H.264 비디오 압축을 위한 정보은닉 기술

오 관 정, 호 요 성
광주과학기술원 정보통신공학과
전화 : 062-970-2258 / 핸드폰 : 019-645-0603

Information Hiding Scheme for H.264 Video Codec

Kwan-Jung Oh, Yo-Sung Ho
Gwangju Institute of Science and Technology (GIST)
E-mail : {kjoh81, hoyo}@gist.ac.kr

Abstract

H.264 is the most recent international video coding standard, which achieves a significant improvement in coding efficiency compared to existing standards, such as MPEG-4 and H.263. However, it is difficult to apply the conventional information hiding schemes to H.264. In this paper, we present a new information hiding scheme for H.264, which is applied to selective mode decision.

I. 서론

정보은닉 기술은 고대로부터 인간사와 밀접한 관계를 가져온 기술로 최근에는 다양한 디지털 미디어 데이터들에 대한 정보은닉 기술 및 응용에 관한 연구가 활발히 진행되고 있다. 워터마킹(watermarking)과 스테가노그래피(steganography)는 정보은닉 기술의 대표적인 분야들이다. 워터마킹은 디지털 컨텐츠의 불법적인 복제나 유통을 막아 지적재산권을 보호하기 위한 대안으로 떠오르고 있고, 스테가노그래피는 일종의 암호화 기술로 워터마킹과 달리 어떠한 정보를 은닉한 사실 자체까지도 숨기는 일종의 비밀통신 기술이다 [1].

기존의 정보은닉 기술들은 암호화와 같은 기술들이 주류를 이룬 반면에 디지털 컨텐츠가 대두되는 정보화 시대에는 디지털 컨텐츠를 이용한 정보은닉 기술들이 주류를 이루고 있다. 이러한 정보은닉 기술은 두 가지 원칙을 지켜야 한다. 하나는 숨긴 정보를 훼손시키기 어렵게 만드는 강인성(robustness)을 유지하는 것이고 다른 하나는 정보은닉 여부에 대해 느끼지 못하도록 만드는 비인지성(imperceptibility)이다. 일반적으로 워터마킹의 경우 위의 두 가지 특성을 모두 만족해야 하고, 스테가노그래피의 경우 비인지성에 무게를 두고 있다. 이 밖에도 얼마나 많은 정보를 삽입 할 수 있는지에 대한 정보량도 하나의 중요한 요소이다 [2].

H.264는 최신의 비디오 압축 부호화 표준으로 차세대 방송뿐만 아니라 다양한 영상 관련 분야에서 그 활용이 크게 기대된다. H.264는 기존의 비디오 표준에 비해 월등하게 우수한 압축 성능을 보이는데, 이는 더욱 정교해진 예측 방법과 새로운 부호화 방식 등에서 기인한다. 그러나 H.264의 경우 기존의 비디오 표준 방식과 다른 다양한 기술의 채택으로 기존의 비디오 표준에 적용되었던 정보은닉 기술의 적용이 쉽지 않다.

본 논문에서는 영상의 특성에 적합하도록 최신 비디오 압축 표준인 H.264의 다양한 매크로블록 유형들을 효과적으로 분류하여 H.264에 적합한 새로운 정보은닉 기술을 제안한다. 본 논문에서 제안한 알고리즘은 외부의 공격을 고려하지 않는 스테가노그래피 기술이다.

II. H.264 특성 및 압축 방식

H.264는 압축 성능 향상을 위해 다양한 기술들을 채택하였으나, 동시에 이로 인해 기존의 정보은닉 알고리즘들이 H.264에는 적용되기 힘들다.

