Journal of Korea Multimedia Society Vol. 10, No. 1, January 2007(pp. 58-65)

동적 셔플링을 이용한 MPEG기반의 동영상 암호화 방법에 관한 연구

이지범[†], 이경학[††], 고형화[†††]

요 약

본 논문에서는 MPEG 기반의 동영상 데이터를 보호하기 위한 알고리즘을 제안하였다. 기존의 고정된 셔플링 테이블을 사용하는 단순 전치 암호화의 경우 계산량이 적은 반면에 선택적 평문 공격에 취약한 단점을 가지고 있다. 이러한 단점을 보완하기 위해서는 프레임 단위로 셔플링 테이블을 동적으로 생성해야 하는데 이 경우, 동적인 셔플링 테이블 생성 시간과 키를 관리하는 것이 문제가 된다. 이러한 문제를 해결하기 위해 영상의 특징에 따라 적응적으로 변하는 인터리빙 알고리즘을 제안하고 이를 이용하여 DPCM 처리된 8*8 블록을 셔플링하여 일차적으로 영상을 스크램블링한 후 기존의 랜덤 셔플링 테이블을 이용하여 최종적으로 영상을 암호화하였다. 실험 결과 기존의 SEED를 이용한 암호화 방식에 비해 수행 시간이 약 10% 정도에 불과했고 암호화에 따른 압축률 감소 등의 문제는 보이지 않았다. 동영상 암호화는 인트라 프레임에 대해서는 정지 영상과 동일한 방식의 암호화 방법을 적용하고 예측 프레임에서는 DC 계수 및 AC 계수에 비해 상대적으로 데이터량이 적으면서 암호화 효과가 좋은 움직임 벡터를 대상으로 암호화하였고 예측 프레임내의 인트라 블록에 의한 암호화 효과가 떨어지는 것을 방지하기 위해 매크로 블록 셔플링 알고리즘을 이용하였다.

A Study on Video Data Protection Method based on MPEG using Dynamic Shuffling

Ji-Bum Lee[†], Kyoung-Hak Lee[††], Hyung-Hwa Ko[†††]

ABSTRACT

This dissertation proposes digital video protection algorithm for moving image based on MPEG. Shuffling-based encryption algorithms using a fixed random shuffling table are quite simple and effective but vulnerable to the chosen plaintext attack. To overcome this problem, it is necessary to change the key used for generation of the shuffling table. However, this may pose a significant burden on the security key management system. A better approach is to generate the shuffling table based on the local feature of an image. In order to withstand the chosen plaintext attack, at first, we propose a interleaving algorithm that is adaptive to the local feature of an image. Secondly, using the multiple shuffling method which is combined interleaving with existing random shuffling method, we encrypted the DPCM processed 8*8 blocks. Experimental results showed that the proposed algorithm needs only 10% time of SEED encryption algorithm and moreover there is no overhead bit. In video sequence encryption, multiple random shuffling algorithms are used to encrypt the DC and AC coefficients of intra frame, and motion vector encryption and macroblock shuffling are used to encrypt the intra-coded macroblock in predicted frame.

Key words: MPEG(동영상 압축), Dynamic Shuffling(동적 셔플링), Video Protection(동영상 데이터 보호), Interleaving(인터리빙)

※ 교신저자(Corresponding Author) : 이지범, 주소 : 서울시 노원구 월계동 447-1(139-701), 전화 : 02)940-5137, FAX : 02)940-5137, E-mail : haje@rifatron.com
접수일 : 2006년 10월 10일, 완료일 : 2006년 10월 26일
[†] 이화트론 주식회사 (E-mail : haje@rifatron.com)
[††] 한국산업기술평가원 선임연구원 (E-mail : goldbug@itep.re.kr)
[†††] 광운대학교 전자통신공학과 교수 (E-mail : hhkoh@kw.ac.kr)

