논문 2009-46SD-1-5

타원 곡선 암호화를 이용한 영상 저작권 보호 시스템 설계

(Design of Digital Media Protection System using Elliptic Curve Encryption)

이 찬 호*

(Chanho Lee)

요 약

통신 기술이 발달하면서 유무선을 통한 네트워크 접속이 빈번해지고 고화질의 비디오/오디오 압축 방식의 출현으로 데이터의 교류는 더욱 활발해지고 있다. 데이터 교류의 증가로 개인 정보와 비디오/오디오 콘텐츠 등의 사업적 이윤을 목적으로 하는 유료정보에 대한 접근권한과 보호가 중요한 요소로 인식되고 있다. 따라서 본 논문에서는 타원 곡선 암호화 알고리즘을 이용한 디지털 미디어 저작권 보호 기술을 제안한다. 제안된 방식에서는 H.264 영상신호의 핵심 파라미터만을 암호화하여 암호 및 복호에 따른 부담을 줄이고 해당 정보를 복호하지 못할 경우 영상 재생이 안 되거나 매우 열악한 화질의 영상이 재생되도록 한다. 이러한 시스템을 구현하기 위해서는 영상 재생 단말기에 암호 복호화 하드웨어가 필요하다. 제안된 시스템의 동작을 검증하기 위해 재구성 가능한 타원곡선 암호화 프로세서를 구현하고 H.264 영상 복호기에 적용하였다. 검증 결과 암호화된 데이터를 복호하지 못하는 경우 영상이 제대로 재생되지 않음을 확인하였다.

Abstract

The advance of communication and networking technology enables high bandwidth multimedia data transmission. The development of high performance compression technology such as H.264 also encourages high quality video and audio data transmission. The trend requires efficient protection system for digital media rights. We propose an efficient digital media protection system using elliptic curve cryptography. Only key parameters are encrypted to reduce the burden of complex encryption and decryption in the proposed system, and the digital media are not played back or the quality is degraded if the encrypted information is missing. We need a playback system with an ECC processor to implement the proposed system. We implement an H.264 decoding system with a configurable ECC processor to verify the proposed protection system. We verify that the H.264 movie is not decoded without the decrypted information.

Keywords : 타원곡선 암호화, 암호화 프로세서, H.264, 영상 저작권 보호

I. 서 론

멀티미디어 처리기술 발전과 네트워크 속도의 급격한 증가로 기존 시장의 발전과 새로운 시장 출현의 계기가 되었다. 디지털 비디오/오디오 컨텐츠는 손쉽게 생성되고 수정이 가능하고 무한히 반복하여 사용해도 품질의 저하가 발생하지 않는다. 그리고 네트워크로 통해 대용량의 디지털 콘텐츠를 짧은 시간에 전송과 배포가 가능하다. 이러한 특성은 디지털 컨텐츠의 배포 및 손쉬운 접근 환경을 제공함으로써 누구든지 쉽게 콘텐츠를 이용할 수 있도록 순기능을 제공하였다. 하지만, 디지털 콘텐츠의 불법 복제로 인한 지적재산권자들의 권익이 위협 받고 있다. 그 결과로 디지털 콘텐츠 보호는 유무선 네트워크를 통한 데이터 전송의 중요한 요소로 인식되었다[1].

DRM(Digital Rights Management)은 디지털 콘텐츠의 생성과 이용까지 유통 전 과정에 걸쳐 디지털 콘텐츠를 안전하게 관리/보호하고, 부여된 권한정보에 따라 디지털 콘텐츠의 이용을 제어/통제하는 기술이다. DRM

* 정회원, 숭실대학교 정보통신전자공학부
(School of Electronic Engr., Soongsil University)
※ 본 논문은 숭실대학교 교내연구비 지원을 받았습니다.
접수일자: 2008년7월16일, 수정완료일: 2009년1월5일

은 3가지의 구성요소로 되어있다. 디지털 콘텐츠의 관리와 배포를 하는 콘텐츠 서버, 라이센스를 관리하는 라이센스 서버와 디지털 콘텐츠를 이용하는 클라이언트이다. 클라이언트는 콘텐츠 서버에서 암호화된 디지털 콘텐츠를 받는다. 암호화된 디지털 콘텐츠는 라이센스 서버에서 라이센스를 받은 후 클라이언트는 디지털 콘텐츠를 사용할 수 있다[2].

