논문 2005-42SP-2-4

DCT-기반 영상/비디오 보안을 위한 암호화 기법 및 하드웨어 구현

(Ciphering Scheme and Hardware Implementation for MPEG-based Image/Video Security)

박 성 호*, 최 현 준**, 서 영 호***, 김 동 욱***

(Sung-Ho Park, Hyun-Jun Choi, Young-Ho Seo, and Dong-Wook Kim)

요 약

본 논문에서는 MPEG과 JPEG, H.26X계열 등의 DCT-기반 영상/비디오 컨텐츠에 효과적인 암호화 방법을 제안하였고, 이를 최적화된 하드웨어로 구현하여 고속동작이 가능하도록 하였다. 영상/비디오의 압축, 복원 및 암호화로 인한 많은 연산량을 고려하여 영상의 중요한 정보(DC 및 DPCM계수)만을 암호화 대상 데이터로 선정하여 부분 암호화를 수행하였다. 그 결과 암호화에 소요되는 비용은 원 영상 전체를 암호화하는 비용이 감소하였다. 여기서 Nf는 GOP내의 프레임수이고 PI는 B와 P 프레임에 존재하는 인트라 매크로블록의 수이다. 암호화 알고리즘으로는 다중모드 AES, DES, 그리고 SEED를 선택적으로 사용할 수 있도록 하였다. 제안한 암호화 방법은 C++로 구현한 소프트웨어와 TM-5를 사용하여 약 1,000개의 영상을 대상으로 실험하였다. 그 결과 부분 암호화된 영상으로부터 원 영상을 추측할 수 없어 암호화 효과가 충분함을 확인하였으며, 이 때 암호 화에 의한 압축률 감소율은 1.6%에 불과하였다. Verilog-HDL로 구현한 하드웨어 암호화 시스템은 하이닉스 0.25μm CMOS 팬텀-셀 라이브러리를 사용하여 SynopsysTM의 디자인 컴파일러로 합성함으로써 게이트-수준 회로를 구하였다. 타이밍 시뮬레이션은 CadenceTM의 Verilog-XL을 이용해서 수행한 결과 100MHz 이상의 동작 주파수에서 안정적으로 동작함을 확인하였다. 따라서 제안된 암호화 방법 및 구현된 하드웨어는 현재 중요한 문제로 대두되고 있는 종단간(end-to-end) 보안에 대한 좋은 해결책으로 유용하게 사용될 수 있으리라 기대된다.

Abstract

This thesis proposed an effective encryption method for the DCT-based image/video contents and made it possible to operate in a high speed by implementing it as an optimized hardware. By considering the increase in the amount of the calculation in the image/video compression, reconstruction and encryption, an partial encryption was performed, in which only the important information (DC and DPCM coefficients) were selected as the data to be encrypted. As the result, the encryption cost decreased when all the original image was encrypted. As the encryption algorithm, one of the multi-mode AES, DES, or SEED can be used. The proposed encryption method was implemented in software to be experimented with TM-5 for about 1,000 test images. From the result, it was verified that to induce the original image from the encrypted one is not possible. At that situation, the decrease in compression ratio was only 1.6%.The hardware encryption system implemented in Verilog-HDL was synthesized to find the gate-level circuit in the SynopsysTM design compiler with the Hynix 0.25μm CMOS Phantom-cell library. Timing simulation was performed by Verilog-XL from CadenceTM, which resulted in the stable operation in the frequency above 100MHz. Accordingly, the proposed encryption method and the implemented hardware are expected to be effectively used as a good solution for the end-to-end security which is considered as one of the important problems.

Keywords: MEPG, JPEG, DCT, Image Encryption, Security

I. 서 론

현재 멀티미디어 기술은 정보 산업 뿐만 아니라 경제, 문화 등 사회 각처에서 활용되고 있을 정도로 우리 생활의 주요한 요소로 자리 잡고 있다. 멀티미디어의 핵심미디어는 영상과 음향이다. 특히 영상데이터는 그 양이 방대하여 이들을 PCM(Pulse Code Modulation)으로 처리할 경우 저장매체의 과다한 용량이 요구된다. 또한 이들을 유/무선 네트워크의 한정된 대역폭(band-width)을 이용하여 전송할 때에도 많은 어려움이 따른다. 이러한 문제점을 극복하기 위해서 영상/비디오 압축에 관한 연구 및 기술개발은 계속 진행되어 왔다[1]~[3].

영상/비디오에 관한 국제 압축부호화 표준의 예로 ITU-T(International Telecommunication Union-Telecommunication standardization)의 MPEG 및 JPEG, H.26X계열 등의 DCT-기반 표준들을 들 수 있다[4]~[6].

* 정회원, ** 학생회원, *** 평생회원, 광운대학교 전자재료공학과
(Dept. of Electronic Materials Eng. Kwangwoon University)

※ 본 논문은 정보통신부 정보통신진흥원에서 지원하는 정보통신기초연구지원사업의 연구결과입니다.
접수일자: 2004년7월5일, 수정완료일: 2005년2월14일

통신기술이 발달하면서 유/무선을 통한 서로 다른 컴퓨터간 상호접속이 빈번해지고 압축된 영상/비디오 데이터의 용량이 감소하면서 이들 데이터의 교류는 더욱 활발해지고 있다. 따라서 신분증 및 X-ray 등의 개인정보와 영상/비디오 컨텐츠 등의 사업적 이윤을 목적으로 하는 유료정보, 공공기관의 비밀정보 등에 대한 접근권한과 보호가 중요한 사항으로 대두되었다. 이에 따라서 정보보호를 포함한 전달 및 저장형태의 보안을 위해 암호학[7],[8]을 이용하고 있다.

암호학을 이용한 DCT-기반 영상/비디오 컨텐츠의 암호화의 연구는 1997년부터 현재까지 계속 진행되어 왔다. 1997년, Lintian Quiao 와 Nahrstedt는 DCT후의 스캔(scan)순서를 암호화하였다[9]. 이 방법은 암호화 과정이 매우 간단하지만 양자화 후 런-길이 부호화(Run-Length Coding, RLC)[1],[10] 수행시 암호화로 인해서 블록내의 DCT계수 분포가 불규칙해진다. 그러므로 RLC효율을 감소시키며 LCA(Linear Crypto Analysis)[8] 공격에 취약하다는 단점이 있다. 1998년, Changgui와 Bhargava은 인트라(Intra, I) 프레임의 DCT영역에서 DC계수만 암호화 하는 방법을 제안하였다[11]. 그러나 이 방법은 움직임이 빠른 비디오 컨텐츠의 경우 B 프레임 및 P 프레임에서 인트라 매크로블록(intra macroblock)이 많이 발생함에 따라 암호화 효과가 크게 떨어지게 한다. 이외 Jiangtao 및 Severa는 가변길이 부호화(Variable Length Coding, VLC)[1],[10]수행 후 인덱스를 그룹단위로 섞어서 암호화시켰다[12]. 이 방법은 암호화 효과가 우수하나 데이터 및 VLC후의 인덱스를 두 번 암호화시키므로 연산량이 많다. 또한 암호화를 위한 인덱스를 별도로 필요로 하고 제어가 복잡하므로 부가적인 비용이 많이 요구된다.

