논문 2009-46IE-2-5

무선 이동 단말기의 특성을 이용한 MPEG 기반의 멀티미디어 데이터 보안 시스템

(A Multimedia Data Security System Based on MPEG Using The Specific of Wireless Device)

이 종 갑*, 성 홍 석*, 원 영 진*, 이 종 성*, 임 승 하*, 임 영 환**

(Jong-Kap Lee, Hong-Seok Seong, Young-Jin Won, Jong-Sung Lee, Seung-Ha Lim, and Young-Hwan Lim)

요 약

본 논문에서는 무선 이동통신환경에서 다양한 멀티미디어 데이터에 대한 정보제공자와 사용자를 위한 데이터 보안을 위한 시스템을 제안한다. 무선 이동통신환경은 편리성과 유용성으로 사용자가 매우 많으며 대역폭의 증가로 인한 멀티미디어 데이터의 사용량이 증가 했지만 데이터의 보안에 대한 부분은 부족한 부분이 많아 저작권이 보호되지 못하고 있다. 따라서 본 논문에서는 부적합 사용자에게는 멀티미디어 컨텐츠의 내용을 숨기고 적절한 사용자에게는 정확한 데이터를 제공할 수 있는 컨텐츠 보호시스템에 대한 내용을 제안한다. 정보제공자와 사용자는 상호 신뢰성을 확립할 수 있으며 이동단말기와 PC의 특성을 이용한 간단한 인증과정을 통해 쉽고 편리하게 원하는 컨텐츠를 사용할 수 있다.

Abstract

In this article, the protection system on wireless mobile communication circumstance for the information providers and the users is recommended. Because of its usefulness and convenience, the users of the wireless mobile communication are growing explosively. However, the function of protecting data systems is not secured enough so, personal information may disclose to the outside, regardless of one's intention. Therefore, the contents protection system, which can provide information to the user or hide it depending on user's identity, is suggested. If so, the providers and the users can trust each other for interchanging information, also the users may safely use contents menu whatever they want by doing simple certification process.

Keywords : 정보보호(Security), 멀티미디어(Multimedia), 모바일(Mobile), 씨드(SEED)

Ⅰ. 서 론

인터넷을 통한 정보의 공유는 대부분 빠른 대역폭과 빠른 성능을 갖는 개인 PC환경에서 주로 이루어 졌으나 3세대 이통통신의 HSDPA(High Speed DATA Packet Access)의 경우 최대 14.4Mbps의 데이터 전송률이 가능하기 때문에 무선 이동단말기에서 빠른 속도의 인터넷 이용이 가능해졌다[1]. 따라서 PDA나 UMPC는 물론 무선 이동단말기를 통한 정보의 전달과 공유가 활발히 이루어지고 있다. 무선 이동단말기는 개인화와 휴대성을 장점으로 대다수의 사용자들이 사용하고 있으며 무선 인터넷은 물론 DMB나 모바일TV등과 같은 멀티미디어 컨텐츠 활용에 적극 이용되고 있다. 일반 데

* 정회원, 부천대학 전자공학과
(Department of Electronic Engineering, Bucheon University)
** 정회원, 숭실대학교 미디어학부
(Department of Media, Soongsil University)
접수일자: 2009년4월21일, 수정완료일: 2009년6월10일

이터에 비해서 크기와 CPU점유율이 높은 멀티미디어 데이터를 퀄컴의 MSM 씨리즈 칩셋이 하드웨어적으로 뒷받침을 해주기 때문에 QVGA는 물론 VGA급 동영상까지 무선 이동단말기에서 활용이 가능하다[2]. 이렇듯 무선 이동단말기에서의 멀티미디어 컨텐츠 활용은 늘고 있지만, 사용자가 취득한 디지털 정보는 복제, 불법 유통 등이 매우 쉬운 디지털 데이터이기 때문에 정보제공자의 입장에서는 저작권 보호나 수익율 저하의 문제가 생길 수 있다. 이동단말기를 위한 컨텐츠 서비스는 쉽고 편리하면서도 안전하게 서비스되어야 저작권자와 사용자와의 신뢰를 확립할 수 있다. 따라서 유선은 물론 무선 상에서의 정보보호 기술 역시 이러한 추세에 대처해야 한다.

무선 이동단말기를 통한 정보의 불법 공유나 전달의 문제를 해결하기 위해서는 컨텐츠 자체의 정보보호도 중요하지만 무선 이동단말기의 장점인 편리성을 해치지 않는 범위에서 정보보호가 이루어져야한다. 무선 이동단말기는 휴대성과 편리성이 장점이지만 휴대성을 강조한 작은 크기는 인터페이스가 PC에 비해서 불편하다는 단점을 갖는다. PC의 키보드에 익숙한 사용자들이 이동단말기의 키패드를 이용해 한글과 영어 및 특수문자를 바꿔가며 자유롭게 사용하기는 쉽지 않다. 따라서 어떤 컨텐츠를 이용하기 위해서 매번 아이디와 비밀번호를 넣는다던지 별도의 암호를 입력해야 한다면 무선 이동단말기의 장점인 편리성은 없어진다. 즉, 정보보호는 유지하면서 사용자의 편리성을 유지하기 위해서는 무선 이동단말기의 특성과 인터페이스의 단점을 극복한 형태의 정보보호 시스템이 필요하다.

본 연구에서는 다양한 멀티미디어 데이터를 이동단말기와 PC에 서비스할 때 아이디와 비밀번호를 입력하는 과정없이 간단하게 사용자 인증을 하며 개개인의 사용자에게 사용허가를 주는 방식에서 벗어나 단말기별로 사용허가를 줄 수 있는 방법에 대해 기술한다. 또한 불법으로 컨텐츠를 획득한 사용자가 불법배포나 복사 등을 할 수 없도록 멀티미디어 컨텐츠 자체를 암호화하는 방법에 대해 기술한다. 디지털 권리 관리(Digital Rights Management, DRM) 기술은 디지털 컨텐츠 유통과정에서 발생하는 권리와 신뢰성, 컨텐츠의 안전성 및 재 활용성, 유통의 투명성을 보장하는 종합적인 구조로서 정의 할 수 있다. 따라서 DRM은 암호화 기술, 워터마킹 기술, 변조방지 기술을 포함하며 저작권자와 정보 이용자 간의 신뢰를 제공하며 DRM이 적절한 체계를 갖추었는지는 다음과 같은 관점에서 판단할 수 있다[3]. 첫째, 저작권자와 유통업자 사이에 서로 신뢰할 수 있게 구조적인 체계를 지원해야 한다. 둘째, 유통업자와 소비자 사이에 컨텐츠의 안전한 전송과 사용이 보장되어야 하며 마지막으로 컨텐츠를 타인에게 제공했을 때 타인이 합법적으로 해당 컨텐츠를 사용 할 수 있게하는 Superdistribution의 구조를 지원해야한다. 따라서 저작권에 대한 권리를 갖는 컨텐츠 제공자는 저작권의 보호를 위해 허가되지 않은 사용자로부터 데이터를 안전하게 보호해야 하며 허가된 사용자가 데이터를 재배포할 경우에도 데이터에 대한 저작권 보호를 위한 재배포 금지가 이루어져야한다. 저작권 보호를 위한 기술은 암호화 기술을 중심으로 연구되었으며 디지털 워터마킹[4], 암호화 기술[5], 접근제어 기술[6~7] 등이 사용된다. 이와 같은 정보보호 기술은 컨텐츠 자체를 보호하고 저작권자가 누구인지를 알아내는 방법은 훌륭한지만 불편한 인터페이스를 가지며 편리성을 우선시하는 무선 이동단말 환경에는 적합하지 않다. 그러므로 강력한 정보보호를 유지하면서 쉽고 편리하게 사용할 수 있는 무선 이동단말기에 적합한 방법이 필요하다.