이러한 DRM은 암호화 알고리즘과 밀접한 관계가 있고 멀티미디어 데이터를 보호하기 위해서 많은 암호화 알고리즘의 연구되었다. 암호화는 영상압축을 하기 전, 주파수 도메인에서, 그리고 영상압축을 한 후에 할 수가 있다. 영상압축을 하기 전에 암호화를 하면 암호화에 따라서 압축효율이 떨어지며, 주파수 도메인에서 암호화는 하드웨어의 유연성이 떨이진다. 영상압축을 한 후 암호화는 약간의 오버헤드만으로 충분한 암호화 효과를 볼 수 있다[3]. 또한 연구된 암호화 알고리즘은 그 복잡도에 따라 소프트웨어 또는 하드웨어로 구현된다. 소프트웨어 방식으로 구현되면 다양한 암호화 알고리즘을 손쉽게 구현할 수 있으나 휴대용 기기의 경우 많은 연산량으로 인해 복잡한 알고리즘을 쓰기 어렵거나 속도가 느려지는 문제점이 있다. 하드웨어 방식은 복잡한 알고리즘도 빠른 속도로 처리할 수 있으나 암호화 시스템이 공격을 받아 무력화되거나 새로운 암호화 시스템을 도입하여할 때 개발 시간과 비용이 많이 소요되어 시스템을 개발하기가 어렵다. 이러한 문제를 해결하기 위해서는 하드웨어 방식의 성능과 소프트웨어 방식의 유연성을 결합한 새로운 암호화 시스템을 필요로 한다.

본 논문에서는 디지털 미디어 데이터의 보호를 위해 암호화와 부호화 알고리즘을 분리시키고 데이터를 복호할 때 필요한 핵심 파라미터만을 암호화하는 방법을 제안한다. 이러한 핵심 파라미터의 접근 제한을 통해 데이터 복호화를 제한하거나 복호화된 데이터의 품질을 떨어뜨려 사용자의 만족도를 크게 저하시킬수 있다. 따라서 제안된 시스템은 일반적인 부호화 알고리즘으로 디지털 미디어 데이터를 부호화하고 이중 핵심 파라미터만을 암호화한다. 복호시에는 암호를 복호하는 알고리즘으로 파라미터를 다시 복원하여 일반적인 데이터 복호 시스템에서 복호가 되도록 한다. 파라미터의 암호를 풀지 못하는 경우 부호화 방식에 따라 차이가 있을 수 있지만 데이터의 복호는 불가능하거나 불완전하게 진행된다. 이러한 시스템의 동작을 보이기 위해 가장 좋은 압축률과 품질을 보이는 H.264 영상 복호 시스템과 공개 키 암호화 알고리즘 중 비트 당 가장 높은 안전도를 갖고 있는 타원 곡선 암호화 방식을 이용하여[4] 영상 데이터 보호 시스템을 구성하였다. 이 시스템은 마이크로프로세서와 FPGA를 이용하여 검증하였다.

