채널 부호화된 워터마크 신호에 기반한 MPEG-2 비디오의 전송 오류 검출과 저작권 보호

배 창 석[†] · Yuk Ying Chung[††]

요 약

본 논문에서는 채널 부호화를 통해 MPEG-2 비디오의 전송 오류를 검출하고 저작권을 보호하는데 사용할 수 있는 정보은닉 방법을 제안한다. 비디오 데이터의 저작권 정보를 길쌈 부호기로 부호화하여 워터마크 신호를 구하며, 입력 비디오 신호를 MPEG-2 비디오 스트림으로 부호화하는 동안 모든 프레임의 매크로 블록에 워터마크 신호를 은닉한다. 복호기에서는 모든 프레임의 매크로 블록으로부터 은닉된 신호를 검출하고 검출한 신호를 이용하여 입력 비디오 스트림에서의 전송 오류의 위치를 판정한다. 동시에 검출한 신호를 저작권 정보로 재구성함으로써 비디오 데이터의 저작권을 주장하는 데 사용할 수 있다. 이 과정에서 채널 복호기는 검출된 워터마크 신호에서의 에러를 정정한다. 제안한 MPEG-2 비디오 코덱을 이용하여 300개의 프레임으로 구성되는 3개의 시퀀스를 대상으로 실험한 결과 제안한 방법이 복호 과정에서 비디오 스트림에서의 전송 오류를 검출할 수 있으며 저작권 정보를 보다 정확히 재구성한다는 것을 보여준다.

키워드 : 디지털 워터마크, MPEG-2, 채널코딩, 전송오류 검출

Transmission Error Detection and Copyright Protection for MPEG-2 Video Based on Channel Coded Watermark

Changseok Bae[†] · Yuk Ying Chung[††]

ABSTRACT

This paper proposes an information hiding algorithm using channel coding technique which can be used to detect transmission errors and to protect copyright for MPEG-2 video. The watermark signal is generated by applying copyright information of video data to a convolutional encoder, and the signal is embedded into macro blocks in every frame while encoding to MPEG-2 video stream. In the decoder, the embedded signal is detected from macro blocks in every frame, and the detected signal is used to localize transmission errors in the video stream. The detected signal can also be used to claim ownership of the video data by decoding it to the copyright information. In this stage, errors in the detected watermark signal can be corrected by channel decoder. The 3 video sequences which consist of 300 frames each are applied to the proposed MPEG-2 codec. Experimental results show that the proposed method can detect transmission errors in the video stream while decoding and it can also reconstruct copyright information more correctly than the conventional method.

Key Words : Digital Watermark, MPEG-2, Channel Coding, Transmission Error Detection

1. 서 론

집밖에서의 네트워크와 홈네트워크가 고속화됨에 따라 대용량의 데이터를 고속으로 처리해야 하는 여러 종류의 서비스가 일반화되고 있다. 이러한 서비스들 중에서 멀티미디어 서비스가 가장 대표적인 것이며 이러한 종류의 서비스는 집안과 밖에서 모두 제공되기를 요구받고 있다[1-3]. 멀티미디어 서비스에 사용되는 디지털 멀티미디어 데이터는 복제가 용이하고 복제 시 원본과 복제본이 동일하기 때문에 불법 복제의 심각한 위험성에 항상 노출되어 있다. 따라서 불법 복제를 방지하기 위하여 디지털 멀티미디어 데이터에 대한 저작권을 보호하기 위한 방안을 마련할 필요가 있다. 디지털 워터마크[4-7]가 이러한 문제를 해결하기 위한 한 가지 방법이 될 수 있다. 디지털 워터마크는 저작권자가 저작권을 침해 받았을 때 자신의 권리를 주장할 수 있는 수단을 제공한다.

디지털 워터마크는 멀티미디어 데이터의 저작권을 보호하기 위하여 투명성과 강인성이라는 두 개의 조건을 최소한

※ 이 논문은 2005년도 한국학술진흥재단의 지원에 의하여 연구되었음 (KRF-2004-D00137).
† 종신회원 : 한국전자통신연구원 차세대PC플랫폼연구팀 책임연구원
†† 비 회 원 : School of Information Technologies, University of Sydney, Australia, Lecturer
논문접수 : 2005년 8월 12일, 심사완료 : 2005년 10월 26일

만족시켜야 한다. 워터마크 신호는 눈에 띄지 않기 위하여 정보가 은닉되는 데이터에 최소한의 손상만 가져와야 한다. 또한 멀티미디어 데이터에 대한 다양한 종류의 조작이나 손상에 강인해야 한다.

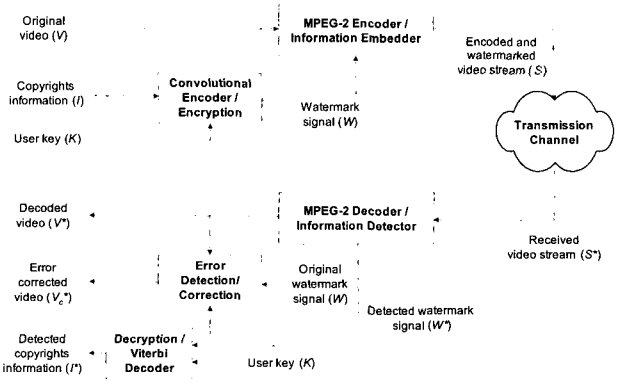
MPEG-2는 디지털 TV 방송과 DVD 비디오 타이틀에서 널리 사용되고 있으며 고화질의 비디오 데이터를 지원한다. 따라서 잡음이 많은 채널을 통한 MPEG-2 비디오의 전송 과정에서 화질의 유지가 강력히 요구된다. 또한 고화질을 지원하는 MPEG-2 비디오의 특성 상 저작권을 보호하는 것도 중요한 문제이다.

본 논문에서는 MPEG-2 비디오 스트림에 대한 DCT 영역에서의 워터마킹 기술과 채널 부호화 기술[8]의 조합을 제안한다. 채널 부호화 방법의 하나인 길쌈 부호기에 의해 부호화된 디지털 워터마크 신호는 잡음 채널에서의 전송 오류를 검출하는데 도움을 준다. 정지영상에 대한 디지털 워터마킹에서 채널 부호화 방법의 유효성은 BCH(Bose-Chaudhuri-Hocquenghem) 부호를 이용하는 방법[9,10]이 제안되어 있다. 또한 H.263 비디오에서 정보은닉을 이용하는 오류 교정 방법[11]이 제안되어 있다. 이들의 연구에서 은닉된 정보는 전송 오류를 검출하는 데에만 사용되며 부호화 과정 동안 DCT 계수에만 정보를 은닉하므로 DCT 계수에서 발생된 오류만 검출할 수 있다. 디지털 워터마크를 이용하여 전송 오류를 검출하고자 하는 또 다른 연구[12]에서는 첫 번째 프레임과 비디오 스트림의 헤더 부분에는 에러가 발생하지 않는 다는 가정을 하고 있으며 비디오 데이터에 대한 저작권 보호는 고려하지 않고 있다. 이는 워터마크 신호의 특성 상 컨텐트의 저작권 보호를 위해서는 공격에 강인한 워터마크 신호를 은닉해야 하고 전송 오류를 검출하기 위해서는 손상되기 쉬운 워터마크 신호를 은닉해야 된다. 이들은 서로 상반된 목적과 방법을 가지고 있다. 본 논문에서는 채널 부호화된 워터마크 신호를 비디오 데이터에 은닉함으로써 비디오 데이터의 저작권 보호를 가능하게 하며 동시에 전송 과정에서 발생되는 오류를 검출할 수 있는 알고리즘을 제안한다.

