MPEG 비디오 부호화기 내의 scrambling 기술

권구락* · 윤주상**

Scrambling Technology in MPEG Video Environment

Goo-Rak Kwon* · Joo-Sang Youn**

요 약

멀티미디어 기술의 발달로 인터넷을 이용하는 사용자 사이의 멀티미디어 공유가 현재 중요한 이슈가 되고 있다. 이는 일반적인 네트워크에서 보호되지 않은 컨텐츠와 보호된 컨텐츠가 사용자에게 P2P 배포로 전송 가능하다. 필연적으로 이러한 환경은 무료로 저작권이 있는 미디어 데이터가 제공되어지고 불법적인 기술들이 발생한다. 결과적으로 불법적인 공격과 배포를 보호하기 위해서 디지털 저작권이 필요하다. 본 논문에서는 DES 암호기술을 이용하여 저작권이 있는 멀티미디어를 보호하기 위해 복잡도가 낮은 scrambling 기술을 제안한다. 실험적인 결과에서 제안한 기술은 압축속도, 안전성, 파일크기를 고려하여 좋은 성능을 실험을 통해 확인된다.

ABSTRACT

With the advance of multimedia technology, multimedia sharing among multiple devices has become the main issue. This allows users to expect the peer-to-peer distribution of unprotected and protected contents over public network. Inevitably, this situation has caused an incredible piracy activity and Web sites have begun to provide copyrighted A/V data for free. In order to protect the contents from illegal attacks and distribution, digital right management (DRM) is required. In this paper, we present the minimal cost scrambling scheme for securing the copyrighted multimedia using the data encryption standard (DES) encryption technique. Experimental results indicate that the proposed scrambling techniques achieve a very good compromise between several desirable properties such as speed, security, and file size.

키워드

Multimedia scrambling, contents access, contents protection, copyright protection, DRM

* 조선대학교 정보통신공학과
** 동의대학교 멀티미디어공학과 (교신저자)

접수일자 2008. 12. 22
심사완료일자 2009. 02. 04

Ⅰ. 서 론

멀티미디어 기술의 발달로 인터넷을 이용하는 사용자 사이의 멀티미디어 공유가 현재 중요한 이슈가 되고 있다. 이는 일반적인 네트워크에서 보호되지 않은 컨텐츠와 보호된 컨텐츠가 사용자에게 P2P 배포로 전송 가능하다. 필연적으로 이러한 환경은 무료로 저작권이 있는 미디어 데이터가 제공 되어지고 불법적인 기술들이 발생한다. 결과적으로 불법적인 공격과 배포를 보호하기 위해서 디지털 저작권이 필요하다.

기존의 제안된 암호화 방법들은 주로 DES나 AES와 같은 직접적인 암호화와 DCT 변환과 같은 공간적 영역에서의 암호화, 그리고 움직임 벡터와 같은 시간적 영역에서의 암호화 방법들이 있다. DES나 AES를 이용한 암호화는 압축 영상 신호 자체에 직접적으로 암호화를 하는 것이다.[1] 이는 암호화 효과는 가장 좋을 수 있으나, 계산량이 매우 많기 때문에 대용량 데이터이고 실시간 처리를 요구하는 비디오에 적용하기에는 부적합하다. 이를 보완하기 위해 영상의 중요한 정보 몇 가지에만 적용하는 방법도 제안되었으나 아무리 적은 양의 영상 신호를 암호화한다 하더라도 암호화 알고리즘 자체의 계산량이 매우 크기 때문에 정상적인 속도로 영상을 복호화 할 수 없다.

DCT 기반의 암호화는 DCT 변환 계수들을 섞는 방법들이 있다[1]-[2]. 이는 특정 테이블을 이용하여 DCT 계수의 zigzag순서를 바꾸거나, 동일 주파수 위치의 계수들을 섞는 것으로 계산 복잡도는 낮지만 압축 효율이 떨어 질 수 있는 단점이 있다. 또는 인트라 프레임의 DCT 영역에서의 DC계수만 암호화 하는 방법이 있다[3]. 그러나 이 방법은 움직임이 빠른 비디오 컨텐츠의 경우 B-프레임 및 P-프레임에서 인터 매크로블록이 많이 발생함에 따라 암호화 효과가 크게 떨어진다.