1. 서 론

인터넷의 급속한 발달로 인해 인터넷을 통한 방송이나 MPEG(Moving Picture Experts Group) 영상 서비스, 화상 회의, 감시 카메라 등의 서비스도 발달하게 되었다. 인터넷 방송이나 영상 서비스 등과 같이 모든 사람이 그 내용을 보게 하기 위한 것이 있는가 하면 화상 회의나 감시 카메라와 같이 특정 대상인만 그 내용을 볼 수 있고 관련 없는 사람들에게는 보안상의 이유로 그 내용을 숨겨야 할 필요가 있는 것이 있다. 이에 따라 디지털 영상 데이터의 보호 문제가 대두되었다. 이러한 디지털 영상 데이터 보호 방법에는 암호화와 워터마킹, 전자서명 등이 있다[1]. 디지털 영상 암호화는 원래의 영상을 특정한 암호 키에 의해 변형 또는 암호화함으로써 복호 키(Decryption key)를 가진 수신자만이 원래의 영상을 복원할 수 있도록 하는 기술이다. 최근 몇 년간 영상 데이터를 보호하기 위한 다양한 암호화 알고리즘에 대한 연구가 이루어지고 있다. 그러나 대부분의 기존 디지털 영상 암호화 방법은 RSA, DES(Data Encryption Standard)와 같은 텍스트 데이터 암호화를 영상 데이터에 직접적으로 적용하기 때문에 계산량이 많은 것이 문제가 되었다[2,3]. 이러한 문제를 극복하기 위해서 영상의 특징을 반영하여 영상의 내용 일부를 판단할 수 없도록 부분적으로 암호화한다거나 또는 시각적으로 내용 판단을 하기가 어렵도록 중요 부분을 선택적으로 암호화하는 방법들이 소개되었다[4-8]. 그러나 이러한 방법은 경우에 따라서 압축 효율을 저하시키거나 암호화 강도가 낮다는 문제점을 가지고 있다. 이와 같은 문제점을 개선하여 암호화 후 압축률에 전혀 변화가 없고, 계산량이 적으면서 평문 공격에 강인한 암호화 알고리즘을 제안하였다.

2. 기존의 MPEG 동영상 암호화

Meyer와 Gadegast[4]는 MPEG-1 동영상 데이터를 4단계로 구분하고 헤더 및 인트라 블록을 단계별로 선택하여 블록 암호화 알고리즘(DES or RSA)을 적용하는 암호화 알고리즘을 제안하였고, T.B. Maples와 G.A Spanos[5]도 인트라 프레임에만 DES 암호화를 적용하여 전체적인 암호화 데이터량을 줄이는 선택적 암호화 알고리즘을 제안하였다. I. Agi와 L. Gong[6]은 인트라 프레임만의 암호화 방식이 전방향(Forward) 또는 양방향(Bidirectional) 예측 프레임내에서 예측되지 않은 인트라 매크로 블록 때문에 암호화 효과가 떨어지는 문제점이 있음을 지적하고 이런 문제점을 보완하기 위해서는 모든 데이터의 암호화가 필요함을 보였다.

2.1 전체 데이터 암호화(Naive algorithm)

MPEG 비트 스트림을 암호화하는 가장 직접적인 방법은 DES와 같은 표준 블록 암호화 알고리즘을 사용하는 것이다. 이 방법을 전체 데이터 암호화 또는 Naive algorithm 이라고 한다. 전체 데이터 암호화 알고리즘은 MPEG 비트 스트림을 기존의 텍스트 데이터로 취급하고 특정 MPEG 구조를 사용하지 않는 것이다.

DES나 RSA를 동영상 데이터에 직접 적용하는 경우 암호화의 보안성 측면에서는 만족할 수 있으나 암호화시에 걸리는 시간이 문제가 된다. 영상 데이터의 경우 일반적인 데이터와 달리 영상 자체를 완벽하게 볼 수 없도록 하는 것보단 서비스의 등급에 따라 일부 내용만을 볼 수 있도록 하는 것이 오히려 더 효율적일 수 있다.

2.2 선택적 암호화(Selective or partial algorithm)

선택적 암호화는 DES나 RSA와 같은 블록 암호화 알고리즘을 사용하되 데이터 전체를 암호화하지 않고 MPEG의 계층 구조를 이용하여 일부 데이터만을 암호화하는 방법이다. 가장 기본적인 선택적 알고리즘은 MPEG 프레임 구조를 기반으로 하는 것이다.

Tang은 DCT 변환된 8*8 블록의 ZigZag 패턴에 랜덤 순열 테이블을 적용하여 1*64 벡터 형태로 표현하는 암호화 알고리즘을 제안하였다[7]. 연산량이 적은 반면에 순열 테이블이 평문 공격에 의해서 깨질 수 있는 단점과 ZigZag 패턴의 변화로 인하여 데이터량이 최대 50% 정도까지 증가하는 문제가 있다.

Qiao와 Nahrstedt는 압축된 MPEG 비트 스트림을 암호화하는 동영상 암호화 알고리즘(Video Encryption Algorithm : VEA)을 제안하였다[8]. MPEG의 픽처층(Picture layer)에 해당되는 모든 데이터를 암호화하는 것으로 먼저 비트 스트림을 128 바이트 단위로 쪼개서 나누고 이것을 다시 두개의 64 바이트 블록으

로 나눈 후, 두개의 64 바이트 블록을 XOR하여 1차 암호화된 64 바이트 블록을 생성한 후 이것을 최종적으로 DES를 이용하여 암호화한다.