본 논문은 2장에서 제안한 MPEG-2 코덱의 전체 구조를 보여주고 있으며 3장에서 정보은닉 기능을 가지는 제안한 MPEG-2 부호기에 대해 자세히 설명한다. 제안한 비디오 부호화 방법은 일반적인 MPEG-2 부호기에 길쌈부호기, 암호화 모듈, 그리고 정보은닉 모듈을 추가한 형태이다. 4장에서는 대응하는 MPEG-2 복호기에 대해 설명하고 있다. 제안한 복호기는 일반적인 MPEG-2 복호기와 은닉정보 검출 모듈, 오류 검출 및 복구 모듈, 암호해독 모듈, 그리고 비터비 복호기로 구성되어 있다. 5장에서 제안한 방법에 의한 실험 결과를 제시하고 있으며 마지막으로 6장에서 결론과 향후 연구방향에 대해 논의하고 있다.

2. 채널 부호화된 워터마크 신호에 대한 은닉, 검출 기능을 가진 MPEG-2 코덱

제안한 방법의 전체적인 구조는 (그림 1)에서 보여주고 있다. 워터마크 신호(W) 는 멀티미디어 데이터에 대한 저작권 정보(I)를 길쌈 부호기에 적용함으로써 구해진다. 다음으로 길쌈 부호화된 신호는 사용자 키(K)를 이용하여 암호화된다. 워터마크 신호는 입력 비디오 시퀀스(V)를 부호화하는 동안 MPEG-2 스트림의 모든 프레임에서 각각의 매크로블록에 은닉된다. 워터마크 신호가 은닉된 MPEG-2 스트림은 잡음 채널을 통해 수신단으로 전송된다.



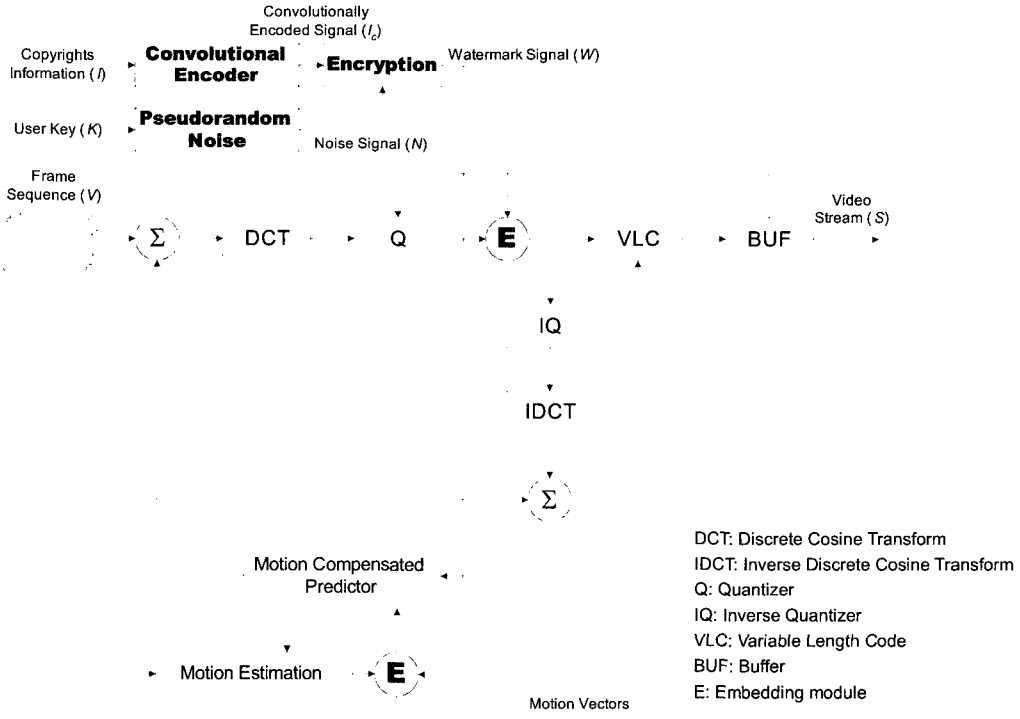
(그림 1) 제안한 시스템의 전체 구조

수신단에서는 전송되어 온 MPEG-2 비디오 스트림(S^*)의 모든 프레임의 매크로 블록으로부터 은닉된 워터마크 신호가 검출된다. 검출된 워터마크 신호(W^*)는 두 가지 목적으로 사용된다. 먼저, 이 신호는 원래 은닉에 사용된 워터마크 신호(W)와의 비교에 의해 수신된 MPEG-2 스트림에 존재하는 전송 오류를 찾는데 사용된다. 이러한 전송 오류가 정확히 발견된다면 오류가 복구된 비디오(V_c^*)를 용이하게 생성할 수 있다. 다음으로 검출된 신호는 비터비 복호기에 적용됨으로써 수신된 MPEG-2비디오 스트림(S^*)의 저작권을 주장하는데 사용된다. 비터비 복호기가 검출된 신호에 존재하는 오류를 찾아 복구할 수 있으므로 복원되는 저작권 정보(I^*)의 비트 오류율(BER)은 현저히 감소될 수 있다. 그 밖에 워터마크된 MPEG-2 스트림은 MPEG-2 부호화 표준을 위반하지 않으므로 일반적인 MPEG-2 복호기에서도 문제없이 재생된다. 하지만 일반적인 MPEG-2 복호기를 사용하여 복호된 비디오는 잡음 채널에서 화질 개선을 기대할 수 없다.

3. 정보 은닉 기능을 가진 MPEG-2 부호기

본 논문에서 저작권 정보와 워터마크 신호는 완전히 다른 개념을 가진다. 먼저, 저작권 정보는 MPEG-2 비디오의 저작권을 보호하기 위한 특수한 부호를 의미한다. 반면에 워터마크 신호는 비디오 데이터를 MPEG-2 스트림으로 부호화하는 동안 모든 프레임의 매크로 블록에 직접 은닉되는 신호를 의미한다. 워터마크 신호는 저작권 정보를 길쌈 부호기에 적용시켜서 구할 수 있다.

제안한 정보 은닉 기능을 가지는 MPEG-2 부호기는 (그림 2)에서 보여주는 바와 같이 길쌈 부호기를 사용한다. 비디오 스트림에 채널 부호화된 워터마크 신호를 은닉하기 위하여 길쌈 부호기, 의사 랜덤 잡음 생성기, 암호기, 그리고 정보 은닉 모듈(E: Embedding Module)과 같은 칠해진 블록



(그림 2) 정보 은닉 기능을 가지는 MPEG-2 부호기

이 추가되었다. 이와 같이 추가된 블록을 제외하고는 일반적인 MPEG-2 비디오 부호기와 동일하다.

제안한 MPEG-2 부호기에서 저작권 정보(I)는 길쌈 부호기를 사용하여 부호화되고 부호화된 신호(I_c)는 사용자 키(K)에 의해 생성되는 의사 랜덤 잡음 신호(N)를 이용하여 암호화된다. 본 논문에서는 이와 같이 암호화된 신호를 워터마크 신호(W)로 고려하고 있으며 이 신호가 입력 비디오 시퀀스(V)를 부호화하는 동안 모든 프레임의 매크로 블록에 은닉된다.

MPEG-2에서 모든 프레임은 인트라 프레임 또는 인터 프레임 중의 하나로 부호화된다. 제안한 정보 은닉 알고리즘은 이러한 두 가지 종류의 프레임 모두에 정보를 은닉한다. 인트라 프레임에 대해서는 각 매크로 블록의 DCT 계수에 워터마크 신호를 은닉한다. 반면에 인터 프레임에서는 워터마크 신호가 매크로 블록의 움직임 벡터에 은닉된다.