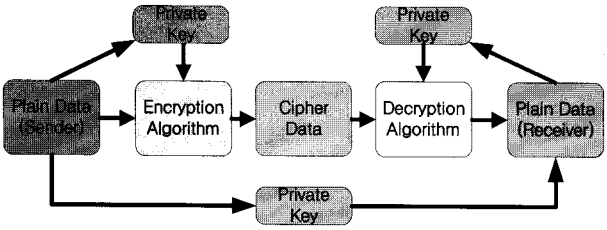
Ⅱ. 타원곡선 암호화와 H.264 복호기

1. 타원곡선 암호화

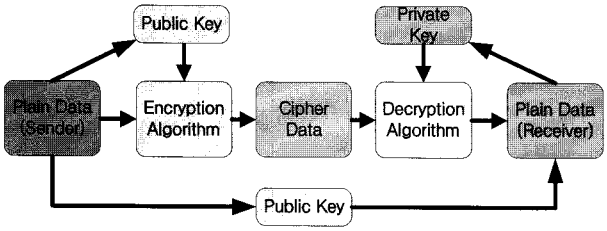
정보보호를 위해 많은 암호화 알고리즘이 개발 되었다. 네트워크에 사용된 암호화 알고리즘은 2가지로 분류된다. 암호화키의 공개여부에 따라 대칭키/비대칭키 암호화 알고리즘으로 나누어진다. 대칭키(비밀키) 암호화 알고리즘은 개인 비밀키를 이용하여 암호화를 수행하며 비대칭키(공개키) 암호화 알고리즘은 공개키와 개인키 두 가지를 이용하여 동작한다. 이러한 암호화 알고리즘에 필요한 키들은 프로세싱 기술의 발달로 인한 더 높은 안전도를 요구하게 된다. 따라서 짧은 키 길이를 가지면서도 높은 안전도를 갖는 암호화 알고리즘의 중요성이 대두된다[5].

여러 가지 암호화 알고리즘 중 타원곡선 암호화(ECC) 알고리즘은 구현된 공개키 암호 알고리즘 중 비트 당 가장 높은 안전도를 갖는다. 예를 들어, 1,024bit 키를 갖는 RSA 알고리즘은 160bit 키를 갖는 ECC 알고리즘과 같은 안전도를 보인다[6]. 작은 키 길이는 보다 작은 메모리 공간과 처리 전력을 필요로 하므로 시스템의 구현에 있어서 유리하다. 기존의 여러 ECC와 관련된 표준들에서 안전도를 고려하여 160 비트 이상의 권장 타원곡선들을 제시하고 있으며 이러한 타원곡선에서의 연산은 그 바탕을 유한체 연산에 두고 있다. 유한체 연산은 다양한 암호화 알고리즘이 이용되고 있으나 같은 암호화 알고리즘이라도 유한체 연산을 위한 키 크기에 따라 하드웨어의 구조가 바뀌어야하므로 암호화의 키 크기가 바뀔 때마다 암호화를 위한 하드웨어가 바뀌어야하는 어려움이 있다. 본 논문에서는 이러한 문제점을 해결한 ECC 암호프로세서를 사용하였다. 이용된 암호화 프로세서 구조의 특징은 프로그램 가능한 마이크로 코드 방식의 연산 제어 구조와 임의 크기의 유한체 연산이 가능한 가변 곱셈기, 그리고 모듈화 된 프로세서 구조를 가지고 있다[5]. 그리고 마이크로 코드를 바꿔줌으로써 키의 크기와 값을 변경할 수 있어 그 안전도가 매우 뛰어나다.

그림 1은 네트워크에서 많이 사용되는 암호화 방법



(a) 비밀키(대칭키) 시스템



(b) 공개키(비 대칭키) 시스템

그림 1. 비밀키와 공개키 암호화 방법[7]
Fig. 1. Encryption methods of private and public key system[7].

을 보여준다. (a)는 비밀키(대칭키)를 이용한 시스템 구조이고 (b)는 공개키(비 대칭키)를 이용한 시스템이다. 비밀키 시스템은 송/수신자가 같은 키를 이용하여 암호화/복호화를 한다. 반면에, 공개키 시스템은 송/수신자가 서로 다른 키를 가지고 암호화/복호화를 수행한다. ECC는 공개키 시스템으로 공개키를 이용하여 디지털 미디어를 암호화하고 개인은 비밀키를 부여받아 암호를 해독한다.

2. H.264 복호기

최근에 개발된 비디오 압축 코딩 기법의 H.264는 ITU-T의 VCEG(Video Coding Experts Group)과 ISO/IEC의 MPEG(Moving Picture Experts Group)의 합작으로 만들어진 압축규격이다[8]. 그림 2는 H.264 복호기의 구조를 보여 준다. H.264 복호기는 총 5개의 연산 유닛으로 구성되는데 이중 VLD(Variable Length Decoder)는 엔트로피 복호기와 재배치기로 나누어진다. VLD는 비트 스트림을 받아 양자화된 계수와 파라미터를 생성한다. 파라미터는 모든 연산 유닛으로 보내지고, 양자화된 계수는 ITQ(Integer Transform/Quantization)로 보내진다. ITQ는 받은 계수들을 역 양자화와 역 변환과정을 거쳐 오차 값을 생성 한다. MC/IP(Motion Compensation/Intra-Prediction)는 VLD에서 보내온 파라미터를 가지고 예측 블록을 생성한다.

