主題

워터마크와 공개키 암호 알고리즘을 이용한 멀티미디어 컨텐츠 보호에 관한 연구

광운대학교 김진묵, 유황빈

차 례

요 약

인터넷의 급속한 발달과 성장으로 인해 기존의 현실 세계에서 사용하던 방대한 양의 자료들이 전자문서화 되어 가고 있다. 이에 따라 인터넷상의 멀티미디어 컨텐츠들에 대한 소유권 보호와 인증에 대한 문제가 심각하게 대두되고 있다. 이에 본 고에서는 인터넷상의 멀티미디어 컨텐츠에 대한 저작권 보호와 인증에 대한 문제를 해결하기 위한 방안인 워터마크 방법과 공개키 암호 알고리즘을 이용한 멀티미디어 컨텐츠 보호에 관한 아이디어를 제시한다.

I. 서 론

현대 정보화 사회는 컴퓨터 사용 인구의 급속한 증가로 인해 기존의 현실 세계에서 사용하던 방대한 자료들이 전자 문서로 변하고 있다. 이와 같이 많은 사람들이 전자 문서를 사용되게 되면서 기존의 종이를 이용한 문서 보급으로 방식에서 발생하는 막대한 비용 지출과 편집, 수정의 어려움 등이 없어졌고 문서의 복사가 용이하게 되어 다양한 매체의 멀티미디어 데이터들이 전자기적 장치들에 의해 디지털화 되고 효율적으로 저장, 복사 및 이용이 가능하게 되었다.

하지만, 전자문서가 인터넷을 통하여 상호 교환됨으로 인해 멀티미디어 데이터의 빠른 디지털화 현상은 멀티미디어 데이터의 편집, 전송 및 저장에 편리함을 제공하는 순기능과 함께 역기능으로 저작권 분쟁과 무단 복사 등과 같은 문제가 발생할 수 있다.

이처럼 인터넷 환경에서 전자문서는 사용함에 있어 두 가지 측면의 순기능과 역기능을 갖게 되는데, 순기능으로 인하여 얻는 장점은 문제를 발생시키지 않겠지만, 역기능으로 인하여 발생하는 지적 재산권 보호 문제나 무단 복사로 인하여 발생하는 정보 상실감에 대한 역기능은 커다란 문제가 되고 있다. 하지

만, 이를 방지해 줄 수 있는 대안이 없다.

현실 세계에서는 자신이 제작한 문서나 정보를 담고 있는 다른 매체에 대해 저작자의 동의 없이 내용을 위, 변조하거나 무단으로 복사하여 자신의 이익을 위해 사용한다면 법적인 제재를 받게 된다. 하지만, 인터넷 환경과 같은 가상의 세계에서는 위와 같이 불법적으로 저작자의 양해를 구하지 않고 정보를 무단으로 복사하거나 이를 악용하여 위.변조 한다하더라도 어떤 법적인 제재를 마련하기가 쉽지 않다. 그러므로, 현실 세계와 달리 가상의 세계인 인터넷 환경에서는 자신의 지적 정보 재산에 대해 악용하려는 시도에 대해 무방비 상태일 수밖에 없는 것이다.

가상 세계에서 웹 브라우저를 사용하여 개인의 정보를 복사하여 참고하는 것은 직접적인 범죄행위는 아니다. 이미 인터넷 환경에서 자신의 정보를 공개하는 행위가 자신의 정보를 다른 사람들이 참고하는 것에 대해 저작권자 스스로가 자신의 전자문서를 복사하여 참조하는 행위에 대해서는 묵인한 것이기 때문에 이를 범죄행위라 할 수는 없다. 하지만, 이와 달리 저작자에게 동의를 구하지 않고 웹 브라우저를 사용하여 인터넷상에 있는 정보를 자신이 생산한 것처럼 위.변조하는 행위는 현실세계에서와 마찬가지로 범죄행위에 속하게 된다. 그렇다면, 현실 세계와 마찬가지로 이러한 범죄 행위에 대하여 법적인 제재를 가하지는 않더라도 원래의 저작권자의 권리를 보호할 수 있는 방안은 없는 것인가?

이와 같은 화두를 가지고 많은 과학자들이 연구를 하였다. 전자 문서의 저작권을 보호하기 위한 방안을 마련하기 위해서는 어떤 방안들이 있을 것인가 하고 말이다. 이런 연구들 가운데 대표적인 3가지 방안에 대해 알아보면 다음과 같다.

첫째, 보안 알고리즘을 사용해 전자문서의 내용을 암호화하는 방법이다. 암호화 방법은 원래의 데이터를 암호 알고리즘을 사용하여 데이터를 보호할 수 있다. 하지만, 암호 알고리즘을 사용하여 데이터를 암호화하는 경우 암호를 해독하지 않으면 정당하게 데이터를 이용하려는 사용자도 데이터를 볼 수 없다는 단점과 암호를 해독한 후에 자신의 데이터라는 저작권에 대한 법적인 근거가 나약해 진다는 단점을 갖게 된다.