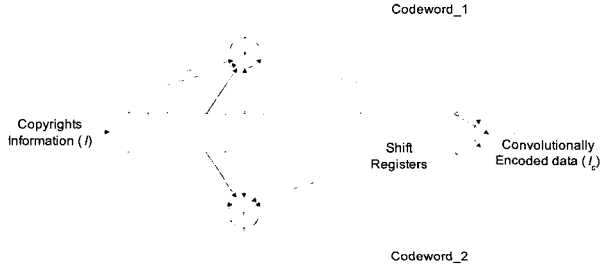
본 장에서는 길쌈 부호기, 암호화 방법, 그리고 프레임 종류에 따른 정보 은닉 알고리즘을 포함하는 제안한 부호기의 각 단계에 대해 설명한다.

3.1 길쌈 부호기

채널 부호화 기법[8]은 원래의 데이터에 여분의 정보를 부가함으로써 통신 채널에서 발생되는 오류를 교정하기 위해 제안되었다. 만약 은닉과 검출 과정에서 전달해야 하는 신호가 워터마크 신호라면 원래의 영상 데이터와 워터마크된 데이터에 대한 조작은 채널 잡음으로 고려될 수 있다. 따라서, 은닉 과정에서의 채널 부호화 기법에 의해 검출된 워터마크 신호의 비트 오류율은 감소될 수 있다.

본 논문에서는 검출된 워터마크 신호의 오류를 교정하기 위한 채널 부호화 기법으로 길쌈 부호기를 사용한다. 가장 대표적인 오류 교정 부호인 길쌈 부호는 원래의 데이터가 쉬프트 레지스터로 순차적으로 입력될 때 생성 다항식과의 연산에 의해 부호화된 부호어를 출력한다. 이는 길쌈 부호기가 생성 다항식과 쉬프트 레지스터의 수를 변화시킴으로써 부호화된 신호의 출력 비트율을 쉽게 조절할 수 있다는 것을 의미한다. 생성 다항식과 쉬프트 레지스터의 수는 여분의 정보의 양을 결정한다. 일반적으로 더 많은 여분의 정보가 포함될수록 더 나은 오류 교정 능력을 가진다. 하지만, 이는 전달해야 하는 비트율의 증가를 가져온다. 손상된 매크로 블록을 검출하기 위하여 본 논문에서는 각 매크로 블록에 한 비트의 워터마크 신호를 은닉한다. 따라서 길쌈 부호화된 신호의 비트 수와 각 프레임에서의 매크로 블록의 수를 같게 한다.

(그림 3)은 복원되는 저작권 정보에서의 비트 오류율을 감소시키기 위해 사용되는 길쌈 부호기의 구조를 보여주고



(그림 3) 길쌈 부호기의 구조 (레이트=1/2)

있다. 하나의 비트의 데이터가 입력될 때마다 길쌈 부호기는 두 개의 부호어(codeword)를 출력한다. 부호어를 출력하기 위해 사용하는 생성 다항식은 다음과 같다.

$$g_1(x) = 1 + x + x^2 + x^3 + x^6,$$
$$g_2(x) = 1 + x^2 + x^3 + x^5 + x^6. \quad (1)$$

(그림 3)에서 보여주는 바와 같이 길쌈 부호화된 데이터를 구성하는 부호어 1은 생성 다항식 1 (g_1)을 이용하여 구하고, 부호어2는 생성 다항식 2(g_2)를 이용하여 구한다.

본 논문에서 사용하는 길쌈 부호기는 2개의 부호어를 출력하고 제한장(constraint length)이 7이므로 m-비트의 데이터 스트림은 $2(m+6)$-비트의 길쌈 부호화된 데이터로 변환된다.

본 논문에서는 24 개의 문자를 구성하는 ASCII 부호를 저작권 정보로 고려한다. 따라서 저작권 정보의 비트 수는 24×8=192 비트가 된다. 이와 같은 저작권 정보는 다음과 같이 표현된다.

$$I = \{i_k | 0 \le k < m\}, \quad (2)$$

여기서 m은 192이고 i_k는 0 또는 1 중 하나의 값을 가진다. 이 정보(I)는 (그림 3)에서 보여주는 바와 같은 길쌈 부호기에 의해 부호화된다. m-비트로 구성되는 저작권 정보가 $2(m+6)$-비트의 길쌈 부호화된 신호로 부호화되므로, 길쌈 부호화된 신호(I_c)의 길이는 2×(192+6)=396 비트가 된다. 이와 같이 길쌈 부호화된 신호의 길이는 다음과 같이 표현된다.

$$I_c = \{i_{ck} | 0 \le k < 2(m+6)\}, \quad (3)$$

여기서 m은 192이고 i_{ck}는 0 또는 1 중 하나의 값을 가진다. 이 신호는 다음의 암호화 모듈로 전달된다.

3.2 암호화 방법

은닉된 정보의 비밀을 보호하기 위하여 사용자 키에 기반한 의사 랜덤 잡음을 사용하는 일반적인 암호화 방법을 적용한다. 워터마크 신호는 길쌈 부호화된 신호로부터 구해진다. 길쌈 부호화된 저작권 정보와 동일한 길이의 비트 수를 갖는 의사 랜덤 잡음 신호가 사용자 키로부터 생성된다. 의사 랜덤 잡음신호는 다음과 같이 고려할 수 있다.

$$N = \{n_k | 0 \le k < 2(m+6)\}, \quad (4)$$

여기서 m은 192이고 n_k는 0 또는 1 중 하나의 값을 가진다. 워터마크 신호(W)는 길쌈 부호화된 저작권 정보와 동일한 길이를 가지며 다음과 같이 표현될 수 있다.

$$W = \{w_k | 0 \le k < 2(m+6)\}, \quad (5)$$

여기서 m은 192이고 모든 요소의 값은 길쌈 부호화된 저작권 정보(I_c)와 의사 랜덤 잡음 신호(N)에 의해 결정된다. 워터마크 신호(W)는 사용자 키(K)에 의해 생성되는 의사 랜덤 잡음 신호(N)의 비트 값이 1일 때 길쌈 부호화된 저작권 정보(I_c)의 대응하는 비트 값을 변화시킴으로써 구해진다. 이는 다음과 같이 표현된다.

$$w_k = \begin{cases} i_{ck}, & if\ n_k = 0, \\ 1 - i_{ck}, & otherwise. \end{cases} \quad (6)$$

워터마크 신호의 길이는 길쌈 부호기의 구조를 변경함으로써 조정할 수 있다. 각 프레임에서 하나의 매크로 블록에 한 비트의 워터마크 신호를 은닉하기 위해서는 워터마크 신호의 길이가 입력 비디오 시퀀스에서 하나의 프레임에 있는 매크로 블록의 수와 정확히 같아야 한다. 실험에서는 CIF크기(352×288 화소)의 영상 시퀀스를 고려하고 있으므로 이들 영상은 각각 396개의 매크로 블록을 가진다. 따라서 여기서 구한 396-비트의 워터마크 신호의 각 비트는 MPEG-2 부호화 과정 동안 각 프레임의 대응하는 매크로 블록에 은닉된다.

