

저작권 보호를 위한 디지털 비디오 화면 모호화 기법에 관한 연구

부희형[†], 김승호^{**}

요 약

본 논문에서는 디지털 비디오 인코딩 과정에서 인트라 프레임의 DC 성분과 인터 프레임의 움직임 벡터를 이용한 저작권 보호를 위한 디지털 비디오 화면 모호화 기법을 제안한다. 제안한 기법은 저주파 영역과 중간 주파수 영역에 민감한 반응을 보이는 HVS (human visual system)의 특성을 고려한 방법으로서, 영상의 주요 정보를 포함하는 인트라 프레임의 DC 계수와 윤곽선 움직임 정보를 포함하는 인터 프레임의 움직임 벡터의 부호를 인증 신호와 XOR 연산하여 신호를 왜곡시키고, 적합한 인증 신호를 적용한 경우에만 정상적인 화면을 볼 수 있도록 하는 기법이다. 실험은 제안한 기법을 적용한 비디오의 PSNR을 구하고, PSNR에 의해 정상적인 기능 여부를 알아본다. 실험 결과, 디코더에서 적합한 인증 신호를 적용한 경우 Y, U, V PSNR이 모두 극치 값을 나타냄으로써 원 압축 비디오와 같은 화질을 알 수 있었고, 인증 신호를 적용하지 않은 경우 원 압축 비디오에 대한 평균 PSNR이 12.25dB을 나타냄으로써 화질 차이가 크음을 알 수 있었다. 결과로부터, 디지털 비디오 화면 모호화 기법은 정상적으로 기능하였고, 서명 또한 저작권자의 비밀 키에 의해 정상적으로 검출되어 저작권을 증명할 수 있었다.

A Study on the Digital Video Frame Obfuscation Method for Intellectual Property Protection

Hee Hyung Boo[†], Sung Ho Kim^{**}

ABSTRACT

In this paper, we propose the digital video frame obfuscation method for intellectual property protection using the DC component of the intra frame and the motion vector of the inter frame at digital video encoding. The proposed method considers characteristics of the HVS (human visual system) which is sensitive at the low frequency and the middle frequency. This method makes the signal distorted as operating XOR between authentication signal and the DC coefficient of the intra frame including main information and the sign of the motion vector including edge motion, so that the video is normally displayed only when suitable authentication signal is applied.

Key words: Digital Video Frame Obfuscation(디지털 비디오 화면 모호화), Intellectual Property Protection(저작권 보호), Authentication Signal(인증 신호), Human Visual System(시각 시스템)

※ 교신저자(Corresponding Author): 김승호, 주소: 대구광역시 북구 대학로 80 경북대학교 IT대학 컴퓨터학부 E9-529(702-701), 전화: (053) 950-5556, FAX: (053) 957-4846, E-mail: shkim@knu.ac.kr
접수일: 2011년 6월 15일, 수정일: 2011년 10월 21일
완료일: 2011년 10월 27일

[†]준회원, 경북대학교 전자전기컴퓨터학부
(E-mail: hhboo@knu.ac.kr)

^{**}정회원, 경북대학교 컴퓨터학부 교수

※ 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2011-0004184)

1. 서론

최근 디지털 콘텐츠 산업이 성장함에 따라 디지털 콘텐츠의 배포 및 유통도 빠르게 진행되고 있다. 이러한 활발한 움직임은 디지털 콘텐츠의 위·변조와 무단 접근 및 복제 등의 문제를 일으키게 되었다. 이러한 문제들로부터 디지털 콘텐츠의 품질 보장과 저작권 보호를 위한 기술의 필요성이 높아짐에 따라, 최근 DRM (digital rights management) 기술에 대한 연구가 활발히 이루어지고 있다[1,2]. 그의 한 분야로서 디지털 비디오에서의 DRM 기술은, 협의의 기술로 디지털 비디오 워터마킹 분야에서 주로 연구가 이루어지고 있다.

