적응적인 인터리빙과 셔플링을 이용한 디지털 영상의 암호화

정회원 이 호 준*, 위 진 우**

Digital Image Encryption Method Using Adaptive Interleaving and Shuffling

Ho-Joon Lee*, Jinwoo Wee** *Regular Members*

요 약

본 논문에서는 디지털 콘텐츠의 저작권 보호를 위해 기존의 고정된 셔플링 테이블을 이용한 암호화의 가장 큰 단점인 평문 공격에 대한 취약성을 보완할 수 있는 암호화 기법을 제안하였다. 이를 위해 우선, 영상의 특징 값에 따라 적응적으로 변하는 스크램블 방법을 제안하고, 사용하여 DCT에서 처리된 8x8블록을 셔플링하는 암호화 방법과 기존의 셔플링 방법을 결합한 적응적인 셔플링 방법을 이용하여 영상을 암호화하는 두 가지 방법을 제안하였다. 제안한 적응적인 인터리브와 셔플링 방법을 이용한 암호화 방법은 기존의 셔플링 테이블 방법에 비해 공격에 강인한 특징을 가졌고, 모의실험을 통해 JPEG 등의 DCT(Discrete Cosine Transform) 기반 영상 콘텐츠를 위한 효과적인 암호화 방법으로 사용될 수 있음을 보였다.

Key Words : Interleaving, Scrambling, Video Encryption, Shuffling, DRM

ABSTRACT

n this paper, we propose a digital image encryption method using adaptive interleaving and multiple random shuffling table to improve the existing encryption methods which use a fixed random shuffling table. In order to with stand the plaintext attack, we propose a interleaving method that is adaptive to the local feature of image. Secondly, using the proposed Adative interleaving only shuffling method and multiple shuffling method that is combined interleaving with existing shuffling method, we encrypted image by shuffled the DCT processed 8×8 blocks. In this paper, we proposed digital image encryption method using Adaptive interleaving and shuffling to protect right of contents authorship. Experimental results show that proposed method can be used to encrypt digital image data.

Ⅰ. 서 론

정보통신 기기를 통해 자신만의 이미지를 강조하기 위해 컴퓨터를 이용한 다양한 소프트웨어를 통해 고유의 상표를 만들 수 있는 비약적인 발전으로 인해 전문가들에 의해서만 가능하였던 디지털 콘텐츠가 복사, 변경이 손쉽게 일반인들에 의해서도 가능하게 되었다. 광대역 정보통신망의 발전으로 인터넷상에서 많은 콘텐츠 공유가 가능하게 되면서, 디지털 콘텐츠의 불법 복제 및 위변조가 성행하게 되었다. 디지털 콘텐츠는 사용하는데 여러 가지 공유하는 장점이 있으나 많은 문제점을 야기하고 있다.

* 한림성심대학 컴퓨터정보기술과(hojoon@hsc.ac.kr), ** 한국폴리텍1대학 통신전자과(jwwee@kopo.ac.kr)
논문번호 : 07091-1119, 접수일자 : 2007년 11월 19일

따라서 콘텐츠의 제작자는 소유권 주장이나 내용의 변질에 대한 인증과 검증을 필요로 하게 되었다[1].

디지털 멀티미디어 콘텐츠를 보호하는 방법에는 콘텐츠가 불법적으로 유통되었을 때 배포자가 누구인지 또는 원 소유자가 누구인지를 구분하기 위한 대응책으로 소극적인 성격의 워터마크 방법이 있고 불법적인 형태의 멀티미디어 콘텐츠에 대한 접근 자체를 원천적으로 막을 수 있는 적극적 성격의 암호화 방법도 있다. 데이터 암호화를 영상에 적용하여 원영상 자체를 암호화하거나 JPEG/MPEG등 압축방식과 함께 사용되어 압축된 비트스트림에 블록(DES or RSA)암호화 방법을 그대로 적용하는 방법이 있는데 이 경우, 처리 시간이 가장 문제가 되며, 비트스트림 전체를 대상으로 할 경우 헤더 정보를 이용하여 동기화를 하거나 트릭 모드와 같은 부가적인 기능을 수행하는 데 문제가 된다[2]. 따라서 비트스트림 전체를 대상으로 하는 것보다는 헤더를 제외하고 암호화를 하는 것이 바람직하며 압축과 암호화를 동시에 진행하면서 압축 과정의 구조적 특성을 이용하는 선택적 암호화방법이 효과적이라고 할 수 있다[3].