기존의 비디오 압축 표준에서 8×8 DCT 특성에 기반을 둔 알고리즘들은 H.264의 4×4 정수 변환에 적용이 불가능하다. 기본적으로 채택한 변환 블록의 크기가 다르고 매크로블록의 유형에 따라 각 블록의 특성 또한 다르기 때문이다. 또한 VLC 부호화를 이용하여 정보를 은닉했던 방법의 경우 인접 블록의 특성에 기반을 둔 H.264의 CAVLC(context adaptive variable length coding)나 CABAC(context adaptive binary

arithmetic coding)에는 적용이 힘들다.

이처럼 H.264에는 기존의 정보은닉 기술들의 적용이 쉽지 않고 이에 따라 H.264에 적합한 정보은닉 기술에 대한 필요성이 크게 대두되고 있다. 따라서 본 논문에서는 H.264의 이러한 특성과 정보은닉 기술의 원칙들을 고려하여 매크로블록 유형 분류를 통한 정보은닉 알고리즘을 제안한다. 그림 1은 H.264에서 사용되는 다양한 매크로블록의 유형들이다 [3].

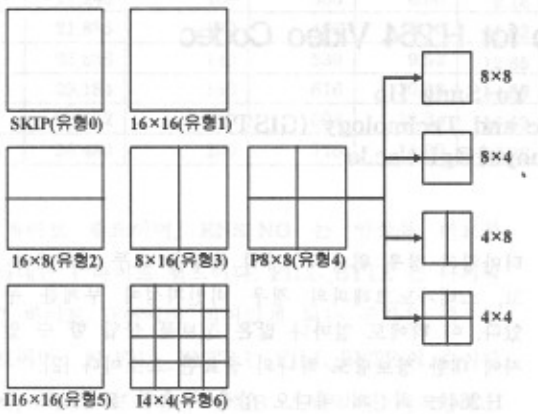

그림 1. H.264의 다양한 매크로블록 유형

H.264는 이러한 다양한 형태의 블록들로 움직임 예측을 하고 비용 함수를 이용하여 비용이 가장 작은 유형으로 현재 매크로블록을 부호화한다. 일반적으로 여기에 이용된 비용은 비트율과 왜곡을 고려하여 둘 중 어느 하나에 치우치지 않고 두 가지 관점에서 모두 적합한 최적의 유형을 선택하도록 고안되었다. 식 (1)은 일반적인 비용 함수의 형태를 보여주고 있다 [4].

$$Cost = D + \lambda R \tag{1}$$

여기서 D는 왜곡을 R은 비트율을 λ는 비트율에 대한 가중값을 의미한다. 식 (2)는 H.264에서 실제로 사용되는 비용 함수이다.

$$J_{mode}(s, r, MODE|\lambda_{mode}) = SSD(s, r, MODE) + \lambda_{mode} \cdot R(s, r, MODE) \tag{2}$$

여기서 s와 r은 각각 현재 블록과 참조 블록을 의미하고, $MODE$는 다양한 매크로블록의 유형을 나타내다. $SSD(s, r, MODE)$는 현재 유형에 대한 왜곡도를 나타내며 식 (3)과 같다. $R(s, r, MODE)$은 현재 유형들을 이용하여 실제로 부호화했을 때 발생되는 비트수를 의미한다. λ_{mode}는 비트율에 대한 가중값으로 H.264에서는 양자화 변수 QP를 고려한 $(0.85 \times 2^{(QP/3)})^2$을 사용한다.

$$SSD(s, r, MODE) = \sum_{x \in H, y \in V} (s(x,y) - r(x - m_x, y - m_y))^2 \tag{3}$$

여기서 H와 V는 각각 영상의 가로와 세로 크기를, (m_x, m_y)는 움직임 벡터의 좌표를 의미한다. SSD는 원영상과 참조영상의 블록간의 제곱 오차를 의미한다.

H.264는 모든 매크로블록에 대해 식 (2)의 비용함수를 이용하여 그림 1의 다양한 유형의 비용을 비교한 후 가장 좋은 유형으로 해당 매크로블록을 부호화하는 방식을 취하고 있다. 본 논문에서는 이러한 점에 착안하여 그림 1의 다양한 매크로블록 유형을 두 그룹으로 나누어 정보은닉에 이용하고자 한다.