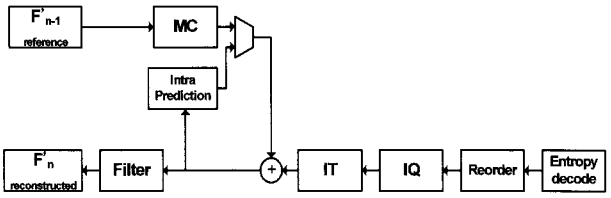


그림 2. H.264 복호기 구조
Fig. 2. Block Diagram of H.264 Decoder.

그림 3. H.264 표준의 비트 스트림 구조
Fig. 3. Bit steam format of H.264 video coding standard.

MC/IP에서 생성된 예측 블록과 ITQ에서 생성된 오차 값을 더하면 픽셀 데이터가 만들어진다. 이렇게 만들어진 데이터는 DF(Deblocking Filter)로 보내져 필터링을 통해 복호화된 블록 F'n를 생성한다.

그림 3은 H.264 복호기의 입력인 비트 스트림 구조를 보여준다. 비트 스트림은 여러 개의 NAL(Network Abstraction Layer) 유닛 조합으로 구성되고 NAL 유닛은 SPS(Sequence Parameter Set), PPS(Picture Parameter Set)와 VCL(Video Coding Layer)로 나누어진다. SPS는 프로파일, 레벨, 해상도, 포맷 등 영상 전체의 부호화 정보를 저장하고, PPS는 사용되는 픽쳐의 부호화 정보 파라미터를 저장하고 있다. VCL은 각 슬라이스의 헤더와 데이터를 저장하고 있다. 슬라이스 헤더와 데이터는 가변 길이 부호화를 거치므로 앞에서부터 차례로 복호하지 않으면 중간부터는 복호가 불가능하다. 즉, VCL은 슬라이스 헤더가 시작 부분은 바이트 단위로 시작하여 그 위치를 알 수 있지만 그 이후는 파라미터에 따라 비트 단위로 부호 크기가 변하므로 차례로 복호하면서 그 위치를 추적하지 않으면 올바른 데이터를 추출할 수 없다. 따라서, 입력되는 VCL의 시작 부분이 손상되면 슬라이스 데이터의 영상 정보를 추출할 수 없다. 입력되는 데이터의 대부분은 VCL의 슬라이스 데이터이고 SPS와 PPS, 그리고 슬라이스 헤더는 극히 일부분을 차지한다. SPS와 PPS는 해당 파라미터가 바뀔 때만 나타나고 슬라이스 헤더는 한 프레임에 한번 나타나는데 그 크기가 20~40 비트 정도이다. 이러한 슬라이스 헤더와 영상 데이터가 포함된 슬라이스 데이터 일부가 사라지면 그 이후 데이터의 복호는 불가능하다. 즉, 특정 파라미터나 데이터의 시작 비트는 바이트 정렬이 되어 있지 않아 임의로 일부 비트가 사라지면 그 이후로는 슬라이스 데이터의 끝부분에서 바이트 정

렬이 되고 시작 비트열이 나타나는 다음 VCL의 시작까지는 비트 스트림의 시작 값을 찾을 수 없다.

Ⅲ. 디지털 미디어 저작권 보호 시스템

본 논문에서 제안하는 저작권 보호시스템은 기본적으로 네트워크를 이용한 VOD(Video on demand) 또는 AOD(Audio on demand) 방식에 적합하다. 사용자는 디지털 미디어를 재생할 수 있는 단말기를 가지고 있고 이 단말기에는 영상을 재생할 수 있는 하드웨어가 포함되어 있다. 영상의 암호 해독 및 복호는 주로 복호 칩에 의해 이루어지는데 이 복호 칩에는 비밀키가 포함되어 있다.