이동 통신 단말기는 낮은 성능의 프로세서를 가지고 있으며 휴대용 전원을 사용하기 때문에 짧은 프로세싱을 통해 빠른 시간에 수행되는 것이 유리하다. 접속시간은 무선 통신 비용과도 연결되기 때문에 접속 시간을 최대한 줄이는 방법이 유리하다.

동영상 암호화와 관련된 연구 방법으로는 컨텐츠 사용자가 정상적인 과정을 거치지 않는다면 영상을 왜곡시켜 수신자의 권리를 보호하기 위한 방법이 연구되었다.

주파수 공간에서 웨이블릿 기반의 왜곡 방법은 웨이블릿 변환으로 생성된 부대역을 블록으로 나누고, 블록내의 계수값을 블록별로 섞음으로서 영상의 왜곡을 만든다. 하지만 이런 접근 방법은 웨이블릿 변환을 수행하지 않는 대부분의 영상 압축 코딩방법에는 적용할 수 없다는 단점을 갖는다[8].

모션벡터를 이용한 방법은 이전 매크로블록(Macro Block)의 모션벡터와 추정된 매크로블록의 예측 모션벡터의 차이인 차동 모션벡터(Differential Motion Vector)를 구한 후, 가변 길이 부호화(Variable Length Codeing)전 전송 블럭의 형태 값을 모듈러스 33으로 연산한 후 연산된 결과만큼 부호화 테이블에서 떨어져 있는 부호를 이용해 부호화한다. 하지만 이 방법은 모듈러스 연산을 통해 변위된 결과를 이용해 부호화를

하기 때문에 변위된 코드의 길이가 기존 코드와 같지 않을 수 있으며 비트량이 증가 할 수 있다는 단점을 갖는다[9].

AES나 DES 알고리즘을 이용해 영상 신호 자체를 암호화하는 방법은 영상 전체를 암호화 하는 경우 복잡도가 매우 높다는 문제가 있다. 따라서 이 같은 문제를 해결하기 위해 영상의 중요도에 따라 모션벡터나 매크로블록, 인트라 프레임이나 인트라 블록만을 암호화 하고 가장 낮은 중요도를 갖는 영상은 헤더정보만을 암호화함으로서 복잡도는 낮추는 정책을 사용했다. 하지만 이같은 선택적 암호화 방법은 영상의 중요도를 판단하는 기준에 따라 암호화 시간이 달라질 수 있으며 데이터의 일부분만 암호화하며 멀티미디어 데이터의 고유 코딩 특성을 이용하기 때문에 범용적 적용이 어렵다.[10~12].

가장 확실하고 보안이 보장되는 방법은 전체 컨텐츠에 대한 암호화를 수행하는 것이지만 일반적으로 무선 이동단말기는 연산장치의 성능과 메모리가 적기 때문에 전체 컨텐츠를 암호화하기에는 시공간복잡도가 너무 높아진다. 또한 무선 이동단말기는 전원이 한정되어있고 무선 통신접속 시간이 길어질수록 이용요금 또한 많아지기 때문에 빠른 시간에 적은 연산으로 처리되는 것이 유리하다. 따라서 본 연구에서는 전체 컨텐츠를 암호화하지 않고 중요 프레임에 대한 암호화를 선택적으로 적용한다. 이때, RTP 전송 스트림의 페이로드(Payload)로 전송되는 I 프레임을 암호화 대상으로 삼으며 중요 정보인 매크로블록에 대한 선택적 암호화를 수행함으로서 시간복잡도를 낮춘다.

본 연구는 무선 단말기의 불편한 UI로 인한 문제점을 단말의 고유값을 이용해 별도의 인증과정없이 쉽게 컨텐츠를 이용하고, 동영상을 전송할 때 사용자의 고유값으로 암호화를 함으로서 불법 사용자가 패킷을 전송받는다고 하더라도 정상적인 재생이 불가능하다. 이때, 전체 프레임을 암호화하지 않고 동영상의 중요 프레임인 I 프레임의 매크로블록에 대한 암호화를 수행함으로서 암호화 시간을 단축시킬 수 있으며 파일포맷이 변경되지 않고 비트량의 증가도 없다는 장점을 갖는다. 만일 키가 없는 불법 사용자가 동영상을 디코딩 하더라도 파일 규약에는 맞기 때문에 화면 재생은 되지만 정상적인 복호화 과정을 거치지 않았기 때문에 원래의 영상은 볼 수 없다.

Ⅱ. 시스템 구성

Ⅱ-1. 시스템의 처리구조

본 시스템의 기본 구성요소와 흐름은 그림 1과 같다. 시스템의 중요부분은 단말기의 접속과 서비스를 담당하는 단말기 관리자(Device Manager, DM)와 컨텐츠에 대한 암호화를 담당하는 컨텐츠 부호기(Contents Encryptor, CE)로 나뉘어진다. XCrawler는 멀티미디어 컨텐츠의 크기나 형식 등이 이동단말기에 적합하게 서비스 될 수 있도록 최적화된 크기와 형식으로 변화시켜주며 적합한 마크업 언어로 웹페이지를 변환하는 역할을 수행하며 이때 단말기의 특징 정보는 단말기 정보 데이터베이스를 통해 검색된다[13].

컨텐츠 서비스를 원하는 단말기가 접속하면 각 단말기는 우선 DM을 통해 접속이 된다. 이때 DM에서는 각 단말기의 특성정보와 단말기의 고유식별 정보를 파악해서 컨텐츠 접속이 허가된 사용자인지에 대한 검증을 수행한다. 단말기의 중요 구분요소는 ESN(Electronic Serial Number), MIN(Mobile Identification Number), SCM(Station Class Mark)등으로 구분할 수 있다. ESN은 모든 휴대전화에 내장된 8자리의 핵사코드(32bits)로서 단말기의 고유 ID로서 교환기와 호처리시 사용된다. 그리고 사용자 관리와 요금 청구에 활용되며 변경이나 복제 시 문제가 된다. MIN은 단말기의 전화번호이며 SCM(Station Class Mark)은 사용모드를 정의하는 파라메터로서 단말기의 기능에 따라서 NAM(Number Assignment Module) 프로그래밍으로 입력되어야 한다.