기존의 디지털 비디오 워터마킹 기법에는 DCT 계수, 모션 벡터, GOP 구조 등을 이용한 방법들이 있다 [3,4,5]. 대표적인 예로, Langelaar et al (1998)은 I-프레임의 8×8 Y 블록의 차단 주파수 이상을 제거하여 라벨링을 수행하는 방법을 제안하였다[4]. 이 방법은 차단 주파수 조건을 만족시키는 인덱스가 주로 고주파 영역에 존재하게 되어, 고주파 제거 시 연속적인 서명 검출이 불가능하다고 볼 수 있다. 또한, 차단 주파수의 인덱스를 낮추게 되어도 Y 성분이 많이 손상되기 때문에, 밝기 성분은 더욱 떨어지게 된다.

그 외 중간 주파수 대역을 이용한 워터마킹 기법들이 제안되고 있으나, 밝기, 색상 등이 다양한 비디오들에 시각적인 변화 없이 모두 적용된다고 보기에 는 부족한 면이 있다. 이러한 면들로부터 기존 연구에서는 어느 한 쪽 면에서의 손실을 감수해야만 했다.

다시 원점으로 돌아가서, 디지털 비디오 워터마킹의 정의는 디지털 비디오 콘텐츠에 저작권 정보의 워터마크를 삽입하는 기술이다. 이 기술은, 디지털 비디오 콘텐츠에 대한 지적 재산을 보호하기 위한 방법으로서, 저작권 분쟁이 일어날 경우 워터마크에 의해 저작권 정보를 식별함으로써 저작권을 증명해 줄 수 있다.

본 논문에서는 저작권 정보를 이용한 방법으로서, 저작권 정보가 포함된 인증 신호가 있어야만 비디오를 정상적으로 재생시킬 수 있는 디지털 비디오 화면 모호화 기법을 제안한다. 이 방법은 기존의 디지털 비디오 워터마킹에서, 화질 열화, 압축 코드 유지, 고주파 제거 공격, 압축 공격 등의 대책에 어려움이 많

았던 부분들을 역으로 공격함으로써 서명까지도 증명할 수 있는, 기존의 기법과는 다른 해결방법이다. 이 방법은 비디오를 재생시키기 전에 사용자 비밀번호를 입력받는 로그인 사용자 인증과 함께 혼합인증으로 이용될 수 있다.

제안한 디지털 비디오 화면 모호화 기법은 저주파 영역과 중간 주파수 영역에 민감한 반응을 보이는 HVS (human visual system)의 특성을 고려한 방법으로서[6-8], 영상의 주요 정보를 포함하는 인트라 프레임의 DC 계수와 윤곽선 움직임 정보를 포함하는 인터 프레임의 움직임 벡터의 부호를 인증 신호와 XOR 연산하여 신호를 왜곡시키고, 적합한 인증 신호를 적용한 경우에만 정상적인 화면을 볼 수 있도록 하는 기법이다. HVS는 아래 그림 1과 같이 시야각 1도에서 공간 주파수가 5~10 사이클일 때, 가장 민감한 반응을 보이고, 고주파에서 상대적으로 둔감한 반응을 보인다[6].

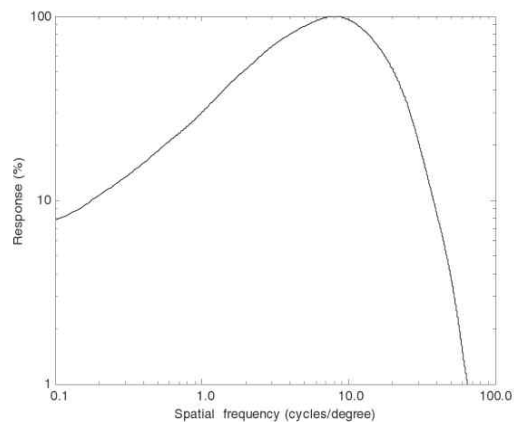


그림 1. 시각 시스템에서 공간 주파수 응답

본 논문의 실험에서는 제안한 기법을 적용한 비디오에 대하여, 디코더에서 적합한 인증 신호를 적용한 경우와 적용하지 않은 경우, 원 압축 비디오에 대한 PSNR을 비교해봄으로써 정상적인 수행 여부를 알아본다.

