레터논문 (Letter Paper)
방송공학회논문지 제25권 제6호, 2020년 11월 (JBE Vol. 25, No. 6, November 2020)
https://doi.org/10.5909/JBE.2020.25.6.1013
ISSN 2287-9137 (Online) ISSN 1226-7953 (Print)

IVC 코덱을 위한 선택적 암호화 및 복호화 방법

이 민 구[a], 김 규 태[a], 장 의 선[a]‡

Selective Encryption and Decryption Method for IVC Codec

Min Ku Lee[a], Kyu-Tae Kim[a], and Euee S. Jang[a]‡

요 약

본 논문에서는 IVC 비트스트림의 시작 코드(Start Code)를 이용한 선택적 암호화 및 복호화 방식을 제안한다. 비디오를 위한 기존의 암호화 방식은 크게 전역 암호화 알고리즘(Naive Encryption Algorithm, NEA)과 선택적 암호화 알고리즘(Selective Encryption Algorithm, SEA)의 2가지 방식으로 분류한다. NEA 방식은 비트스트림의 모든 데이터를 암호화 하기 때문에 보안성이 높지만 계산 복잡도 역시 높은 문제가 있다. SEA 방식은 비트스트림의 일부를 암호화 하여 암호화 속도를 NEA 방식에 비해 개선하였지만 상대적으로 보안성이 낮아지는 문제가 있다. 제안 방식은 IVC 비트스트림의 시작코드를 이용하여 기존 SEA 방식의 보안성을 높이면서 암호화 속도를 개선하였다. 실험 결과 제안 방식은 NEA 방식에 비하여 평균적으로 암호화 속도는 96%, 복호화 속도는 98% 줄일 수 있었다.

Abstract

This paper presents a selective encryption and decryption method exploiting the start code of the IVC bitstream. The existing encryption methods for video are largely classified into two methods: Naive Encryption Algorithm (NEA) and Selective Encryption Algorithm (SEA). Since NEA encrypts the entire bitstream, it has the advantage of high security but has the disadvantage of high computational complexity. SEA improves the encryption and decryption speed compared to NEA by encrypting a part of the bitstream, but there is a problem that security is relatively low. The proposed method improves the encryption and decryption speed and the security of the existing SEA by using the start code of the IVC bitstream. As a result of the experiment, the proposed method reduces the encryption speed by 96% and the decryption speed by 98% on average compared to the NEA.

Keyword : IVC, start code, video encryption

a) 한양대학교 컴퓨터소프트웨어학과(Department of Computer Science, Hanyang University)
‡ Corresponding Author : 장의선(Euee S. Jang)
E-mail: esjang@hanyang.ac.kr
Tel: +82-2-2220-1086
ORCID: https://orcid.org/0000-0002-5312-7078
※ 이 연구는 방위사업청 및 국방과학연구소의 재원에 의해 설립된 신호정보 특화연구센터 사업의 지원을 받아 수행되었음(This work was supported by the research fund of the Signal Intelligence Research Center supervised by the Defense Acquisition Program Administration and Agency for Defense Development of Korea.).
· Manuscript received October 7, 2020; Revised November 9, 2020; Accepted November 9, 2020.

Ⅰ. 서 론

최근 유무선 통신 기술의 발전은 대용량의 데이터를 언제 어디서나 사용 가능하게 하였고 대용량의 비디오 데이터 사용도 크게 증가하고 있다. 통신 기술의 발전으로 대역폭이 점점 증가하지만 비디오 해상도도 증가하기에 저장공간을 효율적으로 이용하기 위한 비디오 압축 기술은 필요하다. 그리고 비디오 압축 기술과 함께 최근 빈번하게 발생하고 있는 인터넷 연결 카메라로의 촬영한 동영상 해킹으로 인한 사생

활 침해와 불법 다운로드를 통한 유료 비디오 콘텐츠의 유출로 인해 비디오 보호 기술의 필요성이 증대되고 있다.