무선 이동통신사의 통화연결과정은 사용자가 통신을 시도하면 사용자 단말의 ESN과 MIN이 MSC(Mobile Switching Center)를 통해 HLR(Home Location Register)로 연결된다. 이때 MSC는 교환기이며 HLR은 단말기 정보나 가입자 정보 그리고 부가서비스 등에 대한 정보를 저장하고 있어서 정상적인 확인이 되면 통신

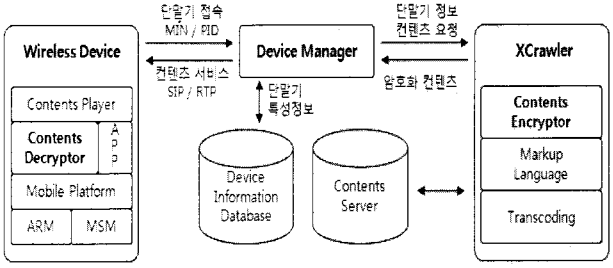

그림 1. 시스템 기본 구성 요소
Fig. 1. Draft System Configuration.

접속이 이루어진다. 따라서 ESN과 MIN은 단말기의 고유정보를 포함하기 때문에 불법 단말기 복제에도 사용된다. ESN을 고유키로 이용하는 것이 MIN을 이용하는 것보다 좋지만 ESN을 마음대로 이용하는 것은 법적인 문제도 있으며 통신사와 협의가 되야 할 부분도 있기 때문에 본 연구에서는 MIN과 PIN (Personal Identification Number)을 이용한다. PIN은 사용자가 사용하는 개인암호로서 MIN과 PIN을 조합함으로서 통신 중 불법 사용자가 패킷을 가로채는 경우가 생긴다고 하더라도 정상적인 디코딩을 할 수 없다.

DM은 이동 단말기일 경우는 이동 단말기의 고유 전화번호를 추출해서 사용자 인증을 한다. 적합한 사용자인 경우 DM은 XCrawler로 단말기 정보와 컨텐츠 서버에서 어떤 컨텐츠를 서비스할 것인가에 대한 정보를 전달한다. XCrawler는 전달받은 정보를 기반으로 서비스할 컨텐츠를 암호화 한다. 이때, 웹페이지에 대한 마크업 변환이나 컨텐츠 변환이 필요한 경우 단말기에 적합한 형태로 크기나 비트율 변환을 수행한다. 컨텐츠 암호화를 수행하는 CE는 DM으로부터 전달받은 단말기의 특징정보를 기반으로 암호화 키 값을 생성하고 이 키값을 기반으로 암호화를 수행한다. 컨텐츠 서버에 있는 텍스트, 이미지, 오디오나 비디오 같은 멀티미디어 데이터는 컨텐츠 자체에 대한 암호화가 없는 일반 데이터이다. 따라서 CE는 컨텐츠 서버에 있는 각 멀티미디어 데이터를 서비스 요청한 사용자의 단말기 전화번호와 MAC Address를 이용해 암호화된 컨텐츠를 생성한다. 이때 CE에서 사용하는 암호 알고리즘은 SEED 알고리즘을 이용하며 SEED는 민간 부분인 인터넷, 전자상거래, 무선 통신 등에서 공개 시에 민감한 영향을 미칠 수 있는 정보의 보호와 개인 프라이버시 등을 보호하기 위하여 개발된 128비트 블록암호알고리즘으로서 전자상거래, e-mail, 인터넷 뱅킹, 데이터 저장, VPN, 지적재산권 보호 등의 다양한 분야에서 사용되고 있다[5].

단말 고유 키 값으로 암호화된 컨텐츠 데이터는 DM을 통해 요청 단말기로 전달된다. 이때, 단말기로 전송하는 패킷은 RTP Stack을 이용한다(그림 2). RTP Payload는 1024KB로 구성되며 전체 Payload를 암호화하면 보안성은 높아지지만 암복호화에 소요되는 시간복잡도가 높아지기 때문에 실시간 스트리밍정보 전송에 적합하지 않다. 따라서 영상의 중요 정보인 I 프레임에만 암호화를 수행함으로서 시간복잡도를 낮추고 동영상

그림 2. RTP Payload
Fig. 2. RTP Payload.

의 기준이 되는 I 프레임을 암호화 함으로서 복호화없이 재생한다면 P픽처 또한 정상적인 화면이 출력되지 않는다.

암호화된 데이터를 전달받은 무선 이동단말기는 위피(WIPI)기반의 컨텐츠 복호기에서 자체 단말기의 정보를 이용해 복호화 키 값을 생성한 후 복호화를 수행하면서 동영상이나 이미지를 재생한다.

II-2. 접속 단말기 정보 분석

DM에 접속된 이동단말기의 헤더 정보를 분석하면 그 단말기의 특정 정보를 획득할 수 있다. 유저 에이전트(User Agent, UA)정보에서 앞의 3자리는 이동통신사의 식별 번호를 의미한다. 예를 들면 SKT는 011, LGT는 019, KTF는 016, 010은 010식별 번호를 의미한다. 그리고 지원 단말기의 모델이나 지원되는 브라우저, 마크업 언어 등에 대한 정보를 알아 낼 수 있다[13~14]. 본 연구에서는 UA정보 중 사용자의 고유 특성이라 볼 수 있는 이동 단말기의 전화번호를 기준으로 보안 키 값을 생성한다. 물론 MIN값을 고유키로 이용하는 것은 보안상 취약할 수 있기 때문에 사용자가 정의한 PIN값을 함께 이용한다. PIN값은 사용자가 사이트에 등록할 때 입력하기 때문에 사용자의 암호화 키로 사용될 수 있다. PIN을 함께 적용하는 이유는 사용자의 MIN값만 암복호화 키로 사용하는 경우 불법사용자가 중간에 패킷을 가로채게 되면 사용자의 MIN값을 이용해 쉽게 복호화를 할 수도 있기 때문에 PIN값을 함께 적용한다. 이때, 단말의 고유정보인 ESN을 키로 적용하면 좋지만 ESN을 임의로 이용하는 것은 현재 법적으로 불법이기 때문에 MIN과 PIN을 테스트에 이용했다. 이때, 암복호화에 사용되는 키는 다음과 같이 계산된다.

$$KEY_{(m+n)} = PIN_{(m)} + MIN_{(n)} + P \quad (1)$$
(이때, m+n+P=16, P : zero padding)

암복호에 사용되는 키는 128비트를 이용하기 때문에 PIN 4바이트를 기본으로 하고 MIN값은 통신사 식별번호를 포함해 2G 번호일 경우는 10바이트, 3G번호일 경우는 11바이트를 사용한다. 따라서 16바이트 키를 생성

하기 위해 모자란 1~2바이트는 0패딩 한다. 이 과정을 통해 설령 특정 단말기로 전송되는 패킷을 불법 사용자가 가로채더라도 사용자의 MIN을 알아야하며 또한 PIN값 또한 알아야 패킷 디코딩이 가능하다. 그리고 전체 프레임을 암호화하지 않고 I프레임만 암호화함으로서 시간적 복잡도를 낮출 수 있다.