실험 결과, 적합한 인증 신호를 적용한 경우 정상적인 화면이 나타났고, 그 외의 경우 심하게 왜곡된 화면이 나타났다. 정상적으로 재생된 비디오는 Y, U, V PSNR이 모두 극치 값을 나타냄으로써 원 압축 비디오와 같은 화질임을 알 수 있었고, 왜곡된 비디

오는 원 압축 비디오에 대한 평균 PSNR이 12.25dB을 나타냄으로써 화질 차이가 크을 알 수 있었다. 정상적인 화면이 재생된 경우 인증 신호를 적합한 신호라고 판단하였고, 인증 신호에 포함된 서명 정보를 저작권자의 비밀 키에 의해 검출함으로써 저작권을 증명할 수 있었다.

다음 2장에서는 서명 신호와 M-수열로 구성된 인증 신호에 대해서 설명하고, 3장에서는 제안한 디지털 비디오 화면 모호화 기법을 상세히 서술한다. 4장에서는 실험 방법 및 결과를 보이고, 기존의 기법과 비교한다. 마지막으로 5장에서는 결론을 맺는다.

2. 서명 신호와 M-시퀀스로 구성된 인증 신호

본 논문에서 이용된 인증 신호는 서명 신호와 M-수열로 구성된다. 서명 신호는 블록 크기를 저장하는 헤더와 RSA 암호화된 서명으로 구성되고, M-수열은 선형 피드백 시프트 레지스터 (linear feedback shift register)에서 생성된 비트열 (bit-stream)로 구성된다.

RSA 암호화 기법은 n 비트의 길이를 갖는 메시지 블록, 공개 키 (public key), 비밀 키 (private key), 모듈러스 (modulus) 수를 이용하여 암호화 및 복호화 연산을 수행하는 방법이다[9].

M-수열은 서로 다른 수열들 사이에 상호관계가 없는 특징을 가진 수열로서, 피드백 시프트 레지스터 (feedback shift register)에 의해 생성되고, 레지스터 개수 m 에 대하여 $2^m - 1$ 길이의 2진 수열을 발생시킨다[10]. 이 수열은 반복주기가 충분히 길어서 거의 랜덤으로 나타나는 주기적인 수열이며, 일반적으로 의사 난수 (pseudo random numbers)로서 참조된다. 본 논문에서는 실험을 위해 7개의 레지스터에서 127 비트열 (bit-stream)을 주기적으로 생성하여 비디오의 고유 식별번호로 이용한다.

인증 신호는 서명 신호와 M-수열을 파일로 읽어 들인 후, DC계수와 움직임 벡터에 이용될 두 개의 배열에 각각 순서대로 결합시킴으로써 생성된다. 인증 신호는 XOR 연산 과정에서 30프레임마다 배열의 포인트를 0으로 하여 배열의 시작부터 다시 연산한다. 이것은 일부 비트가 잘못되어도 30프레임 이후에 정상적인 동작을 할 수 있도록 해준다.

서명 신호의 생성과 서명 검출 과정은 코덱의 XOR 연산과는 별도로 이루어진다. 아래 그림 2는 저작권자의 정보를 서명 신호로 생성하고, 생성된 신호를 다시 서명 문자로 변환하는 과정을 나타낸다. 서명 신호의 생성 과정에서 추가되는 8비트 헤더에는 검출 시, 서명 신호를 블록 단위로 읽기 위한 블록 사이즈가 저장된다. 서명 검출 과정에서는 저작권자의 비밀 키가 필요하고, 그 비밀 키에 의해서만 저작권자의 정보를 검출할 수 있다.

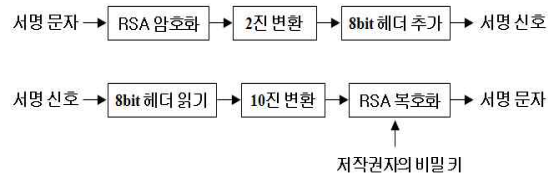


그림 2. 서명 신호의 생성과 서명 검출 블록도

3. DC 성분과 움직임 벡터를 이용한 디지털 비디오 화면 모호화 기법

본 논문에서는 인트라 프레임의 DC 성분과 인터 프레임의 움직임 벡터를 이용한 디지털 비디오 화면 모호화 기법을 제안한다. 제안한 기법은 HVS에 민감한 반응을 보이는 핵심 부분만을 이용함으로써 계산 비용을 최소화한다. HVS는 주요 정보를 포함하는 저주파 영역과 윤곽선 정보를 포함하는 중간주파수 영역에 민감하고, 상대적으로 고주파 영역에 둔감한 특성을 보인다.