사용자가 단말기의 고유번호와 함께 영상 데이터를 요청하면(①) 서버에서는 고유번호를 통해 비밀키를 파악하고 적절한 공개키를 이용하여 영상을 암호화하여(②) 공개키와 함께 보낸다(③). 단말기는 암호화된 데이터를 받으면 서버와의 인증 절차를 거친 후(④, ⑤) 복호화 작업을 시작하여 영상을 재생한다(⑥). 이 때 서버와의 인증 절차는 제공된 영상의 재생 횟수를 제한하기 위한 것으로 단말기는 받은 영상 데이터의 일련번호를 서버로 보내 재생 허용 여부를 묻고 서버는 이에 대한 응답을 통해 재생 횟수를 제한 할 수 있다. 이는 암호화된 인증 과정을 통해 이루어지므로 해킹으로 보안 시스템을 무력화시키기는 어렵다. 그림 4에 영상 재생 과정을 나타냈다.

서버에서는 SPS와 PPS, 그리고 필요에 따라 슬라이스 헤더와 데이터의 일부를 암호화하는데 SPS와 PPS는 처음 시작할 때와 해당 파라미터 값이 바뀌어야 할 때, 슬라이스 헤더는 한 프레임에 한번 발생한다. 일반적으로는 I-프레임의 슬라이스 헤더와 일부 데이터만

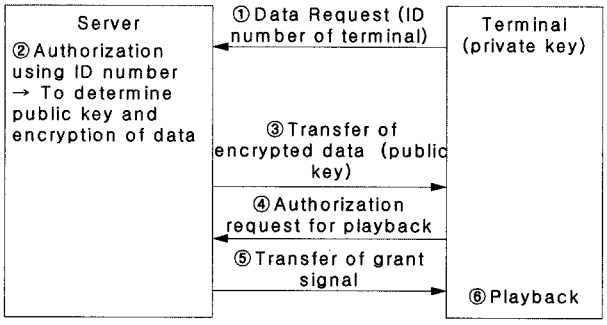


그림 4. 영상 재생을 위한 인증 및 암호화 과정
Fig. 4. Process for playback of digital media between a server and a terminal.

암호화하여 복호를 못하도록 하면, P-프레임은 참조 픽셀이 없어 영상 복호가 불가능하거나 임의의 영상을 참조 픽셀로 이용하여 복호를 시도할 경우 영상의 화질이 극히 나빠진다. 일반적으로 I-슬라이스가 수백 또는 수천 프레임에 한 번 나타나고 본 논문에서 대상으로 하고 있지는 않지만 가장 I-슬라이스가 많은 DMB 방송도 30 프레임에 한번 나타난다. 따라서 I-슬라이스만 암호화할 경우, 수백 또는 수천 프레임에 한번씩 4개의 워드 정도만 암호화하면 되므로 연산량에 대한 부담은 거의 없다. 단말기에서도 암호 해독은 동일한 비율로 하면 되므로 역시 부담이 거의 없다. 연산량에 대한 부담이 없으므로 필요할 경우 주기적으로 P-프레임이나 B-프레임에서도 암호화를 하도록 할 수 있다. 단말기는 정해진 특정 프레임에서는 무조건 암호 복호를 시도하므로 암호화되지 않은 영상을 재생하거나 암호화가 제대로 되지 않은 영상을 복호하려 하면 오히려 데이터가 손상되는 결과를 가져와 재생이 불가능하다.

제안된 시스템은 기본적으로 VOD 기반에서 효과적으로 사용될 수 있으나 디스크를 이용한 오프라인 시스템에서도 온라인 접속이 가능한 경우에는 그림 4의 ④번부터 시작하여 인증 과정을 거칠 수 있다. 그러나 온라인 시스템보다는 상대적으로 보안이 취약하다.

