한국산학기술학회논문지
Vol. 9, No. 4, pp. 936-944, 2008

디지털 컨텐츠 보호를 위한 메트릭스 퍼즐 암호화방법에 대한 연구

민소연[1*], 김정재[2]

A Study on Encrypted Matrix Puzzle for Digital Contents Protection

So-Yeon Min[1*] and Jung-Jae Kim[2]

요 약 DRM 시스템은 저작권 보호 기술을 이용하여 저작원자의 권리 및 이익을 보호하고 관리하는 기술이다. 본 논문에서는 DRM 시스템에서의 암호화 키 전송과 암복호화 처리시간에서 개선을 목적으로 하고 있다. 제안하는 방법은 첫째, 기존의 단순 One-path XOR 방법보다 안전한 다차원 배열 기법을 이용한 Key 전송방법을 제안한다. 둘째, 생성된 다차원 배열은 서버에 저장하지 않으므로 기존의 시스템보다 보안성이 높은 방법을 제안한다. 셋째, 클라이언트에서 복호화 할 때 OTP와 함께 다차원 배열을 복호화 하는 클라이언트 복호화 시스템을 제안한다. 넷째, 다차원 배열기법과 OTP를 조합으로 보다 안전한 키 전송을 제안한다.

Abstract DRM system is a technology that protects and manages copyright holder's privilege by using a copyright protection technology. This paper contributes to improvement of the secret key transmission and encryption/decryption processing time base on DRM system. In this paper, we will suggest that as follow: First, we will propose the algorithm to transmit the encryption key which use Multidimensional Method more safe than the existing One-path XOR method. Second, we will provide the high quality algorithm of security than the existing system because the Multidimensional which generated from the algorithm does not saved to the server side. Third, we will support the client decryption system which can decrypt the Multidimensional with OPT in decryption with client side. Fourth, we will adopt the more safe method of transmission with the compound of Multidimensional Method and OPT.

Key words : DRM(Digital Rights Management), Multidimensional, OTP(One Time Password)), Key Exchange

1. 서론

오늘날의 정보화 시대를 가져온 디지털 환경은 우리에게 많은 가능성을 심어주었으며, 아날로그 환경에서는 불가능하게 여겼던 콘텐츠의 생산을 가능하게 하였다. 디지털 콘텐츠의 특성은 인터넷이라는 매체를 통해서 시공간을 초월하여 전달될 수 있는 데이터라는 것이다. 이러한 디지털 콘텐츠는 잡음에 강하고, 복제가 용이하며, 원본의 보존이 영구적으로 가능하다는 또 하나의 특징을 갖고 있다.

이것은 디지털 콘텐츠의 불법복제라는 부정적 요소를 안고 있으며, 디지털 콘텐츠의 창작자나 권리 소유자, 서비스 사업자의 경제적 활동을 저해하는 요소가 된다. 이러한 디지털콘텐츠의 불법복제 기승으로 인해 기존 오프라인 또는 아날로그 콘텐츠의 유통 구조를 장악하던 음반사 또는 영화제작사 등은 심한 타격을 받게 되었다. 이들 콘텐츠 공급자들은 궁여지책으로 P2P 사이트에 대하여 불법복제 조장이라는 명목으로 소송을 제기하는 한편 인터넷을 통한 어떠한 형태의 디지털콘텐츠 유통 서비스도 강하게 반발하고 있다.

그러나 콘텐츠의 유통 구조가 기존의 오프라인 또는 아날로그 콘텐츠에서 디지털콘텐츠로 전환되어 가는 추세를 피할 수 없다는 인식하에 품질의 손상 없이 복제가 가능한 저작물의 불법복제 방지를 위한 디지털 저작권 보호문제가 중요한 이슈로 대두되고 있다[1,2].

디지털 저작물 보호를 위해서는 안정성과 보안성 확보

본 논문은 2007년도 서일대학 학술연구비에 의해 연구되었음.
[1]서일대학 정보통신과
[2](주)RetailTech
*교신저자: 민소연(symin@seoil.ac.kr)
접수일 08년 7월 06일 수정일 08년 7월 25일 게재확정일 08년 8월 11일

를 위하여 정보보호 기술이 필요하고, 디지털 저작권과 저작물 유통의 전반을 감시하고 추적하기 위한 디지털 저작권 관리(DRM: Digital Rights Management) 기술이 필요하다. 기존 DRM 솔루션들은 암호화에 사용하는 키로 비밀키를 사용하여 사용자가 파일을 다운로드할 때 암호화를 수행하므로 많은 시간이 소요가 되며, 복호화를 수행하는 경우에도 대용량의 저작물인 경우 전체 파일에 대하여 복호화를 먼저 수행한 후에 실행을 할 수 있으므로 사용자가 실시간으로 파일을 플레이해서 볼 수 없는 문제점이 있었다. 또한 암호화와 복호화에 사용하는 키가 사용자에 의하여 노출이 된다면 해당 저작물에 대한 보호는 더 이상 보장하지 못하는 단점이 있다[3,4].

