디지털산업정보학회 논문지 제4권 제1호 - 2008년 3월

모바일 기기내의 비디오 코덱에서 DCT 계수와 움직임 벡터의 암호화를 이용한 저작권 보호

권 구 락* · 김 영 로**

Copyright Protection using Encryption of DCT Coefficients and Motion Vector in Video Codec of Mobile Device

Kwon, Goo Rak · Kim, Young Ro

〈Abstract〉

With widespread use of the Internet and improvements in streaming media and compression technology, digital music, video, and image can be distributed instantaneously across the Internet to end-users. However, most conventional Digital Right Management are often not secure and fast enough to process the vast amount of data generated by the multimedia applications to meet the real-time constraints. In this paper, we propose the copyright protection using encryption of DCT coefficients and motion vector in MPEG-4 video codec of mobile device. This paper presents a new Digital Rights Management that modifies the Motion Vector of Macroblock for mobile device. Experimental results indicate that the proposed DRM can not only achieve very low cost of the encryption but also enable separable authentication to individual mobile devices such as Portable Multimedia Player and Personal Digital Assistants. The performance of the proposed methods have low complexity and low increase of bit rate in overhead.

Key Words: Multimedia Encryption and Security, Video Scrambling, MPEG-4, Mobile Device

Ⅰ. 서 론

디지털 전송기술의 발전에 따라 다양한 디지털 콘텐츠가 서비스 되고 있다. 영상 콘텐츠의 고품질 서비스를 위해 영상 압축표준으로 개발된 MPEG-4는 CD-ROM, DVD, 디지털 텔레비전, 인터넷 방송 등의 스트리밍 서비스가 가능하게 한다. MPEG-4 비디오를 이용한 다양한 영상 콘텐츠가 서비스됨에 따라 비인가 복사 혹은 부적절한 콘텐츠로의 접근을 방지할 필요성이 증대되고 있다. 특히, 휴대폰이나 PMP등의 모바일 기기의 사용이 급증함에 따라 온라인 혹은 무선으로 제공되는 영상콘텐츠 사용이 증가하고 있고 이에 따라 서비스 제공자는 제공하는 콘텐츠에 대한 저작권 보호를 필요로 한다. 저작권을 보호하기 위한 디지털 저작권 관리(DRM) 시스템은

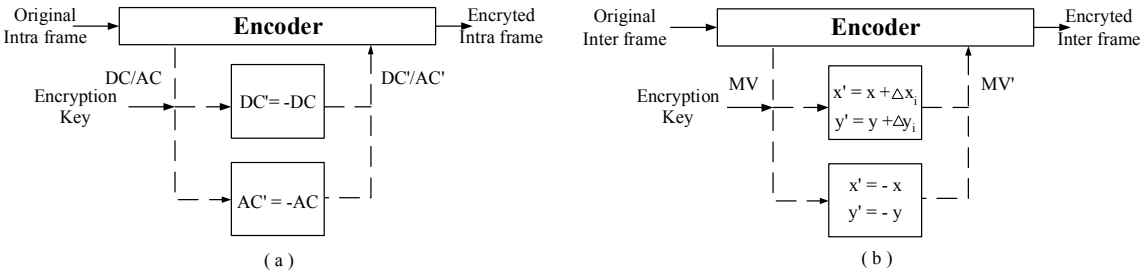
* 조선대학교 정보통신공학과
** 명지전문대학 컴퓨터정보과

콘텐츠 보호를 위해 두 가지 방법을 사용한다. 첫 번째는 인증된 사용자만 접근 가능하도록 디지털 콘텐츠를 암호화(Encryption)하는 것이고, 두 번째는 미디어 복사 이후에도 저작권을 확인할 수 있는 워터마크(Watermark), 플래그, XrML (eXtensible Right Markup Language)을 삽입하는 것이다. MPEG-4에서의 암호화 방법은 DES를 이용한 암호화하는 방법이나 MPEG-4 영상 프레임에서의 암호화 방법이 많이 사용되고 있다[1]-[3]. DES를 사용한 암호화는 MPEG-4 비트 스트림의 일부분 혹은 전체비트를 암호화 하는 방법으로 MPEG-4 영상 압축 후 비트스트림을 이용한다. 이 방법은 MPEG-4 고유의 특성을 이용한 것은 아니다. 영상 프레임에서의 암호화 방법으로는 I-프레임에서 정지영상에서의 암호화 기법들이 주로 사용되고 있다. DES를 이용한 암호화 과정은 MPEG-4의 복호화 과정과 더불어 과도한 계산량으로 인해 배터리 소모 등의 문제를 발생시킬 수 있다[2]. 정지영상에서의 암호화 방법들은 I-프레임에서의 암호화 기법으로 MPEG-4 영상압축의 특성을 이용하지 못하였다. I-프레임에 대한 암호화로 몇몇 영상 암호화 시스템은 비디오 영상 데이터의 픽셀 도메인에서 직접적인 셔플링이나 암호화를 시도하였다. 이러한 영상들은 데이터를 복호화하지 않으면 정상적인 영상을 볼 수 없게 하기 위함이다. 그러나 이런 영상을 직접적으로 암호화하면서 원 영상 신호를 변형시켜 영상 압축시 압축률과 압축된 데이터에 영향을 미치게 만들어 비효율적으로 되는 문제가 발생한다. 다른 방법으로 DCT 도메인에서 DC/AC 계수의 부호를 변환하거나 매크로 블록간의 셔플링 기법이나 DCT된 매크로 블록을 회전시켜 영상 복호시 영상을 왜곡시키는 방법 등이 사용되었다[3]-[9].