III. 제안한 정보은닉 기술

3.1 정보은닉 기술

본 논문에서 제안한 정보은닉 방법은 스테가노그래피 기술이므로 정보은닉으로 인한 원영상의 변화가 없다. 여기서 변화란 눈에 띄만한 화질의 변화뿐만 아니라 유형의 발생 확률과 같은 통계적 특성 등의 변화도 포함한다. 제안하는 정보은닉 알고리즘의 정보은닉 순서는 다음과 같다.

1. 정보를 은닉하고자 하는 영상을 부호화하여 그 영상에 대한 특성을 파악한다.
2. 과정 1에서 파악한 특성을 고려하여 매크로블록 모드를 '0' 그룹과 '1' 그룹으로 구분한다.
3. 과정 2에서 각 그룹의 확률을 고려하여 은닉하고자 하는 정보를 암호화한다.
4. 암호화된 정보를 비트 단위로 읽어, 해당 비트 그룹만을 이용하여 부호화한다.
5. 정보가 은닉된 영상의 특성을 원영상과 비교한다.

과정 1에서는 원영상의 각 유형에 대한 발생 확률, 영상의 PSNR 값, 그리고 발생 비트량을 조사한다. 과정 2에서는 1의 결과를 바탕으로 그림 1의 다양한 매크로블록 유형들을 '0' 그룹과 '1' 그룹으로 나누는데 이 과정에서는 모든 유형을 이용하여 정보를 은닉하는 것이 아니기 때문에 그룹화로 인한 부호화 효율의 손실을 가장 적도록 그룹화하는 것이 중요하다.

식 (4)는 그룹화로 인해 발생할 수 있는 손실을 비용 함수를 이용하여 수치적으로 나타낸 것이다.

$$E = (SSD(s,r,best_{mode}) - SSD(s,r,group_{mode})) + \lambda_{mode} \cdot (R(s,r,best_{mode}) - R(s,r,group_{mode})) \quad (4)$$

여기서 E는 정보은닉으로 인해 발생할 수 있는 오류를 비용함수로 나타낸 값이며, 모든 유형을 사용했을 경우와 비교하여 해당 그룹의 유형만을 사용했을 때 발생할 수 있는 왜곡과 비트율의 손실을 의미한다. 그룹화 과정에서는 이 값을 최소화시켜야 한다. 과정 3은 과정 2의 각 그룹의 확률을 고려하여 은닉하고자 하는 확률을 암호화하는 과정으로 다음과 같다.

$$I_K = R(K, P\{Group0\}) \otimes I_O \quad (5)$$

여기서 I_K는 암호화된 정보를 의미하고, R은 비밀키 K와 '0' 그룹의 확률을 이용하여 발생된 원정보 I_O와 같은 크기의 임의의 비트를 의미한다. 이러한 과정을 통해 정보은닉 후에도 원영상과 비슷한 통계적 특성을 유지할 수 있다. 과정 4는 실제 정보를 은닉하는 과정으로 다음과 같다.

은닉하고자 하는 비트가 '1'이면
→ '1' 그룹만을 이용하여 부호화 (6)
은닉하고자 하는 비트가 '0'이면
→ '0' 그룹만을 이용하여 부호화

과정 5는 원영상과 정보가 은닉된 영상의 통계적 특성을 비교하는 과정이다. 만약 이 과정에서 통계적 특성이 원영상과 차이가 많이 나면 그만큼 정보 은닉에 대한 안전성이 떨어지므로, 이전 과정의 문제점을 분석하여 재과정을 거쳐야 한다. 또한 각 그룹의 발생확률이 원영상과 다른 경우에는 정보를 검출하고자 하는 측에 키 값과 유형 그룹화 정보 외에도 각 그룹의 발생확률까지 보내 주어야 한다 [5].