본 논문에서는 MPEG 및 JPEG, H.26X계열 등 DCT-기반의 비디오 컨텐츠를 보호하기 위한 효율적인 암호화 방법을 제안한다. 압축 및 복원과 블록암호 알고리즘을 이용한 암/복호화의 많은 연산량을 고려하여 영상의 중요한 정보(DC 및 DPCM계수)만을 암호화시킬 데이터로 선정해서 부분적으로 암호화 한다. DC계수는 영상의 명암성분의 평균값이고 인접 화소 및 프레임에 파급효과가 크므로 암호화 효과를 쉽게 전파시킨다. DPCM계수도 DC계수와 성질이 유사하므로 이들만 암호화시킴으로써 암호화 비용을 현격히 절감시킬 수 있다. 암호화 알고리즘은 다중모드 AES, DES, SEED를 선택적으로 사용 한다. 아울러 제안한 암호화 방법에 최적화된 고속 암호화 시스템을 하드웨어로 구현하여 암호화를 위한 연산을 하드웨어가 처리하도록 함으로써 암호화시간을 크게 단축시킨다.

Ⅱ. 영상/비디오 압축과 암호화

Ⅱ-1. DCT-기반 영상/비디오 압축기

현재 가장 많이 응용되고 있는 영상/비디오 압축 기술들은 대부분 공간적 중복성을 제거하기 위하여 DCT를 사용하고 있다. 비디오의 경우 DCT와 더불어 시간적 중복성을 제거하기 위하여 화면 간 객체(object)들의 움직임 추정(Motion Estimation, ME) 및 움직임 보상(Compensation, MC)을 이용한 예측부호화 기법을 이용한다[1],[10].

그림 1은 암호화 시스템이 삽입된 MPEG-2 엔코더의 전체 블록도이다. MPEG-2 엔코더는 크게 3개의 프레임 버퍼와 DCT/IDCT(Inverse DCT) 블록, ME/MC 블록, 양자화기와 역양자화기, 그리고 엔트로피 코딩부로 구성된다. 엔트로피 코딩부는 RLC, VLC, FLC(Fixed-Length Coding)부로 다시 나뉘어진다. 점선으로 표시된 JPEG 엔코더는 MPEG-2 엔코더에서 IDCT, 역 양자화기, ME, MC를 제외한 부분이며 정지영상 압축방식은 동일하다. 단 양자화 계수 및 RLC, VLC, FLC 표는 MPEG-2 코덱과 다소 차이가 있다[1],[12],[13]~[15]. 그림 1에서 회색으로 표시한 암호화 시스템의 구조는 Ⅲ-4장에서 자세히 설명하겠다.

Ⅱ-2. 암호화

암호화는 접근 권한이 부여되지 않으면 원래의 정보를 알아내기 어렵게 하기 위해 수학 알고리즘을 적용하여 정보를 부호화하는 작업이다. 이 작업의 핵심은 키라고 하는 수학적인 값으로서 고유하고 복잡한 방법으로 정보를 부호화하는 과정에서 사용된다. 암호화된 데이터가 노출되더라도 암호화시 사용된 키가 없으면 복호가 불가능하다. 따라서 암호화시 가장 중요한 것은 키를 비공개적으로 보존 및 전송하는 것이다. 암호화 알고리즘은 크게 공개키 알고리즘과 대칭키 알고리즘, 그리고 해쉬함수로 분류할 수 있다. 이외 카오스시스템도 암호화의 수단으로 사용되지만 일정한 패턴을 갖는 암호화 데이터(cipher text)를 출력함으로써 brute-force 공격에 취약하므로 응용이 제한적이다[7],[8][20].

본 논문에서 사용하는 대칭키 암호화 알고리즘은 블록암호 알고리즘이라고도 한다. 대표적인 국제 표준 블록암호 알고리즘은 AES, DES이며 SEED는 대한민국 표준 블록 암호 알고리즘이다[21]~[23]. 블록암호 알고리즘은 일정단위 블록의 데이터를 동일한 키로 암호화 및 복호화하는 특징이 있다. 따라서 암/복호화를 위해 일정단위 블록의 데이터를 버퍼링하기 위한 데이터 대기 지연시간을 필요로 한다. 일반적으로 블록암호 알고리

즘을 이용하여 모든 데이터를 암/복호화 하는 경우 데이터의 양에따라 블록수가 결정된다. 이때 각 블록들간의 연관성 또는 의존성을 부과하여 암호화 효과를 더욱 강화하기 위해서 다중-모드(multi-mode)를 사용한다. 블록암호화 알고리즘의 동작모드에는 ECB(Electronic Code Book), CBC(Chipher Block Chaining), CFB(Chipher FeedBack), OFB(Output FeedBack), CTR(CounTeR)모드 등이 있다[8]. 블록암호 알고리즘은 데이터 대기지연시간과 연산시간이 길다는 단점이 있으나 암호화 강도는 우수하다.

블록암호 알고리즘을 통해서 암호화된 데이터가 복호되기 위해서는 암호화 시킬 당시의 암호 알고리즘에 대한 복호 알고리즘과 키, 암호화된 데이터가 필요하다. 따라서 영상/비디오 컨텐츠를 암호화할 때 암호화된 데이터가 코덱의 압축과정에서 훼손된다면 디코더에서 복호가 불가능해진다. 그러므로 엔코더에서의 암호화는 양자화 단계 이후의 무손실 압축구간에서 수행되어야 하며 디코더의 역 양자화단계 이전에 복호화 되어야 한다.

Ⅲ. 제안한 암호화 알고리즘과 하드웨어 구현

DCT-기반의 압축 코덱은 DCT 및 움직임 추정과 보상과정 수행시 많은 연산을 필요로 한다. 블록암호 알고리즘 역시 암호화 강도는 높으나 암/복호화시 많은 연산을 필요로 한다. 따라서 블록암호 알고리즘을 이용하며 이들 컨텐츠를 암호화한 후 한정된 대역폭의 유/무선 네트워크를 통해 전송할 때 암호화로 인해 많은 대기 지연시간이 발생할 수 있다. 따라서 암호화 비용을 최소화 하면서 최대의 암호화 효과를 얻을 수 있도록 적은 양의 데이터만 선택적으로 암호화 하는 것이 필요하다. 이때 암호화 시킬 데이터를 신중히 선정해야 한다.

본 장에서는 암호화시킬 데이터 영역의 선정조건과 선정된 데이터에 대한 효율적인 암호화 방법을 제시한다. 또한 제안된 알고리즘에 최적화된 고속 암호화 시스템의 하드웨어 구조와 동작을 설명한다.

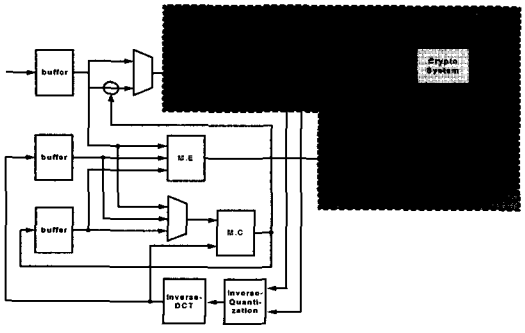


그림 1. 암호화시스템이 삽입된 MPEG-2 엔코더의 구조
Fig. 1. The structure of MPEG-2 encoder including crypto system.