W. Zeng은 DCT 영역에서 DC 및 AC 계수의 부호를 변환하거나 매크로 블록간의 셔플링, 회전 등을 이용하여 영상을 왜곡시키는 알고리즘과 슬라이스 단위로 DCT 블록내의 동일한 위치의 계수 값들을 모아서 셔플링하는 알고리즘을 제안하였다[9,10].

G. Liu는 DC 계수는 DES를 이용하여 암호화하고 AC 계수는 런-길이 값(Event list)을 셔플링하는 선택적 암호화 알고리즘을 제안하였다[11].

Kim은 예측 프레임에서 움직임 벡터를 이용한 암호화를 제안하였다[12]. MPEG 동영상에서는 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. 단점으로 움직임 벡터 방향 변화에 의해 비트량의 증가가 발생한다.

3. 셔플링 기반의 영상 암호화

일반적인 경우 암호화 강도는 셔플링 공간의 크기가 n 이라면 n!의 값을 갖는다. 그런데 평문 공격의 경우 암호화 강도가 n의 반복횟수와 약간의 요소간 비교 계산으로 기하급수적으로 떨어진다. 특히 특정한 형태의 평문을 공격자가 무한대로 가지고 있거나 만들 수 있는 상황에서의 공격(chosen text attack) 시에는 공격의 반복 횟수는 최소 1회로 떨어질 수 있다. 즉, 이 경우 공격자는 1회의 반복 및 약간의 추가적인 연산에 의해서 셔플링 테이블를 알 수 있거나 사용된 암호화키를 알 수 있게 된다. 만약 셔플링 테이블이 고정되지 않고 시간이나 또는 영상의 국소적인 특징에 따라 가변적으로 변한다면 현재 구한 셔플링 테이블은 의미가 없기 때문에 공격자는 매번 동일한 반복행위를 해야 하고 실제적인 해킹에 어려움이 있다고 볼 수 있다. 따라서 보안성을 높이기 위해서 랜덤 셔플링 테이블을 시간에 따라 지속적으로 변경해줘야 하는데 이 때 비밀키 관리의 문제점과 랜덤 테이블을 지속적으로 만드는데 소요되는 계산량이 문제가 된다.

4. 제안한 동영상 암호화

영상 데이터 암화화시 암호화 시간을 줄이기 위해서는 MPEG 압축 방법의 특성을 최대한 활용할 수 있어야 한다. 영상 데이터의 복원 과정에서 올바른 영상 복원을 위해 필요한 중요 정보에는 인트라 프레임의 DC, AC 계수, 예측 프레임에서의 움직임 벡터 등이 있다. 일반적으로 인트라 프레임에 대해서는 정지 영상 암호화 방법을 그대로 적용하여 DC 계수와 AC 계수를 암호화 하고 예측 프레임에 대해서는 동영상 데이터의 중요 정보의 하나인 움직임 벡터를 암호화하는 방법을 이용한다[12,13]. 움직임 벡터 암호화의 경우 움직임 벡터가 존재하지 않은 예측 프레임의 인트라 블록의 경우에는 암호화를 할 수가 없다. 이러한 문제점을 해결하기 위해 예측 프레임에서의 매크로 블록 단위의 셔플링 방법을 추가적으로 이용해서 암호화를 수행하였다. 또한 매크로 블록 단위의 셔플링시 움직임 벡터 값에 의한 비트량 증가가 발생할 수 있는데 이를 방지하기 위해 움직임 벡터의 차분 값을 먼저 구한 후 셔플링하였다. 그림 1은 제안된 영상 데이터 암호화의 블록도를 나타낸다.

4.1 영상특징에 따라 가변적인 셔플링 방법

4.1.1. 제안한 인터리빙

제안한 인터리빙은 아래의 순서에 의해서 수행되어 진다.

step 1 : 셔플링 요소를 원래 순서형태로 배열한다.
step 2 : 첫 번째 요소는 재배치하지 않고 상태 값만 1로 한다.
step 3 : 첫 번째 요소에서 특징 값을 구한다.
step 4 : 구해진 특징 값과 간격지수와의 XOR 연산을 수행한다. 이 결과 값을 재배치 간격이라 한다.