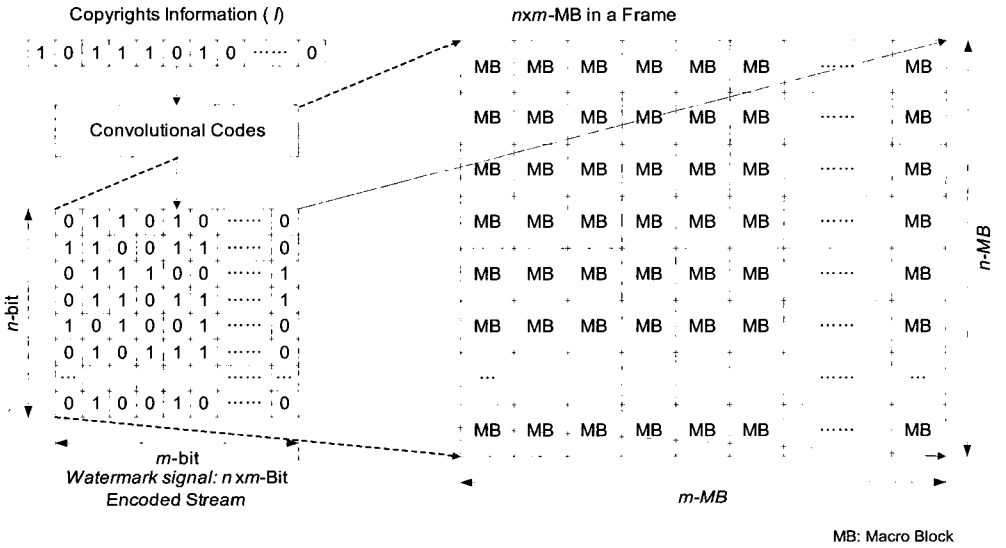
3.3 정보 은닉 알고리즘

입력 비디오 프레임 시퀀스가 비디오 스트림으로 부호화되는 동안 워터마크 신호는 인트라 프레임과 인터 프레임 모두를 포함하는 비디오 데이터의 모든 프레임에 은닉된다. MPEG-2는 블록 기반의 부호화 방법이고 입력 비디오 시퀀스에서의 모든 프레임은 16×16 화소를 갖는 매크로 블록으로 구성된다. 앞 절에서 구해지는 워터마크 신호의 각 비트는 각 프레임에서 대응하는 매크로 블록에 은닉된다. 각각의 매크로 블록에 대해 워터마크 신호의 각 비트는 (그림 4)에서 보여주는 바와 같이 매크로 블록의 DCT 계수 또는 움직임 벡터를 변화시키는데 사용된다.

인트라 프레임에 대해 워터마크 신호의 각 비트는 대응하는 매크로 블록의 DCT 계수에 은닉된다. MPEG-2 부호화 방법에서 하나의 매크로 블록은 6개의 8×8 화소 블록으로 구성되며 이중 4개의 블록은 밝기 정보를 가리키고 2 개의 블록은 색상 정보를 나타낸다. 워터마크 신호는 이들 블록 모두에 은닉된다. 모든 매크로 블록에 대해 각 블록에서의 DCT 계수의 합을 다음과 같이 구한다.

$$S_{ij} = \sum_{k=0}^{63} c_k \quad (7)$$

여기서 i와 j는 j-번째 매크로 블록에서 i-번째 블록을 나타내고 c_k는 k-번째 DCT 계수를 의미한다. 만약 이 합이 홀수이고 은닉하고자 하는 워터마크 신호가 '0'이거나 이 합이 짝수이고 은닉하고자 하는 워터마크 신호가 '1'이면 DCT 계수의 DC값을 부호에 따라 1 더하거나 빼서 정보를 은닉한다. 이는 다음과 같이 표현될 수 있다.

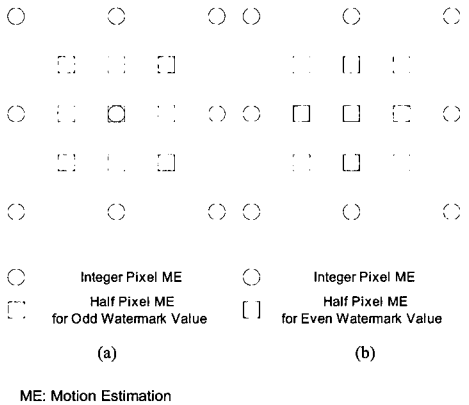


(그림 4) 매크로 블록으로의 정보 은닉 과정

$$
\begin{aligned}
&\textit{If } S_{ij} \textit{ is odd and } w_j \textit{ is even or } S_{ij} \textit{ is even and } w_j \textit{ is odd}\\
&\quad c_0 = \begin{cases} c_0 + 1, & \textit{if } c_0 >= 0, \\ c_0 - 1, & \textit{otherwise}, \end{cases}\\
&\textit{otherwise}\\
&\quad c_0 = c_0,
\end{aligned} \tag{8}
$$

여기서 c_0는 DCT 계수의 DC 성분을 의미한다.

인터 프레임에 대해서는 워터마크 신호에서의 각 비트는 대응하는 매크로 블록의 움직임 벡터에 은닉된다. 만약 은닉하고자 하는 워터마크 신호의 값이 '1'이면 움직임 벡터의 x 성분과 y 성분 모두가 홀수 값으로 설정된다. 만약 '0'이면 x 성분과 y 성분 중 최소한 하나의 값은 짝수로 설정된다. 이는 (그림 5)와 같이 반화소 움직임 벡터를 구하는 위치를 제어함으로써 설정할 수 있다. 워터마크 신호가 '1'인 경우 반화소 움직임 예측은 (그림 5) (a)에서 칠해진 4 군데의 위치에 대해서만 이루어진다. 반면에 워터마크 신호가 '0'인 경우에는 반화소 움직임 예측이 (그림 5) (b)에서 보여주는 바와 같이 칠해진 나머지 5 군데의 위치에 대해서만 이루어진다.



(그림 5) 반화소 움직임 예측의 위치 (a) 워터마크 신호가 '1'인 경우 (b) 워터마크 신호가 '0'인 경우

제안한 MPEG-2 부호기는 워터마크 신호를 출력 비디오 스트림의 DCT 계수와 움직임 벡터에 은닉한다. 이와 같이 워터마크 신호가 은닉된 출력 비디오 스트림을 전송 채널을 통해 수신기로 전송한다. 이 과정 동안 전송 채널에서의 잡음의 영향으로 전송되는 스트림은 쉽게 손상될 수 있다. 이는 수신기에서 복원되는 영상의 화질을 열화시키고 비디오 데이터에 대한 저작권 정보의 복원 및 주장을 어렵게 한다.

4. 오류 검출과 저작권 보호 기능을 가지는 MPEG-2 복호기

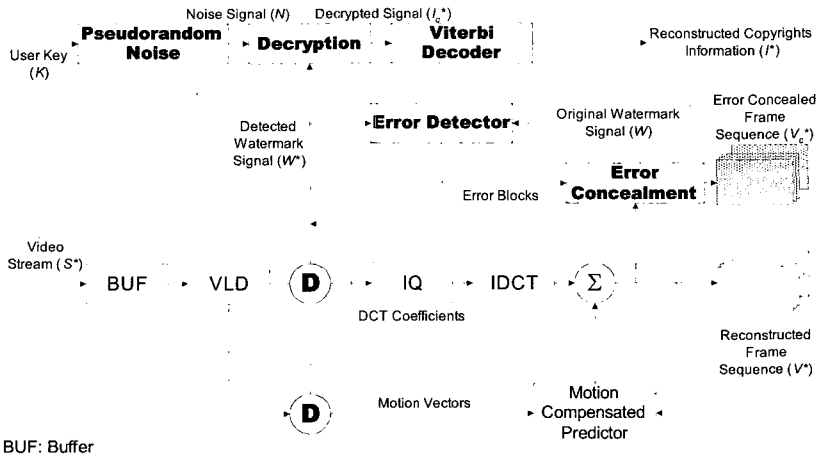
제안한 MPEG-2 복호기의 구조를 (그림 6)에서 보여주고 있다. 제안하고 있는 복호기는 5가지 모듈을 가지고 있다. 먼저, 부호화 과정 동안 은닉된 워터마크 신호가 검출된다. 수신된 MPEG-2 스트림(S^*)에서 가변장 복호된 각 매크로 블록의 DCT 계수 또는 움직임 벡터로부터 은닉된 워터마크 신호를 검출한다. 검출된 워터마크 신호(W^*)는 다음과 같이 표현될 수 있다.

$$
W^* = \left\{ w_k^* \middle| 0 \le k < 2(m+6) \right\}, \tag{9}
$$

여기서 $2(m+6)$은 하나의 프레임 내에 존재하는 매크로 블록의 수와 동일하다.