Ⅲ-1. 암호화 데이터의 선정조건

암호화 시킬 데이터는 다음과 같은 요건을 갖추어야 한다.

① 압축과정 동안 암호화된 데이터가 손실되지 않아야 한다. 영상/비디오 압축은 크게 손실압축과 무손실 압축으로 분류된다.[1] 2-2절에서 언급한 바와 같이 블록암호화 알고리즘 특성상 암호화된 데이터가 한 비트라도 손상된다면 디코더에서 복호화가 불가능하다. 따라서 MPEG 및 JPEG, H.26X계열 등의 압축과정 중 양자화 단계 이후의 손실되지 않는 데이터가 암호화 대상이 되어야 한다.

② 영상의 식별에 중요한 역할을 해야 한다. 영상을 구성하는 요소는 명암성분과 색차성분, 휘도성분이다. 일반적으로 사람이 영상을 식별할 때 영상의 명암성분에 가장 크게 의존하므로 명암성분은 세 가지 요소 중 가장 중요하다. 만약 주파수 영역에서 명암성분이 훼손된다면 단위블록에 대한 명암차이가 흐트러지므로 명암성분만 암호화한다면 복원된 원 영상이 식별될 수 없다. 그러므로 영상의 명암성분에 관계되는 정보를 암호화시켜야 한다.

③ 인접한 화소와 프레임에 큰 파급효과를 가져야한다. 거의 모든 영상/비디오 압축기술들과 같이 MPEG 및 JPEG, H.26X계열 등의 표준에서도 대부분의 압축은 영상의 시/공간적 중복성을 제거하는 과정으로 이루어진다. 압축과정에서 참조대상의 데이터가 훼손된다면 디코딩시 참조대상의 데이터와 복원될 데이터간 인과성이 사라지게 된다. 그러므로 영상을 제대로 복원할 수 없다. 따라서 복원 과정시 참조대상이 되는 정보를 찾아서 암호화해야 한다.

④ 원활한 디코딩을 위하여 헤더정보는 훼손되지 말아야 한다. MPEG 및 JPEG, H.26X계열 등의 압축결과인 비트스트림은 대부분 고정된 길이의 헤더정보와 VLC계수들로 구성되어 있다. 네트워크상에서는 데이터의 헤더정보를 참고하는 레이어(layer)단위의 전송이 이루어진다.[3] 만약 헤더정보가 손상된다면 패킷의 길이가 불규칙해지므로 네트워크 환경에 부하를 줄 수 있다. 한편 VLC계수는 VLC테이블을 참조하여 부호화 및 복호화된다. 데이터 전송시 잡음이나 암호화로 인해서 데이터가 한 비트라도 추가되거나 제거된다면 디코더에서 VLC계수 복호시 오류가 발생하게 되어 파일에

대한 접근 자체가 불가능해진다. 따라서 암호화시 이런 정보는 훼손하지 말아야 한다.

본 논문에서에서는 위와 같은 조건을 모두 만족시키는 데이터로 인트라 매크로블록내의 DC 및 DPCM계수들로 선정하였다.

Ⅲ-2. DC 및 DPCM계수의 암호화

Ⅲ-2-1. DC 계수의 암호화

DC계수는 영상/비디오에서 전체 명암에 밀접한 관계가 있는 주파수 성분이다. 그러므로 단위블록 내에서 DC계수만 암호화한 후 영상을 복원시키더라도 그 블록 전체의 명암이 흐트러져 영상을 식별할 수 없다. 따라서 인트라 매크로블록 내의 DC계수를 암호화한다면 B와 P 프레임의 인트라 매크로블록을 참조해야 하는 생략된 매크로블록 및 움직임이 적용된 매크로 블록들을 암호화시키지 않고도 암호화 효과를 전파시킬 수 있다. 인트라 매크로블록이 많이 생성되는 비디오, 즉 움직임이 느린 비디오일수록 암호화 효과는 증가한다.

표 1에서 두 개의 실험영상을 대상으로 I 프레임을 포함하여 7 프레임으로 구성된 GOP(Group Of Picture) 내에서 생략된 매크로 블록 및 움직임이 적용된 매크로블록이 차지하는 비율을 보였다. 실험영상은 상대적으로 움직임이 없는 발레(Ballet, 720×480)와 움직임이 많은 미식축구(Soccer, 720×480)를 사용하였으며 각각 1,350개의 매크로블록으로 구성되어 있다. GOP내에 평균 80% 정도가 생략된 매크로 블록과 움직임이 적용된 매크로 블록이다. 그러므로 I 프레임의 인트라 매크로블록 내의 DC계수만 암호화시키더라도 GOP 전체의 80% 정도를 암호화시키는 효과를 기대할 수 있다.

단위블록이 8×8화소로 이루어졌다고 가정할 때 DC계수는 단위블록의 데이터량의 1/64을 차지한다. 따라서 I 프레임의 모든 인트라 매크로블록내의 DC계수만 암호화한다면 1개의 GOP를 암호화하는데 필요한 데이터 및 연산시간이 한 프레임 당 1/64로 감소한다. 암호화 데이터 비용 감소율을 R_{en}이라고 한다면 한 GOP를 암호화시킬 때 R_{en}은 식 (1)과 같다.

$$R_{en} = \frac{1}{64 \times N_f} \tag{1}$$

여기서 N_f 는 한 GOP내의 프레임수를 나타낸다. GOP가 7개 프레임으로 이루어진다면 N_f =7 이므로 R_{en}은 1/448이다.

움직임이 빠른 비디오일수록 움직임 추정간 참조프레임과의 오차가 많이 발생한다. 그러므로 B와 P 프레

표 1. GOP 내의 생략된 매크로블록과 움직임이 적용된 매크로블록의 비율

Table 1. Ratios of skipped macroblock and motioned macroblock in a GOP.

Frame	Skiped MB				Motion applied MB				Sum			
	Number		Ratio (%)		Number		Ratio (%)		Number		Ratio (%)	
	Ballet	Soccer	Ballet	Soccer	Ballet	Soccer	Ballet	Soccer	Ballet	Soccer	Ballet	Soccer
P1	921	764	68.2	56.6	363	370	27.9	27.4	1284	1134	95.1	84.0
B1	790	512	58.5	38.0	240	331	17.8	24.6	1030	843	76.3	62.4
B2	745	480	55.2	35.6	218	297	16.1	22	963	777	71.3	57.6
P2	893	867	66.1	64.2	391	403	29.0	29.9	1284	1270	95.1	94.1
B3	812	691	60.1	51.2	268	357	19.9	26.4	1080	1048	80.0	77.6
B4	780	601	57.8	44.6	243	355	18	26.3	1023	956	75.8	70.8
								Average		84.8		78.1

