptanalysis of Some Multimedia Encryption Schemes," IEEE Tr. Multimedia, Vol. 10, No. 3, pp. 330-338, 2008.

[3] X. Liu and A. Eskicioglu, "Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions," Proc. of Conf. Communications, Internet, and Information Technology, pp. 17-19, Nov. 2003.

[4] J. Watkinson, The MPEG Handbook, Elsevier, 2004.

[5] J. Meyer and F. Gadegast, "Security Mechanism for Multimedia Data with the Example MPEG-1 Video," *Project Description of SECMPEG*, Technical University of Berlin, May 1995

[6] T. Lookabaugh, et al., "Security Analysis of Selectively Encrypted MPEG2 Streams," Proc. of Multimedia Systems and Applications, pp. 10-21, Sep. 2003.

[7] T. Seidel, D. Socek, and M. Sramka, "Cryptanalysis of Video Encryption Algorithms," Proc. of Central European Conf. on Cryptology, vol.29, pp. 1-9, Sep. 2004.

[8] A. Gurijala, et al., "On Encryption-Compression Tradeoff of Pre/Post-Filtered Images," Proc. of SPIE, Vol. 5915, pp. 1-10, Sep. 2005.

[9] J. Woods, "Center for Image Processing Research," http://www.cipr .rpi.edu/ftp_pub/sequences/sif/yuv/.

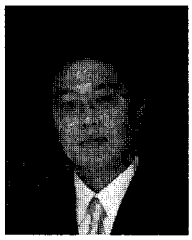
[10] A. Massoudi, et al., "Overview on Selective Encryption of Image and Video: Challenges and Perspectives," EURASIP J. on Information Security, Nov. 2008.

[11] F. Liu and H. Koenig, "Survey of Video Encryption Algorithms," *Computers & Security*, Vol. 29, No. 1, pp. 3-15, June 2009.

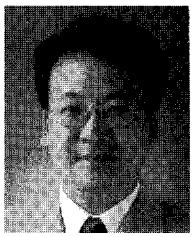
[12] N. Kulkarni, B. Raman, and I. Gupta, "Multimedia Encryption: A Brief Overview," *SCI* 231, pp. 417-449, Sep. 2009.

〈著者紹介〉

정 서 현 (Seohyun Jeong) 학생회원
2010년 2월: 고려대학교 컴퓨터정보학과 학사
2010년 3월~현재: 고려대학교 컴퓨터정보학과 석사과정
〈관심분야〉 멀티미디어데이터, 정보보호

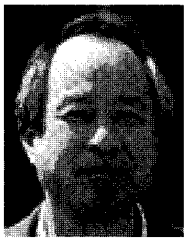


이 성 주 (Sungju Lee) 학생회원
2006년 2월: 고려대학교 전산학과 학사
2006년 3월~2008년 2월: 고려대학교 전산학과 석사
2008년 3월~현재: 고려대학교 전산학과 박사과정
〈관심분야〉 멀티코어, 에너지 효율성, 정보보호



정 용 화 (Yongwha Chung) 종신회원
1984년: 한양대학교 전자통신공학과 학사
1986년: 한양대학교 전자통신공학과 석사
1997년: Univ. of Southern California 전기공학과(컴퓨터공학 전공) 박사
1986년~2003년: 한국전자통신연구원 생체인식기술연구팀장
2003년~현재: 고려대학교 컴퓨터정보학과 교수
〈관심분야〉 성능 평가, 정보 보호, 멀티미디어데이터 보호

김 상 춘 (Sangchoon Kim) 종신회원
1986년: 한밭대학교 전자계산학과 학사
1989년: 청주대학교 전자계산학과 석사
1999년: 충북대학교 전자계산학과 박사
1983년~2001년: 한국전자통신연구원 정보보호연구단
2001년~현재: 강원대학교 정보통신공학과 부교수
〈관심분야〉 정보보호, 보안 시스템 설계 및 구현, 네트워크 및 RFID 보안



민병기 (ByoungKi Min) 정회원
1980년: 서울대 공대 전자공학과 학사
1982년: KAIST 전기 및 전자공학과 석사
1991년: Telecom ParisTech(ENST) 전자공학과 박사
1983년~2000년: 한국전자통신연구소 책임연구원
2000년~현재: (주)아스텔 부설연구소장
〈관심분야〉 멀티미디어, VLSI 구조 및 ASIC설계