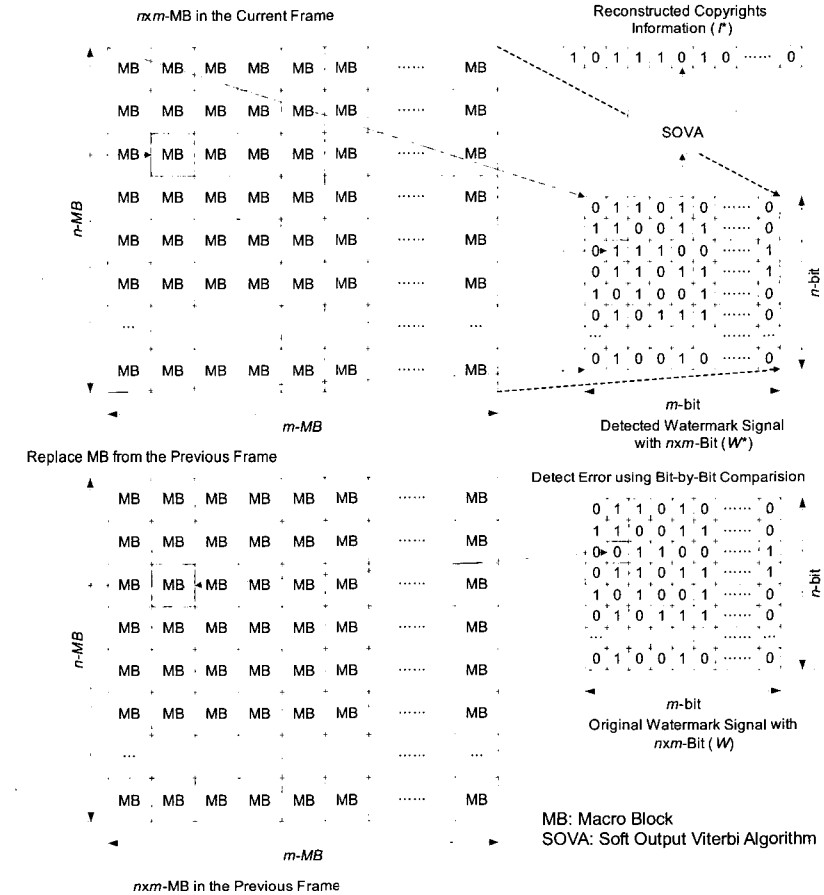
다음으로는 부호기에서 사용된 것과 동일한 사용자 키(K)를 사용하여 검출된 워터마크 신호(W^*)의 암호를 해독한다. 이 사용자 키를 사용하여 부호기에서와 동일한 의사 랜덤 잡음 신호를 생성한다. 식 (4)와 같은 잡음 신호를 사용하는 암호 해독 과정은 식 (6)에서 보여주는 바와 같은 암호화 과정의 역과정으로 수행되며 이는 다음과 같이 나타낼 수 있다.

$$
i_{ck}^* = \begin{cases} w_k^*, & \textit{if } n_k = 0, \\ 1 - w_k^*, & \textit{otherwise}. \end{cases} \tag{10}
$$



BUF: Buffer
VLD: Variable Length Decoder
D: Detection Module
IQ: Inverse Quantization
IDCT: Inverse Discrete Cosine Transform

(그림 6) 정보 검출 기능을 가지는 MPEG-2 복호기



(그림 7) 은닉된 정보를 이용하는 저작권 정보의 복원과 오류 검출 및 복구 과정

세 번째로 암호가 해독된 신호(I_c^*)는 저작권 정보(I^*)를 복원하기 위하여 비터비 복호기에 입력된다. 비터비 복호기는 MPEG-2 부호기에서의 길쌈 부호기와 대응된다. 비터비 복호기는 검출된 워터마크 신호에서 발생되는 오류를 교정할 수 있고 저작권 정보를 보다 정확히 복원할 수 있도록 한다.

네 번째 단계는 손상된 매크로 블록의 위치를 발견하기 위하여 검출된 워터마크 신호(W^*)와 원래의 워터마크 신호(W)를 비교하는 단계로 두 번째, 세 번째 단계와 동시에 수행된다. 수신단에서의 검출된 신호를 이용한 오류 검출 및 교정과 저작권 정보의 복원 방법은 (그림 7)에서 보여주고 있다. $n\times m$-비트로 구성되는 워터마크 신호가 비디오 복호

화 과정 동안 각 프레임의 모든 매크로 블록으로부터 검출된다. 이와 같이 검출된 신호의 비트 값이 원래 은닉에 사용된 신호의 대응하는 비트 값과 다른 경우 그 매크로 블록에 손상이 있다고 고려할 수 있다. 이 과정에서 은닉에 사용된 워터마크 신호는 저작권 정보, 사용자 키, 그리고 은닉 과정에서 사용한 것과 동일한 길쌈 부호기와 암호화기로 쉽게 구할 수 있다.

마지막 단계는 오류 복구 과정이다. 손상된 매크로 블록에 있는 오류는 이들 오류의 위치가 정확히 발견된다면 용이하게 복구될 수 있다. 손상된 매크로 블록을 복구하기 위한 접근법은 여러가지가 있다. 만약에 MPEG-2 복호기로부터 부호기로의 피드백 채널이 있다면, 복호기는 수신된 스트림에서 발생하는 손상된 매크로 블록의 위치를 대응하는 복호기로 알려줄 수 있다. 그러면 부호기는 부호화 동작을 조정하고 손상된 매크로 블록을 다시 전송한다. 하지만 이러한 접근은 아주 긴 처리 시간 지연을 가져오고 고속 광대역 통신망과 같은 특정한 조건을 요구한다. 따라서 이 방법은 실시간 적용에는 적합하지 않다. 손상된 매크로 블록을 복구하기 위한 또 다른 간단한 방법은 이전 프레임에서 손상된 매크로 블록과 동일한 위치에 있는 매크로 블록의 내용을 활용하는 방법이다. 손상된 매크로 블록은 (그림 7)에서 보여주는 바와 같이 이 매크로 블록의 내용을 대체 시킴으로써 복구된다. 따라서 제안한 방법은 오류가 복구된 비디오 시퀀스(V_c^*)를 생성할 수 있다.

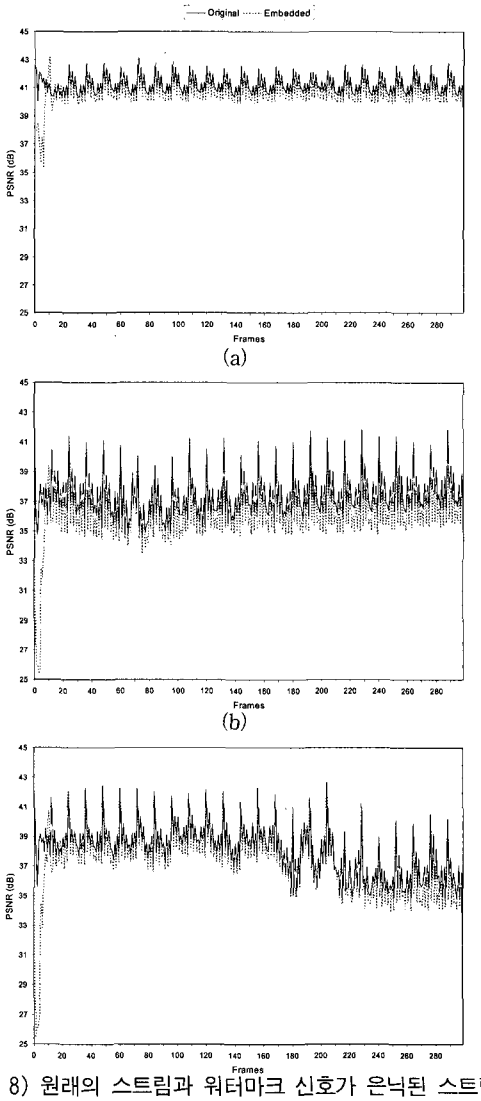
워터마크 신호가 은닉된 수신된 스트림은 MPEG-2 표준을 위반하지 않는다. 따라서 복호기가 정보 검출과 오류 보정 능력을 가지지 않더라도 비디오 시퀀스를 재구성할 수 있다.