M.S. Kankanhalli와 T.T. Guan은 인트라 프레임에만 DES 암호화를 적용하여 전체적인 암호화 데이터량을 줄이는 선택적 암호화 방법을 제시하였다. 이 방법은 인트라 프레임을 정상적으로 복원하지 못하면 예측 프레임에 해당하는 P, B 프레임은 무의미하다는 기본 아이디어가 적용되었다.

C.K. Ho and C.T. Li는 DCT 영역에서 DC, AC 계수의 부호를 변환하거나 매크로 블록간의 셔플링, 회전 등을 이용하여 영상을 왜곡시키는 방법을 소개하였다[4, 5]. 이러한 셔플링 기반의 영상 암호화의 경우 셔플링 자체의 연산시간이 기존 DES나 RSA에 비해 상대적으로 빠르다는 장점이 있는 반면에 평문 공격에 취약하다는 단점이 있다[6, 7].

Ⅱ. 영상 암호화의 셔플링 기법

영상 암호화 기법에서 스크램블과 셔플링은 가장 많이 이용하는 암호화 기법이다. Tang은 DCT 변환된 8×8 블록의 ZigZag 패턴에 랜덤 순열 테이블을 적용하여 1×64 벡터 형태로 표현하는 암호화 방법을 제안하였다[8]. 일반적으로 DCT 계수 중 DC 계수는 가장 큰 값을 갖기 때문에 쉽게 예측이 될 수 있으므로 DC 계수 값은 가장 큰 값을 갖기 때문에 쉽게 예측이 될 수 있으므로 DC 계수를 상위 4 비트와 하위 4 비트로 나누어 특정 AC 계수 영역에 은닉시키는 방법으로 DC 계수가 쉽게 예측되는 문제점을 보완한다. S. Lian은 의사(pseudo) 공간 채움 곡선(Space Filling Curve)을 셔플링 테이블로 사용하여 DCT 계수들을 섞는 방법을 제안하였고, 순열 테이블이 평문 공격에 의해서 깨질 수 있는 단점과 ZigZag 패턴의 변화로 인하여 데이터 량이 최대 50% 정도까지 증가하는 문제가 있다. W.Zeng은 슬라이스 단위로 DCT 블록내의 동일한 위치의 계수 값들을 모아 셔플링하는 방법을 제안하였다. 압축 효율과 통계적 특성에 최대한 영향을 미치지 않도록 하기 때문에 Tang의 방법에 비해 증가하는 비트량이 상대적으로 적은 장점이 있지만, 평문 공격에 취약하다는 단점이 있다. 평문 공격에 대한 단점을 해결하기 위해 W. Zeng은 셔플링에 관여하지 않는 지역적인 정보에 의해 셔플링 테이블을 만드는 방법을 제안하였다.

G. Liu는 DC 계수는 DES 암호화하고 AC 계수는 런-길이 값(event list)을 셔플링하는 선택적 암호화 방법을 제안하였다[9]. 평문 공격에 약한 단점이 있어서 추가적으로 부호 비트를 반전하는 보완책을 제시하였다. 셔플링 방식의 암호화 강도는 셔플링 공간의 크기가 n 이라면 n!의 값을 갖는다. 그런데 평문 공격의 경우 암호화 강도가 n의 반복횟수와 요소간 비교 계산으로 기하급수적으로 떨어진다. 만약 셔플링 테이블이 고정되지 않고 가변적으로 변한다면 현재 구한 셔플링 테이블은 의미가 없기 때문에 공격자는 매번 동일한 반복행위를 해야 하고 실제적인 해킹에 어려움이 있다고 볼 수 있다. 따라서 암호화의 보안성을 높이기 위해서 랜덤 셔플링 테이블을 지속적으로 변경해줘야 하는데 이 때 비밀 키 관리의 문제점과 랜덤 테이블을 지속적으로 만드는데 소요되는 계산량이 문제가 된다[10]. 논문에서는 영상 암호화의 셔플링 테이블 사용에 따른 단점을 보완하기 위해 영상의 특징에 따라 변하는 적응적인 스크램블과 셔플링 방법과 결합된 형태의 다중 셔플링 방법을 제안하며 이를 JPEG 영상의 암호화에 적용하여 그 효용성을 실험하였다.