대표적인 비디오 보안 알고리즘은 크게 2가지로 전역적 암호화 알고리즘(Naive Encryption Algorithm, NEA)와 선택적 암호화 알고리즘(Selective Encryption Algorithm, SEA)이 있다. NEA는 비디오 비트스트림 전체를 암호화 한다. 전체 비디오 비트스트림을 암호화 하기 때문에 NEA는 뛰어난 보안성을 갖지만 계산 복잡도가 매우 크다. 반면에 SEA는 비디오 비트스트림에서 일부분을 선택하고 암호화 하여 NEA의 계산 복잡도를 낮추었다. 하지만 일반적으로 SEA에 의해 암호화된 비디오 비트스트림은 암호 해제하지 않고도 디코딩이 가능한데 암호화된 일부분으로 인해 영상 화질의 왜곡이 발생하여 영상 정보를 온전하게 파악하기 어렵지만 대략적인 내용 파악이 가능하여 보안성이 낮은 문제가 있다.

본 논문에서는 국제 표준 비디오 코덱 중에서 라이센스를 지불하지 않아도 되어 범용적으로 사용한 코덱인 IVC의 비트스트림 중에서 시작 코드와 인접한 일부분을 뒤섞는 새로운 방식의 선택적 암호화 방식을 제안하고자 한다. 제안 방식은 NEA의 계산 복잡도 문제와 SEA의 보안성 문제를 개선하였다.

Ⅱ. NEA와 SEA

최근 수년 동안 NEA의 계산 복잡도를 줄이기 위한 여러 SEA에 관한 연구들이 있었다. Secure MPEG (SECMPEG)[1]와 Aegis[2]는 일반적으로 비디오 디코더에서 압축된 비트스트림을 복원하는데 있어서 필수 요소인 I 프레임 또는 키 프레임만 선택적으로 암호화하는 SEA이다. 압축 비트스트림 내에서 I 프레임을 선택적으로 암호화 하면 I 프레임을 참조하여 재구성하는 P와 B 프레임도 정상적으로 재구성하지 못하게 할 수 있어 효과적인 선택적 암호화 방법일 수 있다. 하지만 전체 압축 비트스트림 중에서 I 프레임이 차지하는 비중은 일반적으로 30~60%를 차지하므로 NEA에 비해 계산 복잡도는 크게 줄어들지는 않았다.

지그재그 순열 알고리즘[3]은 비디오 압축 과정 중 I 프레임을 생성하는 과정에서 DCT 이후에 지그재그 순서로 변형계수를 정렬하는데 변형계수를 선택하고 재배열하여 암호화하는 SEA이다. 지그재그 순열 알고리즘은 NEA에 비해 계산 복잡도는 1.56%이었지만 변형 계수의 순서를 재배열하는 것이 비트스트림의 크기를 대략 50% 증가시키는 문제가 있었다.

Video encryption algorithm(VEA), modified VEA(MVEA), real-time VEA(RVEA)는 I 프레임에서 DCT 계수들의 부호 비트와 P, B 프레임에서 움직임 벡터들의 부호 비트를 선택하여 암호화하는 SEA이다[4]. DCT 계수들과 움직임 벡터들의 부호 비트는 전체 비트스트림 중에서 차지하는 비중이 작아 NEA에 비해 RVEA의 계산 복잡도는 10%이었다. 하지만 단순히 모든 암호화된 DCT 계수를 128로 설정하고 모든 암호화된 AC 계수를 양수로 수정하는 것만으로도 유용한 비디오 정보를 복원할 수 있어 비디오 정보를 철저하게 보호하지는 못하는 문제가 있었다.

Ⅲ. 제안 방식

본 논문에서는 비디오 비트스트림에 일반적으로 포함되어 있는 시작 코드와 인접하고 비디오 디코딩에 있어 중요한 일부분을 선택적으로 암호화하는 새로운 방식을 이용하여 기존의 SEA 보다 보안성이 높고 빠른 암호화 방식을 제안하고자 한다.