5. 실험 결과

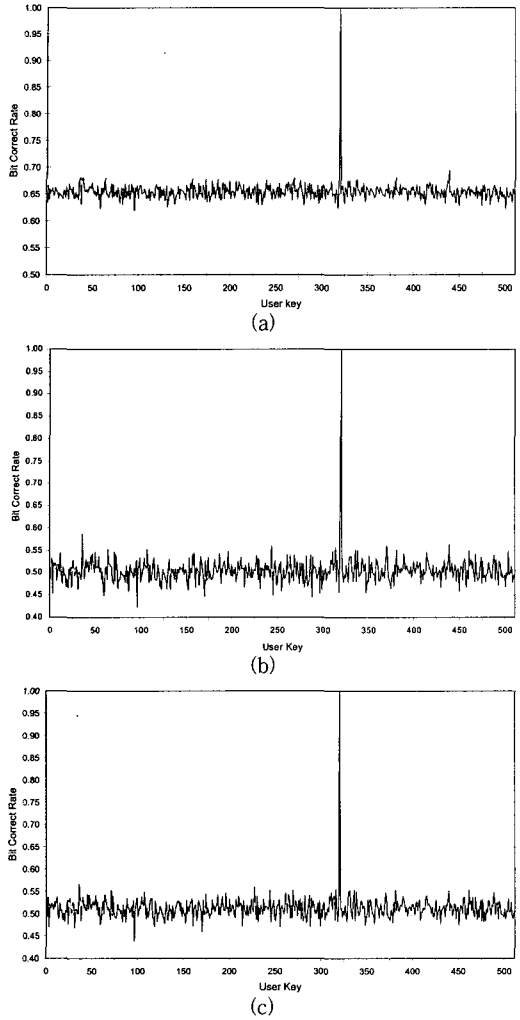
실험에서는 각각 300 개의 CIF(Common Intermediate Format) 크기 영상(352×288 화소)으로 구성되는 Akiyo, Coastguard, 그리고 Foreman 3 개의 비디오 시퀀스를 고려한다. 이들 3 개의 비디오 시퀀스에 대해 각 프레임은 MPEG-2 스트림으로 부호화된다. 이 과정에서 각 프레임에는 정보가 은닉된다. 본 논문에서는 24 개의 임의의 문자에 해당하는 ASCII 부호를 비디오 데이터에 대한 저작권 정보로 사용한다. 따라서 저작권 정보의 비트 수는 24⊗8=192 비트이다. 또한 본 논문은 CIF 크기(352×288 화소)의 영상을 갖는 비디오 시퀀스를 고려한다. 따라서 하나의 프레임은 22×18=396 개의 매크로 블록을 가진다. 한 비트의 워터마크 신호를 하나의 매크로 블록에 은닉하기 위해 제한장이 7인 길쌈 부호기가 사용된다. 이 길쌈 부호기는 192 비트의 저작권 정보를 $2\times(m+k-1)=2\times(192+6)=396$ 비트의 길쌈 부호화된 신호로 부호화한다. 이 신호의 각 비트는 입력 비디오 시퀀스를 부호화하는 동안 각 프레임의 대응하는 매크로 블록에 은닉된다.

본 논문에서는 3 개의 비디오 시퀀스에 대해 4 가지 종류의 실험을 수행하였다. 실험에는 원래의 부호화된 스트림과 워터마크 신호가 은닉된 스트림 사이의 PSNR(Peak Signal to Noise Ratio) 값에 대한 비교, 사용자 키의 유효성에 대한 실험 결과, 잡음 채널을 통해 전송되어온 스트림으로부터 재구성되는 영상의 화질을 개선하기 위한 오류 검출 및 복구, 그리고 채널 부호화 방법의 효과를 살펴보기 위한 저작권 정보의 복원 결과가 포함된다.

먼저, 원래의 정보가 은닉되지 않은 비디오 스트림과 은닉된 스트림의 PSNR을 비교한다. (그림 8)은 3 개의 테스트 스트림에 대한 모든 프레임에서의 PSNR값을 보여주고 있다. Akiyo 시퀀스에 대해 원래의 비디오 스트림과 워터마크된 비디오 스트림의 평균 PSNR은 각각 41.2 dB와 40.6 dB이고 이들 사이의 차이는 0.6 dB이다. Coastguard 시퀀스에 대해서는 원래의 비디오 스트림과 워터마크된 비디오 스트림의 평균 PSNR은 각각 37.3 dB와 36.0 dB이고 이들 사이의 차이는 1.3 dB이다. Foreman 시퀀스에 대한 원래의 비디오 스트림과 워터마크된 비디오 스트림의 평균 PSNR은 각각 38.0 dB와 37.2 dB이고 이들 사이의 차이는 0.8 dB이다. Coastguard의 경우 영상 내에 존재하는 움직임 성분이



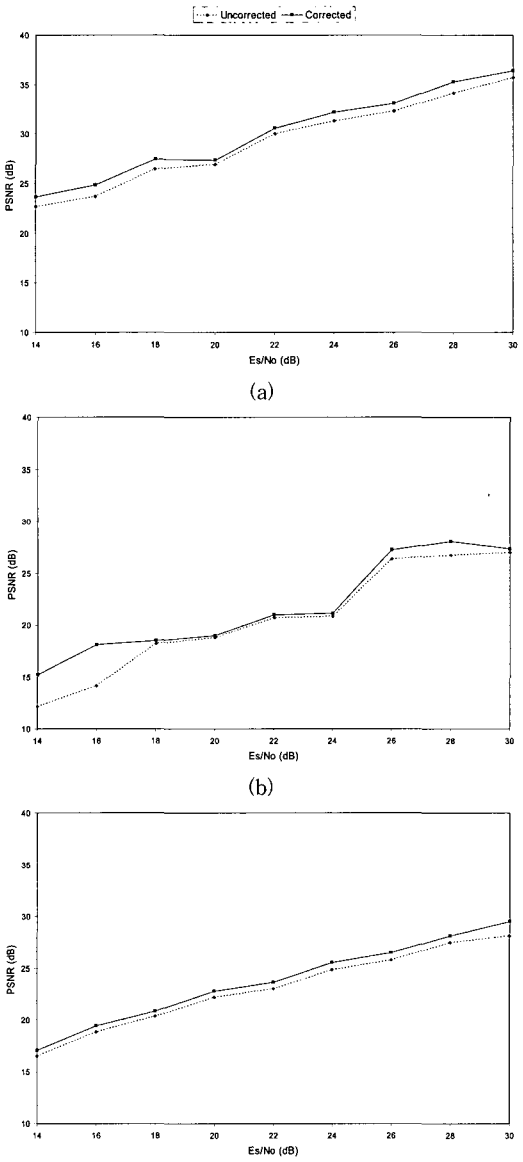
(그림 8) 원래의 스트림과 워터마크 신호가 은닉된 스트림의 PSNR 값. (a) Akiyo, (b) Coastguard, (c) Foreman



(그림 9) 사용자 키 값의 변화에 따른 복원되는 저작권 정보의 정확도. (a) Akiyo, (b) Coastguard, (c) Foreman (320이 사용자 키인 경우)

많아서 다른 두 테스트 시퀀스보다 차이가 크게 나는 것으로 고려된다. 본 논문에서는 전송 오류가 발생한 블록의 복구를 위해 이전 블록의 동일한 위치의 내용을 그대로 이용한다. 따라서 영상 스트림의 초반부에서 발생된 오류가 연속되는 프레임으로 전파되는 것을 방지하기 위해 영상 스트림의 처음 5 프레임을 인트라 모드로 부호화하였다. 인트라 모드에서는 모든 매크로 블록에 데이터를 은닉하므로 (그림 8)에서 보여주는 바와 같이 스트림의 처음 5 프레임에서는 정보가 은닉된 영상과 그러지 않은 영상의 PSNR 차이가 다른 부분에 비해 크다. 하지만 전 영상 시퀀스에 대해 워터마크된 스트림의 PSNR값이 원래의 스트림에 대한 값보다 적지만 그 차이는 크지 않고 특히 재구성되는 영상 내에서의 차이는 구별하기가 힘들다.