Ⅲ. 제안한 영상 암호화

영상 데이터 암호화에 대한 연구는 1990년대 중반에서 본격적으로 연구가 되었다. 초기에는 일반 텍스트 데이터에 비해 영상의 데이터량이 상대적으로 많기 때문에 주로 암호화의 연산 시간을 효율적

으로 줄이기 위한 연구가 주를 이루었다. 현재는 부가적인 기능을 충족시키기 위한 호환성 지원 부분에 대한 연구가 진행되고 있다. 정지 영상에 대한 암호화는 주로 랜덤 스캐닝 패턴을 이용하여 공간 영역에서 암호화하는 방법과 JPEG 영상의 8x8 DCT 블록을 셔플링하거나 스크램블링하는 경우 암호화 과정이 단순하고 경우에 따라 비트 오버헤드가 발생하지 않는다는 장점이 있는 반면에 평문 공격에 취약하다는 단점이 있다[11, 12, 13]. 본 논문에서는 기존의 다중 셔플링 테이블을 이용한 방법의 최대 약점인 평문 공격에 대한 취약성을 보강하기 위해 영상의 특징에 의해서 적응적인 셔플링 형태를 갖는 방법을 제안하였다.

3.1 영상특징에 적응적인 셔플링 방법

3.1.1 적응적 인터리빙 (방법1)

적응적인 인터리빙의 방법은 그림 1에 제안한 적응적 인터리빙 방법을 아래의 순서로 진행하는 과정을 설명하였다[14].

정상 순서	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11	12,	13
재배치 간격	3,	1,	2,	1,	2,	1,	2,	3,	1,	1,	3,	2,	1
상태 코드 값	0,	0,	0,	0,	0,	0,	0,	0,	0,	0,	0,	0,	0
반복 횟수	3												

1. 인터리빙 요소를 원래의 순서형태로 배열한다.
2. 첫 요소는 재배치하지 않고 상태 값만 1로 한다.
3. 첫 요소에서 특징 값을 구한다.
4. 구해진 특징 값과 간격지수와의 XOR 연산을 수행한다. 이 결과 값을 재배치 간격이라 한다.
5. 재배치 간격만큼 떨어져 있는 위치의 요소를 첫 요소 다음에 위치시키고, 해당 위치 요소의 상태 값을 1로 한다.
6. 3 - 5단계의 과정을 반복한다. 만약 현재 요소가 마지막 요소이면 1회 반복이 끝난다.
7. 반복횟수만큼 6의 과정을 수행하고 모든 상태 값이 1이거나 제한된 반복 횟수가 되면 종료한다.

배열의 크기가 13인 "WELCOMTOKOREA"의 문자열이 인터리빙에 의해서 섞이는 과정을 예를 들면 다음과 같다.

1. 첫 요소인 "W"는 재배치되지 않고 현재의 위치에 둔다. 첫 요소로부터 구한 재배치 간격이 "3"이므로 첫 요소로부터 거리가 3 떨어져 있는 4번째 요소(C)가 재배치된다.
2. 4번째 요소의 재배치 간격이 "1"이므로 5번째 요소가 재배치된다. 11번째 요소의 재배치 간격이 3이므로 다음 위치 값은 14번째 요소이나 배열에는 14번째 요소가 없으므로 11번째 요소가 마지막 재배치 요소가 되고 1회 반복이 끝난다.
3. 재배치되지 않은 배열 색인 중에서 가장 순서가 빠른 두 번째 요소가 두 번째 반복의 첫 번째 요소가 되며, 동일한 방법을 거치면 2, 3, 8번째 요소가 재배치된다.
4. 6번째 요소의 재배치 간격이 "1"이고 이후로 재배치되지 않은 요소 중에서 6번째 요소로부터 1만큼 떨어져 있는 12번째 요소가 재배치된다. 12번째 요소의 재배치 간격이 '2" 이므로 13번째 마지막 요소는 재배치되지 않고 3번째 반복이 종료된다.
5. 3회 반복으로 반복은 종료되고 전체 요소 중 재배치되지 않은 나머지 요소를 순서대로 재배치한다.

복호화 단에서는 디인터리빙을 하여야 하는데 수신된 요소를 미리 정해진 인터리빙 공간의 크기만큼의 임시 메모리 영역에 저장한다. 첫 번째 요소의 특징 값을 추출하고 추출된 특징 값과 간격 지수와의 XOR 연산을 통해서 재배치 간격을 구한다. 구해진 재배치 간격이 "3"이라면 수신 메모리의 두 번째 위치에 있는 요소의 원래의 위치는 1번째 위치로부터 3만큼 떨어져 있는 4번째가 된다. 이와 같은 방법을 주어진 반복 횟수만큼 반복하거나 또는 상태 값이 모두 "0"이 될 때까지 반복한다. 디인터리빙 과정에서 사용되는 간격 지수는 인터리빙에서 사용되는 값과 동일한 비밀키에 의해서 생성된 값이다.