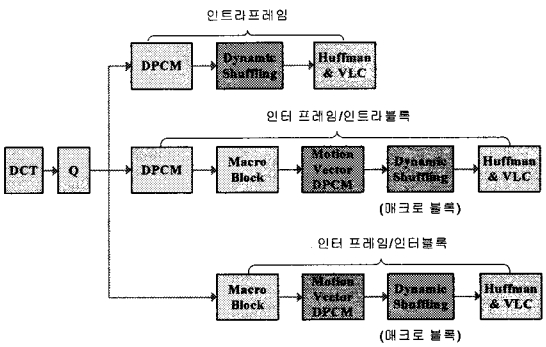


그림 1. 영상 데이터 암호화 블록도

step 5 : 계산된 재배치 간격의 값만큼 떨어져 있는 위치의 요소가 첫 번째 요소 다음에 위치한다. 해당 위치 요소의 상태 값을 1로 한다.

step 6 : 3단계와 5단계의 과정을 반복한다. 다만 첫 번째 요소가 아닌 현재의 요소를 기준으로 다음 요소의 위치를 구한다. 만약 현재 요소가 마지막 요소이면 1회 반복이 끝나고 처음으로 되돌아간다.

step 7 : 반복횟수만큼 6의 과정을 수행하고 모든 상태 값이 1이거나 제한된 반복 횟수가 되면 종료한다.

배열의 크기가 13인 "KOREA FIGHTING"의 문자열이 인터리빙에 의해서 섞이는 과정을 예를 들면 다음과 같다. 그림 2는 인터리빙전의 초기 메모리 상태를 나타낸다.

요소의 정상 순서	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 12, 13
재배치 간격	3, 1, 2, 1, 2, 1, 2, 3, 1, 1, 3, 2, 1
상태 코드 값	0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
최대 반복 횟수	3

step 1 : 첫 번째 요소인 "1"은 재배열되지 않고 현재의 위치 값을 갖는다. 첫 번째 요소로부터 구한 재배치 간격 값이 "3"이므로 첫 번째 요소로부터 거리가 3 떨어져 있는 4번째 요소가 재배치된다.

step 2 : 4번째 요소의 재배치 간격이 "1"이므로 5번째 요소가 재배치된다. 배열 색인 값을 증가하면서 계속적인 반복을 수행한다. 11번째 요소의 재배치 간격이 3으로서 다음 위치 값은 14번째 요소이나 배열에는 14번째 요소가 없으므로 11번째 요소가 마지막 재배치 요소가 되고 첫 번째 pass 가 끝난다.

배열 색인	1	2	3	4	5	6	7	8	9	10	11	12	13
재배치전의 원래 요소	K	O	R	E	A	F	I	G	H	T	I	N	G
상태 값	0	0	0	0	0	0	0	0	0	0	0	0	0
인터리빙에 의해 재배치된 요소들	0	0	0	0	0	0	0	0	0	0	0	0	0

그림 2. "KOREA FIGHTING" 이라는 문자열의 재배치를 위한 초기 메모리 상태

배열 색인	1	2	3	4	5	6	7	8	9	10	11	12	13
재배치전의 원래 요소	K	O	R	E	A	F	I	G	H	T	I	N	G
상태 값	1	0	0	1	1	0	1	0	1	1	1	0	0
재배치 배열 색인	1	4	5	7	9	10	11						
인터리빙에 의해 재배치된 요소들	K	E	A	I	H	T	I	0	0	0	0	0	0

그림 3. 첫 번째 pass 후의 메모리 상태

그림 3은 첫 번째 pass후의 메모리 상태이다.

step 3 : 동일한 과정을 거쳐 두 번째 pass에서 2, 3, 8번째 요소가 재배치된다.

step 4 : 3번째 pass는 아직 재배치되지 않은 6번째 요소부터 시작한다. 6번째 요소의 재배치 간격이 "1"이고 이후로 재배치되지 않은 요소들 중에서 6번째 요소로부터 1만큼 떨어져 있는 12번째 요소가 재배치된다. 12번째 요소의 재배치 간격이 "2" 이므로 13번째 마지막 요소는 재배치되지 않고 3번째 pass가 종료된다.

step 5 : 최대 반복 횟수를 3으로 정했으므로 전체 요소 중 재배치되지 않은 요소를 순서대로 재배치한다.

그림 4는 재배치 완료후의 메모리 상태를 나타낸다.

4.1.2 인터리빙과 랜덤 셔플링의 결합

본 논문에서는 기존의 랜덤 셔플링 테이블을 이용한 방법의 최대 약점인 평문공격(특히, chosen-text attack)에 대한 강인성을 보강하기 위해 고정된 형태의 셔플링이 아닌 영상의 특징에 의해서 불규칙한 셔플링 형태를 갖는 방법을 제안하였다.