기존의 DRM의 문제점을 해결하기 위해서 매트릭스 Puzzle 프로토콜을 사용하여 온라인상에서 멀티미디어 저작물에 대한 사용자 인증과 데이터 자체의 암호화를 통해 불법적인 실행을 방지할 수 있는 통합적인 DRM 시스템을 제안한다.

2. 관련 연구

2.1 공유키 풀 암호화 시스템 키 교환 기법

공유 키 풀(Shared Key-Pool)을 구성하기 위해서 저작물 제작자는 분배할 동영상을 비밀키 Ks를 사용하여 암호화한다. 비밀키 Ks는 다음과 같이 k개의 비트열로 나눌 수 있다.

일반적으로 비밀키 암호화에서 비밀키 Ks는 128 비트를 사용한다. 암호화에 사용한 비밀키의 보안성을 높이기 위해서 비밀키를 암호화한다. 비밀키를 암호화하여 사용자가 접근할 수 없도록 하기 위하여 공유 키 풀을 사용한다.

키의 크기에 맞게 적용할 수 있도록 k개의 행과 $2^{\frac{n}{k}}$ 개의 열을 갖는 행렬 <표 1>과 같이 나타낼 수 있다. 각 사용자에 대한 개인용 키 Kp는 k비트로 이루어진 다음과 같은 비트열의 집합이다.

[표 1] 암호화 키 Ks에 대한 공유 키 풀

a_1^0	a_1^1	$\cdots$	$a_1^{2^{\frac{n}{k}}-1}$
a_2^0	a_2^1	$\cdots$	$a_2^{2^{\frac{n}{k}}-1}$
$\vdots$	$\vdots$	$\vdots$	
a_k^0	a_k^1	$\cdots$	$a_k^{2^{\frac{n}{k}}-1}$

$$Kp = a_1^{b_1} | a_2^{b_2} | \cdots | a_k^{b_k} \quad (1)$$

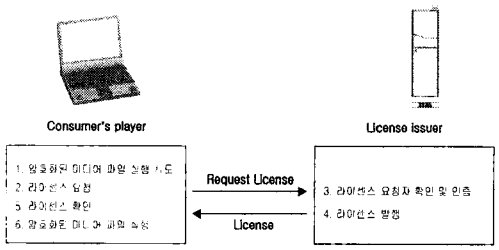
이 때 b_i는 키 풀에서 각 i 번째 행의 값으로서 사용자의 개인용 키를 결정하는 중요한 값이다. b_i는 사용자 인증서의 공개키에서 추출한다.

$$B = b_1 | b_2 | \cdots\cdots | b_k \quad (2)$$

사용자의 공개키는 일반적으로 비도가 낮은 경우에는 512비트의 값을 사용하고 비도가 큰 중요한 정보인 경우에는 1024비트의 값을 사용한다. 일반적으로 n비트의 공개키를 사용하는 경우 개인용 키의 길이가 k비트라면 이 때 키 풀의 각 항목 값들은 $2^{\frac{n}{k}}(0 \sim 2^{\frac{n}{k}}-1)$의 범위를 가지게 된다[5,6].

2.2 Microsoft의 DRM 시스템

Microsoft의 DRM 시스템은 저작물 제공자와 소비자들에게 디지털 미디어 파일을 안전하게 분배하는 종단간 DRM 시스템이다. 핵심 제어 부분은 WMRM(Windows Media Rights Manager)으로서 WMRM의 Rights Manager는 저작물 제공자에게 인터넷 상에서 암호화된 파일 형식으로 보호된 음악, 비디오 등의 미디어를 배달한다. WMRM에서 각각의 서버 또는 클라이언트 인스턴스들은 개인화(indivisualization)과정을 통해 키 쌍을 할당받게 되며, 크래킹 되었거나 안전하지 않다고 판단되는 인스턴스에 대해서는 인증서 취소목록을 이용하여 서비스 대상에서 제외시키게 된다. 인증서 취소목록은 마이크로소프트사의 웹사이트를 통해 배포된다. 키는 라이선스에 포함되고, 라이선스와 저작물은 분리되어 분배된다.



[그림 1] 라이선스 획득 단계

[그림 1]은 WMRM에서 라이선스 획득 단계로서 클라이언트가 패키징되어 보호된 저작물을 실행시키면

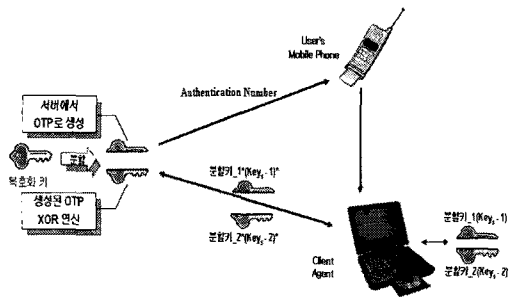
플레이어는 라이선스 서버에 라이선스를 요청한다. 서버는 라이선스 요청에 대해 사용자의 인증과 지불여부를 확인한 후에 라이선스를 발행한다. 서버는 라이선스 발행 후 라이선스를 클라이언트의 플레이어에 전송한다. 클라이언트 플레이어는 서버에서 전송받은 라이선스를 확인한 후 사용규칙에 따라 저작물을 실행한다[7,8].