제안한 기법은 인트라 프레임의 DC 계수와 인터 프레임의 움직임 벡터의 부호를 서명이 포함된 인증 신호와 XOR 연산하여 신호를 왜곡시키고, 왜곡된 신호를 저장한다. 제안한 인코더 구조는 아래 그림 3과 같고, 디코더 구조는 그림 4와 같다.

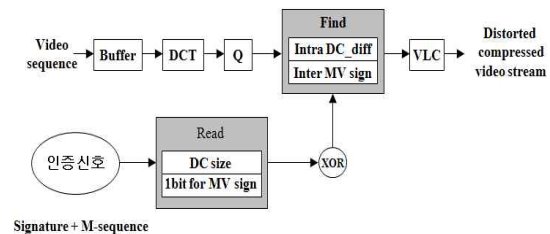


그림 3. 제안한 인코더 블록도

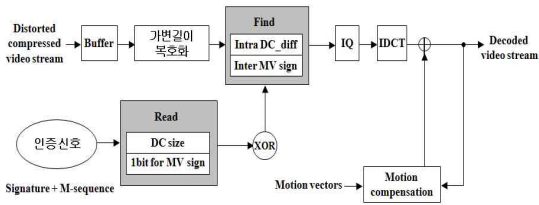


그림 4. 제안한 디코더 블록도

위 그림 3은 움직임 추정 및 보상을 제외한 MPEG 기본 인코더 구조에서 인증 신호에 대한 연산이 추가된 블록도이다.

인트라 프레임의 양자화된 8×8 블록에서, 좌 상단의 DC 성분은 영상의 평균에 해당되고, 대부분의 정보를 포함하고 있어서 가장 큰 값이 나오는 특징이 있다. 이 값은 DPCM (differential pulse code modulation) 방식으로 부호화된 후, 크기 (size)는 VLC (variable length coding) 코드로 비트스트림에 들어가고, DC 성분은 실제 DC 차이 값이 비트스트림에 들어간다. 인터 프레임의 움직임 벡터는 움직임 벡터 차이 값이 VLC 코드로 비트스트림에 들어가고, 그 다음 부호 비트가 들어간다.

본 논문에서는 2개의 동일한 인증 신호에 대하여 DC 계수와 움직임 벡터의 부호에 각각 연산을 수행한다. 첫 번째 인증 신호에 대해서는, 실제 DC 차이 값이 비트스트림에 들어가기 전에 XOR 연산을 수행하고, 두 번째 인증 신호에 대해서는, 움직임 벡터 차이 값의 부호가 비트스트림에 들어가기 전에 XOR 연산을 수행한다. 이와 같이, 비트스트림에 바뀐 값을 넣음으로써 제안한 인코더의 최종 결과는 왜곡된 압축 비디오 스트림이 된다.

본 논문에서 제안한 디코더 구조는 위 그림 4와 같다. 왜곡된 압축 비디오 스트림이 입력으로 들어오면, 인트라 프레임의 DC 사이즈는 가변길이 복호화 과정을 수행하고, 변환된 DC 차이 값은 인증 신호와 XOR 연산을 수행한다. 인터 프레임에서도 움직임 벡터 차이 값은 가변길이 복호화 과정을 수행하고, 움직임 벡터 차이 값의 부호는 두 번째 인증 신호와 XOR 연산을 수행한다.