제안된 인터리빙 방법은 영상의 특징 값과 간격 지수에 의해 인터리빙 형태가 불규칙하게 나타나므로 인터리빙으로 나타나는 결과를 기존의 랜덤 셔플링 테이블을 이용하여 2차적으로 재배열을 한다면

배열 색인	1	2	3	4	5	6	7	8	9	10	11	12	13
재배치전의 원래 요소	K	O	R	E	A	F	I	G	H	T	I	N	G
상태 값	1	1	1	1	1	1	1	1	1	1	1	1	1
재배치 배열 색인	1	4	5	7	9	10	11	2	3	8	6	12	13
인터리빙에 의해 재배치된 요소들	K	E	A	I	H	T	I	O	R	G	F	N	G

그림 4. 인터리빙에 의한 재배치 완료후의 메모리 상태

최종적인 랜덤 셔플링이 일정한 형태가 아닌 불규칙한 형태를 나타내게 되어 공격자가 이미 알고 있는 암호화 전의 평문도 1차의 인터리빙의 결과에 의해 원래의 평문과는 다른 형태로 만드는 특징을 갖게 된다. 따라서 인터리빙과 랜덤 셔플링 방법을 결합하면 평문 공격에도 강인한 암호화 방법이 될 수 있다.

4.1.3. 제안한 알고리듬을 이용한 암호화

암호화 과정은 다음의 절차에 의해 이루어진다.

step 1 :. 입력되는 프레임이 인트라 프레임인지 예측(인터) 프레임인지 구분한다.

step 2 : 인트라 프레임의 경우는 다음의 절차를 수행한다

2.1. 셔플링 원소 및 셔플링 공간의 크기를 결정한다.

2.2. 임의의 Seed 값을 이용하여 랜덤 셔플링 공간의 크기에 맞는 랜덤 수를 생성한다.

2.3. 각 블록을 DCT, 양자화를 수행하고, 양자화된 블록에서 DPCM 값을 구한다.

2.4. 제안한 인터리빙 절차에 의해 블록의 특징값, 재배치 간격 등을 구한다. 특징 값은 DPCM 계수의 하위 4비트로 하였다.

2.5. 블록을 인터리빙 절차에 의해 재배치한다. 재배치 반복 횟수는 3회로 제한한다.

2.6. 재배열된 블록을 다시 랜덤수로 생성된 셔플링 테이블에 의해 무작위로 섞는다.

2.7. 섞여진 블록을 런길이 및 허프만 부호화 등을 거쳐 MPEG부호화를 수행한다.

step 3 : 인터 프레임의 경우 다음의 절차를 수행한다.

3.1 모든 8*8 블록의 DPCM 값을 구하고 이를 DC 계수와 교체한다.

3.2 움직임 벡터를 구한다.

3.3 차동 움직임 벡터의 DPCM 부호화한 후 암호화 한다.

3.4 예측 프레임내에 있는 인트라 매크로 블록에 의해서 기밀성이 떨어지는 것을 방지하기 위해 매크로 블록을 셔플링한다.

3.5 매크로 블록 셔플링시 호환성을 유지하기 위해서 경계 영역 내에 있는 매크로 블록은 건너뛴 블록과 교체되지 않도록 한다.

step 4 : 허프만 부호화 및 가변길이 부호화를 수행한다.

5. 모의 실험

실험 동영상은 Akiyo, Foreman, Stefan 시퀀스를 이용하였고 CIF(352*288)포맷의 해상도를 가지며, GOP 구성은 인트라 프레임, 순방향 예측 프레임(Forward prediction frame)으로 구성되어 있으며 GOP 크기는 15로 하였으며 전체 영상은 60 프레임으로 구성하였다. 양자화 스케일 값은 7로 고정하였다.

표 1은 실험에 사용된 동영상 시퀀스에 대한 분석표로서 예측 프레임에서 인트라 블록으로 부호화되는 경우, 부호화된 블록의 수, 건너뛴 매크로 블록의 수, 전방향 움직임 벡터가 있는 경우 등을 조사한 결과표이다. 전체 매크로 블록의 수는 396개 이고 부호화될 블록 수는 2376개이다.