접속 단말기의 UA를 분석해 MIN을 추출하는 과정과 키를 생성하는 과정을 자동적으로 사용자의 기본 정보를 이용해 생성함으로서 아이디와 비밀번호를 이용해 컨텐츠를 보호하려는 노력에 비해서 다음과 같은 장점을 가질 수 있다.

우선 이동 단말기의 경우 입력 장치의 편의성이 PC와 같이 충분히 편리하지 못하기 때문에 접속 시 매번 아이디와 비밀번호를 입력해야 한다면 컨텐츠의 접근 편리성이 매우 감소 될 수 있다. 그리고 아이디와 비밀번호가 누출되거나 혹은 타인과 공유할 경우 컨텐츠 제공자의 입장에서는 부적절한 사용자에 대한 거부 수단이 부족하다. 하지만 이동 단말기의 고유번호를 이용한다면 네트워크 접속 시에 사용자의 고유번호를 인증 수단으로 사용할 수 있기 때문에 별다른 사용자의 입력 없이 쉽게 컨텐츠로의 접근이 가능하며 다른 단말기로는 정보 접근이 제한된다.

II-3. 멀티미디어 데이터 암호화

SEED 알고리즘은 입력된 128비트 블록을 64비트 두 개의 L_i-1과 R_i+1 블록으로 나누어서 수행된다. 이때 R_i+1 는 키 생성 알고리즘에 의해 생성된 32비트의 라운드 키와 F함수의 입력이 되며 F 함수의 출력과 L_i-1블록의 값을 Bitwise ExclusiveOR 연산을 수행하여 다음 라운드의 R_i블록으로 처리된다(식 2). 이때 F함수는 라운드 키 생성과정을 통한 32비트 라운드키를 입력 받아 처리된다. 이와 같은 과정을 16라운드 수행하여 128비트 암호

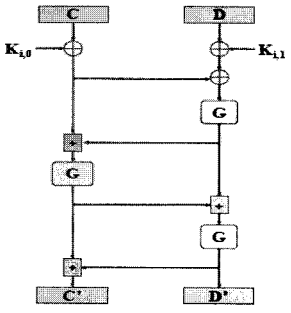

그림 3. F함수 동작과정
Fig. 3. Operation Process of F Function.

문을 생성한다[5, 15~16]. F함수는 각 32비트 블록 2개(C, D)를 입력받아 (C′, D′)를 출력한다(그림 3). 이때, C′와 D′는 다음 식에 의해 결정된다[17].

암호화된 멀티미디어 데이터는 DM을 통해 서비스 요청 단말기로 컨텐츠를 서비스 하게 되며 암호화된 데이터를 전송하기 때문에 중간에 누군가 데이터를 가로채거나 잘못 전송되더라도 고유 단말의 키 값이 다르기 때문에 정상적으로 복호화 되지 않는다.

암호화 데이터를 전송 받은 서비스 요청 단말기는 별도의 인증과정이 불필요하기 때문에 편리하고 쉽게 복호화된 컨텐츠를 이용할 수 있다.

$$
\begin{aligned}
C' &= G[G[G\{(C\oplus K_{i0})\oplus(D\oplus K_{i1})\}\boxplus(C\oplus K_{i0})]\boxplus G\{(C\oplus K_{i0})\oplus(D\oplus K_{i1})\}]\boxplus G[G\{(C\oplus K_{i0})\oplus(D\oplus K_{i1})\}\boxplus(C\oplus K_{i0})] \\
D' &= G[G[G\{(C\oplus K_{i0})\oplus(D\oplus K_{i1})\}\boxplus(C\oplus K_{i0})]\boxplus G\{(C\oplus K_{i0})\oplus(D\oplus K_{i1})\}]
\end{aligned} \tag{2}
$$

$a\oplus b$ = a bit-wise ExclusiveOR b

$a\boxplus b = (a+b) \bmod 2^{32}$

$K_{i,0}$ = i라운드 F함수의 오른쪽 입력키(32비트)

$K_{i,1}$ = i라운드 F함수의 왼쪽 입력키(32비트)

기본적으로 키 값은 UA정보를 통해 분석된 MIN과 PID를 이용해 텍스트나 이미지, 사운드, 동영상 같은 파일을 암호화시킨다. 이동단말기의 기종이나 사용자는 같거나 혹은 다르더라도 단말기에 부여된 고유분류는 할당된 전화번호를 이용해 구별할 수 있다. 따라서 단말기의 전화번호를 키 값으로 이용하기 때문에 사용자 단위로 사용허가를 방식이 아닌 단말기별 사용허가가 가능하다.

텍스트나 이미지 같은 경우 전체 파일을 암호화 할 경우 시간 소모량이 크지 않지만 사운드나 동영상 같은 경우는 데이터 자체의 크기가 매우 크기 때문에 전체 파일에 대한 암호화를 수행하기에는 시간복잡도가 많이 증가한다는 단점을 가지게 된다. 따라서 컨텐츠의 중요데이터인 I 픽처에 대해 암호화를 수행함으로서 암복호화에 수행되는 시간복잡도를 줄인다. 이 과정을 거치는데 두 가지 경우가 있다. 첫 번째는 기존의 컨텐츠를 사용자에게 서비스하는 경우이고 두 번째 경우는 실시간 촬영된 영상을 사용자에게 전송하는 경우이다. 두 가지 경우 모두 RTP를 통한 영상전송을 수행하며 기본적인 처리방법은 다음과 같다.

입력 영상이 실시간 촬영되는 영상이면 영상 전송을

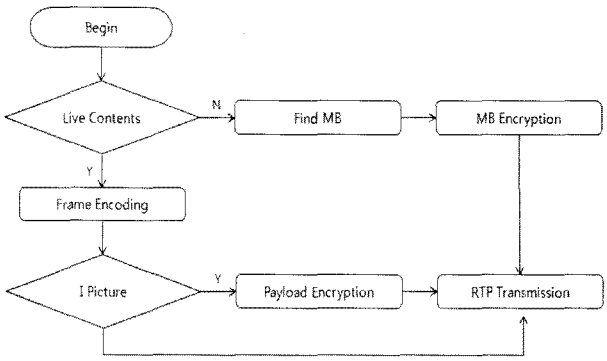

그림 4. 실시간 영상과 동영상 파일 암호화
Fig. 4. The Encryption of Real time's Image and MPEG file.