WMRM의 경우 Key ID와 Key seed를 결합하여 저작물 암호화키를 생성하는데, Key ID는 저작물 헤더에 포함되어 저작물과 함께 패키징되어 배포되고, Key seed는 클리어링하우스에 저장되어 관리된다. 복호화키를 생성하기 위해서는 저작물에 포함되어있는 Key ID와 서버가 관리하는 Key seed가 필요하다. WMRM은 윈도우미디어플레이어에 탑재되어 널리 사용되지만, 동적변화변경에 제한적이고 자사의 동영상 파일 포맷인 asf와 WMA파일 포맷에만 적용되어 다양한 파일 형식을 지원하지 못한다. 또한 라이선스를 발급 받기 위한 [그림 1]의 2단계와 3단계의 인증단계에서 특정한 암호기술을 적용하지 않고 사용자의 정보를 전송하므로 사용자의 정보가 노출되는 보안 위협요소가 존재한다.

2.3 해쉬 체인 암호화 시스템 키 교환 기법

시스템의 전체적인 개요는 정보유출 방지 및 사용자 확인을 위하여 서버는 인증된 사용자를 확인한 후 무선으로 사용자 인증번호(UAN : User Authentication Number)를 제공한다. 사용자는 인증번호를 키 값으로 입력하여 복호화 키를 유선으로 요청하게 한다. 사용자 인증번호를 확인한 에이전트는 OTP(One Time Password)로 복호화 키를 생성하여 생성된 키를 안전한 방법으로 사용자에게 제공하는 알고리즘을 통해 키를 제공한다.

생성된 키는 키 분할 알고리즘을 이용하여 두개의 키(Keys_1, Keys_2)로 분할 한 후 에이전트를 이용하여 Keys_1과 Keys_2를 각각 암호화 하여 사용자에게 전송하는 절차를 거쳐 키 값을 [그림 2]와 같이 전송한다[9,10].



[그림 2] 복호화 키 생성 및 전송 기법

키 분할 알고리즘은 다음과 같다.

$$\text{키 분할 알고리즘 : Key} \oplus \text{OTP} = \text{Temp}$$
$$\text{OTP(Ka) : Keys\_1} \qquad \text{Temp(Kb) : Keys\_2} \tag{3}$$

[그림 3]에서는 안전한 키 전송을 위하여 사용자 인증과정을 통해 사용자를 확인한 후 사용자에게 전송할 키를 OTP를 이용하여 키를 생성한 후 생성된 키를 전송하는 키 전송 프로토콜을 나타내고 있다.

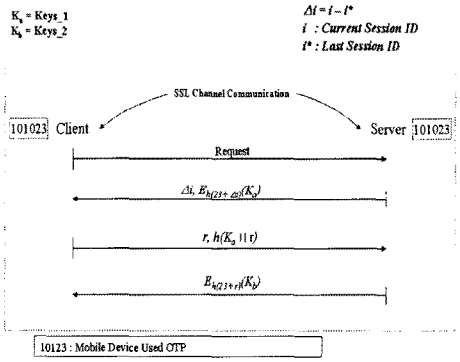
Ka를 Keys_1이라하고, Kb를 Keys_2라 하여 두 번에 나누어 제공 할 수 있도록 하였다.

첫째 UAN(ex : 101023)는 서버에서 생성하여 사용자에게 SSL 채널을 통해 모바일로 제공함으로써 사용자에게 안전하게 제공할 수 있도록 하였다.

둘째 UAN을 이용하여 복호화 키를 요구할 수 있도록 하였으며, 처음 사용자는 인증번호를 이용하여 복호화 키를 요청하면 서버는 키 분할 알고리즘을 이용하여 키를 생성한 후, 키 전송 프로토콜을 이용하여 안전하게 키를 제공받는다.

셋째 서버는 세션 증가값(△i)과 UAN을 더한 값을 암호화 키로 사용한 암호화된 Ka값을 클라이언트로 전송을 한다.

넷째 사용자는 Ka를 복호화 한 후, 난수 값 r을 생성하여 Ka값과 r 값을 연접(Concatenation)하여 해쉬한 후, 서버로 다시 전송을 하게 된다.



[그림 3] 키 전송 프로토콜

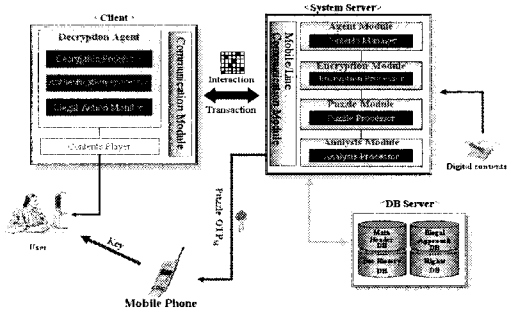
마지막으로 서버에서는 클라이언트에서 발생한 난수 값 r값과 UAN을 더한 값으로 다시 암호화 하여 Kb를 전송한다.