5.1 인트라 프레임만을 암호화하는 경우

인트라 프레임 암호화는 상대적으로 적은 암호화 데이터를 이용하여 동영상을 암호화할 수 있는 방법이다. 인트라 프레임을 참조하여 영상을 복원하는 예측 프레임의 경우 인트라 프레임의 정확한 복원 없이는 올바르게 영상을 복원할 수 없기 때문이다. 인트라 프레임만을 암호화하는 경우 표 1에 나타난 것과 같이 Akiyo 영상과 같이 움직임이 없고 건너뛴 매크로 블록이 40% 이상인 영상의 경우 인트라 프레임의 암호화 효과가 예측 프레임에도 상당히 많은 영향을 주는 것을 확인할 수 있다. 그러나 움직임이 너무 커서 예측 부호화할 수 없고 인트라 매크로 블록으로 부호화해야 할 블록이 10% 이상을 차지하는 Stefan 영상의 경우 상대적으로 암호화 효과가 낮다고 볼 수 있다. 따라서 인트라 프레임에만 암호화하는 것이 암호화 시간을 줄일 수 있는 장점이 있지만 일부 움직임이 큰 동영상에서는 암호화 능력이 떨어

(a) (b) (c)

그림 5. 실험 동영상 : (a) akiyo, (b) foreman, (c) stefan

표 1. 사용된 데이터의 특성 분석

Frame	Akiyo	Foreman	Stefan
P1	0(0%)	7(1.8%)	19(4.8%)
	687(28.9%)	1850(77.9%)	2006(84.4%)
	131(33.1%)	5(1.3%)	4(1%)
	23(5.8%)	269(67.9%)	250(63.1%)
P5	0(0%)	4(1%)	124(31.3%)
	454(19.1%)	1840(77.4%)	2036(85.7%)
	203(51.3%)	4(1%)	2(0.5%)
	39(9.8%)	227(57.3%)	130(32.8%)
P10	0(0%)	2(0.5%)	108(27.3%)
	481(20.2%)	1830(77%)	2084(87.7%)
	197(49.7%)	3(0.8%)	1(0.3%)
	41(10.4%)	327(82.6%)	187(47.2%)
P14	0(0%)	23(5.8%)	36(9.1%)
	544(22.9%)	1923(80.9%)	2070(87.1%)
	197(49.7%)	3(0.8%)	1(0.3%)
	57(14.4%)	268(67.7%)	273(68.9%)

표 설명

예측 프레임 번호	인트라 매크로 블록 수
	부호화된 8*8 블록 수
	건너뛴 매크로 블록 수
	움직임 벡터가 존재하는 매크로 블록 수

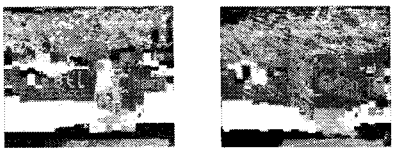
지므로 예측 프레임에도 효과적인 암호화가 적용되어야한다.

5.2 움직임 벡터 암호화

일반적으로 MPEG에서 차동 움직임 벡터의 수평 성분과 수직 성분의 값을 가변길이 부호화하여 전송한다. 이 때 수평 성분과 수직 성분을 랜덤 셔플링 테이블을 이용하여 불규칙하게 교환하게 되면 움직임 벡터의 교환 여부를 알지 못하는 수신자의 경우 영상을 올바르게 복원할 수 없게 된다[12,13]. 그림 6은 움직임 벡터의 잘못된 복구에 의해서 영상이 왜곡된 형태를 보여주며, 영상의 왜곡은 참조 프레임인 인트라 프레임으로부터 시간적으로 멀리 떨어진 프레임일수록 왜곡의 형태가 눈에 띄게 증가함을 볼 수 있다. 그렇지만 그림 6의 (c) 영상과 그림 7의 (a) 영상을 비교했을 때 움직임 벡터 암호화는 예측 부호화되지 않는 인트라 블록수가 많은 영상에서는 암호화효과가 인트라 프레임만을 암호화했을 때와 큰 차이가 없음을 확인할 수 있다.

(a) (b) (c)

그림 6. 인트라 프레임 암호화에 의한 예측 프레임의 영향 (5번째 예측 프레임) : (a) akiyo, (b) foreman, (c) stefan

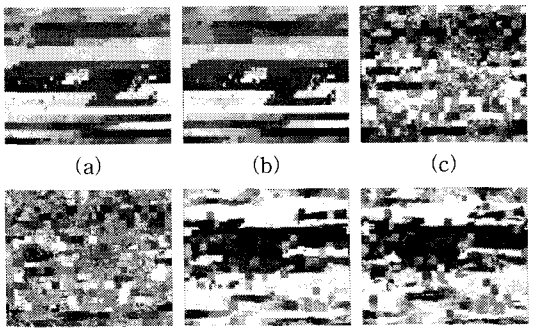


(a) (b)