움직임 벡터를 이용한 암호화는 전송 블록 형태와 움직움 벡터를 이용한 방법이 있다[4]. 이는 전송 블록 형태 값을 모듈러 연산한 결과만큼 떨어져 있는 부호어를 이용하여 부호화 하는 방법으로 scrambling 후 과도한 비트의 양이 증가 할 수 있다는 단점이 있다.

비디오 암호화 기법에서 주요 논제는 적은 암호화 계산량과 신뢰할 수 있을만한 보안성, 그리고 암호화 과정 시 비트 스트림의 초과량이 많지 않아야 한다는 것이다[5]-[8]. 비디오는 그 특성상 실시간적인 복호화가 가능해야 하며, 이를 위해서는 암호화에 대한 계산 복잡도가 낮게 이루어 져야 한다. 특히, 모바일 기기와 같이 저 연산장치이고, 베터리를 사용하는 휴대용 기기에서 암호화 해독 과정에서의 계산량이 많으면 베터리가 과도하게 소모되어 실시간적인 복호화는 기대할 수 없다. 또한 암호화 과정 시 과도한 비트 스트림의 초과로 인해 압축 효율에 문제가 발행하지 않도록 해야 한다.

본 논문은 모바일 기기에서의 비디오 저작권 보호를 중점으로 하고 있다. 데스크탑 PC와 같은 고사양의 기기가 아니기 때문에, 멀티미디어의 처리에 많은 제약이 있다. 따라서 저 사양 성능인 모바일 기기와 현재 가장 대표적이라 할 수 있는 MPEG-4 비디오 코덱에 초점을 두었다. 또한 부호화 및 복호화 시에 추가적인 계산량이 적고, scrambling 후 비트 스트림의 양이 거의 증가 하지 않으며, 선택적인 보안등급을 조절할 수 있다.

Ⅱ. 본 론

제안된 알고리즘 구조에는 인트라 블록 DCT 계수 부호 변환, 인터 블록 DCT 계수 부호 변환, 움직임 벡터의 방향 변환과 크기 증감을 하는 4가지의 scrambler와 descrambler가 있으며, 또한 선택적인 암호화를 위한 Secret key가 있다.

그림 1의 (a)에서와 같이 부호화기에서는 DCT 기반의 두 가지의 scrambling을 한다. 인트라 프레임에서는 한 프레임내에 인트라 블록만이 존재하므로 모든 블록이 인트라 블록 scrambler에 의해 scrambling 된다. P, B와 같은 인터프레임에서는 매크로블록의 형태에 따라 인트라 블록 scrambler와 인터 블록 scrambler에 의해 scrambling 된다. scrambling된 영상은 양자화 후 엔트로피 코딩되어 부호화 된다. 또한 인터 프레임에서 움직임 벡터 기반의 scrambling은 움직임을 추정하여 움직임 벡터를 구한 후 움직임 벡터 scrambler에 의해 scrambling되고 엔트로피 코딩되어 부호화 된다.

그림 1의 (b)에서와 같이 복호화기에서는 인트라 프레임의 경우, 압축된 비디오 비트스트림은 엔트로피 복호화 후에 인트라 블록 descrambler에 의해 descrambling 되고, 역양자화와 IDCT 변환을 거쳐 영상이 복원된다. 인터 프레임에서는 압축된 비디오 비트스트림은 엔트로피 복호화 후에 움직임 벡터와 인트라 블록 또는 인터

블록이 descrambling 되고, 디scrambling된 움직임 벡터와 역양자화 후 IDCT 변환을 거친 현재 영상과 이전영상으로 부터 영상을 복원하게 된다.

Secret key에는 부호화 시에 적용된 암호화 알고리즘에 대한 정보가 있으며, 복호화 시에 Secret key의 정보에 따라 descrambler가 동작하게 된다. 만약 복호화할 때 Secret key가 없거나, 정보가 올바르지 않을 경우에는 왜곡된 영상을 보게 된다.