처음 사용자와 재 사용자를 구별하여 재사용자는 이중으로 키를 요구하지 않고도 계속 사용할 수 있도록 이전

사용하던 세션 값 i를 보관하고 있다가 서버에 세션 값을 확인한 후 계속 사용할 수 있도록 설계하였다. i는 세션 값을 나타내며 Δi는 세션의 증가 값으로 이전 세션을 i* 이라하고 i를 현재 세션 값으로 정의하여 계속 사용자에게는 세션 증가 값을 확인하여 계속 사용할 수 있도록 하고, 처음 사용자는 세션의 증가 값이 없으므로 키 값을 제공받아 사용하도록 하였다[5].

3. 제안 시스템 구조

제안하는 시스템은 [그림 4]와 같이 클라이언트/서버 구조로 구성되어 운용되고, 서버는 에이전트 모듈과 암호화 모듈, Puzzle 모듈, 분석 모듈과 데이터베이스로 구성되며 클라이언트는 복호화 처리기와 저작물 실행기로 구성된 복호화 에이전트가 있다.



[그림 4] 제안하는 개선된 DRM 시스템 구성도

3.1 서버의 에이전트 모듈

콘텐츠 제공자(CP : Content Provider)에 의해 제공되는 콘텐츠들을 제공받아 등록시켜주는 역할을 제공하며, 등록된 콘텐츠를 서버의 암호화모듈로 전송시켜주는 역할을 한다. 클라이언트의 복호화 모듈에서 들어오는 모든 값들을 수집하여 통계 분석 모듈과 직접 통신하여 정보를 처리 및 관리하는 모듈이다. 서버의 암호화 모듈은 서버의 에이전트모듈로 부터 받은 디지털 콘텐츠를 저작권보호를 위하여 암호화하는 모듈이다.

3.2 서버의 Puzzle 모듈

디지털 콘텐츠를 사용하고자하는 사용자에게 콘텐츠 암호화키를 다차원 기법으로 암호화하는 역할을 한다. 인증된 사용자에게 다차원 배열과 OTPM의 조합으로 암호화키를 암호화하고 유선으로 다차원 배열을 무선으로는 OTPM 값을 전송한다.

3.3 서버의 통계 분석 모듈

서버에이전트 모듈로부터 받은 클라이언트의 모든 행위에 대한 정보를 감시하고, 데이터베이스 시스템과 연동하여 정보를 얻어내어 분석하는 모듈이다. 처음 접속한 사용자인지 기존 사용자인지를 확인하여 처음 접속한 사용자일 경우 인증번호를 인증절차를 걸쳐 발급하고, 기존 사용자일 경우 재발급할지 발급된 인증번호를 계속 사용할지를 결정할 수 있는 정보를 제공한다.

3.4 클라이언트의 복호화 에이전트

클라이언트의 복호화 에이전트는 암호화된 콘텐츠를 복호화 하기 위하여 필수적으로 설치해야 한다. 클라이언트의 복호화 에이전트 설치는 사용자가 서버에 처음 접속하였을 때 서버로부터 다운로드하여 설치되며 클라이언트 시스템에서 암호화된 콘텐츠를 복호화하여 실행시키기 위해 사용자가 직접 실행시켜야 한다.

에이전트는 동영상의 실행시 동영상의 사용자정의 데이터를 확인하여 암호화되어 있는 동영상과 일반 동영상을 구분하여 암호화되어 있는 동영상일 경우 우선 서버의 데이터베이스에서 라이선스를 확인한다. 만약 라이선스가 있다면 이를 바탕으로 해당 동영상 파일에 대한 다차원 배열을 요청하게 된다. 이때 클라이언트에서 서버에 접속할 때 입력된 사용자의 아이디와 패스워드가 서버에게 전송되어 허가된 사용자인지를 확인 후 콘텐츠를 클라이언트 사용자에게 다차원 배열로 암호화하여 보내주게 된다. 사용자는 유선으로 다차원 배열을 전송 받으며, 사용자의 모바일 폰을 이용하여 OTPM의 값을 전송 받는다. 이렇게 다차원 배열과 OTPM를 이용하여 복호화된 콘텐츠 파일의 내용은 콘텐츠 전용 플레이어를 이용하여 재생이 가능하다.

실시간으로 사용자의 불법 행위 감시를 하게 되고 모든 사용자의 불법적인 행위는 감시 인터페이스를 통해 서버의 데이터베이스에 저장된다. 인증된 사용자라 할지라도 사용권한에 따라 제한적인 사용을 위해 저작물 자체 암호화에 의해 저작물을 보호한다. 사용자가 저작물에 대한 라이선스를 초과하여 사용하려고 시도하거나 사용자 임의의 복호화를 시도하는 등의 불법적인 사용 행위를 시도할 경우 이를 봉쇄하도록 저작물에 대한 지속적인 모니터링을 수행하게 된다. 사용자가 저작물에 대해 불법적인 사용을 몇 회나 시도 했는지, 또한 사용권한 범위가 어느 정도인지 등 저작권 위배 사례 수집 및 분석을 통하여 사용자 관리와 각종 통계 정보를 계산하여 그 정보를 갱신 및 유지하는 작업을 수행한다[11,12].