Ⅳ. ECCP를 적용한 H.264 복호기 구조

그림 5는 H.264 비트 스트림이 암호화/복호화 되는 과정을 보여 준다. H.264 부호기는 암호화 시스템으로 H.264 비트 스트림을 보내며 암호화 시스템은 타원 곡선 암호화 방법으로 H.264 비트 스트림의 SPS와 PPS, 그리고 슬라이스 헤더와 데이터의 일부에 해당하는 부분을 암호화 한다. 그 이외의 데이터는 그냥 통과시킨다. 슬라이스 헤더와 데이터 일부를 추가로 암호화해도 복호에 부담을 주지는 않으나 결과를 쉽게 볼 수 있도록 SPS와 PPS만을 암호화하였다. 그림 5의 E(NAL,

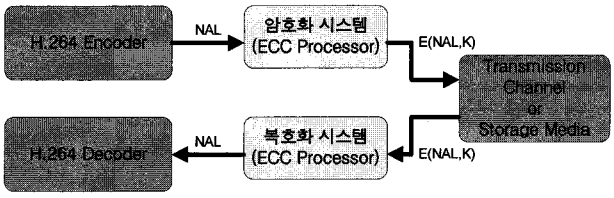


그림 5. ECCP를 이용한 암호화/복호화 과정
Fig. 5. Process of encryption and decryption using ECCP.

K)는 암호화된 H.264 비트 스트림을 나타낸다. 암호화된 H.264 비트 스트림은 인터넷의 스트리밍 서비스나 저장 매체를 통해서 클라이언트(소비자)로 보내진다. 암호화된 H.264 비트 스트림은 복호화 시스템을 통해서 원본 H.264 비트 스트림으로 복호되며, H.264 복호기로 보내진다. 복호화 시스템의 공개키가 맞지 않으면 H.264 복호기로 보내지는 H.264 비트 스트림은 오류가 발생하여 정상적으로 영상을 출력을 할 수 없다. 기존의 하드웨어 영상 암호화 시스템은 비밀키가 고정되어 있어 비밀키가 노출될 경우 암호 시스템이 무력화되는 문제가 있다. 그러나 제안한 시스템은 설계에 이용된 암호 프로세서의 비밀키를 바꿀 수 있어 하나의 비밀키가 노출되어도 비밀키 변경을 통해 암호화를 계속 유지할 수 있다.

설계에 이용된 ECCP를 이용한 타원 곡선 암호화/복호화는 프로그램 가능한 마이크로 코드 방식이기 때문에 코드의 수정을 통해 키의 크기와 값의 변경이 가능하다. 키의 크기는 1 비트부터 1,024 비트까지 가능하며, 내부 메모리를 증가시키면 키의 크기를 증가시켜 안전도를 높일 수 있다. 또한 키값이나 원시함수 등을 소프트웨어적으로 수정하는 것이 가능하므로 매우 강력한 보안기능을 갖는다. 위에서 언급한 ECCP를 이용하여 암호화 또는 복호화 연산을 수행할 때 193 비트 키를 이용할 경우 1,216 사이클이 필요한데 영상의 수십 프레임당 한번만 연산을 수행하면 되므로 연산 부담은 거의 없다. H.264 디코더가 25MHz의 동작 주파수에서 SD급 영상을 초당 30 프레임 처리하고 암호화를 1초 한 번씩 한다고 가정하면 영상 복호에 2,500만 사이클이 필요하고 암호화 처리에 1,216 사이클이 추가되어 0.005%가 증가한다. 1초에 한번 암호화는 매우 자주 하는 것으로 실제로는 이보다 훨씬 적은 영향을 받는다. 따라서 실적으로 암호화 과정에 영상 복호 성능에는 영향을 미치지 않는 것을 알 수 있다.

Ⅳ. 구현 결과

본 논문에서 제안한 방법에 따라 타원 곡선 암호화를 이용한 H.264 복호기 구조를 설계하였다. 재구성 가능한 ECC 프로세서를 사용하여 타원 곡선 암호화를 구현하였으며, H.264 복호기는 Verilog-HDL을 이용한 하드웨어와 소프트웨어를 연동하여 설계하였다. 구현된 하드웨어는 Xilinx의 Virtex4 FPGA를 이용하여 동작을

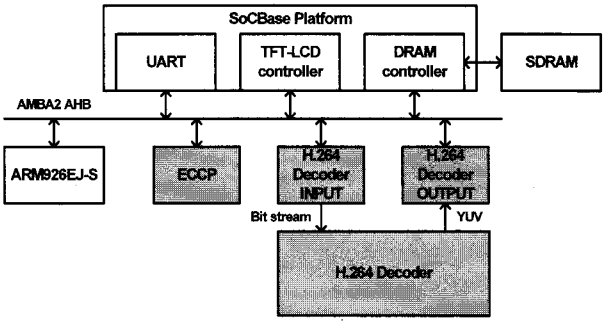


그림 6. 타원 곡선 암호화를 이용한 H.264 복호기 구조
Fig. 6. Block diagram of the H.264 decoder using elliptic curve encryption.