임내에 생략된 매크로 블록과 움직임이 적용된 매크로블록의 비율은 줄어드는 반면 인트라 매크로 블록의 비율은 증가한다. 표 1에서 미식축구의 경우 인트라 매크로 블록의 비율은 21.9%이다. 이는 움직임이 느린 발레보다 6.7% 많다. 움직임이 빨라질수록 이러한 차이는 더욱 두드러진다. 이때 B와 P 프레임의 인트라 매크로블록의 DC계수를 암호화하지 않는다면, 부분적으로 암호화되지 않은 매크로 블록이 노출될 수 있다. 따라서 움직임이 빠른 비디오의 경우 B와 P 프레임의 인트라 매크로 블록내의 DC계수도 추가로 암호화시켜야 한다. 그러므로 미식축구의 경우 21.9%의 인트라 매크로 블록내의 DC계수를 추가로 암호화해야 한다. 움직임이 빠른 비디오에서 B와 P 프레임의 DC계수를 추가로 암호화 시킬때 R_{en}은 식 (2)과 같다.

$$R_{en} = \frac{1}{64 \times N_f} + P_I \tag{2}$$

여기서, P_I는 B와 P 프레임내의 인트라 매크로 블록의 비율이고 $0 \le P_I \le 1/448$이다.

비트스트림에서 DC계수는 다음 절에서 언급될 DPCM 수행 후 VLC되어 매크로블록 헤더와 AC계수의 VLC사이에 삽입된다. 그러므로 헤더정보를 흐트러뜨릴 우려가 없다. 따라서 디코더에서의 VLC계수 복호시 오류가 없을 뿐만 아니라 무손실 압축과정의 데이터이므로 100% 복호화 할 수 있다. 단, 차 영상의 DC계수는 단위블록 영상에 크게 영향을 주지 못하므로 암호화 대상에서 제외시킨다.

Ⅲ-2-2. DPCM계수의 암호화

영상/비디오가 단조롭고 움직임이 없을수록 인접 블록간의 DC계수는 유사하다. 그러므로 DC계수간의 차이는 작아져서 DPCM계수의 길이는 감소한다. 따라서 DPCM계수의 길이에 대한 VLC계수의 길이는 감소하

므로 압축률은 증가한다. 반면 영상/비디오가 복잡해지고 움직임이 많아지면 인트라 매크로블록이 많이 생성된다. 따라서 부호화해야 할 DC계수는 많아지고 전송해야 할 DPCM계수의 길이에 대한 VLC계수의 길이는 증가한다.

암호화되는 DC계수가 많아지면 인접 블록간 DPCM계수가 매우 불규칙해진다. 그러므로 다양한 길이의 DPCM계수에 대한 VLC계수가 생성되어 전체적인 압축률은 감소한다. 그림 2에 이러한 현상을 실험한 결과를 보였다. 암호화하기 전의 그림 2(a)에 비해서 암호화 후 의 그림 2(b)에서 절대값이 큰 DPCM계수가 급격히 증가함을 알 수 있다. 따라서 Ⅲ-2-1절에서 제안한 DC계수의 암호화는 비교적 간단하지만 복잡한 영상이나 움직임이 많은 비디오를 암호화할 때 압축률을 증가시킬 우려가 있다. 일반적인 영상/비디오의 압축 코덱은 네트워크 환경을 고려하여 압축률을 최적화하는 rate control을 수행함으로써 네트워크를 이용한 전송에 최적화된 비트스트림을 생성한다. 그러나 암호화로 인해서 데이터 량이 증가한다면 데이터 전송시 네트워크에 부하를 증가시킬 수 있다.

이러한 압축률의 감소는 DPCM계수 자체를 암호화시킴으로써 해결할 수 있다. DPCM계수는 DC계수와 거의 모든 성질이 유사하다. 따라서 Ⅲ-1절에서 제시한 암호화 데이터의 조건에 부합하면서 Ⅲ-2-1절에서 제안한 암호화 방법과 유사한 암호화 효과를 얻을 수 있다. 단 암호화된 DPCM계수가 양자화 후 최대 임계값

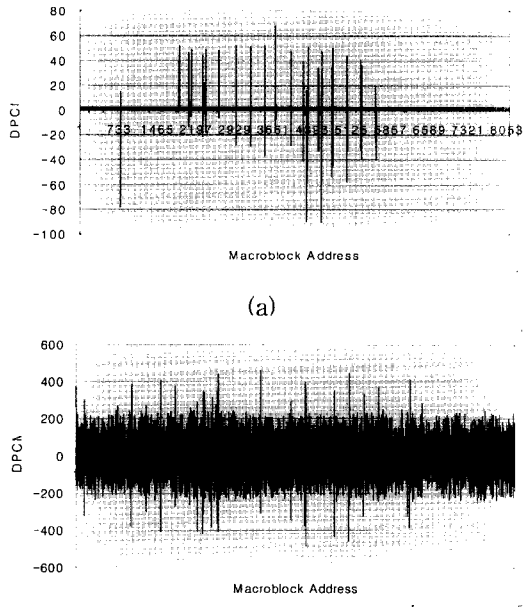


그림 2. Ⅰ 프레임 DPCM계수분포 암호화(a)전(b)후
Fig. 2. Distribution of DPCM coefficients for I frame. (a) Before (b) After encryption

보다 커지게 되어 수렴(saturation)과정에서 손실되지 않도록 해야 한다. 그러므로 암호화는 양자화 단계의 수렴과정 이후에 이루어져야 하며 복호화는 역 양자화 단계의 잘림 과정 이전에 이루어져야 한다. 또한 DC계수의 암호화에서와 같이 B와 P 프레임에서 암호화 대상 DPCM계수를 선택할 때 암호화 효과가 크지 않은 차 영상의 DPCM계수는 암호화시키지 않는다.

Ⅲ-3. 암호화 대상 및 데이터의 선택

본 절에서는 암호화 비용을 감소시키기 위하여 Ⅲ-2절에서 제안한 암호화 방법을 모든 블록에 대해서 적용시키지 않고 인접 블록간의 인과성, 계수분포와 시스템의 특성에 맞게 일부분의 블록과 비트만을 선택하여 적용하는 부분 암호화 방법을 제안한다.

Ⅲ-3-1. 암호화 대상 블록의 선택

앞 절에서 언급한바와 같이 DPCM계수는 인접블록과 인과적인 관계에 의해 생성된다. 따라서 모든 블록의 DPCM계수를 암호화하지 않고 암호화시킬 블록을 주기적으로 선택하여 선택된 인트라 블록의 DPCM계수만 암호화시키더라도 인접 블록에 암호화 효과를 전파시킬 수 있다. DPCM은 인트라 매크로블록내의 블록스캔 순서에 따라서 생성된다. 그러므로 각 인트라 매크로블록내의 첫 번째 블록의 DPCM계수만 암호화시키더라도 디코더에서 나머지 블록이 정상적으로 복원되지 않는다. 한편 암호화에 필요한 일정비트의 데이터를 버퍼링 할 때 모든 블록의 DPCM계수를 암호화시킬 때보다 4배 많은 블록의 DPCM계수를 버퍼링 시킬 수 있다. 따라서 암호화 연산시간은 4배 빨라지고 암호화 데이터량은 4배 감소시킬 수 있다. 이 암호화 방식을 식 (3-2)에 적용하면 전체적인 Ren은 식 (3)과 같다. NBp는 암호화 시킬 블록의 간격이다.