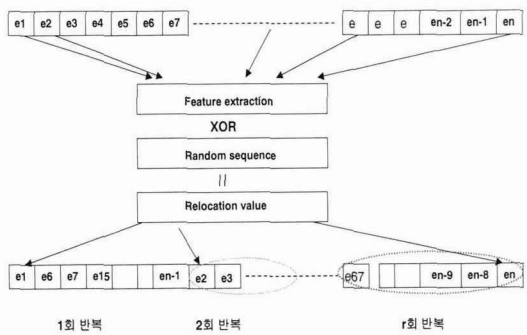


그림 1. 제안한 적응적 인터리빙

3.1.2 적응적인 인터리빙과 셔플링의 결합 (방법2)

제안한 인터리빙 방법은 영상의 특징에 의해서 해당 영상을 불규칙하게 섞는 특성을 가진다. 영상 전체를 골고루 불규칙하게 섞기 위해선 가능한 많은 반복 횟수와 적은 크기의 재배치 간격 값이 필요하게 된다. 만약 너무 큰 재배치 간격과 너무 적은 횟수의 반복으로 인터리빙을 수행한다면 암호화 수행 시간은 상대적으로 적게 걸리지만 영상이 골고루 섞이지는 않는 문제점을 보이게 된다. 이러한 문제점을 극복하기 위해선 적절한 반복 횟수를 정하고 인터리빙을 단독적으로 사용하기 보다는 1차는 인터리빙에 의해 셔플링하고 2차는 적응적인 셔플링 테이블 방식을 결합하는 것이 암호화 후 영상의 가시성을 좀 더 떨어져도 암호화의 보안성을 높일 수 있게 된다.

3.2 제안한 알고리듬을 이용한 영상 암호화

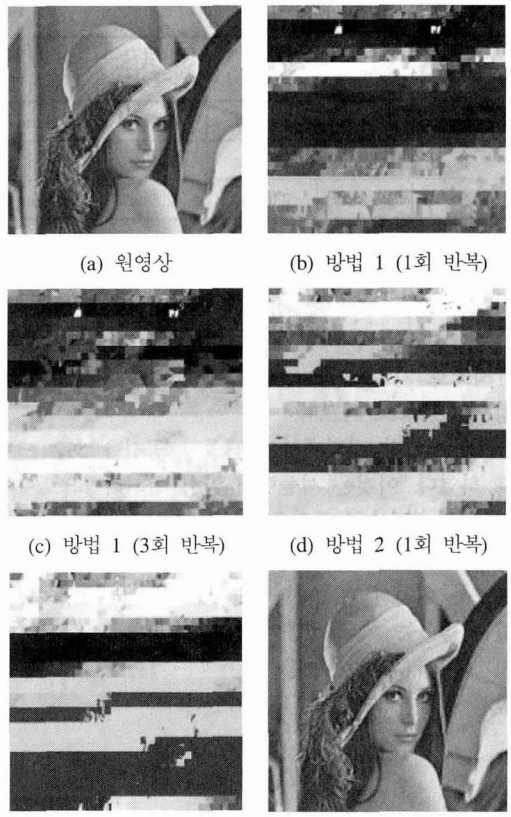
제안한 적응적인 인터리빙과 셔플링을 결합한 다중 셔플링 방법을 이용하여 DCT 블록을 셔플링하는 암호화의 효용성을 알아보기 위해 정지영상을 대상으로 실험을 하였다. 양자화 후의 8×8 블록을 셔플링하는 경우 DCT 값의 통계적 특성이 변하므로 압축률을 감소시킬 수 있다(동영상에 적용시 인트라 프레임에 해당하는 경우). 반면 연산후의 DCT 블록을 셔플링 하면 비트량 증가는 나타나지 않는다. 본 논문에서는 DPCM 값을 구한 후의 8x8 블록을 적응적인 인터리빙과 셔플링을 이용하여 불규칙하게 섞었다.

제안한 방법을 이용한 암호화 과정에 따라 다음과 같이 진행한다.