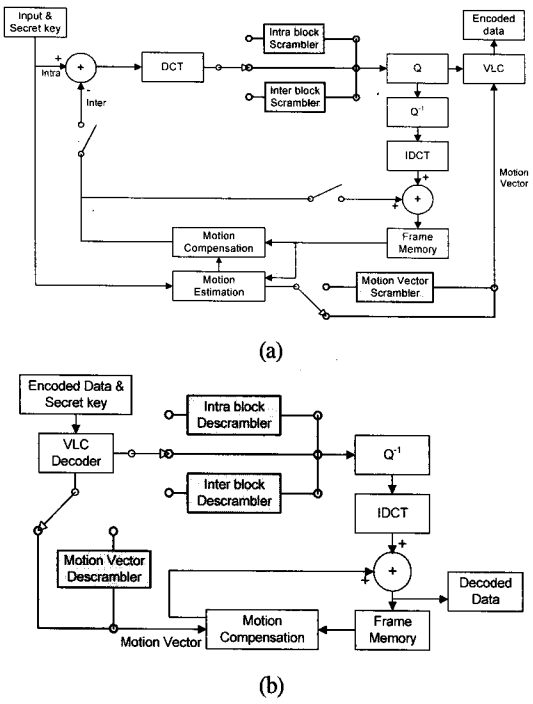

그림 1. 제안된 MPEG-4 비디오 코덱의 암호화 구조
(a) MPEG-4 비디오 부호화기의 scrambler 구조
(b) MPEG-4 비디오 복호화기의 descrambler 구조
Fig. 1 Structure of the proposed encryption in MPEG-4 Video Codec (a) Structure of scrambler in MPEG-4 Video coder (b) Structure of descrambler in MPEG-4 Video coder

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 DC 계수와 AC 계수로 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. 이는 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
Table. 1 Encryption of intra/interframe with Secret key

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.

2.2 화면내 DCT 계수의 부호변환

DC 계수는 영상의 공간영역에서의 명암 성분들의 평균값으로 인접 화소 및 프레임 간의 파급 효과에 큰 영향을 준다. 그러므로 단위 블록 내에서 DC 계수만 scrambling 후 영상을 복원시키더라도 그 블록 전체의 명암이 흐트러져 영상을 왜곡시킬 수 있다. AC 계수는 DC 계수에 비해 상대적으로 영상에 미치는 영향이 적다. 특히 AC 계수들 중 우측 하단에 위치할수록 영상에 미치는 영향이 미약하다. 그러나 DC 계수 주변의 AC 계수들은 블록 전체에 미치는 영향이 크기 때문에 이 값들의 부재 및 열화는 영상의 화질을 떨어뜨릴 수 있으며, AC 계수를 scramblin하면 블록 내에서의 화질 열화뿐만 아니라 블록간의 블록차가 발생하게 되어 영상을 왜곡시킬 수 있다. 또한 인트라 매크로블록 내의 DC 및 AC계수를 scramblin하면 인터 프레임의 인트라 매크로 블록을 참조해야 하는 생략된 매크로 블록 및 움직임이 적용된 매크로 블록에 영향을 주게 되어 인터 프레임 내에서 scramblin하지 않고도 영상을 왜곡시킬 수 있다.

2.3 화면간 DCT 계수의 부호 변환

인터 모드로 부호화하게 되는 P, B프레임에 대해서는 움직임 추정 및 움직임 보상을 함으로써 오차 프레임 구한 후 이를 DCT 변환한다. 이때 움직임이 추정된 블록, 즉 인터 블록에 대한 DCT 변환은 인트라 블록과 구분하여 처리를 하게 된다. 만약 원 영상과의 오차인 인터 블록 DCT 변환 계수를 암호화하게 된다면 원 영상을 그대로 복원할 수 없고, 인터 프레임간의 화면 오차가 심해져 영상을 왜곡할 수 있다.