$$R_{en} = (\frac{1}{64 \times N_f} + P_I) \times \frac{1}{N_{Bp}} \quad (3)$$

여기서, $0 \le N_{Bp} \le MB_{Hor}$ 이고 MB_{Hor}는 영상의 가로방향의 인트라 매크로블록의 수이다. N_{Bp}는 시스템 및 네트워크 환경을 고려하여야 하는 요소이다. N_{Bp}가 작을수록 촘촘하게 암호화시킬 블록을 선택하게 되므로 암호화 강도는 높아지지만 암호화 비용은 증가한다. 그러므로 N_{Bp}는 암호화시키려는 강도와 시스템 및 네트워크의 상황에 따라서 적절히 조절되어야 한다. 단 N_{Bp}가 너무 커지면 영상에 따라서 복호시 역 양자화 단계 이전에 잘림 현상이 발생할 수 있다. 실험적으로 N_{Bp}는 움직임이 느린 비디오의 경우 $0 \le N_{Bp} \le 48$, 움직임이 빠른 비디오의 경우

$0 \le N_{Bp} \le 12$가 적당하다. 앞 절과 같이 차영상에 대한 DC 계수의 DPCM계수는 암호화 대상에서 제외한다.

Ⅲ-3-2. 암호화 대상 비트의 선택

DPCM계수는 실험적으로 0에서 32이내의 값을 갖는다. 따라서 5비트이하로 모든 DPCM계수를 표현할 수 있다. 또한 가중치(weight)가 높은 비트일수록 DPCM 계수에 큰 영향을 준다. 따라서 가중치가 높은 순으로 일부 비트(N_{Bn})만 암호화시킨다면 R_{en}은 식 (4)과 같다.

$$R_{en} = (\frac{1}{64 \times N_f} + P_I) \times \frac{N_{Bn}}{5} \quad (4)$$

여기서 N_{Bn}은 암호화되는 DPCM 계수의 비트 수이며 $0 \le N_{Bn} \le 5$ 이다. N_{Bn}은 N_{Bp}와 달리 영상의 특성에 따라 신중히 결정되어야 한다. 대체적으로 단조로운 영상은 인접블록간 DPCM계수의 차이가 3비트 미만인 경우가 많다. 만약 대부분의 DPCM계수가 3비트보다 낮은 범위에 분포한다면 많은 부분이 암호화되지 않아 복원 후 많은 매크로블록이 노출될 수 있다. 따라서 이 방법을 적용할 때에는 영상의 복잡도 특성을 시스템 및 네트워크 환경에 의한 요소보다 먼저 고려해서 N_{Bn}을 결정한다.

대부분의 영상/비디오의 경우 실험적으로 N_{Bn}=2인 경우에서 충분한 암호화 효과를 얻을 수 있다. 일반적인 영상/비디오 압축 코덱에서 DC계수에 대해서도 양자화를 실시하지만 DPCM계수의 상위 5비트는 양자화 이후에도 손실되지 않으므로 이 방법은 양자화 이전의 DC계수에 대해서도 적용가능하다. 이 방법 역시 인트라 매크로블록 내 DC 및 DPCM계수에 대해서만 암호화를 수행한다.

Ⅲ-3-3. 혼합적인 암호화 대상 데이터의 선택

본 절에서 Ⅲ-3-1, Ⅲ-3-2절에서 제안한 데이터 선택 방법들을 혼합하여 적용시키는 방법을 예를 들어 설명한다. 영상/비디오의 특성, 시스템 및 네트워크의 환경 등을 고려해서 N_{Bp}와 N_{Bn}을 동시에 조절하여 암호화를 수행한다면 R_{en}은 식 (5)과 같다.

$$R_{en} = (\frac{1}{64 \times N_f} + P_I) \times \frac{1}{N_{Bp}} \times \frac{N_{Bn}}{5} \quad (5)$$

Ⅲ-3-1절에서 언급한바와 같이 N_{Bp}가 너무 커지면 복호시 DPCM계수가 역 양자화단계 이전에 잘림 현상이 발생할 수 있다. 따라서 N_{Bp}을 작게 하는 반면 N_{Bn}을 크게 하면 똑같은 암호화 비용으로 더 많은 매크로블록내의 DPCM계수를 암호화할 수 있다. 그러므로 Ⅲ-3-1, Ⅲ-3-2절에서 제안된 암호화 방법은 함께 운용되어야 효율적이다.

Ⅲ-4. 고속 암호화 시스템의 하드웨어 구현

Ⅲ-4-1. 암호화 시스템의 구조 및 동작

그림 3은 그림 1에 삽입된 암호화 시스템의 세부구조이다. 암호화 시스템은 크게 제어부와 데이터 패스부로 구성된다. 제어부는 상태 레지스터와 상태 디코더로 구성된다. 데이터 패스부는 프로그래밍이 가능한 동작 모드 레지스터와 암/복호화 수행부[24], DPCM수행 및 비트스트림 출력부로 구성된다. Ⅱ-2절에서 언급한 바와 같이 블록암호 알고리즘은 알고리즘마다 정해진 일정량의 데이터를 단위별로 암/복호화하는 특징이 있다. 암/복호화 수행부의 입/출력단 버퍼는 이를 위한 것이다. 버퍼는 블록암호화 알고리즘 선택/운용모드에 따라서 최소 64비트에서 최대 256비트의 데이터를 버퍼링한다.

암호화 시스템은 4가지의 동작 모드에 따라서 동작한다. 표 2에서 암호화 시스템의 동작 모드를 나타내었다. 'X'는 무정의 조건이다. 동작 모드는 시스템 운용모드, 컨텐츠 암호화 모드, 블록 암호화 알고리즘 선택/운용 모드, 데이터 입/출력 모드 등이 있으며 17비트의 코드로 표현된다. 동작 모드는 암호화 시스템 운용 전에 프로그래밍에 의해서 모드 레지스터에 저장된다.

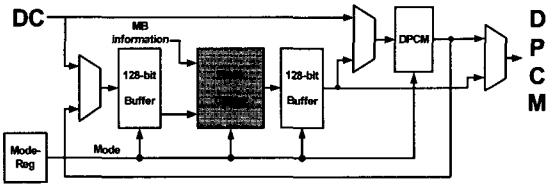


그림 3. 암호화 시스템의 내부구조
Fig. 3. Internal structure of crypto system.

Ⅲ-4-2. DPCM 수행 및 비트스트림 출력부

DPCM 수행부는 이전 블록의 DC계수 저장을 위한 9비트 레지스터와 감산기, DPCM계수의 길이판정을 위한 비교기와 룩-업 테이블(Look-Up Table, LUT) 등으로 구성된다. 비트스트림 출력부는 LUT와 비트스트림 생성을 위한 카운터그룹 등으로 구성된다. LUT는 명암 및 색차 성분 DPCM계수의 길이에 대한 VLC 테이블을 저장하고 있으며 프로그래밍이 가능하다.