아래 그림 5는 본 논문에서 이용된 인코더의 인증 신호에 대한 XOR 연산 코드를 나타낸다. 첫 번째 코드는 DC 차이 값과 인증 신호의 XOR 연산 코드이다. 주석으로 처리된 ①번에서는 DC 값 val의 크기

```

Int IntraDC_dpcm(Int val, Int lum, Image *bitstream)
{
    :
    if( drm==1 )
    {
        for( i=(size-1) ; i>=0 ; --i ) // ①
        {
            if( DCpncode[dc_ptr]=='W0' ) { dc_ptr=0; }
            // 끝일 때 시작 포인트로 이동

            if( val & (1<<i) ) // ②
                val = DCpncode[dc_ptr]=='1' ? ( val & ~(1<<i) ) :
            ( val | (1<<i) ); // ③
            else
                val = DCpncode[dc_ptr]=='1' ? ( val | (1<<i) ) :
            ( val & ~(1<<i) ); // ④

            dc_ptr++;
        }

        BitstreamPutBits(bitstream, (long)(val), (long)(size)); // ⑤
        n_bits += size
    }
}

Int PutMV (Int mvint, Image *bitstream)
{
    :
    if((drm==1) && (absmv!=0))
    {
        if(MVpncode[mv_ptr]=='W0') { mv_ptr=0; } // 끝일 때
        시작 포인트로 이동

        sign = ((sign==1) && (MVpncode[mv_ptr]=='1')) ||
        ((sign==0) && (MVpncode[mv_ptr]=='0')) ? 0 : 1; // ⑥
        mv_ptr++;

        BitstreamPutBits (bitstream, mvtab[absmv].code,
        mvtab[absmv].len); // ⑦

        if (mvint != 0) {
            BitstreamPutBits (bitstream, sign, 1); // ⑧
            return mvtab[absmv].len + 1;
        }
        else
            return mvtab[absmv].len
    }
}
    
```

그림 5. 인코더에서 이용된 인증 신호에 대한 XOR 연산 코드

(size)만큼 반복문을 돌린다. ②번에서는 val 크기의 첫 번째 비트부터 1인지 체크한다. 크기가 4인 경우 1을 왼쪽으로 3번(size-1) 이동시켜 val의 비트 값을 체크한다. val의 비트 값이 1인 경우 ③번에서 DCpncode[dc_ptr]에 저장된 값이 1일 때, val의 해당 비트 값은 0, 저장된 값이 0일 때, val의 해당 비트 값은 1이 된다. val의 비트 값이 0인 경우 ④번에서 DCpncode[dc_ptr]에 저장된 값이 1일 때 val의 해당 비트 값은 1, 저장된 값이 0일 때 val의 해당 비트 값은 0이 된다. 이와 같은 방법으로 4회 반복한 후 ⑤번에서 최종 변환된 값이 변환 전의 크기 (size)만큼 비트스트림에 들어간다.

두 번째 코드는 움직임 벡터의 부호와 인증 신호의 XOR 연산 코드이다. 이 코드는 DRM이 설정되어 있고 움직임 벡터 차이 값이 0이 아닌 경우에만 수행

한다. 주석으로 처리된 ⑥번에서 부호 비트와 인증 신호의 XOR 연산을 수행한 후, ⑦번에서 움직임 벡터 차이 값이 VLC 코드로 비트 스트림에 들어가고, ⑧번에서 부호 비트가 비트 스트림에 들어간다.

4. 실험방법 및 결과

본 논문에서는 인트라 프레임의 DC 성분과 인트라 프레임의 움직임 벡터를 이용한 디지털 비디오 화면 모호화 기법을 제안한다.

실험은 디코더에서 인증 신호를 적용한 경우와 적용하지 않은 경우, 원 압축 비디오에 대한 PSNR을 비교해봄으로써 정상적인 수행 여부를 확인한다. 또한 인증 신호가 비디오 크기에 따라 몇 비트가 들어가는지 예측할 수 있도록, 30프레임에서 인증 신호가 적용된 개수를 구하고, 기존 기법과의 비교를 통해 장점을 알아본다. 프로그램은 MPEG-4 VM 코드를 이용하고[11], 실행은 Intel® Core™ 2 Duo CPU E8400 @ 3.00GHz, 3.25GB RAM, Windows 7 환경에서 수행한다. 테스트 비디오는 CIF (352×288) ‘foreman.yuv’, ‘flower.yuv’, ‘mobile.yuv’, ‘stefan.yuv’, ‘bus.yuv’ 5개의 비디오와 SD (720×480) ‘whale_show.yuv’, ‘opening_ceremony.yuv’, ‘driving.yuv’ 3개의 비디오를 이용한다[12,13]. 제안한 기법을 적용하기 위한 인코더의 환경설정은 아래 그림 6과 같다.