2.4 화면간의 암호화 방법

비디오 압축 부호화는 프레임들 사이의 중복 요소를 제거하기 위해 현재 프레임과 이전 프레임으로부터 움직임 벡터을 추정하고, 추정된 움직임 벡터를 가변 길이 부호화한다. 복호화 시에는 추정된 움직임 벡터와 이전 프레임으로부터 현재 프레임을 복호화를 하게 되는데 만약 움직임 추정이나 움직임 벡터의 값이 잘못되는 경우에는 복호화 시에 원 영상을 복원하지 못하게 되며, 화면 간의 에러 확산도 크기 때문에 보다 큰 영상의 왜곡을 일으키게 된다. 제안하고자 하는 움직임 벡터를 이용한 scrambling 알고리즘은 움직임 벡터의 방향과 크기를 변환하는 방법으로 움직임 벡터의 수평, 수직 성분의 크기를 증감하거나 부호를 변환하여 움직임 벡터의 위상각도를 변경하는 것이다.

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 위상각도이다. 이때 $\theta[i]$는 한계치 T를 넘는 각도를 가진다.

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

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 할 수 있다.

Ⅲ. 실험 방법 및 평가

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 2.1의 (a)는 DC와 AC 계수에 암호화를 한 영상으로 영상의 휘도 및 블록 내의 영상 일그러짐이 인트라 프레임뿐만 아니라 인터 프레임까지도 전파되어 암호화 효과를 나타낼 수 있다. 그러나 DC와 AC 계수의 암호화는 인트라 프레임에서의 효과가 가장 크며 인터 프레임으로의 복호화가 될 수록 암호화 효과가 떨어지게 되며, 따라서 이를 보완하기 위해서는 인터 프레임에서의 암호화가 필요하다. (b)는 AC 계수와 인터 블록 DCT 계수를 (c)는 DC 계수와 인터 블록 DCT 계수를 (d)는 인트라 블록과 인터 블록 DCT 계수를 암호화 한 영상으로

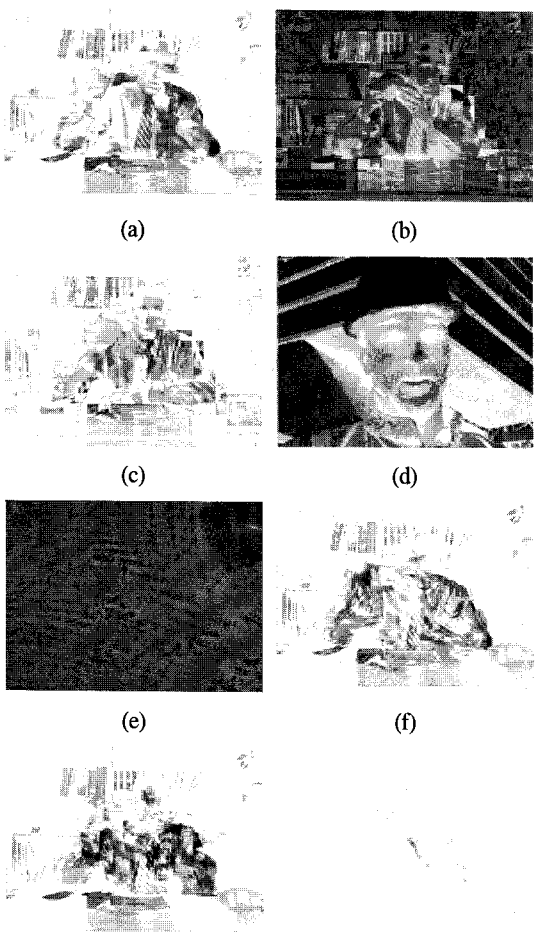

그림 2. 암호화 방법에 따른 결과 영상 비교
(a) 화면내 부호변환 (b) 화면내 AC와 화면간 DCT 계수 (c) 화면내 DC와 화면간 DCT 계수 (d) 화면내 DC와 AC 계수 및 화면간 DCT 계수 (e) MV의 부호와 크기 (f) 화면간 DC와 AC 계수 및 MV (g) 화면내 DC와 AC 계수 및 화면간 DCT 계수와 MV 부호 (h) 제안된 방법
Fig. 2 Comparison between the result images each encryption methods (a) Sign conversion in intraframe (b) AC coefficients in intraframe and DCT coefficients in interframe (b) DC coefficients in intraframe and DCT coefficients in interframe (d) DC and AC coefficients in intraframe and DCT coefficients in interframe (e) Magnitude and sign of MV (f) DC and AC coefficients, MV in interframe (g) DC and AC coefficients in intraframe and DCT coefficients and sing of MV in interframe (h) Proposed method