암호화되거나 그렇지 않은 DC 및 DPCM계수는 DPCM 수행부로 입력된다. MPEG 및 JPEG, H.26X 계열의 엔코더는 압축률 향상을 위해서 DCT계수가 음수인 경우 '1' 의 보수 형태로 비트스트림을 출력한다. 반면 디코더에서는 '2' 의 보수 형태로 복원되므로 암호화 후 DPCM 수행시 주의해야 한다. DPCM 수행부를 통

표 2. 암호화 시스템의 동작 모드
Table 2. Definition modes of operation for crypto system.

Mode		Specified item		Code			Number of bits
System operation		Security	En	0	0		2
			De		1		
		Bit-stream gen		1	0		
		System test			1		
Contents encry-ption		DC	N_{Bn}	0	0	000~111	5
			N_{Bn}		1	00~11	
		DPCM	N_{Bn}	1	0	000~111	
			N_{Bn}		1	00~11	
Block cipher	Select	AES	128bit	00	00		4
			192bit		01		
			256bit		10		
		SEED		01	XX		
		DES	Single	10	00		
			Double		01		
			Three		10		
	Mode	ECB		000			3
		CBC		001			
		CFB		010			
		OFB		011			
		CTR		100			
Data I/O		Serial		0	XX		3
		Parallel	8bit	1	00		17
			32bit		01		
			direct		10		
Total							

과하는 계수는 시스템 모드에 따라서 그것의 부호, 길이에 대한 VLC계수 등과 함께 비트스트림으로 출력된다. 암호 및 복호를 위한 키는 GOP마다 달리하여 RSA 및 ECC 등의 공개키 암호화 알고리즘으로 암호화한 후 비트스트림의 사용자 정의(User_Data)영역에 삽입된다.[25],[26]

Ⅳ. 실험 및 하드웨어 구현결과

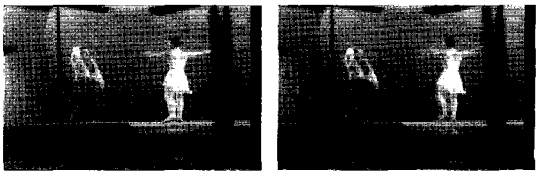
본 논문에서 제안한 암호화 알고리즘을 C++언어로 암호화 소프트웨어를 구현한 후 MPEG-2의 실험 소프트웨어 코덱인 TM-5를 이용하여 발레와 미식축구 중 여러개의 GOP(7개 프레임)에 대하여 실험을 수행하였다. 그림 4 (a)와 (b)는 각각 발레의 첫 번째 I 프레임과 P1 프레임으로 부호화될 원 영상이다. 그림 5 (a)와 (b)는 발레보다 복잡하고 움직임이 빠른 미식축구의 첫 번째 I 프레임과 P1 프레임으로 부호화 될 원영상이다.

영상의 색상정보는 암호화에 많은 영향을 끼치지 못하므로 본 논문에서는 흑백 영상의 명암성분에 대해서만 암호화를 수행하였다. 암호화는 256비트 키 AES를 CFB모드로 동작시켜서 암호화를 수행하였다.

Ⅳ-1. 암호화의 효율 비교

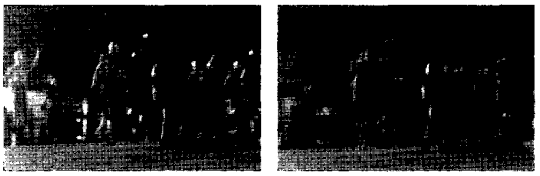
Ⅳ-1-1. DC계수의 암호화

그림 6 (a)와 (b)은 그림 4 (a)와 (b)의 인트라 매크로 블록의 DC계수만 암호화한 영상이다. 그림6 (a)는 I 프레임의 인트라 매크로블록의 DC계수만 암호화한 결과(식 (1))이다. 그림 6 (b)는 그림 4(a)에서 암호화된 대부분의 매크로 블록을 참조하였다. 그러나 하얀색으로 표시된 부분은 움직임 추정과정 동안 참조 매크로블록과 오차 비교시에 오차가 많이 발생하여 인트라 매크로블록이 부호화된 부분이다. 이는 전체 매크로블록의 21.9%를 차지한다. 새롭게 발생한 DC계수들이 암호화되었기 때문에 주위 매크로 블록과 암호화 패턴이 다르다. 이를 제외한 대부분의 매크로블록은 생략된 매크로블록과 움직임이 적용된 매크로 블록이다.



(a) (b)

그림 4. 발레의 원 영상 (a) I 프레임 (b) P1 프레임
Fig. 4. Original images of Ballet. (a)I frame (b)P1 frame



(a) (b)

그림 5. 미식축구의 원 영상 (a) I 프레임 (b) P1 프레임
Fig. 5. Original images of Soccer. (a)I frame (b)P1 frame

(a)

그림 6. DC계수를 암호화한 영상 (a) I 프레임 (b) P1 프레임
Fig. 6. Encrypted image for DC coefficients. (a) I frame (b) P1 frame

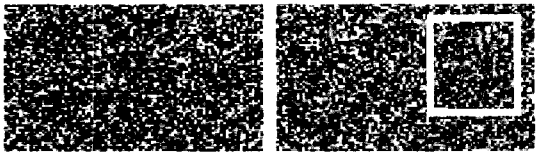
Ⅳ-1-2. DPCM계수의 암호화

그림 7 (a)와 (b)에서 그림 4 (a)와 (b)에 대해 DPCM 계수를 암호화한 영상을 각각 비교하였다. 그림 7 (a)는 I 프레임의 인트라 매크로블록의 DPCM계수만 암호화한 결과이다. DC계수와 DPCM계수의 성질은 유사하므로 그림 7 (b)의 하얀색으로 표시된 부분은 새로 발생한 인트라 매크로블록내의 DPCM계수가 새롭게 암호화된 영상이다. 암호화 효과는 Ⅳ-1-1절과 유사하다. 그러나 DCT후의 DC계수가 8비트내의 값이라고 가정할 때 DPCM계수는 0에서 5비트로 이내의 값이므로 R_{en}은 5/8 이다

Ⅳ-1-3. 블록과 비트선택에 의한 암호화

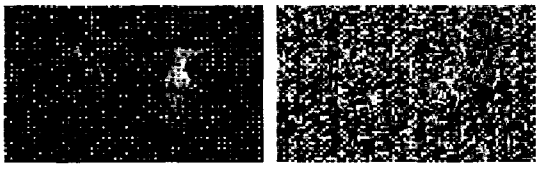
그림 8 (a)와 (b)에서는 발레의 원영상의 I 프레임을 N_{Bp}=4와 N_{Bp}=2 일 조건으로 각각 암호화한 영상을 비교하였다. 그림 7 (a)에 비해 그림 8 (a)와 (b)를 암호화하는데 필요한 데이터 및 연산시간이 각각 1/4, 2/4로 감소하였다. 그림 8 (b)와 비교할 때 그림 8 (a)에서는 영상의 윤곽이 노출된다. 이처럼 암호화 비용과 강도는 서로 상보관계이다. 그림 9 (a)와 (b)에서 발레의 I 프레임을 N_{Bn}=1과 N_{Bn}=2인 조건으로 암호화한 영상을 각각 비교하였다. 그림 9 (a)에서 전체 영상의 윤곽이 희미하게 드러나는데, 이는 대부분의 DPCM계수가 32보다 작기 때문에 DPCM계수의 상위 1비트를 암호화하여도 암호화되지 않는 DPCM계수가 존재하기 때문이다. 단조로운 영상과 움직임이 없는 비디오일수록 DPCM계수가 작아지므로 이러한 현상은 더욱 두드러진다.