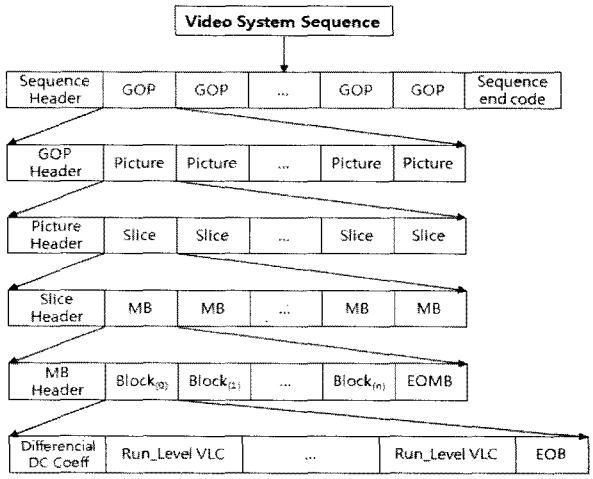

그림 5. MPEG 동영상의 데이터 구조
Fig. 5. Data Structure of MPEG.

위한 인코딩을 수행하고 한 프레임이 완성되면 상대방에게 실시간 영상을 전송한다. 이때, 인코딩 영상이 I 프레임이라면 RTP 페이로드를 암호화한 후 전송한다. 그리고 파일 형태의 동영상이라면 I 프레임의 매크로블록에 대해서 암호화를 수행한 후 사용자에게 전송한다. 이와 같은 과정을 통해 일반 동영상은 물론 실시간 영상 전송에도 낮은 복잡도로 안전하게 영상 전송이 가능하다.

이 같은 과정은 DCT(Discrete Cosine Transform)에 기반한 동영상의 인코딩 특성을 이용한다. MPEG 동영상의 경우 Video Sequence layer는 GOP(Group Of Picture)로 구성되며 GOP는 Picture Layer, Picture Layer는 Slice Layer로 구성되며 Slice Layer는 Macro Block Layer로 이루어지기 때문에 하나의 레이어에 대한 구성이 올바르지 못하다면 전체적으로 올바른 영상을 재생하지 못한다. 그림 5는 MPEG 동영상의 데이터 구조를 보이고 있다.

일반적 멀티미디어 데이터는 헤더의 구조가 정형적인 것이 아니라 다음 블록의 내용이 가변적으로 변하기 때문에 다음 블록부분에 대한 정보를 담고 있기 때문에 특정 부분의 정보를 숨기게 되면 다음 부분의 정보를 정확히 파악할 수 없기 때문에 정상적이 재생이 어렵게 된다. 빠른 암복호화를 위해서 헤더부분만을 암호화할 수도 있지만 헤더의 변경으로 인해 잘못된 포맷으로 인식될 수도 있기 때문에 제안 방법에서는 하위레벨의 레이어 부분을 포함한 매크로블록 단위까지 암호화한다.

이때, 동영상의 파일 헤더 부분만을 암호화하기 위한 계산은 (3)과 같다.

$$V^{E}_{(HDR+SC(HDR))i} = SEED(V_{(HDR+SC(HDR))i} \oplus K) \quad (3)$$

V는 입력영상이고 V^E는 암호화 결과 영상이며, HDR는 Sequence Header, GOP Header, Picture Header, Slice Header, MB Header등의 헤더의 시작데이터를 의미한다. S는 각 Header의 Start Code를 의미한다. 계산에서 얻어진 각 헤더나 MB는 사용자 고유 키에 의해서 결과를 생성한다. K는 식(1)에 따라 생성된 값이며 i는 동영상내에 포함된 MB나 Header의 수다. 복호화에 사용되는 계산은 식(4)과 같으며 V^D는 복호화된 영상을 의미한다.

$$V^{D}_{(HDR+SC(HDR))i} = SEED(V^{E}_{(HDR+SC(HDR))i} \oplus K) \quad (4)$$

동영상 I 프레임의 매크로블록의 암복호화는 다음과정에 따라 수행된다(그림 6). 각 Slice Header의 매크로블록의 각 매크로블록 데이터에 대해서 SEED알고리즘을 적용한다. 16바이트 매크로블록 데이터와 고유키를 적용함으로서 암호화데이터를 생성하고 복호화도 같은 방법으로 적용된다.

실시간 영상의 I 픽처에 대한 암호화도 거의 동일한 과정을 거치며 n번째 프레임이 I 픽처인 경우에 대해서만 매크로블록 암호화를 적용한 후 페이로드의 크기만큼 프레임을 나눠서 실시간 전송을 수행한다.

```
foreach MB(k)
    foreach Block(i)
        SEED(BlockData⊕K)
    endforeach
endforeach
```

그림 6. 매크로블록의 암복호화
Fig. 6. Encrypting and Decrypting of Macro Block.

```
Encode Frame(n)
  if FrameType(n) Equal I
    foreach MB(k)
      foreach Block(i)
        SEED(BlockData⊕K)
      endforeach
    endforeach
```

그림 7. 실시간 영상 패이로드 암복호화
Fig. 7. Payload Encrypting and Decrypting of Real time's Image.

블록단위 암호화 알고리즘은 블록단위로 암호화를 수행하기 때문에 대상 데이터가 특정 바이트로 나눠지지 않는다면 데이터의 모자라는 부분에 패딩데이터를 삽입한다. 하지만 동영상을 암호화할 때 패딩데이터가 삽입되면 데이터의 크기가 변화되며 이로 인해서 파일 포맷에 오류가 생길 수 있다. 따라서 본 연구에서는 모자라는 부분에 대한 패딩은 수행하지 않는다.

Ⅲ. 실 험

Ⅲ-1. 실험 환경

본 시스템은 하드웨어는 펜티엄 4 프로세서의 1기가 메모리, 운영체제는 Windows XP professional, 웹서버는 IIS(Internet Information Server), 개발도구는 Microsoft Visual Studio 2008을 이용했다. 실시간 영상 전송 환경은 위해 30만 화소 웹카메라, OpenCV, RTPlib를 이용했으며, 이동 단말에서의 테스트 환경은 WIPI 플랫폼기반 SKY IM-S330휴대폰에서 WIPI SDK1.2를 이용해 제작된 단말용 어플리케이션에서 테스트를 수행했다.

Ⅲ-2. 무선 단말기의 사용자 인증 및 암호화

이동단말기를 이용해 컨텐츠 서비스 요청을 할 경우 우선 적합 사용자 인증을 위해 아이디와 비밀번호를 요청하는 경우가 일반적이다. 따라서 아이디와 비밀번호를 입력해 사용자 인증을 수행하는 경우와 본 시스템에서 사용하는 자동 생성된 고유번호를 이용한 인증을 수행하는 경우에 대한 접속 시간 비교는 <표 1>과 같다. 18명의 사용자에게 평상시 사용하는 아이디와 비밀번호를 부여한 후 이동 단말기와 PC를 이용해 아이디와 비밀번호를 입력해서 접속하는 방법과 본 시스템에서 사용하는 자동 추출된 고유번호를 이용한 방법을 통한 접속 시간을 비교했다. 각 사용자들에 대해서 5번씩 접속 테스트를 수행한 후 비밀번호를 교체하게 했다. 이 과정을 5번 반복함으로써 1명당 25회 씩 접속 테스트를 수행 했다. 사용자에 따라 손놀림이 익숙한 사용자도 있고 익숙하지 않은 사용자도 있고 각자의 아이디와 비밀번호의 길이가 다르기 때문에 전체적인 평균값을 사용했다. 그리고 사용자가 잘못 입력한 경우 지우고 다시 입력하는 시간도 실제 서비스 이용 시 데이터 사용량에 포함되기 때문에 시간 계산에 적용했다.