암호화 기법에서 주요 논제는 적은 암호화 계산량과 믿을만한 보안성, 그리고 콘텐츠의 비트 초과량이 많지 않아야 한다는 것이다. 모바일 기기에서 압축영상의 디코딩 과정간 암호의 복잡한 복호화 과정은 배터리 수명의 문제를 일으킬 수 있다. 또한 영상콘텐츠의 암호화 과정시 과도한 비트의 초과로 인한 압축효율에 문제가 발생하지 않도록 해야 한다. 비트의 초과는 압축의 문제뿐만 아니라 온라인상에서 콘텐츠의 전송간 오류를 발생시킬 수 있기 때문이다.

본 논문에서는 MPEG-4 비디오에서 영상의 압축간 DCT계수와 움직임 벡터를 이용한 암호화 기법을 제안한다. 이 방법은 영상 압축간 주요 정보인 DCT 계수와 움직임 벡터에 대한 선택적 암호화 기법을 사용하여 비인가 기기에서 복호시 영상의 왜곡을 일으킨다. 선택적 암호키를 통해 보안성을 높일 뿐만 아니라 MPEG-4 비디오 압축에서 비트의 초과가 적어 압축률에 대한 영향이 적을 뿐만 아니라 온라인에서의 전송간 오류를 일으킬 확률이 낮은 장점이 있다.

본 논문의 구성은 다음과 같다. Ⅱ장은 제안한 알고리즘을 설명한다. 그리고, Ⅲ장에서는 실험 결과 및 분석을 하며 마지막으로 Ⅳ장을 끝으로 결론을 맺는다.



〈그림 1〉 화면내/ 화면간 암호화 과정 (a) 화면내 DCT 계수 암호화 (b) 화면간 움직임 벡터 암호화

Ⅱ. MPEG-4 비디오 코덱과 암호화 알고리즘 구조

본 장에서는 MPEG-4에서 화면내 DCT 계수를 선택적으로 변화시키고 화면간 움직임 벡터를 변형하여 비인가 기기에서 영상 이용시 영상을 왜곡하는 방법을 제안한다.

2.1 화면내 DCT 계수의 암호화

영상의 암호화 기법으로 DCT 계수의 부호변화를 이용한 방법은 영상을 효과적으로 왜곡시킬 뿐만아니라 화면내 영상의 왜곡이 화면간 영상의 왜곡으로 전이되는 에러 전파를 일으킬 수 있다. 본 논문에서는 임의의 매크로 블록에 대한 DCT 계수를 DC계수와 AC계수로 구분하여 부호를 전환시킨다. 그림 1의 (a)에서 임의의 매크로 블록에 대한 암호화 과정을 볼 수 있다. 화면내 DCT 계수는 암호키에 의해 DC 계수 혹은 AC 계수의 전환이 결정된다. 그림 2와 같이 영상의 DC 계수와 AC 계수는 각각의 부호 전환으로도 충분한 영상왜곡을 일으킨다. 때문에 DC 계수와 AC 계수로 나뉘어 부호가 전환되며 표 1과 같이 인가된 암호키에 의해 매크로 블록은 선택적으로 암호화 된다.

<표 1> 암호키에 따른 화면내/화면간 암호화

암호키	I-frame	P-frame(B-frame)
0	DC′=-DC	MV′=MV+Δα
1	AC′=-AC	MV′=-MV
· · ·	· · ·	· · ·
i	DCT 부호 전환	움직임 벡터 변환

표 1에서 i는 암호화시킬 매크로 블록의 개수이며 화면내 블록의 개수에 한정된다. 암호키는 서비스 제공자에 의해 생성될 수 있으며 최장 64비트의 암호키가 구성가능하다. 암호키에 따라 매크로블록의 DCT 계수와 움직임 벡터 암호의 방법이 달라지게 되므로 서로 다른 암호키로 비인가 접속이 불가해진다.