국제 표준 비디오 코덱 중에서 IVC는 동영상 압축 기술들 중에서 특허 사용료 기간이 만료되어 라이센스 비용을 지불하지 않아도 되는 기술들을 모아 유료 코덱인 H.264/AVC의 하이 프로파일과 비슷한 객관적 및 주관적 화질을 목표로 개발된 무료 코덱이다. 본 논문에서는 무료 코덱인 IVC가 기술 사용료 없이 범용적으로 사용할 수 있어 IVC 코덱에 제안 방식을 적용해 보았다. IVC 비트스트림 구조를 분석해 보니 현재 널리 사용되고 있는 국제 표준 비디오 코덱인 H.264/AVC, HEVC 비트스트림와 같이 시작 코드로 최상위 레벨의 유닛을 구별하고 있었다. 그리고 시작 코드 바로 다음에 오는 한 바이트 크기의 비트스트림은 시작 코드 타입이었다. IVC 표준 문서[5]에 따르면 시작 코드 타입은 표 1과 같이 정의되어 있는데 디코딩 과정에서는 먼저 시작 코드 타입을 파싱하고 이 시작 코드 타입에 따라 비트스트림에서 시작 코드 타입 다음에 오는 페이로드를 다른 함수로 복원하기 때문에 시작 코드 타입은 디코딩에 있어 아주 중요한 부분이다. 제안 방식에서는 비트스트림

표 1. IVC 비트스트림에서 시작 코드 타입
Table 1. Start code type in IVC bitstream

Start Code Type	Start Code Name
0x00 ~ 0xAF	slice start code
0xB0	video sequence start code
0xB1	video sequence end code
0xB2	user data start code
0xB3	i frame start code
0xB4	reserved
0xB5	reserved
0xB6	pb frame start code
0xB7	video edit code
0xB8	reserved

안에 제 위치에 있어야 하는 시작 코드 타입들을 서로 뒤섞어 암호화 하였다.

시작 코드 타입은 표 1과 같이 0x00에서부터 0xB8까지 “reserved”로 분류된 3가지를 제외하고 182가지의 경우의 수를 갖는다. 시작 코드 타입이 뒤섞여진 암호화된 비트스트림을 원본 비트스트림으로 복원하기 위한 최악의 경우의 수는 182^182으로 거의 무한대에 가까운 수이다. 선형 검색이라고 가정해도 평균 경우의 수는 (182^182)/2으로 이 또한 무한대에 가까운 수이다. 게다가 각 경우의 수가 복원 가능한지에 대해 디코딩 과정을 통해 확인해야 하기 때문에 182개의 시작 코드 타입을 뒤섞는 제안 방식은 풀기 어려운 암호화 방식이다. 무엇보다도 시작 코드가 뒤섞여진 암호화된 비트스트림은 디코딩이 불가하여 디코딩이 가능한 기존의 SEA 보다 높은 보안성을 갖을 수 있다.

그림 1은 제안 방식이 적용된 IVC 비트스트림의 예제이다. IVC 비트스트림에서는 노란색으로 표시된 0x000001의 3바이트 크기의 워드를 시작 코드로 정의한다. 시작 코드 다음에 오는 빨간색으로 표시된 한 바이트가 시작 코드 타입이다. 제안된 암호화 방식을 통해 그림 1-(a)의 IVC 원본 비트스트림에서 시작 코드로 시작 코드 타입인 0xB0, 0xB2, 0xB3, 0x00, 0xB6을 찾아 182가지의 시작 코드 타입 원본 값과 서로 다른 값의 변경 값을 갖는 변경 테이블을 통해 각각 그림 1-(b)의 IVC 암호화된 비트스트림과 같이 0x70, 0x4A, 0x65, 0x78, 0x03으로 변경하여 암호화한다. 제안된 복호화 방식을 통해 그림 1-(b)의 IVC 암호화된 비트스트림에서 시작 코드로 변경된 시작 코드 타입인 0x70, 0x4A, 0x65, 0x78, 0x03을 찾아 암호화 시 사용한 변경 테이블을 통해 각각 그림 1-(a)의 IVC 복호화된 비트스트림과 같이 0xB0, 0xB2, 0xB3, 0x00, 0xB6으로 복원하여 IVC 원본 비트스트림과 같이 복호화한다.