그림 7. 움직임 벡터 암호화(Stefan) : (a) 5번째 예측 프레임, (b) 14번째 예측 프레임

5.3 매크로 블록 셔플링을 이용한 예측 프레임 암호화

본 논문에서는 움직임 벡터 암호화의 단점을 개선하기 위해 예측 프레임에서 움직임 벡터 암호화와 매크로 블록 셔플링 알고리즘을 제안하였다. 그림 8에서와 같이 제안된 암호화 알고리즘을 이용하였을 때 암호화 효과가 모든 프레임에서 나타남을 확인할 수 있었다. Kim[12]이 제안한 움직임 벡터 암호화의 경우, 적은양의 연산으로 영상 정보를 상대적으로 많이 왜곡시킬 수 있지만 움직임 벡터가 존재하지 않은 경우는 암호화 효과가 떨어지는 단점이 있다. Kim이 제안한 움직임 영상 데이터 암호화의 경우 움직임 벡터 변환에 의해 압축 시간은 약 1.2 -1.5% 정도가



(a) (b) (c)

(d) (e) (f)

그림 8. 제안한 방법에 의한 암호화 : (a) 5번째 예측 프레임(akiyo), (b) 14번째 예측 프레임(akiyo), (c) 5번째 예측 프레임(stefan), (d) 14번째 예측 프레임(stefan), (e) 5번째 예측 프레임(foreman), (f) 14번째 예측 프레임(foreman)

표 2. 암호화 알고리즘의 성능 비교표

구분	제안방법	Tang[7]	Kim[12]	Qiao[8]
연산 종류	XOR(k*n bit) Random shuffling	Random shuffling	산술 연산: arctan	XOR, 64바이트 DES
암호 종류	가변적 전치	고정 전치	부호 비트 변경 움직임 벡터	XOR, 블록 암호
암호화 강도(암호문 단독 공격)	n! (n은 영상의 8*8 블록 개수)	n!+n!=64!+64! n은 64로 고정	2^{64} (64bit 암호키)	64바이트 단위의 DES
암호화 강도(평문 공격)	$n*r*2^{k*n}$	2*n(두개의 랜덤 순열 테이블 사용)	n(n=64)	64 바이트 단위의 DES
인트라 프레임	DC, AC 계수 위치 변환	8*8 DCT 블록내 계수 위치 변환	DC/AC의 부호 변환	적용 안됨
인터 프레임	움직임 벡터, 매크로 블록	8*8 DCT 블록내 계수	움직임 벡터	적용 안됨
비트량 증가	0%	25-50%	1.4-2.5%	0%
암호화 공간	DCT 계수	DCT 계수	매크로 블록	bit stream 영역
MPEG 호환성	지원	지원	부분 지원	없음

증가하고, 데이터량은 1.4 - 2.5% 증가하였다. Tang이 제안한 방법의 경우 암호화 시간은 빠른 편에 속하나 압축률 감소가 25 - 50% 정도까지 발생하는 문제와 평문 공격 및 암호문 단독 공격에 약한 단점이 있다[7]. 본 논문에서 제안한 방식의 경우 압축률에 변화가 없고 또한 비트 스트림 호환성을 지켜주는 장점이 있고, 평문 공격에 강한 장점이 있다. 반면에 셔플링 테이블 암호화 방식으로 구현되기 때문에 암호화 강도를 높이기 위해서 상대적으로 많은 메모리를 요구하는 문제점이 있었다. 표 2는 몇 가지 동영상 암호화 방식에 대한 비교를 보여준다.

6. 결 론

본 논문에서는 영상 데이터의 기밀성을 보장하기 위해 입력 영상에 따라 동적으로 변하는 랜덤 셔플링 테이블을 생성하여 암호화하는 알고리듬을 제안하였다. 추가적인 비트량이 발생하지 않고, 기존 셔플링 기반의 암호화 방식이 가지고 있는 평문 공격에 대한 약점을 보완하고자 영상의 국소적인 특징에 따라 적응적으로 셔플링 테이블을 생성하여 사용하였다. 동영상의 인트라 프레임에서 실험한 결과 기존의 SEED를 이용한 암호화 방식에 비해 수행 시간이 약 10% 정도에 불과했고 암호화에 따른 압축률 감소 등의 문제는 보이지 않았다.