(a)

(b)

<그림 2> I-프레임에서 영상 암호화 (a) DC계수 부호 변환에 의한 영상 왜곡 (b) AC계수 부호 변환에 의한 영상왜곡

2.2 움직임 벡터의 암호화

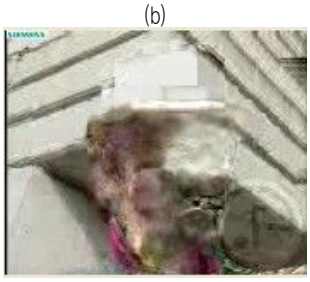
DC 계수는 움직임 벡터를 변형하기 위해 화면 내 DCT 계수의 전환과 같이 두 가지 방법이 쓰인다. 움직임 벡터의 x, y값을 변형함으로써 벡터의 각도를 변형시키거나 벡터의 부호를 바꿔 벡터 방향을 반대로 변형시킨다. 이 방법은 P-프레임이나 B-프레임의 모든 움직임 벡터를 변형시킬 필요는 없다. MPEG-4 비디오에서는 움직임 보상과 예측 방법을 사용하기 때문에 서로 다른 프레임에서 임의의 매크로 블록에 대해 움직임 벡터를 변환할 경우 에러의 확산을 일으켜 영상의 왜곡을 일으킬 수 있다. 움직임 벡터의 위상각도 변화는 다음과 같다.

$$\theta[i] = \arctan\left[\frac{MV_v[i]}{MV_h[i]}\right](0 \le i \le MB, \theta[i] \ge T) \quad (1)$$

i번째 매크로 블록의 움직임 벡터의 수직, 수평 값을 MV_v, MV_h라고 했을때 $\theta[i]$는 움직임 벡터의 위상 각도이다. 이때 $\theta[i]$는 한계치 T를 넘는 각도를 가진다.

$$MV_v' = MV_v + \Delta v$$
$$MV_h' = MV_h + \Delta h \quad (2)$$

(b)



(a)

〈그림 3〉 움직임벡터 변화에 따른 영상 암호화
(a) 움직임 벡터의 부호 변화에 의한 영상 왜곡
(b) 움직임 벡터 위상각도 변화에 따른 영상 왜곡

움직임 벡터의 수직, 수평값이 MV_v', MV_h'로 변화하면 위상각도는 다음과 같이 변화한다.

$$\theta[i]' = \arctan\left[\frac{MV_v'[i]}{MV_h'[i]}\right](0 \le i \le MB) \quad (3)$$

움직임 벡터에서 수직값 혹은 수평값의 변화는 암호화 시킬 서비스 제공자가 결정할 수 있다. 움직임 벡터의 방향 변화는 다음과 같다.

$$MV_v' = MV_v \times -1$$
$$MV_h' = MV_h \times -1 \quad (4)$$

움직임 벡터 암호화에서 벡터의 위상각도 변화 혹은 방향의 변화는 그림 1의 (b)에서처럼 암호키에 의해 결정된다. 표 1의 암호키에 따라 각각의 매크로 블록에 대한 움직임 벡터 암호 방법이 달라지며 서비스 제공자에 따라 다른 암호키를 가지고 영상의 암호화를 할수 있다. 그림 3은 움직임 벡터 암호화에 따라 P-프레임에서의 영상 왜곡을 보여준다.

Ⅲ. 성능 평가 및 분석

본 실험은 MPEG-4 Simple Profile MoMuSys-FPDAM1 소스를 사용하였고 테스트 영상으로는 CIF (352*288)인 "Foreman, Stefan"을 사용하였다.

표 2에서는 원 영상의 압축과 암호화 과정을 포함한 압축시 압축 시간과 압축률에 대한 비교가 나와 있다. 표 2에서 보이는 바와 같이 인코더 내에서 암호화후 비트 초과율은 정상 압축시보다 4% 이상 초과하지 않았다. 또한 암호화 계산량이 적어 압축 시간에서도 크게 증가하지 않음에 따라 압축에 따른 손실은 적으면서 보안성이 뛰어난 것을 알 수가 있다.

그림 4의 (a)와 (b)는 DCT 계수의 부호변환과 움직임 벡터의 변화를 동시에 실행한 것이다. DC 계수의 부호 변화와 움직임 벡터의 위상각도 변화를 동시에 실행하였을 때에 따른 영상왜곡과 AC 계수의 부호 변화와 움직임 벡터의 부호 변화를 동시 실행한 영상왜곡 정도를 볼 수 있다. 그림 4의 (c)는 암호키 64비트로 전체 매크로 블록에 대해서 두 가지 방법을 동시 사용했을 때의 왜곡된 영상을 보여준다.