제안 방식에서 암호화를 위해 IVC 비트스트림 전체에서 선택한 시작 코드 타입들의 비중을 실험을 통해 조사해 보니 평균적으로 0.2%이었다. 앞서 Ⅱ장에서 언급한 기존의 SEA의 경우에 NEA에 비해 SECMPEG는 30~60%, 지그재그 순열 알고리즘은 1.56%, RVEA는 10%의 계산 복잡도를 가진 것에 비해 제안 방식은 암호화를 위해 선택한 부분이 작아보이므로 기존의 SEA 보다 빠른 암호화 방식이 가능해 보인다.

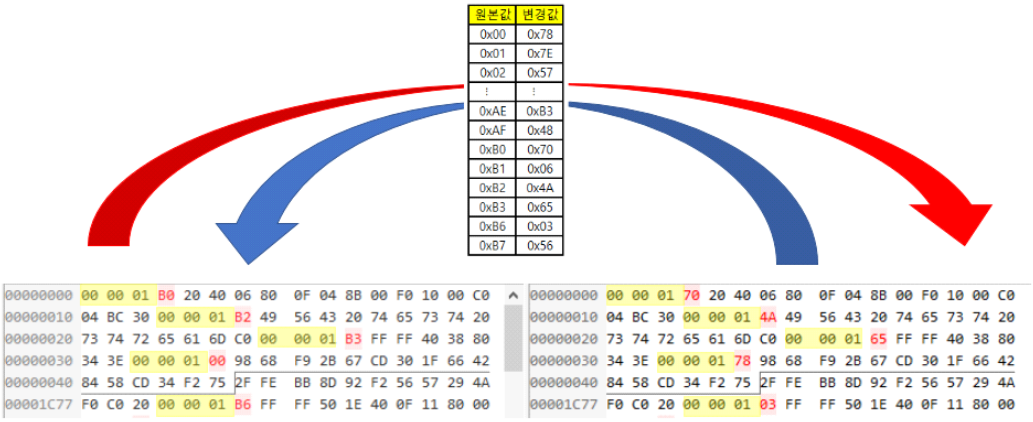

그림 1. IVC 비트스트림의 예제: (a) 원본 또는 복호화된 비트스트림, (b) 암호화된 비트스트림
Fig. 1. Example of IVC bitstream: (a)original or decrypted bitstream and (b) encrypted bitstream

Ⅳ. 실험 및 결과

제안 방식의 성능을 평가하기 위해 NEA와 제안 방식(Proposed Encryption Algorithm, PEA)의 암호화와 복호화에 소요되는 시간을 측정하고 비교하였다. 표 2는 NEA와 PEA의 암호화와 복호화를 수행하는 시간을 측정한 실험 결과이며 시간 단위는 마이크로세컨드이다. 실험에 사용된 IVC 원본 비트스트림은 다양한 압축 설정에 따라 다양한 시작 코드 타입을 포함하고 있는 37개의 IVC conformance 비트스트림들[6]을 사용하였다. 표 2에는 그 중에서 대표 11개와 37개 모두를 합한 결과를 나타낸다. 전체 비트스트림 기준으로 보면 NEA에 비해서 암호화의 경우 PEA의 속도가 96% 정도 감소하였고 복호화의 경우 PEA의 속도가 98% 정도 감소하였다. 또한, 37개의 암호화된 IVC conformance 비트스트림들은 IVC reference decoder[7]로 복호화할 때 모두 디코딩 에러가 발생하며 디코딩 되는 프레임 수가 0 이었다. 이는 앞서 Ⅱ장에서 설명한 기존의 SEA들과 암호화 속도를 비교했을 때 지그재그 순열 방식보다는 느리지만 SECMPEG, RVEA 보다 빨랐다. 하지만 지그재그 순열 알고리즘은 비트스트림의 크기를 50% 증가시키는데 비해 제안 방식은 비트스트림의 변화 없이 암호화가 가능하여 더 실용적인 방법이라 할 수 있다.