1. 인터리빙(셔플링) 요소 및 인터리빙(셔플링) 공간의 크기를 결정한다.
2. 임의의 Seed 값을 랜덤 수로 생성한다.
3. DCT, 양자화를 수행한다.
4. 양자화된 블록에서 DPCM 값을 구한다.
5. 특징값, 재배치 간격 등을 구한다. 특징값은 DPCM 계수의 하위 4비트로 하였다.
6. 블록을 인터리빙 절차에 의해 재배치한다.
7. 재배치된 블록을 셔플링 테이블에 의해 섞는다.
8. 섞여진 블록을 런길이 부호화, 허프만 부호화 등을 거쳐 JPEG 부호화를 수행한다.

Ⅳ. 모의 실험 및 결과

본 논문에서 실험은 Lena(256×256) 컬러 포맷 영상을 대상으로 Windows XP 환경의 펜티엄-4 PC (Clock = 3.0GHz, 1.5Gbyte)에서 수행하였다.



(a) 원영상 (b) 방법 1 (1회 반복)
(c) 방법 1 (3회 반복) (d) 방법 2 (1회 반복)
(e) 방법 2 (3회 반복) (f) 복원된 영상

그림 2. 암호화 영상 제안한 복원 영상

그림 2(a)는 원 영상이고, (f)는 복호화에서 복원된 영상이다. (a), (b) 는 각기 반복 횟수를 1, 3 로 하여 인터리빙만을 적용하여 셔플링했을 때의 암호화된 영상을 보여준다. 1, 3회 반복 시에는 Lena 영상에서 중앙 부분에 색깔 정보 정도 밖에 볼 수 없고 5회 정도의 반복이면 영상의 의미 파악이 힘든 정도이다.

그림 2의 (d), (e)는 각기 1, 3회의 반복 횟수로 적응적인 인터리빙과 셔플링 두가지를 결합하여 셔플링 했을 때의 암호화 결과이며, 인터리빙 반복 횟수와 무관하게 시각적으로 영상의 내용을 판독하기가 어려움을 볼 수 있다. 여기서 기존의 셔플링 방법은 일반적으로 사용되는 랜덤 수 발생기를 이용하여 만든 셔플링 테이블을 이용한 경우이고 제안한 방법은 인터리빙만을 수행했을 경우와 적응적인 인터리빙과 셔플링을 결합한 다중 셔플링 방식을 이용한 암호화에 해당한다. 표 1은 제안된 방법의

표 1. 제안한 알고리듬의 연산 시간 비교

인터리빙 반복 횟수	JPEG picture	기존 방법 수행시간	방법 1 수행시간	방법 2 수행시간
1	10.6ms	21.1ms	1.9μs	2.1μs
3	10.8ms	21.1ms	2.1μs	2.3μs
5	10.8ms	21.1ms	2.6μs	2.8μs

반복 횟수에 따른 연산 시간을 비교한 것이다. 암호화 시에 걸리는 연산 시간은 인터리빙의 반복 횟수에 따라 조금씩의 차이가 있었는데 연산시간이 평균적으로 기존 수행 방법을 했을 때보다 100 여배 정도의 속도로 빠르다.

즉, 제안된 방법에서는 셔플링 공간을 512 크기로 하였다. 이것은 셔플링에 앞서 인터리빙으로 1차적인 적응적인 셔플링을 했기 때문에 셔플링 공간의 크기를 전체 크기의 1/2로 하더라도 두 공간에 골고루 섞이기 때문이다. 반대로 랜덤 셔플링 만을 하는 경우는 휘도 성분이 전체 영역에서 골고루 섞이게 하기 위해 셔플링 공간의 크기를 휘도 성분의 전체 블록 개수인 1024로 하였다.

V. 결 론

본 논문에서는 제안한 인터리빙 방식과 셔플링을 특징값에 따라 적응적으로 변하는 인터리빙 방법을 제안하고 또한 제안된 인터리빙과 기존의 셔플링 방법을 결합한 다중 셔플링 방법을 이용하여 DCT 8×8 영역에서 랜덤하게 섞어서 영상을 암호화 하는 방법을 제안하였다. 모의실험 결과 제안한 적응적인 인터리빙 방법과 기존의 셔플링을 결합하여 영상의 특징에 따라 적응적으로 섞게 됐을 때에는 영상의 가시성이 한층 더 떨어졌으며 일반적인 공격에 대한 암호화 강도도 더 높게 나타났다. 제안한 적응적인 인터리빙과 셔플링 기법을 이용하여 8×8 블록을 랜덤하게 섞었을 때 별도의 추가적인 데이터 량 증가나 복원시의 화질열화도 나타나지 않았고 적응적인 인터리빙과 셔플링 방법을 이용한 블록 셔플링 기반의 암호화 방법은 영상의 국소적인 특징 값에 따라 적응적으로 변하기 때문에 고정된 형태의 셔플링 테이블만을 사용하는 방법에 비해 외부 공격에 강인한 특징을 가진다. 향후 동영상의 암호화에서 8×8 매크로 블록을 대상으로 셔프링 하는 대신 DCT 계수의 런-길이 부호화나, 허프만 부호화 등을 셔플링 요소로 하여 메모리의 사용량을 줄이는 것에 대한 연구가 진행해야 할 것이다.