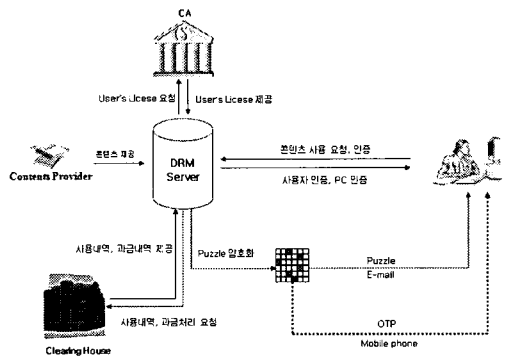
3.5 DB Server

DB Server에는 총 4개의 데이터베이스로 나누어 진다. 첫 번째, 데이터베이스는 동영상의 정보를 담고 있는 메인헤더 데이터베이스, 두 번째 불법 접근을 한 횟수를 저장하는 데이터베이스, 세 번째 사용자 기록의 정보를 저장하는 데이터베이스, 네 번째 콘텐츠에 대한 암호화 키를 저장하는 권한관리 데이터베이스로 구성한다.

4. 다차원 배열 기법을 이용한 인증 프로토콜 설계

4.1 유 · 무선을 이용한 다차원 배열 기법

제안하는 DRM 인증 기법은 기존의 사용자 인증에 이용되었던 대칭키 또는 공개키 암호화 방법을 사용해 암호화키를 전송하는 방법 대신, 다차원 배열 기법을 이용하여 복잡한 암호화 방법이 없는 다차원 기법으로 제안하는 시스템의 전체 구조는 [그림 5]와 같다.



[그림 5] 제안하는 시스템의 전체 구조

사용자는 DRM Server에게 콘텐츠 사용 요청과 인증을 하고, 이때 사용자는 라이선스가 있다고 가정한다. DRM Server는 클리어링하우스에 과금처리 요청과 CA로부터 사용자 라이선스를 확인한다. 확인된 사용자에게 유선으로 다차원 배열과 무선으로 OTPM 값을 전송하고 사용자는 이를 이용하여 암호화된 디지털콘텐츠를 복호화 하여 재생한다.

4.2 다차원 배열 기법 설계

디지털 콘텐츠 제공자로부터 제공 받은 콘텐츠를 DRM Server에서는 암호화하여 DB Server에 저장한다. 사용자로부터 콘텐츠 요청을 받은 DRM Server는 콘텐츠 암호화키를 다차원 배열을 이용하여 암호화 한다.

4.3 다차원 배열과 조합도 생성 방법

다음은 간단히 6 X 6 크기의 값을 예로 설명한다. 먼저 원래 동영상을 암호화하기 위해 키셋을 생성하며, 키셋은 동영상 마다 틀리게 하기위해 랜덤한 값으로 발행한다.예를 들어 "A" 의 값은 "000000" 이 되지만 "000000" 값은 64가지 중 어떠한 문자가 될 수도 있다.

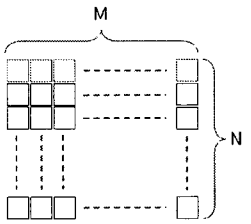
이때 사용되는 문자는 7비트의 값으로 0 ~ 9, a ~ z, A~Z, "+", "-" 까지 총 64개의 문자를 사용한다. [그림 6]에서는 동영상마다 틀린 키셋을 만들기 위하여 난수로 그 값을 하나씩 채우게 되며, 중복되는 값은 없도록 한다.

000000	A
000001	B
000010	C
000011	d
000100	E
000101	8
000110	r
000111	4
...	...
111000	x
111001	Z
111010	s
111101	h
111110	L
111111	6

[그림 6] 키셋(keyset)

다음 DRM Server는 [그림 7]과 같이 암호화 키 길이와 같은 다차원 배열을 생성한다.

마지막 행을 제외한 값들은 일단 64개의 문자들 중 아무값이나 선택되어 들어가게 된다.



[그림 7] 다차원 배열

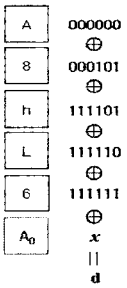
[그림 8]은 난수값을 이용하여 마지막 행을 제외한 나머지를 64가지의 문자를 이용하여 패딩한 결과이다.

이렇게 패딩된 값을 XOR 하여 마지막 행에 들어갈 값을 구한다.