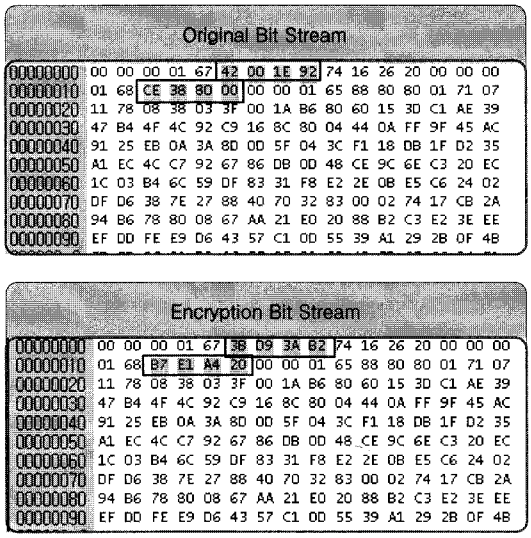


그림 7. H.264 비트 스트림의 암호화 데이터
Fig. 7. Encrypted data of H.264 Bit stream.

검증하였다. 합성 결과 H.264 디코더는 32,824 LUT, ECCP는 5,482 LUT를 사용하여 ECCP가 전체 면적의 14% 정도를 차지한다. 전체 시스템의 검증을 위해서는 ARM9 프로세서와 SoCBase[9] 플랫폼을 사용했다. 그림 6은 제안된 타원곡선 암호화를 이용한 H.264 복호기의 전체 시스템 구성을 보여 준다. ECCP와 H.264 복호기는 AMBA AHB[10]에 연결되어 ARM 프로세서에 의해 제어된다.

원본 영상은 JM 9.0 소프트웨어와 ECCP를 이용하여 인코딩 및 암호화를 진행하고 H.264 복호기의 복호화 시스템은 ARM 프로세서에 의해 구동되는 ECCP와 H.264 디코더를 FPGA에 구현하여 영상 복호를 확인하였다. 그림 7은 H.264 부호기에서 출력된 원본 H.264 비트 스트림과 암호화된 H.264 비트 스트림의 16진 코드이다. 빨간 상자로 둘러싸인 부분이 암호화된 값으로 NAL 유닛의 SPS와 PPS 값이다. 이들은 H.264 복호기

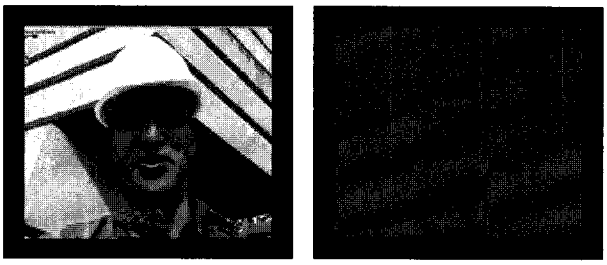


그림 8. 검증 결과 화면 (a) 암호를 복호한 정상 영상 (b) 암호 복호를 하지 않은 오류 영상
Fig. 8. Decoded images (a) Image after decrytion (b) Image without decryption.

가 영상을 복호하기 위한 파라미터 값이다. 복호화 과정은 암호화 과정과 동일하다. 암호화된 H.264 비트 스트림은 ECCP를 통해 원본 H.264 비트 스트림으로 복원된다. 비트 스트림의 0x000001는 NAL 유닛의 시작 패턴이다. 시작 패턴 뒤에는 NAL 유닛의 정보가 포함되어 있다. 시작 패턴 뒤에 있는 0x67, 0x68 이후의 값이 각각 SPS와 PPS를 나타낸다.