Encoder configuration	
⋮	
1	{ Usage DRM : 0 - no, 1 - yes }
../drm/sig.key	{ Signature filename }
../drm/id.key	{ M-sequence filename }

그림 6. 인코더의 DRM 환경설정

아래 그림 7은 DRM이 적용된 3개의 SD 비디오에 대하여, 디코더에서 인증 신호를 적용한 경우와 적용하지 않은 경우의 각 5 프레임의 결과를 보여준다. 결과에 의해서, 적합한 인증 신호를 적용한 경우 비디오가 정상적으로 재생되었고, 인증 신호를 적용하지 않은 경우 심하게 왜곡된 비디오가 재생됨을 확인할 수 있다.

본 논문에서의 화질 평가는 객관적 화질 평가인 PSNR (peak signal to noise ratio)을 이용한다. PSNR은 최대 신호 전력 (peak signal power)과 잡음

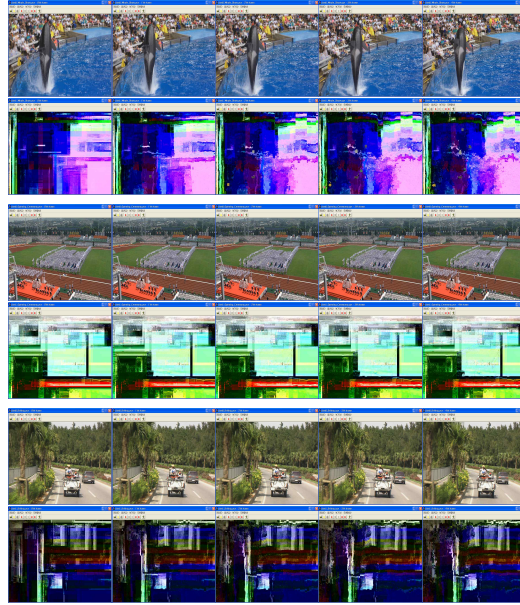


그림 7. DRM이 적용된 3개의 SD 비디오에 대하여, 디코더에서 적합한 인증 신호를 적용한 경우와 적용하지 않은 경우의 각 5프레임

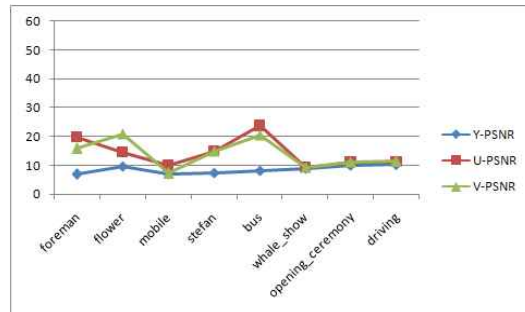


그림 8. 원 압축 비디오에 대한, 8개의 왜곡된 비디오의 Y, U, V 평균 PSNR

전력 (noise power) 비율의 log 표현 방법으로서 PSNR이 클수록 원 영상에 근접함을 나타낸다[14]. 오차 계산은 MSE (mean squared error) 방법을 이용한다. PSNR과 MSE는 아래 식 (1)와 식 (2)과 같다.

$$PSNR [dB] = 10 \log_{10} \frac{255^2}{MSE} [dB] \quad (1)$$

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (x(i, j) - x'(i, j))^2 \quad (2)$$

위 식 (2)에서, M 과 N 은 비디오 화면의 가로 픽셀과 세로 픽셀 수를 나타낸다. $x(i, j)$ 는 본 논문에서

원 압축 비디오 화면의 픽셀 값이고, $x'(i, j)$ 는 테스트 된 비디오 화면의 픽셀 값이다.

위 그림 8은 8개의 왜곡된 비디오들의 30프레임에 대한 각 평균 PSNR을 나타낸다. 그래프에 의해 CIF 영상은 SD 영상과는 달리 U, V PSNR이 상대적으로 높게 나타났다. 이것은 프레임 크기와 색차 샘플링 압축 포맷에 관련된 부분으로서, 인증 신호의 값이 연속적으로 0이 나오는 경우 DC 계수와 움직임 벡터의 부호가 그대로 들어가기 때문에 나타나는 현상이다. 그러나 이것은 한 프레임 내에서 부분적으로만 나타나는 현상이기 때문에, 화면은 처음 의도한 바와 같이 비정상적으로 재생되었다.