표 1. 컨텐츠 접속 소요시간 비교
Table 1. Comparison of Connection Time to Contents.

내용 / 비교	아이디/비밀번호 접근	제안 방법
이동 단말기 이용 접속	12,142ms	81ms
PC 이용 접속	3,622ms	59ms

<표 1>에서와 같이 개개인의 편차와 시간 측정방법에 따른 오차가 있기는 하지만 사용자가 아이디와 비번을 입력하는 방법은 잘못 입력하면 수정하고 한영변환과 특수문자 사용등에 따라 많은 시간이 소모되며 번거롭지만 자동 추출된 고유번호를 이용할 경우 오류가 생길 확률도 매우 낮으며 빠른 시간에 인증이 가능하다는 장점과 더불어 사용자가 별도로 입력해야하는 일이 없기 때문에 등록된 사용자라면 편리하게 접속할 수 있다.

<표 2>는 SEED알고리즘을 이용한 동영상 컨텐츠 암호화에 소요되는 시간을 나타낸다. 동영상의 경우 초당 프레임율이 15FPS(Frame Per Second)인 QVGA영상을 각 시간별로 10개씩 테스트했다. 무선 이동단말과 PC상에서 가장 일반적으로 사용되는 해상도의 멀티미디어 컨텐츠이며 원본 대비 압축품질은 중상으로 압축된 컨텐츠이다. 그리고 컨텐츠 암호화는 XCrawler가 있는 컨텐츠 변환 서버를 통해서 수행되기 때문에 무선 이동단말기에 서비스할 컨텐츠나 PC에 서비스할 컨텐츠나 암호화에 수행되는 시간은 동일하다.

동영상파일과 실시간 영상의 암호화는 매크로블록과 픽처헤더 각 각에 대해 암호화를 수행했다. 이동 단말기에서 일반적으로 서비스되는 30초 동영상의 경우 매크로블록 암호화는 약 136ms가 소요되었고 픽처헤더 암호화에는 45ms가 소요되었다.

5분짜리 영상의 경우 매크로블록 암호화는 1초정도

표 2. 테스트 영상 정보
Table 2. The Information of the Testing Image.

종류 / 정보	30초 QVGA	60초 QVGA	120초 QVGA	180초 QVGA	300초 QVGA
평균 크기	623 KB	1,209 KB	2,686 KB	3,624 KB	6,598 KB
I 픽처 수	15	33	60	104	162
전체 프레임 수	455	902	1802	2704	4507

표 3. 서버에서 동영상파일 암호화 소요 시간
Table 3. The necessary time for the encryption of MPEG file.

종류 / 동영상	30초 QVGA	60초 QVGA	120초 QVGA	180초 QVGA	300초 QVGA
동영상 파일 암호화 (Macro Block)	136ms	216ms	492ms	687ms	1,150 ms
동영상 파일 암호화 (Picture Header)	45ms	72ms	189ms	219ms	392ms

가 소요되었고 픽처헤더 암호화는 약 392ms가 소요되었다. 테스트 영상의 FPS가 15이기 때문에 프레임 당 66ms이내에 모든 영상작업이 끝나야 영상 QoS를 만족할 수 있다. 매크로블록 암호화는 단순 헤더부분만 암호화하는 것이 아니기 때문에 더 많은 시간이 소요되었고 헤더부분만 암호화를 수행할 경우 매크로블록 암호화에 비해 더 빠른 암호화를 할 수 있었다.

실시간영상 암호화에 측정된 시간은 I 픽처로 판단되었을 시점부터 시작해서 암호화가 끝나고 암호화 패킷을 RTP 스택을 통해 전송완료 한 시점까지를 측정했다.

이때 통신 속도에 따라 시간 오차가 발생할 수 있기 때문에 시간 동기화는 하지 않고 전송했다. 표의 시간은 I 픽처에 대해서만 측정된 시간이다. 순수 암호화 시간만 측정하면 <표 3>의 결과와 거의 동일하며 암호화 후 패킷을 나누어 전송했을 때 초당 15FPS를 유지하기 위해서는 최소 66ms이내에 완료가 되야하는데 30초 영상의 경우 I 픽처의 수가 15개이고 암호화 후 전송에 소요된 시간이 약 522ms이기 때문에 I 픽처의 암호화

표 4. 실시간 영상 I 픽처 암호화 전송소요 시간
Table 4. The necessary Encrypting transfer time for the I Picture of Real time's Image.

종류 / 동영상	30초 QVGA	60초 QVGA	120초 QVGA	180초 QVGA	300초 QVGA
스트리밍 암호화 (Macro Block)	522ms	1122 ms	1981 ms	3002 ms	4674ms
스트리밍 암호화 (Picture Header)	175ms	292ms	734ms	1012 ms	1641ms

표 5. 무선 단말에서 동영상파일 복호화 소요시간
Table 5. The necessary Decrypting time for The MPEG File on the Wireless Device.

종류 / 동영상	30초 QVGA	60초 QVGA	120초 QVGA	180초 QVGA	300초 QVGA
동영상 파일 복호화 (Macro Block)	211 ms	274 ms	632 ms	1018 ms	1588 ms
동영상 파일 복호화 (Picture Header)	61 ms	98 ms	275 ms	319 ms	549 ms

표 6. 실시간 영상 I 픽처 복호화 전송소요 시간
Table 6. The necessary Decrypting Transfer time for a Real time Image's I Picture.

종류 / 동영상	30초 QVGA	60초 QVGA	120초 QVGA	180초 QVGA	300초 QVGA
스트리밍 암호화 (Macro Block)	59 ms	76 ms	168 ms	257 ms	402 ms
스트리밍 암호화 (Picture Header)	19 ms	32 ms	71 ms	87 ms	144 ms

전송에 약 35ms가 소요되었다. 이 결과는 30FPS정도의 영상 전송에도 적용이 가능하며 코드의 최적화나 빠른 통신환경을 통한다면 더 높은 FPS의 영상 전송도 가능할 것으로 생각된다.