Ⅴ. 결 론

본 논문은 IVC 비트스트림에서 매우 작은 부분이지만 디코딩 과정에서 필수적인 정보인 시작 코드 타입을 이용한 비디오 암호화 및 복호화 방법을 제안하였다. 제안 방식은 기존의 선택적 암호화 방식에 비해 비트스트림 크기의 변화 없는 가장 빠른 방식이라는 것이 실험을 통해 입증되었다. IVC 코덱 이외 다른 비디오 코덱들도 일반적으로 시작 코드를 포함하고 있을 것으로 보여 시작 코드를 이용한 암호화 및 복호화 방법이 다른 코덱에도 활용 가능한지에 대한 추가 연구가 필요할 것으로 보인다. 또한, 암호화와 복호화 시에 사용한 변경 테이블을 공유하는 방법과 변경 테이블이 전송 오류로 손실되었을 때 대응하는 방법에 대한 추가 연구도 필요할 것으로 보인다.

참 고 문 헌 (References)

[1] J. Meyer and F. Gadegast, “Security Mechanisms for Multimedia Data with the Example MPEG-1 Video,” Project Description of SECMPEG, Technical University of Berlin, 1995.

[2] G.A. Spanos and T.B. Maples, “Performance Study of a Selective Encryption Scheme for the Security of Networked Real Time Video,” *Proceedings of Fourth International Conference on Computer Communications and Networks*, Las Vegas, NV, USA, pp. 2-10, 1995.

[3] L. Tang, “Methods for encrypting and decrypting MPEG video data efficiently,” *Proceedings of the Fourth ACM International Conference on Multimedia,* Boston, MA, USA, pp. 219-229, 1997.

[4] C. Shi, S.Y. Wang, and B. Bhargava. “MPEG video encryption in real-time using secret key cryptography,” *in Proc. Int. Conf. Parallel and Distributed Processing Techniques and Applications*, Las Vegas, NV, USA, pp. 2822-2828, 1999.

[5] “Text of ISO/IEC FDIS 14496-33,” ISO/IEC JTC1/SC29/WG11 N17129, 2017.

[6] “Text of ISO/IEC 14496-4:2004/FDAM46 Conformance testing for Internet Video Coding,” ISO/IEC JTC1/SC29/WG11 N17125, 2017.

[7] “Text of ISO/IEC 14496-5:2001/FDAM41 Information technology - Coding of audio visual objects - Part 5: Reference software, AMENDMENT 41: Reference software for Internet Video Coding ISO/IEC JTC1/SC29/WG11 N17127, 2017.

표 2. 암호화 및 복호화의 속도 비교
Table 2. Comparison of encryption and decryption speed

File name	File size (Bytes)	NEA (μs)		PEA (μs)		PEA/NEA (%)	
		Encryption	Decryption	Encryption	Decryption	Encryption	Decryption
BLKSIZE_A	126856	2502	5325	77	133.8	3.08	2.51
DBLK_A	63175	1204.6	2557.2	50.4	58	4.18	2.27
INFTYPE_A	122694	2271.6	4573	100.8	117.6	4.44	2.57
IPRED_A	226200	4132.8	8425	152.6	204	3.69	2.42
MULH_A	125526	2270.2	4682.6	74	109.6	3.26	2.34
MULQP_A	233827	4184.2	8974.4	135.4	238.6	3.24	2.66
MULSLICE_A	54275	995	2012.4	48	59.4	4.82	2.95
MVRANGE_A	123716	3165.8	4658	85.2	100.8	2.69	2.16
NONREFP_A	113172	2715.8	4219.4	80.4	109.6	2.96	2.60
PDIS_A	135868	3115.8	5038.8	92.2	113.6	2.96	2.25
TRANS_A	226200	4193.4	8387.4	147.6	206.6	3.52	2.46
Total (37 conformance bitstreams)	4724210	91760	182134	3293.8	4510	3.59	2.48