표 1. 8개의 비디오 30프레임에 대하여, 적합한 인증 신호를 적용한 결과

비디오	적용된 인증신호 개수		정상 기능 여부
	DC	MV	
foreman (CIF)	95	107	○
flower (CIF)	79	70	○
mobile (CIF)	123	109	○
stefan (CIF)	90	99	○
bus (CIF)	83	129	○
whale_show (SD)	392	757	○
opening_ceremony(SD)	289	60	○
driving (SD)	325	490	○

위 표 1은 8개의 비디오 30프레임에 대하여 서명 헤더 8bit, 'KOREA' 40bit, M-수열 127bit로 구성된 인증 신호를 적용한 결과이다.

결과에 의해, CIF 비디오에서는 flower가 총 149개로 가장 적게 적용되었고, SD 비디오에서는 opening_ceremony가 총 349개로 가장 적게 적용되었다. 이것은 CIF 비디오에서 최소 약 26,075비트만큼 적용할 수 있고, SD 비디오에서 최소 약 61,075비트만큼 적용할 수 있음을 나타낸다.

정상 기능 여부의 판별은 디코더에서 적합한 인증 신호를 적용했을 때와 적용하지 않았을 때 원 압축 비디오에 대한 PSNR로 판단하였다. 결과에 의해, 적합한 인증 신호를 적용한 경우 비디오 신호 전체에 대하여 Y, U, V PSNR이 모두 극치 값을 나타냈고, 비디오는 정상적으로 재생되었다. 그러나 인증 신호를 적용하지 않은 경우 평균 PSNR은 12.25dB의 낮

은 수치를 나타냈고, 심하게 왜곡된 비디오가 재생되었다. 즉 디지털 비디오 화면 모호화 기법이 정상적으로 기능하였다.

비디오가 정상적으로 재생된 경우 인증 신호를 적합한 신호라고 판단하였고, 서명 검출 과정을 수행하였다. 서명 검출 과정은 2 장의 그림 2에 나타낸 바와 같이, 서명 신호에 대하여 8비트 헤더에 의해 블록 사이즈를 구하고 블록 단위로 10진 변환 후, 저작권자의 비밀 키에 의해 RSA 복호화 과정을 수행하여 검출하였다. 검출 결과 모두 원 저작자의 서명임을 확인할 수 있었다.

아래 표 2는 제안한 기법과 기존 기법과의 비교를 나타낸다. 기존의 기법은 DCT-기반의 비디오 보안을 위한 암호화 기법으로서, 인트라, 인터 프레임의 DC 계수를 암호화한다[15]. 이 기법은 보안에 강한 점과 하드웨어로 구현된 고속 암호화 시스템을 장점으로 제시하고 있다. 단점은 DC 계수 대신 암호화된 숫자를 저장하기 때문에 숫자 크기에 따라 비트스트림이 증가하게 되고, 저작권 정보를 삽입하지 않기 때문에 저작권자의 정보를 얻을 수 없다. 또한, 윤곽선 정보는 주로 중간 주파수 영역에 존재하므로, 저주파 영역에 해당하는 DC 계수만을 암호화한다면, 윤곽선 정보는 그대로 나타날 것으로 생각한다.

표 2. 제안한 기법과 기존 기법과의 비교

	제한한 기법	기존의 기법[14]
적용 부분	DC계수, 움직임벡터	DC 계수
비트 스트림	유지	증가
저작권 정보	있음	없음

6. 결 론

본 논문에서는 인트라 프레임의 DC 성분과 인터 프레임의 움직임 벡터를 이용한 디지털 비디오 화면 모호화 기법을 제안한다.

제안한 디지털 비디오 화면 모호화 기법은 저주파 영역과 중간 주파수 영역에 민감한 반응을 보이는 HVS의 특성을 고려한 방법으로서, DCT, 양자화 과정 후, 영상의 주요 정보를 포함하는 인트라 프레임의 DC 계수와 윤곽선 움직임 정보를 포함하는 인터 프레임의 움직임 벡터의 부호를 인증 신호와 XOR

연산하여 신호를 왜곡시키고, 적합한 인증 신호를 적용한 경우에만 정상적인 화면을 볼 수 있도록 하는 기법이다.