A	E	d	B	r	8
8	C	8	6	B	6
h	4	6	E	h	r
L	r	B	C	4	E
6	d	r	L	C	E
A_0	A_1	A_2	A_3	A_4	A_5

[그림 8] 난수값으로 채워진 2차원 배열

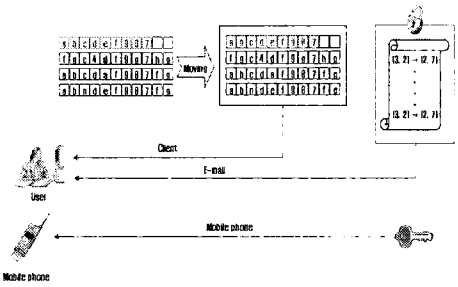
마지막 행에 패딩되는 값은 각 열을 XOR한 값과 각각의 마지막 행에 해당하는 A0값을 XOR한 값이 동영상 복화화 키값이 된다. 만약 동영상 복호화 키 값이 "dCrr4h"라 가정하고 마지막 행의 자세한 생성 방법은 [그림 9]와 같다.



[그림 9] 마지막 행 첫열값 생성 방법

연산으로 A_0 이전의 값들과 A_0값을 XOR하면 [그림 9]와 같이 d(keyID)값이 나오고, A_0의 값을 구한다. 태그 아이 값을 얻는 방법은 식 (4)와 같다.

$$A \oplus 8 \oplus h \oplus L \oplus 6 \oplus A_0 = d(keyID) \ldots\ldots (4)$$



[그림 10] 다차원 배열 기법 암호화 방법

[그림 10]은 다차원 배열 조합도는 랜덤하게 재배치된 암호화키의 위치 값을 의미하며, 다차원 배열 조합도는 암호화하여 사용자로 전송한다. 이렇게 조합도를 암호화한 키는 사용자의 Mobile phone로 전송하는 과정을 나타내고 있다.

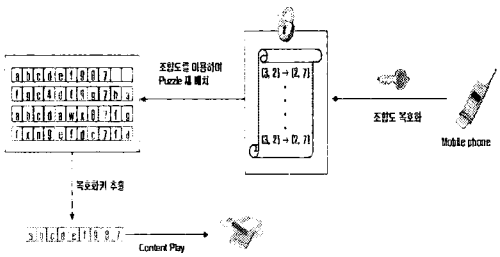
사용자는 이렇게 유무선을 통하여 DRM Server로부터 전송받은 다차원 배열과 조합도, 암호화키를 이용하여 디지털 콘텐츠를 복호화하여 재생한다.

다차원 배열에는 콘텐츠 암호화키와 콘텐츠의 사용기간, 사용횟수 등을 같이 암호화하여 사용자가 오프라인 상태에서 콘텐츠의 사용기간과 사용횟수를 기록하여 온라인 상태가 되었을 때 콘텐츠 사용을 제안하거나 요금지불을 요청할 수 있다.

4.4 다차원 배열 복호화 방법

[그림 11]에서는 다차원 배열 복호화는 DRM Server로부터 다운 받은 콘텐츠와 다차원 배열, 조합도, 조합도 암호화키를 이용하여 복호화 하는 과정을 나타내고 있다. 복호화 과정은 암호화 기법의 역순으로 진행된다.

복호화 과정을 보면 먼저 Mobile phone로 전송받은 키를 이용하여 E-mail로 수신된 다차원 배열과 다차원 배열 조합도 중 다차원 배열 조합도를 먼저 복호화하고 이 다차원 배열 조합도를 이용하여 다차원 배열을 재배치하여 콘텐츠 암호화키를 추출하여 콘텐츠를 복호화 한다.



[그림 11] Puzzle 기법의 복호화

5. 성능평가

5.1 기존 시스템과의 비교 분석

DRM 시스템은 유선 환경만을 이용하여 키 분배를 하며, J사는 공개키로 암호화하여 전송하며, M사의 경우 복호화 키를 전송한다. 또한 키 재요청시 동일한 키를 전송한다. 기존의 DRM 시스템과 제안하는 시스템의 차이는 유·무선 모두를 사용하며, 키 재요청시 새로운 키를 생

성하여 전송하게 된다.

[그림 12]에서 나타내고 있는 제안하는 시스템의 키 분배 방법은 유선으로 다차원 배열과 조합도를 보내면, 무선을 이용하여 사용자의 Mobile phone으로 조합도 암호화키를 공개키로 암호화하여 전송하여 보안성을 높였다. [그림 12]를 통해, 키 분배 환경과 분배 방법, 재전송에 대한 기존 DRM 시스템과 제안하는 시스템을 비교해 볼 수 있다.

I사는 PKI를 사용 유선환경에서 공개키로 암호화하여 전송하였고 키 재전송 요구시 동일한 값을 전송한다.

M사는 PKI 환경이 아니며, 유선환경을 이용하여 복호화키를 전송하며, 키 재전송 요구시 동일한 복호화키를 재전송 한다. 제안하는 시스템은 유·무선 환경을 이용하여 사용자에게 재배치된 다차원 배열과 조합도, 조합도 암호화키를 전송한다. 키 재전송 요구시 새로운 다차원 배열과 조합도, 조합도 암호화키가 모두 재전송된다.

기존의 시스템과 제안하는 시스템과의 전반적인 사항을 비교 분석 해 보면 제안하는 시스템은 기존 시스템과 같이 유선환경을 지원하며 동시에 무선환경을 이용하여 사용자 인증에 있어 기존의 시스템보다 더 향상되었다.