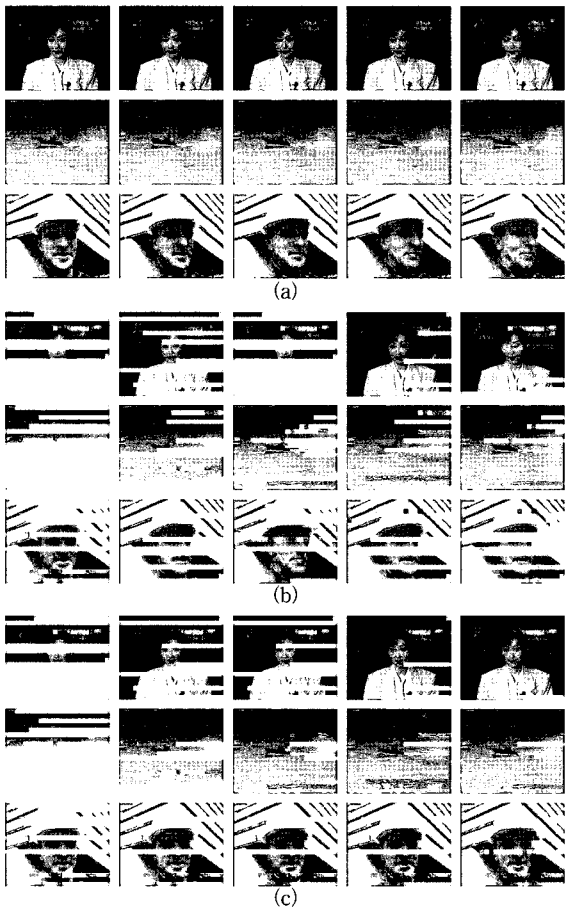
두 번째로 사용자 키의 유효성을 살펴보기 위해 사용자 키 값을 변화시키면서 정보가 은닉된 스트림으로부터 저작권 정보를 복원한 결과를 비교한다. (그림 9)는 사용자 키 값이 0에서 511까지 변화할 때 3 개의 테스트 스트림에 대해 복원한 저작권 정보의 비트별 정확도를 보여주고 있다. 제안한 MPEG-2 부호기에서는 저작권 정보를 길쌈 부호기로 부호화하고 사용자 키로 암호화한 후 스트림의 모든 프레임에 은닉한다. 실험에서는 정수 값 320을 사용자 키로 사용한다. 모든 3 개의 스트림에 대해 부호기에서와 동일한 사용자 키를 사용하는 경우 복호기에서는 완벽하게 저작권 정보를 복원할 수 있다. 하지만 부정확한 사용자 키를 사용하는 경우 복원되는 저작권 정보의 정확도는 현저히 감소한다. Akiyo, Coastguard, 그리고 Foreman 스트림에 대해 부정확한 사용자 키를 사용하는 경우 복원되는 저작권 정보의 정확도는 각각 0.65, 0.50, 그리고 0.53 정도이다. 이러한 결과는 올바른 사용자 키가 없이는 저작권 정보를 정확히 복원하는 것이 어렵다는 것을 알려준다. 따라서 제안한 정보은닉 방법이 MPEG-2비디오 데이터에 대한 저작권을 주장하고 보호하는 수단이 될 수 있다는 것을 보여준다.



(그림 10) 전송 채널의 환경 변화에 따른 복원되는 프레임의 평균 PSNR 비교. (a) Akiyo, (b) Coastguard, (c) Foreman

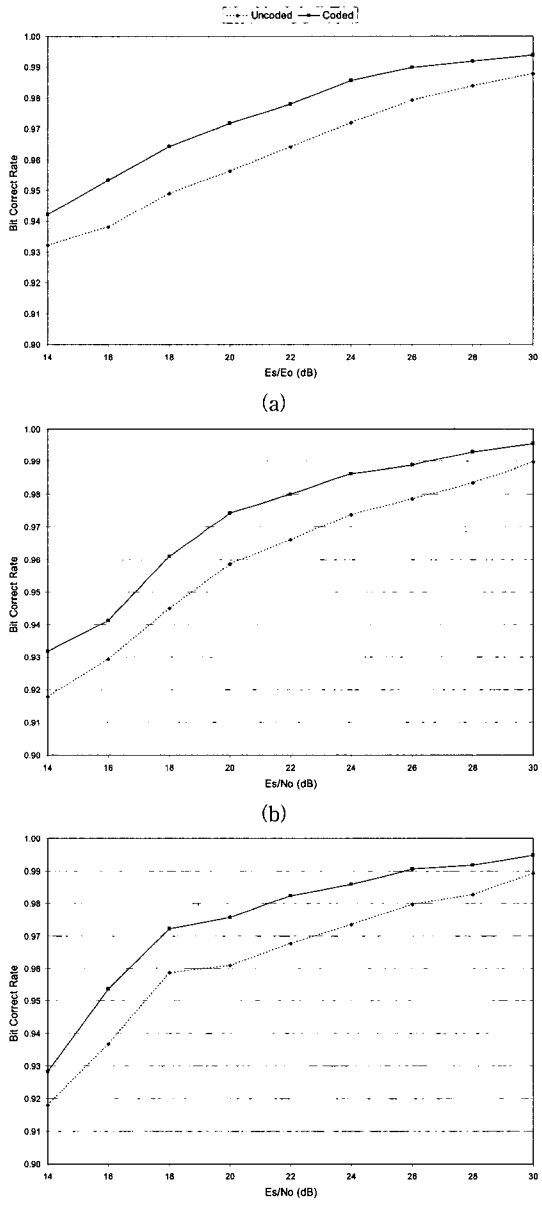
세 번째는 잡음 채널 환경을 통해 수신된 스트림에서 오류를 검출하고 복구하는 결과를 살펴본다. 본 논문에서는 전송 채널로 Rayleigh 페이딩 채널을 고려하며 E_s/N_o 값을 14dB에서 30dB까지 변화시키면서 실험을 한다. (그림 10)은 이와 같은 잡음 채널을 통해 수신된 스트림으로부터 일반적인 MPEG-2 복호기를 사용하여 재구성되는 프레임의 PSNR 값과 제안한 복호기를 통해 재구성되는 프레임의 PSNR을 보여주고 있다. Akiyo, Coastguard, 그리고 Foreman 스트림에 대해 제안한 방법을 사용하는 경우 재구성되는 영상의 평균 PSNR이 각각 0.40dB에서 1.16dB, 0.22dB에서 1.25dB, 그리고 0.48dB에서 1.41dB 정도까지 화질이 개선됨을 알 수 있다. 따라서 제안한 방법은 Rayleigh 페이딩 채널을 통해 수신되는 비디오 스트림으로부터 재구성되는 프레임들의 평균 PSNR을 개선한다는 것을 확인할 수 있다.