<표 5>는 전송된 컨텐츠를 테스트 단말기에서 복호화를 수행했을 때의 시간 소요를 나타낸다. 컨텐츠 변환 서버에서 암호화를 수행했을 때의 시간보다 더 많은

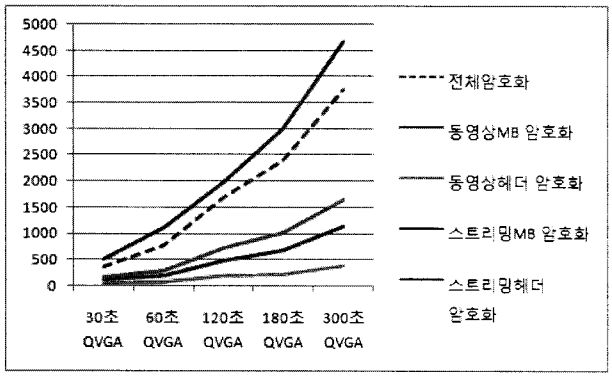

그림 8. 암호화 성능비교
Fig. 8. The Performance Comparison of the encryption.

시간이 소요된 이유는 서버와 무선 이동단말기의 CPU와 메모리 등의 성능차이이지만 이정도 단말의 낮은 성능을 고려하면 느린 성능은 아니며 정상적 재생에도 문제가 없었다.

<표 6>은 실시간 스트리밍 영상의 복호화시간을 보여준다. I 픽처의 암호화 패킷이 전송완료된 시점부터 프레임 복호화가 완료된 시점까지의 측정 시간을 보여준다. 패킷전송에 소요되는 시간은 측정하지 않았기 때문에 훨씬 빠른 성능을 보여준다.

그림 8의 점선으로 표시된 부분은 전체 암호화를 수행하는 방법과의 성능 비교를 보여준다. 스트리밍 매크로블록 암호화가 전체 암호화에 비해서 더 낮은 성능을 보이는 이유는 암호화는 물론 패킷전송을 수행하는 과정까지 포함되어 있기 때문이다. 만일 전체 암호화 영상도 전송과정을 포함한다면 훨씬 많은 시간이 소요되었을 것이다. 게다가 일반 단말 UI를 이용해 컨텐츠에 접근까지 한다면 그보다 더 많은 시간이 소요된다.

<표 7>은 기존방법과 제안방법과의 비교를 보여준다. 기존의 방법들은 무선 단말기의 불편한 UI나 단말용 컨텐츠의 특성 등에 대한 고려가 부족하다. 전체 암호화를 하는 방법은 가장 보안성은 높지만 연산량과 암복호화 시간에서 불리하고 파일 포맷이 변경되며 스트리밍에 적합하지 않다.

모션 벡터 암호화 방법은 파일 포맷변경은 되지 않지만 성능면에서는 보통이고 비트량이 증가될 수 있으며 모션벡터의 연산에 대한 문제로 인해 스트리밍에 적합하지 않다. 이것은 연산량도 낮고 매크로블록 자체를 암호화하기 때문에 비트량의 증가나 파일 포맷의 변경이 되지 않는다. 또한 I 픽처의 매크로블록 자체를 암호화하기 때문에 보안성능도 높으며 스트리밍환경에도 적합하다.

표 7. 제안 방법과의 비교
Table 7. The Comparison to Proposed Method.

방 법 / 비 교	전체 암호화	모션 벡터 암호화	제안 방법
무선 단말 특성 고려	없음	없음	단말 고유키 생성
연산량	높음	보통	낮음
암복호화 시간	느림	보통	빠름
비트량 증가	없음	있음	없음
파일포맷 변경	있음	없음	없음
보안성능	높음	보통이상	높음
스트리밍 암복호화	부적합	부적합	적합

III-3. 복호화 데이터의 무결성 검증

두 개의 영상 간에 유사성을 비교하기 위한 영상 분석 방법으로는 신호대 잡음비인 PSNR(Peak Signal to Noise Ratio)을 주로 사용한다. PSNR은 영상의 신호양에 비례한 노이즈의 양을 측정하여 공간적인 품질 측정을 위해 사용되는 방법으로서 50dB는 원영상과 같으며 30dB이하는 원본에 비해 질적 저하가 발생된다. MSE (Mean Square Error)는 원래의 영상과 복원된 영상의 화소값 간의 평균 자승 오차를 의미한다[18]. 식(5)는 두 영상의 유사 분석을 위해 사용된 PSNR의 수식이며 식(6)은 PSNR분석을 위해 사용된 MSE의 수식이다.

$$PSNR = 10\log_{10}\left[\frac{255^2}{MSE}\right][dB] \tag{5}$$

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left[f(x,y) - f'(x,y)\right]^2$$
$$(M : 이미지\ 가로\ 크기, N : 이미지\ 세로\ 크기)$$
$$(x,y) : 비교하는\ 픽셀의\ 좌표\ 값\ )$$
$$(f(x,y) : 원본\ 이미지의\ x,y\ 좌표\ 픽셀\ 값)$$
$$(f'(x,y) : 비교\ 이미지의\ x,y\ 좌표\ 픽셀값) \tag{6}$$

PSNR을 이용해 측정한 변환 전후의 영상 분석 값은 100개의 이미지에 대해서 수행한 결과 평균 11.9dB의 값을 얻을 수 있었으며 원 영상으로 다시 복원 후의 PSNR값은 원영상과같은 50dB임을 확인 할 수 있었다.

그림 10. 암호화 영상과 복호화 영상
Fig. 10. Encrypted and Decrypted Image.

그림 10은 실험 전 후의 화질의 변화를 나타낸다. 왼쪽의 이미지는 원본 이미지이며 오른쪽의 이미지는 변환 후의 결과이다. 어렴풋이 그림의 흔적은 보이지만 픽셀데이터 부분에 대한 암호화를 수행했기 때문에 정상적으로 원 영상을 보기 어렵지만 다시 복원 했을 경우 원본과 같은 이미지로 복원된다.

이상의 결과를 종합해보면 제안방법은 단말의 고유 특성값을 암호화 키로 이용하기 때문에 불편한 UI의 제약에서 벗어나 자동으로 암호화 키를 생성하고 로그인에 이용할 수 있으며 암호화하지 않고 컨텐츠를 전송하는 방법에 비해서 더 안전한 컨텐츠를 전송할 수 있다는 장점을 갖는다. 그리고 암호화 과정에서 데이터에 대한 패딩을 하지 않음으로서 데이터의 비트량이 증가하지 않고 또한 이로인해서 파일포맷이 변경되는 문제도 발생하지 않는다. 그리고 동영상 파일은 물론 스트리밍 영상에 대한 고려가 되어있기 때문에 컨텐츠의 특성이나 보안레벨에 따라 선택적 적용이 가능하다. 전체 프레임을 인코딩 하지 않기 때문에 속도면에서도 유리하고 비교적 쉽게 시스템에 적용이 가능하다는 장점을 갖는다.