제안한 기법은 3장의 그림 5를 통해 비트 스트림(bit-stream)이 유지됨을 알 수 있었다. 4장의 실험 결과에서는 적합한 인증 신호를 적용한 경우 정상적인 비디오가 재생되었고, 인증 신호를 적용하지 않은 경우 심하게 왜곡된 비디오가 재생되었다. 왜곡된 비디오는 원 압축 비디오에 대하여 평균 PSNR이 12.25dB을 나타냄으로써 화질 차이가 큼을 알 수 있었고, 정상적으로 재생된 비디오는 PSNR이 극치 값을 나타냄으로써 원 압축 비디오와 같은 화질임을 알 수 있었다. 또한, 비디오가 정상적으로 재생된 경우, 서명을 검출함으로써 저작권을 증명할 수 있었다. 화질 면에서는 기존의 워터마킹 기법과는 달리, 적합한 인증 신호를 적용한 경우 아주 적은 손실도 일어나지 않았다.

결과적으로, 제안한 기법은 비트 스트림을 유지하였고, 주요 성분만을 변경시킴으로써 비디오 신호 전체에 걸쳐 재생 권한 인증과정을 정상적으로 수행하였다. 그리고 적합한 인증 신호에 대해서는 서명을 검출함으로써 저작권을 증명할 수 있었다. 이 결과로부터 좀 더 선택적으로 확장 및 보완을 한다면 실제 애플리케이션에서도 이용할 수 있을 것이라 예상된다.

참 고 문 헌

[1] 이창열, "DRM(Digital Rights Management)," 한국정보통신기술협회저널, No.82, pp. 91-94, 2002.

[2] Min-Jen Tsai and Yuan-Fu Luo, "Service-Oriented Grid Computing System for Digital Rights Management (GC-DRM)," *Expert Systems with Applications*, Vol.36, Issue7, pp. 10708-10726, 2009.

[3] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia Data-Embedding and Watermarking Technologies," *Proceedings of the IEEE*, Vol.86, No.6, pp. 1064-1087, 1998.

[4] G. C. Langelaar, R. L. Lagendijk, and J. Biemond, "Real-Time Labeling of MPEG-2 Compressed Video," *Journal of Visual Communication and Image Representation*, Vol.9, No.4, pp. 256-270, 1998.

[5] 권성근, 황의창, 이미희, 정태일, 권기룡, "움직임 벡터 정보를 이용한 SPIHT 부호화 기반의 디지털 비디오 워터마킹," 한국멀티미디어학회 논문지, 제10권, 제11호, pp. 1427-1438, 2007.

[6] John Arnold, Michael Frater, and Mark Pickering, *Digital Television: Technology and Standards*, John Wiley & Sons, 2007.

[7] Rafael C. Gonzalez and Richard E. Woods, *Digital Image Processing*, Prentice Hall, 2001.

[8] Brain A. Wandell, *Foundations of Vision*, Sinauer Associates, 1995.

[9] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[10] Solomon W. Golomb, *Shift Register Sequences*, Holden-Day, 1967.

[11] ISO/IEC 14496-2:2001, *Information technology: Coding of audio-visual objects --Part2: Visual*, ISO/IEC JTC1/SC29/WG11, 2001.

[12] <http://trace.eas.asu.edu/yuv/index.html>

[13] http://scien.stanford.edu/pages/labsite/scien_test_images_videos.php

[14] D. K. Fibush, "Practical Application of Objective Picture Quality Measurements," *SMPTE J.*, Vol.108, No.1, pp. 10-19, 1999.

[15] 박성호, 최현준, 서영호, 김동욱, "DCT-기반 영상/비디오 보안을 위한 암호화 기법 및 하드웨어 구현," 대한전자공학회논문지, 제42권, 제2호, pp. 27-36, 2005.



부 희 형

2004년 목포대학교 컴퓨터공학과
학사
2006년 전남대학교 컴퓨터정보통
신공학과 석사
2008년~현재 경북대학교 전자전
기컴퓨터학부 박사과정

관심분야 : 동영상 압축, 그래픽스, 유한요소법 등



김 승 호

1981년 경북대학교 전자공학과
학사
1983년 한국과학기술원 전산학과
석사
1988년 한국과학기술원 전산학과
박사

1985년 3월~현재 경북대학교 컴퓨터학부 교수
관심분야 : 알고리즘, 멀티미디어, 다시점 동영상, 감시
시스템, 동기식 인터넷 등