비교	기존 I사 DRM	기존 M사 DRM	제안하는 시스템
PKI 사용 여부	Y	N	N
키 분배 환경	유선	유선	유 / 무선
키 분배 방법	공개키로 암호화 후 전송	복호화 키 전송	복호화 키 모델 조합 후 전송
키 재 요청 시	동일 값 전송	동일 값 전송	랜덤 값 전송
Sniffing 가능 여부	Y	Y	Y
복호화 키 노출 여부 (Sniffing 시)	N (본인이 아니면 복호화키 추출 불능)	Y (복호화 키 유출, 보호되지 못함)	N (복호화 키 생성 불가능)

[그림 12] 기존 DRM과 제안하는 시스템

5.2 동영상의 암·복호화 시간 실험평가

M사의 DRM 시스템은 암호화 시 동영상 콘텐츠를 WMV 파일로 인코딩 작업을 수행한 후 암호화 작업을 하기 때문에 암호화에 대한 시간 분석 비교에서 제외시켰다.

그리고 I사의 DRM 시스템은 동영상 전체를 암호화하지 않고, 동영상의 I-Frame만을 암호화하기 때문에 부분 암호화 시스템에 속하지만, I-Frame을 추출하기 위하여 GOP(Group of Picture) 그룹의 모든 헤더의 내용을 읽은 다음 I-Frame의 크기를 계산하여 추출하기 때문에 제안하는 시스템 암호화 방법보다 느리다.

공유키 풀 암호화 시스템 및 해쉬체인 암호화 시스템은 제안한 시스템과 같이 동영상 전체를 대칭키로 암호화하였기 때문에 동일한 시간이 나오기 때문에 실험 대상에서 삭제 하였다.

암호화에 대한 시간은 I사의 시스템보다 1.13배 정도 향상된 결과를 보였다. M사는 위에서 언급했듯이 엔코딩 작업이 약 암호화하는 시간보다 무려 51배의 느린 작업을 거친 후에 암호화하기 때문에 암호화시에는 오랜 시간이 걸린다는 것을 알 수 있었다. 하지만 동영상의 암호화의 경우는 미리 한번만 암호화하여 배포되기 때문에 비중은 두지 않았다.

복호화에 대한 시간을 비교 분석한 결과는 [그림 13]과 같이 기존의 I사의 DRM 시스템 보다 약 1.61배 향상되었다. M사의 DRM 시스템의 경우는 파일전체를 암호화하였기 때문에 복호화 역시 가장 늦으며, I-Frame DRM 시스템은 암호화 방법과 마찬가지로 GOP 그룹의 모든 헤더를 읽어 I-Frame을 얻어내야 하기 때문에 제안한 시스템보다는 복호화 속도가 느린 것을 확인하였다.

5.3 복호화에 대한 키 추출 실험평가

동영상 복호화 키에 대한 추출은 기존 시스템 중에서 I사의 공개키를 이용한 암호화 전송방식과 비교하였으며, 그 외의 시스템은 복호화 키를 그냥 전송함으로 인해 실험대상에서 제외되었다.

실험은 키의 길이가 16Byte크기의 1,000개를 무작위로 생성한 후, 이를 공개키 1,024 Bit로 암호화 시키고 개인키로 복호화 하는 것과, 제안하는 시스템은 16 * 18 크기의 2차월 배열을 생성하여 대칭키 알고리즘인 256Bit AES 복호화 기법을 사용하였다.

암호화에 대한 시간을 비교 분석한 결과는 제안한 시스템이 공개키를 이용한 시스템보다 약 16.3배 빨랐으며, 이는 대칭키가 공개키 보다 빠르며, 키연산시 들어가는 XOR 기법이 간결하기 때문이다.

5.4 암·복호화 키에 대한 안전성 평가

기존 DRM 시스템은 인증서를 사용하는 경우 인증서 확인 작업 및 키를 암호화 복호화 하는데 많은 오버헤드가 발생하며, 인증서 미소지시에는 인증서 발행하기 위한 절차가 많이 까다롭다. 그러나 인증서를 사용한 공개키 암호화 방식은 어떠한 공격에 대해서도 안전하다는 장점이 있다. 인증서를 사용하지 않는 DRM 시스템의 경우는 콘텐츠를 보호하는 암호화키를 대칭키로 사용하여 전송하기 때문에 서로간의 키 교환 문제가 어려우며, 유선망을 사용하기 때문에 스니핑 공격에 대해 취약하다.

제안한 DRM 시스템은 암호화키를 전송하기 위해

다차원 배열을 생성한 후, 다차원 배열과 조합도를 전송하여 모바일 폰으로 전송받은 암호화 키를 이용하여 다차원 배열을 복호화하기 때문에 속도가 매우 빠르며, 무선망을 이용하여 조합도를 암호화한 키를 따로 전송하기 때문에 키 조합으로 인한 키 유추가 매우 어렵다.

또한 다차원 배열 자체에는 어떠한 암호화도 되어있지 않아 바로 실행이 가능하며, 키 요청마다 새로운 다차원 배열을 전송하기 때문에 스니핑, 스푸핑, 재전송 공격에 강한 특징을 가진다.