그림 10 (a)와 (b)는 발레보다 복잡하고 움직임이 많은 미식축구의 I 프레임을 N_{Bn}=1과 N_{Bn}=2인 조건으로 암호화한 영상을 각각 비교하였다. 그림 10 (a)는 그림 9 (a)의 발레의 경우와는 달리 움직임이 많아서 인트라 매크로블록의 수가 상대적으로 많다. 따라서 블록간의 DC계수 차이가 크기 때문에 DPCM계수가 32 이상인 계수가 대부분이다. 따라서 상위 1비트만 암호화 하였음에도 불구하고 대부분의 DPCM 계수가 암호화되어 영상의 윤곽이 드러나지 않는다.



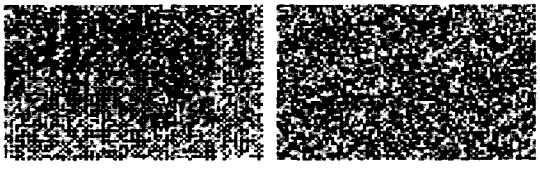
(a) (b)

그림 7. DPCM계수가 암호화된 영상 (a) I (b) P1 프레임
Fig. 7. Resulting image from encrypted DPCM. (a) I frame (b) P1 frame



(a) (b)

그림 8. 블록선택에 의해서 암호화된 발레 영상 (a) NBp = 4 (b) NBp = 2
Fig. 8. Encrypted Ballet image by block selection. (a) NBp = 4 (b) NBp = 2



(a) (b)

그림 9. 비트선택에 의해서 암호화된 발레 영상 (a) NBn = 1 (b) NBn = 2
Fig. 9. Encrypted Ballet image by bit selection. (a) NBn = 1 (b) NBn = 2

(a) (b)

그림 10. 비트선택에 의해서 암호화된 미식축구 영상 (a) NBn = 1 (b) NBn = 2
Fig. 10. Encrypted Soccer image by bit selection. (a) NBn = 1 (b) NBn = 2

Ⅳ-2. 고속 암호화 시스템의 하드웨어 구현결과

제안한 영상/비디오 컨텐츠의 암호화 방법에 최적화된 고속 암호화 시스템을 Verilog-HDL로 구현하였다. 구현한 하드웨어는 하이닉스 0.25μm CMOS 팬텀-셀 라이브러리를 이용하여 Synopsys™의 디자인 컴파일러로 합성했다. 표 2에서 구현된 하드웨어의 자원 사용율을 나타내었다. 7개의 CMOS NAND셀을 하나의 게이트(gate)로 계산할 때 총 124K 게이트를 사용하였다. 블록 암호화 알고리즘 암/복호화 수행부가 상대적으로 많은 게이트를 소비했다. 그중에서도 AES 모듈은 연산속도를 높이고자 총 14개의 LUT를 사용하였으므로 제일 많은 게이트를 소비하였다. 타이밍 시뮬레이션은 Cadence™의 Verilog-XL로 수행하였다. 그 결과 동작주파수 100 MHz 이상에서 안정적으로 동작함을 확인하였다.

Ⅳ-3. 다른 기법과의 비교

표 3에서 7개의 프레임으로 구성된 실험영상 발레의 한 GOP에 대해서 암호화 전후의 압축률 변화를 기존의 두 방법과 비교하였다. Changgui와 Bhargava가 제안한 DC계수의 암호화 방법은 암호화 후 DPCM계수에 대한 VLC계수를 매우 불규칙하게 한다. 따라서 암호화 후 압축률은 9.6% 감소하였다. Lintian quiao 및 Nahrstedt가 제안한 DCT후의 스캔 순서의 암호화 방법은 암호화 후 양자화 과정을 거친 AC계수의 분포가 불규칙하게 한다. 그러므로 RLC 및 VLC의 효율성을 감소시켜 암호화 후 압축률이 26.0% 감소하였다. 반면 본 논문에서 제안한 암호화 방법은 DPCM에 대한 VLC계수중 2에서 5비트 범위내의 값을 암호화하므로 암호화 후 압축률이 단지 1.6% 감소하였다. 한편 DPCM계수는 최대 5비트로 최소 8비트인 DC계수에 비해 적은 비트수를 차지하므로 더욱 많은 블록의 DPCM계수가 암호화에 필요한 데이터로 버퍼링되어 암호화 연산시간을 대략

표 2. 하드웨어 자원 사용율
Table 2. Occupation rate of hardware resource.

Part	Module	Number of gates
System control	Control part	9,760 (1.8 %)
	Mode register	1,006 (0.8 %)
DPCM / bit-stream	DPCM	5,392 (4.3 %)
	Bit-stream gen	2,088 (1.7 %)
Encryption / Decryption	AES	40,521 (32.4 %)
	SEED	23,333 (18.7 %)
	Multiple-DES	23,425 (18.8 %)
	Virtual cipher	1,404 (1.2 %)
	Block mode	14,050 (11.2 %)
Sytem IO	I/O interface	3,941 (3.2 %)
Total		124,920 (100 %)

표 3. 암호화 전 후의 압축률 변화비교
Table 3. Comparision with other method for compression ratio change according to encryption and deryption.

(Original data : 3380Kb, Coded data : 43Kb, Compression ratio : 78.6%)

Proposed algorithm	Encrypted data	After encyption		Difference	
		Coded (Kb)	Comp. Ratio(%)	Coded (Kb)	Comp. Ratio (%)
Changgui, Bhargava's	DC	49	69.0	6	9.6
Lintian quiao, Nahrstedt's	Zigzag scan order	64.3	52.6	21.3	26.0
Ours	DPCM	44.2	76.5	1.2	1.6

37% 감소시켰다. 또한 Jiantao 및 Severa가 제안한 암호화 방법보다 제어가 간단하고 암호화를 위한 별도의 VLC계수가 필요하지 않다. 따라서 기존에 제안되었던 암호화 방법보다 암호화 비용 및 압축률 감소 측면에서 우수하다.

V. 결 론

본 논문에서는 MPEG과 JPEG, H.26X계열 등의 DCT-기반 비디오 컨텐츠를 위한 효과적인 암호화 방법을 제안하였다. 코덱에서의 엔코딩, 디코딩 및 암호화에 따른 많은 연산량을 고려하여 최소의 암호화 비용으로 높은 암호화 효과를 얻을 수 있는 조건으로 암호화 시킬 데이터 영역을 선택하였다. 또한 암호화 비용을 감소시키기 위하여 영상/비디오의 특성 및 시스템, 네트워크 등의 상황을 고려해서 적응적으로 적용시킬 수 있는 블록 및 비트에 대한 선택전인 암호화 방법을 제안하였다.