그림 8(a)는 암호화된 H.264 비트 스트림이 정상적으로 복호된 결과이고, (b)는 암호화 프로세서를 통과하지 않은 경우의 결과 이미지이다. H.264의 특성상 VLD의 파라미터 파싱연산에서 에러가 발생하고 전체 H.264 복호기가 멈추게 되어 TFT-LCD에 초록색 화면이 출력된다.

V. 결 론

본 논문에서는 타원 곡선 암호화를 이용한 디지털 미디어 저작권 보호 방법을 제안하고 그 응용 예로서 타원 곡선 암호화를 적용한 H.264 복호기를 설계하고 FPGA와 ARM 프로세서를 이용하여 동작을 검증하였다. 제안된 시스템에 이용된 타원 곡선 암호화 프로세서는 프로그래밍이 가능한 마이크로 코드 방식의 ECCP를 이용하여 소프트웨어적으로 프로세서를 프로그래밍 하여 재구성이 가능하다. 이에 따라 키 값, 원시함수, 키의 길이 등을 변경 변경시킬 수 있어 안전도를 증가 시킨다. H.264 복호기는 하드웨어 방식으로 동작하고 암호화 프로세서와는 분리되어 있어 별도로 설계할 필요가 없다. 제안된 방식에 따라 타원 곡선 암호화를 이용하여 H.264 비트 스트림의 SPS와 PPS, 그리고 슬라이스 헤더와 일부 데이터를 암호화/복호화한다. 이 작업은 수백 또는 수천 프레임당 한번만 수행하면 되므로 연산 부담이 적은 반면 암호 해독이 제대로 되지 않으면 정상적인 복호가 불가능하거나 영상의 화질이 매우 떨어진다. 설계된 디코더는 FPGA에서 동작을 검증하였다. 구현된 시스템은 인터넷 스트리밍 서비스와 저장매체를 이용한 응용분야에서 유용하게 사용하게 될 수 있으리라 기대된다. 또한 ECC가 아닌 다른 암호화 알고리즘과도 결합하여 비슷한 효과를 볼 수 있다.

참 고 문 헌

[1] C.-C. Chung-Ping, J. Kuo, "Design of Integrated Multimedia Compression and Encryption Systems", IEEE Transactions on Multimedia, Vol. 7, No. 5, pp.828-839, Oct. 2005.
[2] D. Joshua, K. Susan, "Understanding DRM Systems" IDC White Paper, IDC, 2001.
[3] M. Wu, Y. Mao, "Communication-friendly encryption of multimedia", IEEE Workshop on Multimedia Signal Processing, pp. 292-295, Dec. 2002.
[4] K. H. Leung, K. W. Ma, W. K. Wong, and P. H. W. Leong, "FPGA implementation of a microcoded elliptic curve cryptographic processor," 2000 IEEE Symposium on Field - Programmable Custom Computing Machines, pp. 68-76, Napa Valley, USA, Apr. 2000.
[5] 이지명, 이찬호, 권우석, "재구성 가능한 타원 곡선 암호화 프로세서 설계", 대한 전자공학회 논문지 제 42권 SD 제 6호, pp. 67-74, 2005.6
[6] "SEC2: Recommended Elliptic Curve Domain Parameters. v. 1.0," Certicom Corp, pp. 29-32, Sept. 2000.
[7] M. Yang, N. Bourbakis, S. Li, "Data-image-video encryption" IEEE Potential, pp. 28-34, Aug. 2004.
[8] G. J. Sullivan, P. Topiwala, A. Luthra, "The H.264/AVC Advanced Video Coding Standard" SPIE conference, pp. 454-474, Aug., 2004.
[9] Sanggyu Park, Soo-Ik Chae, "SoCBase: An Integrated solution for platform based design," International SoC Design Conference, Seoul, Korea, pp. 862-863, Oct. 2004.
[10] ARM, "AMBA Specification, Revision 2.0", 1999.

저 자 소 개

이 찬 호(정회원)
대한전자공학회 논문지
제43권 SD편 제9호 참조
현재 숭실대학교 정보통신전자공학부 교수