〈표 2〉 암호화 방법간 압축시간과 비트증가율 비교

암호화 방법	Foreman (CIF)		Stefan (CIF)	
	압축시간 (time ratio)	비트증가율 (bit overhead)	압축 시간 (time ratio)	비트증가율 (bit overhead)
정상 압축	0	0	0	0
DC 계수 부호 변환	0	0	0	0
AC계수 부호 변환	0	0	0	0
움직임 벡터 부호 변환	0	0	0	0
움직임 벡터 각도 변화	1.2	1.4	1.5	2.5
DC계수 부호변환 + 움직임 벡터 각도 변화	1.5	1.4	1.9	2.5
AC계수 부호변환 + 움직임 벡터 부호 변환	0.5	1.2	1.1	1.8
제안된 암호화 방법	1.9	2.2	2.1	3.1

(a)

(b)

(c)

〈그림 4〉 제안된 알고리즘에 의한 영상 암호화 (a) DC 계수 부호 변환 및 움직임 벡터 위상각도 변환 (b) AC 계수 부호 변환 및 움직임 벡터 부호 변환 (c) 64비트 암호키에 따른 영상 암호화

Ⅳ. 결 론

제안된 방법은 암호화 계산량이 적으면서도 영상내의 I-프레임과 P-프레임의 주요 정보를 이용하여 효과적으로 영상을 암호화 하였다. 압축률과 압축시간의 손실을 적게 하므로써 모바일 통신이나 온라인상에서 영상 콘텐츠에 대한 서비스가 가능하다. 또한 최장 64비트의 암호키를 이용하여 비인가자의 접속이나 비인가 기기에서 영상 이용을 방지하였다.

참고문헌

[1] Gunhce Kim, Dongkyoo Shin, and Dongil Shin, “Intellectual property management on MPEG-4 video for hand-held device and mobile video streaming service,” Consumer Electronics, IEEE Transactions on Vol. 51, Issue 1, pp. 139 - 143, Feb. 2005.

[2] E.I. Lin, A.M. Eskicioglu, R.L.Lagendijk, and E.J. Delp, “Advances in Digital Video Content Protection,” Proceedings of the IEEE, Vol. 93, Issue 1, pp. 171 - 183, Jan. 2005.

[3] Zeng Wenjun and S. Lei, “Efficient frequency

domain selective scrambling of digital video," Multimedia, IEEE Transactions on, Vol. 5, Issue 1, pp. 118 - 129, Mar. 2003.

[4] Douglas R. Stinson. Cryptography, Theory and Practice. CRC Press, Inc. New York, 1995.

[5] Changgui shi and Bhargave B, "An efficient MPEG video encryption algorithm," Reliable Distributed Systems, Proceeding. Seventeenth IEEE Symposium on Computer Society, vol. 20, no. 23, pp. 381~386, Oct. 1998.

[6] J. Jang, "Digital video scrambling method," KR patent 0151199, Jun. 1998.

[7] B. Macq and J.Quisquater. Cryptology for Digital TV Broadcasting. Proceedings of The IEEE, 83(6), pp.14-24, 1994.

[8] C. Shi and B.Bhargava, "Light-weight MPEG Video Encryption Algorithm," In Proc. of the Int'l Conf. on Multimedia, (Multimedia98, Shoping The Future) January 23-25, 1998, pp. 55-61, New Delhi, India. IETE, Tata Mcgraw-Hill Publishing Company.

[9] L. Tang, "Methods for Encrypting and Decrypting MPEG Video Data Efficiently", Proc. of the fourth ACM International Conference on Multimedia, pp. 219-229, Boston, Nov. 1996.

■ 저자소개 ■

권구락
Kwon, Goo-Rak

2007년 ~현재 조선대학교 정보통신공학과 전임강사
1997년 경일대학교 전자공학과 학사 졸업
1999년 성균관대학교 전기전자 및 컴퓨터공학부 석사 졸업
2007년 고려대학교 메카트로닉스학과 박사 졸업

관심분야 : 멀티미디어 통신 및 처리, 디지털 신호 처리
E-mail : tkkim@stu.ac.kr

김영로
Kim, Young-Ro

2003년~현재 명지전문대학 컴퓨터정보과 부교수
1993년 고려대학교 전자공학과 학사
1996년 고려대학교 전자공학과 컴퓨터공학 석사
2001년 고려대학교 전자공학과 컴퓨터공학 박사
2001년~2003년 삼성전자 시스템LSI 책임연구원

관심분야 : 신호 및 영상처리, 멀티미디어 통신
E-mail : histone@kut.ac.kr

논문접수일 : 2008년 2월 29일
게재확정일 : 2008년 3월 10일