제안한 암호화 방법은 C++로 구현한 소프트웨어와 TM-5를 사용하여 약 1000개의 영상을 대상으로 실험하였다. 그 결과 부분 암호화된 영상으로부터 원 영상을 추측할 수 없어 암호화 효과가 충분함을 확인하였으며, 이 때 암호화에 의한 압축률 감소율은 1.6%에 불과하였다. 한편 제안한 알고리즘에 최적화된 고속 암호화 시스템을 하드웨어로 구현하여 암호화 연산은 전용 암호화 프로세서가 처리하게 함으로써 암호화 연산시간을 크게 단축시켰다. 하드웨어로 구현한 고속 암호화 시스템은 하이닉스 0.25μm CMOS 팬텀-셀 라이브러리를 이용해서 Synopsys™의 디자인 컴파일러를 이용해서 합성했다. Cadence™의 Verilog-XL를 이용해서 타이밍 시뮬레이션을 수행한 결과 동작주파수 100MHz 이상에서 안정적으로 동작함을 확인하였다.

본 논문에서 제안한 방법은 암호화로 인한 데이터 대기시간지연을 최소화하였다. 이로 인해서 암호화된 DCT-기반 영상/비디오 컨텐츠의 유/무선통합 네트워크를 통한 원할한 전송 및 수신이 가능하게 하였다. 그러므로 제안된 암호화방법과 구현된 하드웨어는 현재 중요한 문제로 대두되고 있는 종단간(end-to-end) 보안에 대한 좋은 해결책으로 유용하게 사용될 수 있으리라 기대된다.

참 고 문 헌

[1] R. C. Gonzalez and R. E. Woods, "Digital Image Processing", Prentice Hall, N. J., 2002.
[2] K. Sayood , "Lossless Compression Handbook", Academec Press, S. D, 2003.
[3] Jim Kurose and Keith Ross, "Computer Networking", Addision Wesley, N. Y., 2003.
[4] http://www.itu.int/ITU-T
[5] http://www.mpeg.org/MPEG/index.html
[6] http://www.jpeg.org
[7] 김 철, "암호학의 이해", 영풍문고, 서울, 1996.
[8] Willianm Stallings, "Cryptography and Network security", Prentice Hall, N. J. 2003.
[9] Lintian Qiao and Nahrstedt K. and Ming-Chit Tam, "Is MPEG encryption by using random list instead of zigzag order secure?", IEEE International Symposium on Consumer Electronics, Vol. 2, No. 4, pp.226~229, Dec. 1997.
[10] 이호석, 김준기, "알기쉬운 MPEG-2", 홍릉과학 출판사, 서울, 2002.
[11] 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.
[12] Jiangtao Wen and Severa and M. Wenjun Zeng, Luttrell and M.H., Weiyin Jin, "A format-compliant configuable encryption framework for access control of video", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 12, No. 6 , pp. 545~557, June 2002.
[13] Sobhy and M.I. Shehata and A.-E.R. "Chaotic algorithms for data encryption", IEEE

International Conference on Acoustics, Speech, and Signal Processing, Vol. 7 No. 11, pp.997~1000, May 2001.
[14] ISO/IEC 13818-2 MPEG-2. "Generic Coding of Moving Pictures and Associated Audio", Nov 1993.
[15] ISO/IEC 14496-1 MPEG-4 "Coding of Audio-Visual Objects - Part 2 : Visual", Aug. 2002.
[16] ISO/IEC 10918-1 JPEG, "Information technology - Digital Compression and Coding of continuous tone still images : Requirements and guidelines", 1994.
[17] Alan V. Oppenheim and Ronald W. Schafer and John R. Buck, "Discrete Signal Processing", Prentice Hall, N. J. 1976.
[18] Ahmed, N., and Rao, K. R., "Orthogonal Transforms for Digital Signal Processing", Spierg Verlag, Newyork. 1975.
[19] Iain E. G. Richardson, "Video Codec Design" John Wiley&Son, N. Y, 1988.
[20] Shujun Li, Xuan Zheng, "Cryptanalysis of a chaotic image encryption method", IEEE International Symposium on Circuits and Systems, Vol. 2 No. 5, pp.708~711 May 2002.
[21] National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES), National Technical Information Service, Springfield VA 22161. Nov. 2001.
[22] National Bureau of Standards. FIPS PUB 46 : Data Encryption Standard, January, 1987.
[23] 한국정보보호센터, "128비트 블록 암호알고리즘 (SEED) 개발 및 분석 보고서", Vol. 12. 1998.
[24] 서영호, 박성호, 최성수, 정용진, 김동욱, "네트워크 보안을 위한 다중모드 블록암호 시스템의 설계", 한국통신학회 논문지 제 28권 11C호, pp. 1077~1087, Dec. 2003.
[25] R. L. Rivest and A. Shrmir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems" Communications of the ACM. Vol. 21. No. 2, pp.120~126, Feb 1978.
[26] Victor S and Miller, "Use of Elliptic Curves in Cryptography", Advances in Cryptology - CRYPTO 85 Proceedings, Vol. 12. pp.417~426, 1986.

저 자 소 개

박 성 호(정회원)
2000년 2월 광운대학교 전자재료 공학과 졸업 (공학사)
2004년 8월 광운대학교 대학원 졸업(공학석사).
2004년 8월~현재 LG전자 System IC 사업담당 SIC DCM 그룹 연구원
<주관심분야 : 영상압축, 워터마킹, 암호학, FPGA/ASIC 설계, Design Methodology>
e-mail : lge@lge.com

서 영 호(평생회원)
1999년 2월 광운대학교 전자재료 공학과 졸업(공학사).
2001년 2월 광운대학교 대학원졸업(공학석사).
2000년 3월~2001년 12월 인티스닷컴(주) 연구원.
2003년 6월~2004년 6월 한국전기 연구원 연구원.
2004년 8월 광운대학교 대학원졸업(공학박사)
2004년 12월~현재 유한대학 연구교수
<주관심분야 : 2D/3D 영상처리, JPEG2000 /MPEG, 워터마킹, 암호/보안 FPGA/ASIC 설계>
e-mail : design@kw.ac.kr

최 현 준(학생회원)
2003년 2월 광운대학교 전자재료공학과 졸업 (공학사).
2005년 2월 광운대학교 대학원졸업(공학석사).
2005년 3월~현재 광운대학교 전자재료공학과 박사과정.
<주관심분야 : Image Processing, 암호학, FPGA /ASIC 설계>
chj@kw.ac.kr

김 동 욱(평생회원)
1983년 2월 한양대학교 전자공학과 졸업(공학사).
1985년 2월 한양대학교 대학원 졸업(공학석사).
1991년 9월 Georgia 공과대학 전기공학과 졸업 (공학박사)
1992년 3월~현재 광운대학교 전자재료공학과 정교수, 광운대학교 신기술 연구소 연구원
1997년 12월~현재 광운대학교 IDEC 운영위원.
2000년 3월~현재 인티스닷컴(주) 연구원.
<주관심분야 : 디지털 VLSI Testability, VLSI CAD, DSP 설계, Wireless Communication>
e-mail : dwkim@kw.ac.kr