3.2 정보검출 기술

정보 검출에는 H.264의 복호기를 이용한다. 정보 검출은 정보 은닉의 역 과정으로 다음과 같다.

1. 정보은닉 측에서 받은 키와 유형 정보를 이용하여 임의의 비트를 만든다.
2. 복호화 과정에서 매크로블록의 유형 정보를 이용하여 은닉된 정보를 검출한다.
3. 과정1의 임의의 비트와 과정 2에서 검출한 은닉된 정보를 이용하여 최종 정보를 검출한다.

과정 1은 식 (7)처럼 임의의 비트를 만드는 과정이다.

$$R(K, P\{Group0\}) \quad (7)$$

여기서 정보를 검출하는 측에서는 임의의 비트 생성을 위해 비밀키 K와 각 그룹에 대한 확률을 필요로 한다. 각 그룹에 대한 확률은 정보가 은닉된 영상의 특성이 원영상과 같다면 그룹화 정보를 통해 얻어낼 수 있으나, 그렇지 않은 경우에는 정보를 은닉한 측에서 같이 보내 주어야 한다.

$$I_O = R(K, P\{Group0\}) \otimes I_K \quad (8)$$

과정 1과 과정 2를 거쳐 얻어진 임의의 비트(R)와 검출된 정보(I_K)를 통해 식 (8)과 같이 최종 정보를 검출할 수 있다.

Ⅳ. 실험 결과 및 분석

본 논문에서 제안한 정보은닉 알고리즘의 성능을 실험하기 위해 QCIF 포맷의 실험 영상 5개를 사용하였다. 참조 소프트웨어는 JM 8.2를 이용하여, baseline에서 *IPPP* 구조로 51 프레임을 부호화했고, P 프레임 50개에 대해서만 정보를 은닉했다. QP=28을 이용하였고, 비트율 제어는 사용하지 않았다 [6].

본 실험은 원영상의 통계적 특성에 대해 분석하고 정보가 은닉된 영상과 정보가 은닉된 영상의 통계적 특성을 비교했다. 그림 1의 각 유형을 왼쪽 상단에서 오른쪽 하단의 순서대로 0~6번 유형으로 명명한다. 실험에서는 '0' 그룹={0, 2, 3}을 이용하였고 '1' 그룹={1, 4, 5, 6}을 사용하였다.

표 1. 각 영상의 유형 발생률(%)

실험영상	유형0	유형1	유형2	유형3	유형4	유형5	유형6
Akiyo	83.66	6.36	2.59	3.05	4.32	0.00	0.00
Foreman	26.57	33.41	10.02	17.01	12.91	0.00	0.08
Mobile	3.01	23.92	16.20	16.30	40.55	0.00	0.02
News	77.76	6.95	2.46	4.89	7.82	0.02	0.10
Stefan	18.28	27.41	11.39	10.10	32.38	0.18	0.24

표 1은 각 실험영상에 대해 다양한 유형의 발생 확률을 조사한 것이다. 영상의 복잡도와 움직임 특성에 따라 각 유형의 발생 확률들이 크게 다른 것을 알 수 있다. 유형 5와 유형 6은 인트라 유형으로써 거의 발생하지 않는 것을 알 수 있다. 표 2는 각 영상에 대한 PSNr 값, 비트율과 비용값을 보여주고 있다. 비용값은 식 (9)에서처럼 PSNR 값과 비트율을 고려하여 하나의 화소에 대한 비용값을 계산한 것이다.

$$Cost = \sqrt{\frac{255^2}{10^{\frac{PSNR}{10}}} + \lambda_{mode} \cdot R/(V \times H \times N_P)} \quad (9)$$

여기서 V와 H는 영상의 가로와 세로를, N_P는 P프레임의 수를 나타낸다. R은 부호화된 총 비트수이다.