6. 결론

인터넷의 확산과 컴퓨터 간 상호연결성의 증대로 디지털 자원에 대한 유통환경이 급속히 변화함에 따라 디지털 형태의 음악, 화상, 영상물, 출판물 등 멀티미디어 자료에 대한 수요가 급격히 증가로 인해 불법복제 방지를 위한 디지털 저작권 보호문제가 중요한 이슈로 대두되고 있다.

기존의 DRM 시스템은 하나의 대칭키로 암호화하는 것이므로 사용자가 해당 대칭키를 노출시키면 더 이상 해당 저작물에 대한 보호를 보장받지 못하며, 또한 키를 노출시킨 사용자가 누구인지 알 수 없어서 해당 사용자를 추적할 수 있는 방법이 없다.

기존의 One-path XOR 방식은 비트값이 전부 1일 경우 기존의 키가 나오는 단점과 유·무선으로 전송되는 각각의 값의 결합으로 암호화키가 나온다는 단점도 있다. 그러나 제안하는 방식은 유선의 다차원 배열과 조합도, 무선의 암호화키를 이용하여 암호화키를 획득한다. 유선의 다차원 배열은 어떠한 암호화도 시키지 않았기 때문에 암호화키 유추시 수행시간을 향상 시켰으며 다차원 배열과 조합도가 유추 되더라도 무선으로 보내지는 암호화 킷값 없이는 암호화키(EK)의 유추가 불가능하다. 또한 키 요청마다 새로운 다차원 배열과 조합도를 전송하기 때문에 기존 시스템보다 스니핑, 스푸핑, 재전송 공격에 강한 특징을 가지고 있다.

향후, 다차원 배열 기법과 휴대폰 및 PDA와 같은 이동식 휴대 단말기에서 활용할 수 있도록 시스템을 개선할 계획이다.

참고문헌

[1] 김정재 외 2명, "시큐리티 에이전트를 이용한 사용자 인증과 DRM보안 시스템 설계," 한국정보처리학회 논문지 C, VOL. 12-C NO. 07 pp. 0973 ~ 0980 2005. 12.

[2] 김정재 외 2명, "동영상 데이터 보호를 위한 공유 키 풀 기반의 DRM 시스템," 한국정보처리학회 논문지 C, VOL. 12-C NO. 02 pp. 0183 ~ 0190 2005. 04.

[3] 김정재, "멀티미디어 데이터 보호를 위한 대칭키 암호화 시스템에 관한 연구," 숭실대학교 박사학위논문, 2005.

[4] 정용훈 외 2명, "멀티미디어 데이터 보호를 위한 다중 랜덤 대칭키 기반 부분 암호화 시스템," 한국정보과학회 한국컴퓨터종합학술대회, VOL. 00, NO. 00 pp. 0154 ~ 0156, 2005. 07.

[5] 추연수, "디지털 콘텐츠 보호를 위한 안전한 인증방식 설계 및 구현," 숭실대학교 석사학위논문, 2005.

[6] Brad Cox, Superdistribution : Objects As Property on the Electronic Frontier, Addision-Wesley, May 1996.

[7] Sung, J Park, "Copyrights Protection Tech niques," Proceedings International Digital Content Conference, Seoul Korea, Nov, 28~29, 2000.

[8] Intertrust : http://www.intertrust.com/main/ overview/drm.html

[9] Joshua Duhl and Susan Kevorkian, "Unde rstanding DRM system: An IDC White paper," IDC, 2001.

[10] Shai Halevi, Hugo Krawczyk, "public-key cryptography and password protocols," ACM Transactions on Information and System Security, Vol.2, No3, pp230~268, August 1999.

[11] http://www.microsoft.com/windows/windowsmedia/ drm.asp

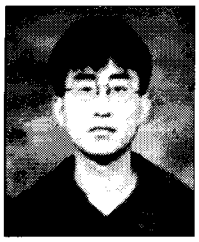
[12] Thomas Wu. "The Secure Remote Password Protocol," 1998 Internet Society Network and Distributed System Security Symposium, San Diego, March 1998.

민 소 연(So-Yeon Min) **[종신회원]**

- 1994년 2월 : 숭실대학교 전자공학과(공학사)
- 1996년 2월 : 숭실대학교 전자공학과(공학석사)
- 2003년 2월 : 숭실대학교 전자공학과(공학박사)
- 2005년 3월 ~ 현재 : 서일대학 정보통신과 조교수

<관심분야>
유성통신, 네트워크, 통신알고리즘

김 정 재(Jung-Jae Kim) **[정회원]**



- 1995년 2월 : 영동대학교 컴퓨터공학과(공학사)
- 1999년 2월 : 숭실대학교 컴퓨터학과(공학석사)
- 2005년 2월 : 숭실대학교 컴퓨터학과(공학박사)
- 2006년 2월 ~ 현재 : (주) RetailTech 수석연구원

<관심분야>
멀티미디어 보안, 멀티미디어 데이터베이스, DRM, RFID