(그림 11)은 3 개의 테스트 스트림에 대해 수신단에서 복호한 영상의 예를 보여주고 있다. 잡음이 없는 경우에 복호한 영상의 예가 (그림 11) (a)에서 보여주고 있고, (그림 11) (b)는 E_s/N_o가 14 dB인 채널을 통해 수신한 스트림을 일반적인 MPEG-2 복호기로 복호한 예를 보여주고 있다. 이 경우 복호된 영상에는 아주 많은 수의 손상된 매크로 블록이 있다. (그림 11) (c)는 (b)와 동일한 채널에서 수신한 스트림을 제안한 복호기로 복호한 영상의 예를 보여주고 있다. 이 경우 (b)에서 보여주는 영상에 비해 손상된 매크로 블록의 수가 감소한 것을 확인할 수 있다. 이 결과는 제안한 방법이 비디오 스트림에 은닉한 정보를 이용하여 오류를 검출하고 복구함으로써 복호되는 영상의 화질을 개선한다는 것을 확인할 수 있다.



(그림 11) 재구성되는 스트림의 예. (a) 잡음이 없는 채널의 경우, (b) E_s/N_o가 14dB인 Rayleigh 페이딩 채널을 통해 수신한 스트림을 일반적인 복호기로 복호한 경우, (c) 동일 채널에서 수신한 스트림을 제안한 복호기로 복호한 예

마지막으로 E_s/N_o가 14 dB에서 30 dB까지 변화할 때 복원되는 저작권 정보의 정확도를 살펴본다. (그림 12)는 3 개의 테스트 스트림에 대한 실험 결과를 보여주고 있다. 모든 실험 대상 스트림에 대해 길쌈 부호화된 워터마크 신호를 사용하는 저작권 정보가 부호화되지 않은 워터마크 신호를 사용하는 경우보다 약 1.0%에서 1.5%까지 정확도가 증가한다는 것을 알 수 있다.



(그림 12) 잡음 채널에서 E_s/N_o 값의 변화에 따른 저작권 정보 복원율. (a) Akiyo, (b) Coastguard, (c) Foreman

6. 결 론

본 논문에서는 비디오 스트림에서의 전송 오류를 교정하고 데이터에 대한 저작권을 주장하기 위한 정보 은닉 기법을 제안하였다. 워터마크 신호는 비디오 데이터에 대한 저작권 정보를 길쌈 부호화함으로써 구하고 사용자 키에 의해 생성되는 의사 랜덤 잡음을 이용하여 이 신호를 암호화한다. 워터마크 신호의 각 비트는 MPEG-2 부호화 과정 동안 매 프레임의 각 매크로 블록에 은닉된다. 수신기에서는 수신된 비디오 스트림으로부터 은닉된 워터마크 신호를 검출하고 은닉에 사용된 것과 동일한 사용자 키를 이용하여 암호를 해독한다. 암호가 해독된 신호는 원래 은닉에 사용된 신호와의 비교에 의해 비디오 스트림에 있는 손상된 매크로 블록을 발견하는 데 사용된다. 길쌈 부호에 있는 오류 정정 기능은 검출된 워터마크 신호에 오류가 많더라도 복원되는 저작권 정보의 비트 오류율을 낮추는 역할을 한다.

CIF 크기 영상 300 개로 구성되는 세 가지 종류의 테스트 시퀀스에 대한 실험 결과 잡음 환경에서도 은닉된 신호를 효과적으로 검출하고, 검출된 신호는 손상된 매크로 블록을 발견하는데 사용되며, 동시에 저작권 정보를 복원하는데 사용될 수 있다는 것을 확인하였다. 길쌈 부호기와 비터비 복호기를 사용하는 제안한 방법이 전송 과정에서의 영상의 손상을 검출하고 복원되는 저작권 정보의 정확도를 향상시킨다는 것을 확인할 수 있다. 그리고 제안한 방법은 MPEG-2 부호화 표준을 위반하지 않으므로 제안한 방법으로 부호화된 스트림은 은닉 정보에 대한 검출 기능이 없는 일반적인 MPEG-2 복호기에서도 아무 문제없이 복호가 이루어진다.

본 논문에서는 현재 프레임에서 손상이 발생했을 때 단순히 이전 프레임의 동일 위치의 내용을 복사함으로써 손상을 복구한다. 하지만 복원되는 영상의 화질을 보다 더 개선하기 위해서는 인접 블록과의 보간을 고려하는 등 보다 우수한 오류 은닉 알고리즘의 적용이 필요하다. 또한 수신된 스트림의 헤더 부분에서 발생되는 오류를 교정하기 위한 구문적인 오류 정정 기능의 적용과 복원되는 영상의 매크로 블록의 경계를 분석함으로써 손상 여부를 파악하는 영상해석 부분도 추가할 필요가 있다.

참 고 문 헌

[1] C. Bae, J. Seok, Y. Choe and J. Lee, "Multimedia data processing elements for digital TV and multimedia services in home server platform," IEEE Tran on Consumer Electronics, Vol.49, No.1, pp.64-70, Feb., 2003.

[2] C. Bae, J. Yoo, K. Kang, Y. Choe and J. Lee, "Home server for home digital service environments," Digest of Technical Papers in International Conference on Consumer Electronics, pp.382-383, June, 2003.

[3] C. Bae, J. Yoo, K. Kang, Y. Choe and J. Lee, "Home server for home digital service environments," IEEE Transactions on Consumer Electronics, Vol.49, No.4, pp.1129-1135, Nov., 2003.

[4] F. Hartung and M. Kutter, "Multimedia watermarking techniques," Proc. of the IEEE Special Issue on Identification and Protection of Multimedia Information, Vol.87, No.7, pp.1079-1107, July, 1999.

[5] I. J. Cox, J. Kilian, F. Leighton and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," Proc. of 1996 Int'l. Conf. on Image Processing (ICIP'96), Vol.3, pp.243-246, 1996.

[6] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information hiding-a survey," Proc. of the IEEE Special Issue on Identification and Protection of Multimedia Information, Vol.87, No.7, pp.1062-1078, July, 1999.

[7] 이형훈, 배창석, 최재훈, 최윤식, "MPEG 비디오를 위한 하이브리드 워터마킹 알고리즘", 정보처리학회논문지, 제6권, 제11호, pp.3157-3164, 1999.

[8] B. Sklar, Digital Communications, Fundamentals and Applications, Prentice Hall, 1988.

[9] J. R. Hernández, J. M. Rodrígez and F. Férez-González, "Improving the performance of spatial watermarking of images using channel coding," Signal Processing, Vol.80, pp.1261-1279, 2000.

[10] C. Desset, B. Macq and L. Vandendorpe, "Block error-correcting codes for systems with a very high BER: Theoretical analysis and application to the protection of watermarks," Signal Processing, Vol.17, pp.409-421, 2002.

[11] F. Bartolini, A. Manetti, A. Piva and M. Barni, "A data hiding approach for correcting errors in H.263 video transmitted over a noisy channel," Proc. of MMSP'01 Cannes France, pp.65-70, Oct., 2001.

[12] T. S. Wang, P. C. Chang, C. W. Tang, H. M. Hang and T. Chiang, "An error detection scheme using data embedding for H.263 compatible video coding," Proposal for Standard ISO/IEC JTC1/SC29/WG11 MPEG99/N6340, July, 2000.

배 창 석

e-mail : csbae@etri.re.kr

1987년 경북대학교 전자공학과(공학사)

1989년 경북대학교 전자공학과(공학석사)

2003년 연세대학교 전기전자공학과(공학박사)

1989년~현재 ETRI 차세대PC플랫폼연구팀 책임연구원

관심분야 : 디지털 영상신호 처리, 디지털 워터마킹, 멀티미디어 코덱

Yuk Ying Chung

e-mail : vchung@it.usyd.edu.au

1995년 University of London, UK(학사)

2000년 Queensland University of Technology, Brisbane(박사)

1999년~2001년 La Trobe University in Melbourne, Australia, Lecturer

2001년~현재 University of Sydney, Australia, Lecturer

관심분야 : 디지털 영상/비디오 워터마킹, 내용기반 영상검색, 디지털 영상처리시스템 등