표 2. 각 영상의 통계적 특성

실험영상	PSNR(dB)	비트율(kb/s)	비용값
Akiyo	38.42	33.01	4.55
Foreman	35.75	105.12	8.90
Mobile	33.42	418.87	24.32
News	36.80	71.05	6.89
Stefan	34.46	338.46	20.08

표 3은 원영상과 정보가 은닉된 후의 각 그룹의 유형 발생 확률을 비교해 보여준다. 표 3에서 보듯이, 각 유형의 발생 확률이 약간의 차이는 있지만 대부분 유사한 것을 알 수 있다. 정수 단위에서 각 그룹의 발생 확률이 같으므로 정보검출 측에서도 해당 그룹의 발생 확률을 받지 않아도 정보 검출이 가능하다.

표 3. 정보은닉 전후의 각 그룹의 발생 확률(%)

실험영상	그룹0(전)	그룹0(후)	그룹1(전)	그룹1(후)
Akiyo	89.31	88.90	10.69	11.10
Foreman	53.60	54.22	46.40	45.78
Mobile	35.52	36.12	64.48	63.88
News	85.11	85.05	14.89	14.95
Stefan	39.78	40.20	60.22	59.80

표 4는 정보은닉 전후의 각 영상에 대한 통계적 특성을 보여주고 있다. PSNR 값은 원영상에 비해 거의 변화가 없지만, 비트율의 경우 상당한 변화가 있음을 알 수 있다. 이는 대부분의 손실이 비트율로 반영되었기 때문이다.

표 4. 정보은닉 후의 각 영상의 통계적 특성의 변화

실험영상	△PSNR(dB)	△비트율(%)	△비용값(%)
Akiyo	-0.04	+8.60	+3.08
Foreman	-0.01	+9.49	+5.06
Mobile	0	+4.22	+3.29
News	-0.04	+8.40	+4.06
Stefan	-0.04	+4.53	+3.54

V. 결론

본 논문에서는 매크로블록의 그룹화를 통해 최신 비디오 압축 표준인 H.264에 적합한 정보은닉 기술을 제안하였다. H.264는 기존의 비디오 압축 표준과 다른 특성을 가지므로 기존의 정보은닉 알고리즘을 직접 적용하기가 어렵다.

제안한 알고리즘은 정보은닉 기술 중 스테가노그래피에 적합한 기술로 정보은닉 후에도 영상 화질과 통계적 특성이 원영상과 유사한 결과를 보였다. 정보량 면에서도 매크로블록당 한 비트를 삽입할 수 있어 상당량의 정보량을 보였다. 그러나 비트율 면에서는 비교적 큰 변화가 있었다. 이를 극복하기 위해서는 각 영상의 특성을 고려하여 정보 은닉으로 인한 손실을 화질과 비트율에 적당히 분배할 수 있는 기술에 관한 연구가 진행되어야 할 것이다.

감사의 글

본 연구는 광주과학기술원(GIST) 실감방송연구센터(RBRC)를 통한 정보통신부대학IT연구센터(ITRC), 교육인적자원부 두뇌한국21(BK21) 정보기술사업, 그리고 디지털콘텐츠협동연구센터(DCRC)의 지원에 의한 것입니다.

참고 문헌

[1] M. Arnold, M. Schmucker, and S. D. Wolthusen, *Techniques and Applications of Digital Watermarking and Content Protection*, Artech House, 2003.

[2] S. Katzenbeisser and F.A.P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, 2000.

[3] T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," *IEEE Trans. Circuits and Systems for Video Technology*, vol. 13, No 7, pp. 560-576, July 2003.

[4] T. Berger, *Rate Distortion Theory*, Englewood Cliff NJ: Prentice Hall, 1971.

[5] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Signal Processing Megazine*, vol. 17, issue 5, pp. 20-46, Sept. 2000.

[6] JVT reference software JM8.2, available online at: http://iphome.hhi.de/suehring/tml/download/old_jm/