예측 프레임에서는 DC 계수 및 AC 계수에 비해 상대적으로 데이터량이 적으면서 암호화 효과가 좋은 움직임 벡터를 대상으로 암호화하였고 움직임 벡터가 존재하지 않는 인트라 매크로 블록에 의한 암호화 효과가 떨어지는 것을 방지하기 위한 매크로 블록 셔플링 방법의 암호화를 이용하였다. 또한 MPEG-2의 비트 스트림 호환성을 100% 만족시켜, 헤더 정보를 이용한 트릭 모드와 같은 편리 기능들을 그대로 사용할 수 있다.

향후 과제로는 메모리 사용량을 줄이는 방법에 대한 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] 원치선, "디지털 영상의 저작권 보호," 정보과학회지 제 15권 제 12호, pp.22-27, 1997. 12.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystem," *Comm. ACM*, Vol. 21, No.2, pp.120-126, 1978.

[3] B. Furht and D. Socek, *Fundamentals of Multimedia Encryption Techniques*, Multimedia Security Handbook, CRC Press, Dec. 2004.

[4] J. Meyer and F. Gadegast, "Security Mechanism for Multimedia with Example MPEG-1 Video," *Tech. Univ. of Berlin*, 1995.

[5] T.B. Maples and G.A. Spanos, "Performance

Study of a Selective Encryption Scheme for the Security of Networked, Real-time Video," *Proc. ICCCN, Las Vegas*, Nevada, Sep. pp.2-10, 1995.

[6] I. Agi and L. Gong, "An Empirical Study of Secure MPEG Video Transmissions," *The Internet Society Symposium on Network and Distributed System Security*, pp.137-144, Feb. 1996.

[7] L. Tang, "Methods for Encrypting and Decrypting MPEG Video Data Efficiently," *Proc. the Fourth ACM International Multimedia Conference*, pp.219-229, 1996.

[8] L. Qiao and K. Nahrstedt, "A New Algorithm for MPEG Video Encryption," *CISST'97 International Conference*, pp21-29, 1997.

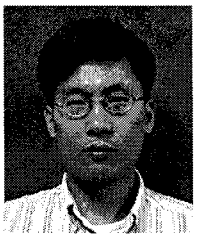
[9] J. Wen, M. Severa, W. Zeng, M. Luttrell, and W. Jin, "A Format Compliant Configurable Encryption Framework for Access Control of Video," *IEEE Trans. Circuits & Systems for Video Technology*, Special Issue on Wireless Video, Vol. 12, Issue 6, pp. 545-557, June. 2002.

[10] W. Zeng and S. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video," *IEEE Trans. Multimedia*, Volume 5, Issue 1, pp. 118-129, March. 2003

[11] G. Liu, T. Ikenaga, S. Goto, and T. Baba, "A Selective Video Encryption Scheme for MPEG Compression Standard," *IEICE Trans. Fundamentals*, Vol. E89-A, No. 1, pp 194-202, Jan. 2006.

[12] 김경호, 권구락, 이태영, 이승현, 고성제, "MPEG-4 비디오 부호화기에서 DCT 계수와 움직임 벡터의 암호화를 이용한 저작권 보호," 한국통신학회, 제18권 1호, pp.144-147, 신호처리합동학술대회, 2005.

[13] 안진행, "멀티미디어 콘텐츠 보호를 위한 디지털 비디오 스크램블링 방법," 석사학위논문, 성균관대학교, 2004.

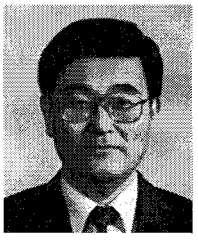


이 지 범

1991년 2월 광운대학교 전자통신공학과(공학사)
1993년 2월 광운대학교 대학원 전자통신공학과(공학석사)
1993년 8월 광운대학교 대학원 전자통신공학과(공학박사)
1996년~2001년 대우통신
2002년~현재 이화트론(주)
관심분야 : 동영상, 워터마킹

이 경 학

1992년 2월 광운대학교 전자통신공학과(공학사)
1994년 2월 광운대학교 대학원 전자통신공학과(공학석사)
2000년 3월~현재 : 광운대학교 대학원 전자통신공학과 박사과정
1994년 4월 ~현재 : 한국산업기술평가원 선임연구원
관심분야 : 동영상, 통신신호처리, DSP



고 형 화

1979년 2월 서울대학교 전자공학과(공학사)
1982년 2월 서울대학교 대학원 전자공학과(공학석사)
1989년 2월 서울대학교 대학원 전자공학과(공학박사)
1985년 3월~현재 : 광운대학교 전자통신공학과 교수
관심분야 : 영상통신, Wavelet 부호화, 임베디드 시스템