참 고 문 헌

[1] 원치선, "디지털 영상의 저작권 보호," 정보과학회지 제15권 제12호, pp.22~27, 1997년 12월.

[2] L.Qiao and K. Nahrstedt, "Comparison of MPEG Encryption Algorithms," inter. Journal on Computer & Graphics, Special Issue on Data Security in Image Comm. and Network, Vol.22, No.3, 1998.

[3] T.B. Maples and G.A. Spanos, "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-time Video," Proc. ICCCN, Las Vegas, Nevada, September 1995.

[4] C.K.Ho and C.T.Li, "Semi-fragile Watermarking Scheme for Authentication of JPEG Image," in Proc. IEEE International Conference on Information Technology: Coding and Computing, Las Vegas, USA, April 2004.

[5] I.Agi and L.Gong, "An Empirical Study of Secure MPEG Video Transmissions," The Internet Spciety Symposium on Network and Distributed System Security, Feb. 1996

[6] W.Puech, J.M.Rodrigues, "Cryptocompression of Medical Images by Selective Encryption of DCT," Proc. EUSIPCO'05, Turkey, September, 2005.

[7] L.Tang, "Methods for Encrypting and Decrypting MPEG Video Data Efficiently," Proc. the Fourth ACM Internal Multimedia Conference, pp.219~229, 1996.

[8] W.Zeng, J.Wen, and M.Severa, "Fast Self-synchronous Content Scrambling by Spatially Shuffling Codewords of Compressed Bitstream," Proc. IEEE ICIP, 2002.

[9] G. Liu, T. Ikenaga, S. Goto and T. Baba, "A Selective Video Encryption Scheme for MPEG Compression Standard," IEICE Trans. Fundamentals, Vol.E89-A, No.1 Jan. 2006.

[10] W. Zeng and S. Lei, "Efficient Frequency Domain Digital Video Scrambling for Content Acess Control," Proceedings of the cnfer-

ence on ACM multimedia '99, 1999.

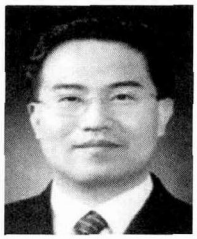
〔11〕 Shi, C., S.Y.Wang, and B. Bhargava:1999, "Fast MPEG Video Encryption Algorithms," Purdue University, USA.

〔12〕 Jennifer Seberry, Josef Pieprzyk, "Cryptography: An Introduction to Computer Security," 1989, Prentice Hall.

〔13〕 J. Watkinson, "MPEG-2," 1999, Focal Press.

〔14〕 이지범, 고형화, "인터리빙과 랜덤 셔플링을 이용한 디지털 영상의 암호화 방법," 한국통신학회 논문지, 제31권, 제5C호, pp.497~502, May, 2006.

이 호 준 (Ho-Joon Lee) 정회원



1988년 2월 광운대학교 전자통신공학과 졸업

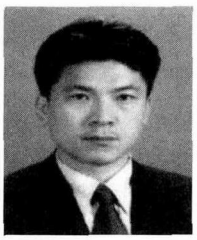
1992년 2월 광운대학교 전자통신공학과 석사

2003년 2월~현 재 광운대학교 전자통신공학과 박사

1996년~현재 한림성심대학 컴퓨터정보기술과 재직

<관심분야> 동영상, 워터마킹, 암호화, DVR 코텍

위 진 우 (Jinwoo Wee) 정회원



1991년 8월 광운대학교 전자통신공학과 석사

2002년 2월 광운대학교 전자통신공학과 박사

1997년~현재 한국폴리텍 I 대학 서울강서캠퍼스 통신전자과 재직

<관심분야> 음성신호처리, 화자인식, 컴퓨터통신