인트라 블록만을 암호화 한 영상보다 더 효과적인 암호화가 가능하며 암호화 패턴을 좀 더 복잡하게 만들 수 있다. (e)는 움직임 벡터의 부호와 크기 변환을 적용하여 암호화 한 영상으로 영상을 전혀 식별할 수 없으나, 암호화를 인터 프레임만을 적용할 경우 앞에서 설명한 것처럼 인트라 프레임이 많은 동영상의 경우 암호화 효과가 떨어지게 된다. (f)와 (g)는 인트라 블록과 인터 블록 DCT 계수와 움직임 벡터의 부호를 암호화 한 영상으로 인트라 프레임만을 암호화하거나 인터 프레임만을 암호화 한 영상에서의 암호화의 단점을 피할 수 있고, 더욱 복잡한 암호화 패턴으로 영상을 암호화할 수 있다. (h)는 제안된 암호화 방법 모두를 적용한 것으로 인트라 프레임 뿐만 아니라 인터 프레임에서도 전혀 영상을 식별할 수 없으며, 암호화된 영상만으로는 암호화 패턴의 이해 및 해독이 전혀 불가능하다.

암호화 방법들을 선택적으로 병행함에 있어서 기존의 암호화 방법에 나타나는 문제로 부호화 및 복호화 시에 압축률의 저하와 복잡도가 증가한다는 것이다. 표 2에서 제안된 암호화 방법에 대한 영상의 압축과 암호화 과정을 포함한 압축 시간, 압축률 및 비트 증가율에 대한 비교한다. 실험 결과적으로 정상 압축시에 3%이상 초과하지 않았으며, 또한 암호화의 계산량이 매우 적어 압축 시간에서도 크게 증가하지 않음에 따라 부호화시에 암호화에 따른 손실이 적다는 것을 알 수 있다.

표 2. 암호화 방법에 대한 압축시간 및 비트 증가율의 비교 (300 frames)
Table. 2 Comparison between compression time and bit-rate incresement in encryption methods

암호화 방법	FOREMAN (QCIF)		CLAIRE (QCIF)	
	압축시간	비트 증가율	압축시간	비트 증가율
정상 압축	1	1	1	1
움직임 벡터의 방향 변환	1	1	1	1
움직임 벡터의 크기 변환	1.2	1.4	1.5	2.5
움직임 벡터의 방향 및 크기 변환	1.2	1.4	1.5	2.5

Ⅳ. 결 론

제안된 방법은 영상내의 I-프레임과 P-프레임의 주요 정보를 이용하여 효과적으로 영상을 암호화를 수행할 뿐만 아니라 복잡도를 낮추는 성능이 있다. 비디오 부호화기에서의 영상 압축률에 따른 압축 시간의 손실이 적으므로 모바일 장치에 대한 저작권이 있는 컨텐츠 서비스가 효과적으로 가능하다. 부가적으로, DES를 이용한 64비트 암호키를 이용하여 비인가자의 접속이나 비인가 기기에서 영상 재배포 및 재생이 불가능하다.

참고문헌

[1] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," IEEE Transactions on Multimedia, vol. 5, pp.118-129, March 2003.

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

[3] 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.

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

[5] 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.

[7] L. Qiao and K. Nahrstedt, "Comparison of MPEG encryption algorithms," Computers and Graphics, Vol. 22, No. 4, pp. 437-448, 1998.

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

저자소개

권구락(Goo-Rak Kwon)

2008년 2월 고려대학교 메카트로닉스학과 (공학박사)
2008년 3월 ~ 현재: 조선대학교 정보통신공학과 전임강사

※관심분야: 디지털 미디어 신호처리 및 응용, 정보보안

윤주상(Joo-Sang Youn)

2008년 2월 고려대학교 전자컴퓨터공과 (공학박사)
2008년 3월 ~ 현재: 동의대학교 멀티미디어공학과전임강사

※관심분야 : 무선 네트워크, ad-hoc/mesh/ multiple access network