IV. 결 론

본 시스템을 적용할 경우 유무선 단말기 고유의 식별번호를 이용하여 편리하고 쉬운 사용자 인증을 사용할 수 있기 때문에 이용 요금이 비싼 무선 통신료를 절약할 수 있으며 사용자 인증을 위한 시간을 단축시킬 수 있다. 또한 컨텐츠 제공자입장에서는 사용자의 아이디와 비밀번호에 의해서 컨텐츠를 제공하는 것이 아니기 때문에 여러 사용자의 한 아이디 돌려쓰기와 같은 문제를 해결할 수 있고, 단순하게 사용되는 암호화 키가 노출이 되더라도 단말에 탑재된 복호기는 현재 단말의 정보를 키 값으로 이용해 복호화하기 때문에 인증된 단말 이외의 단말에서는 정상적으로 재생되지 않는다. 따라서 사용자 입장에서는 더 쉽고 편리하게 무선 인터넷을 즐길 수 있으며 컨텐츠 제공자 입장에서는 적합한 사용자에게만 컨텐츠를 서비스를 할 수 있다. 이와같은 저작권 보호를 통해 사용자와 제공자간의 신뢰를 확립할 수 있다. 적합 인증된 사용자라도 서비스 받은 컨텐츠를 무단으로 배포할 경우 멀티미디어 컨텐츠 자체에 사용자 고유 번호에 의한 개별 암호화가 되어있기 때문에 무단 배포 받은 사용자는 쉽게 컨텐츠를 이용할 수 없다는 장점을 갖는다.

이 방법은 엄격한 보안이 필요한 데이터보다는 치명적이지 않은 데이터에 대해서 적용한다면 쉽고 편리하게 사용할 수 있다. 또한 특정 부분에 대한 암호화를 수행할 경우 풀릴 수도 있기 때문에 추출된 고유 번호에 별도의 키 생성 알고리즘을 적용하고 멀티미디어 데이터의 다른 부분들에 대한 암호화를 시킬 경우 강인성과 효율성은 더 증대될 것이다. 그리고 여러 단말기의 고유 식별번호와 더불어 좀 더 다양한 고유 값을 추출할 수 있다면 인증 식별성은 더 증가할 수 있다.

사용자 고유 키 값을 다른 것으로 변경하고 SEED알고리즘 이외의 다른 알고리즘을 이용한다고 하더라도 적용가능한 모델이기 때문에 응용 분야에 따라서 더 강인한 정보 보호가 가능할 것으로 예상된다. 제안 시스템은 편리성을 위해 각 단말기에 대한 라이센스를 부여한다는 점에서 다른 시스템과 차이가 있으며 단말기 별로 사용허가를 할 수 있기 때문에 컨텐츠 제공자의 과금모델도 더 다양화 시킬 수 있으며 접근 편리성으로 인해 더 많은 사용자가 편리하고 안전하게 무선 인터넷을 사용할 수 있을 것이다

참 고 문 헌

[1] 김남겸, 손인수, 이진구, "HAPS 기반의 HSDPA 시스템 성능 분석", 대한전자공학회 논문지, 제 6호, pp. 20~26, 2008.
[2] www.qualcomm.co.kr
[3] 이창열, "DRM 기술", 한국 정보보호 학회지, 제 12권 제 1호, pp. 1~10, 2002.
[4] I. J. Cox, J.Kikian, T.Leighton, T.Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. on Image Processing, Vol.6, No.12, pp.1673~1687, 1997.
[5] 김홍근 외11, "SEED의 ISO/IEC 국제표준화 추진 보고서", 한국정보통신 연구진흥원, 한국 정보통신 기술협회(TTA) 연구결과 보고서, 2002.

[6] 정호련, 정성원, 박성욱, "다중 무선 방송채널에서의 효과적인 모바일 트랜잭션 처리 기법", 정보과학회 논문지, 제 35권 제3호, pp.257~271, 2008.
[7] 문형진, 김기수, 엄남경, 이영진, 이상호, "민감한 개인정보 보호를 위한 효율적인 접근제어 기법", 한국통신학회논문지, 제32권 제7호, pp.667~673, 2007.
[8] W. Zeng and S.Lei, "Efficient frequency domain selective scrambling of digital video," IEEE Transaction on Multimedia, vol.5, pp.118-129, 2003.
[9] J.Jang, "digital video scrambling method," KR patent 0151199, 1998.
[10] D.S.Ravi, A.R.Raghunathan, P.Kocher, and S.Hattangady, "Security in embeded systems:Design challenges," in ACM Trans. On Embeded Compution Systems, 3(3), pp.461-491, 2004.
[11] B.Macq and J.j.Quisquater, "Cryptology for digital tv boadcasting," in IEEE, Vol.83, No.6, pp.944-957, 1995.
[12] C.P.Wu and J.Kuo, "design of integrated multimedia compression and encryption systems," in IEEE Transactions on Multimedia, Vol.7, No.5, 2005.
[13] 류동엽, 한승현, 임영환, "편리한 무선 인터넷 컨텐츠 생성을 위한 TransGate 시스템" , 한국인터넷정보학회 논문지 제 7권 2호, pp. 37~52, 2006.
[14] 류동엽, 한승현, 임영환, "유비쿼터스 환경을 위한 RSS 뉴스 채널 컨텐츠의 개인화 모바일 서비스 기법", 정보처리학회 논문지, 제14권 제4호, 2007.
[15] 김역, 정창호, 장윤석, 이상진, 이성재, "SEED 구현 적합성 검증 시스템에 관한 연구", 한국 정보보호학회, 제 13권 pp. 69~85, 2003.
[16] 이강, "128-비트 블록 암호화 알고리즘 SEED의 저면적 고성능 하드웨어 구조를 위한 하드웨어 설계 공간 탐색", 정보과학회 논문지, 제 13권 제4호, pp.231~239, 2007.
[17] 한국정보보호진흥원, "SEED 알고리즘 상세 명세서", 1999.
[18] Thrasyvoulos N. Papas, "Perceptual Criteria for Image Quality Evaluation", in Handbook of image and Video Processing, Academic Press, San Diego, pp. 669-684, 2000.

저 자 소 개

이 종 갑(정회원)
1983년 충남대학교 전자공학과 (공학사)
1983년~1996년 Wang Computer Lab.
1988년 숭실대학교 전자및 컴퓨터공학과 (공학석사)
2004년 숭실대학교 미디어학과 (박사수료)
2001년~현재 부천대 강의전담 교수
<주관심분야 : 멀티미디어, 유비쿼터스, 모바일, 임베디드시스템>

성 홍 석(정회원)
대한전자공학회 45권 IE편 제3호 (2008년 9월) 참조

원 영 진(정회원)
대한전자공학회 45권 IE편 제1호 (2008년 3월) 참조

임 영 환(정회원)
1977년 경북대학교 수학과 (이학사)
1979년 한국과학기술원 전산학과 (이학석사)
1979년~1996 한국전자통신연구소 책임연구원
1985년 Northwestern Univ. 전산학과 (이학박사)
1996년~현재 숭실대학교 미디어학부 교수
<주관심분야 : 멀티미디어, 유비쿼터스, 모바일, 임베디드시스템>

이 종 성(정회원)
대한전자공학회 42권 TE편 제4호 (2005년 12월) 참조

임 승 하(정회원)
대한전자공학회 44권 IE편 제4호 (2007년 12월) 참조