둘째, 워터마크라는 외관상으로는 원래 데이터와 거의 차이가 나지 않도록 변환하는 방법이다. 참고적으로 워터마크란, 워터마크를 삽입한 데이터에 대하여 위.변조를 가하더라도 워터마크를 복원함으로 인해서 데이터에 대한 법적 소유권을 주장할 수 있다. 하지만, 워터마크를 사용한다고 하더라도 위.변조 행위자가 이전에 발행된 워터마크를 추출하여 사용하는 경우에는 이를 정당한 워터마크로 인식하는 커다란 문제점과 문서마다 각기 다른 워터마크의 채용이 불가능하다는 단점을 갖고 있다.

셋째, 위의 2가지 방법인 암호화 방법과 워터마크 방법의 단점을 보완하여 데이터에 워터마크를 삽입한 후 공개키 암호방식을 이용하여 암호화하는 워터마크 + 공개키 암호화 혼합 방법을 사용하는 것이다. 이는 워터마크를 삽입한 후에 공개키 암호 알고리즘을 사용하여 좀 더 확실한 지적 소유권에 대한 인증 서비스를 제공할 수 있다.

그럼, 위의 3가지 멀티미디어 데이터에 대한 저작권 보호 및 자료 인증, 소유권 증명에 대한 연구를 위한 기반지식이 되는 워터마크와 공개키 암호 알고리즘에 대해 알아보자.

Ⅱ. 기반지식

1. 공개키 암호 알고리즘

공개키 암호 알고리즘이란, 암호화 알고리즘 중에서 공개키를 사용하여 상대방과 자신 사이에 전달되는 정보를 안전하게 송, 수신하는 알고리즘이다. 공개키 암호 알고리즘의 대표적인 예로 RSA 암호 알고리즘이 있다.

공개키 암호 알고리즘은 먼저, 데이터를 송.수신하고자 하는 두 사람이 쌍이 되는 두 개의 공개키와 비밀키를 생성하여 제 3의 믿을 수 있는 인증 기관인 CA(Certificate Authority)에 공개키를 등록한다.

공개키는 일반적으로 사용하는 전화번호부에 공개적으로 게재된 자신이 비밀성 서비스를 제공받기 위해 공개하는 키 값이다. 이에 반해, 비밀키는 상대방이 자신의 공개키를 이용해 암호화하여 전송한 데이터를 복호화 할 때 사용하기 위해 쌍이 되는 키 값을 말한다. 이렇게 공개키와 비밀키 쌍을 사용하여 데이터의 비밀성을 제공하고, 또한 전송하는 데이터의 일부에 자신의 비밀키를 사용하여 서명을 한 후 데이터에 추가해서 전송함으로서 송.수신되는 데이터에 대한 무결성과 인증성도 제공할 수 있다.

실제로 공개키 암호 알고리즘을 사용함으로서 워터마크만을 사용하는 방법이 갖는 비밀키에 의한 새로운 위조 가능성을 배제시켜 줄 수 있게 된다. 또한, 공개키를 제 3의 믿을 수 있는 신용기관이 관리하여 주기 때문에 더욱 확실하게 사용자 신분에 대한 신분확인에 대한 인증을 보장할 수 있다.

공개키 암호 알고리즘의 동작과정을 간단하게 그림으로 나타내면 그림 1과 같다.

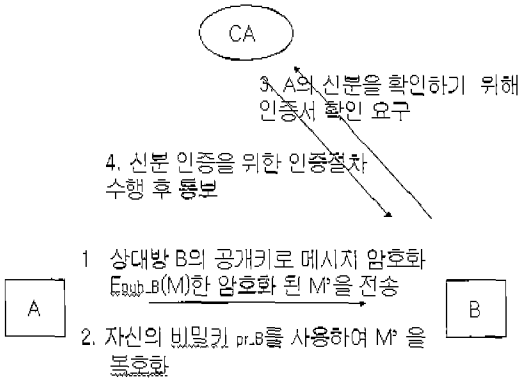

그림 1. 공개키 암호 알고리즘의 동작

본 고에서는 다양하게 많은 공개키 암호 알고리즘 중에서 RSA(Rivest, Sha- mir, Adleman) 알고리즘을 사용하여 워터마크화 된 멀티미디어 데이터를 암호화하도록 한다. RSA 공개키 암호 알고리즘은 인수분해 문제(factoriza- tion problem)의 어려움을 수학적 근거로 한다. 즉, 주어진 합성수 n의 소인수를 찾는 문제로 n의 자릿수가 매우 큰 경우(1024비트 이상)에는 n의 소인수를 현실적으로 찾기가 어렵다는 수학적인 성질을 이용한 암호 알고리즘이다.

2. 워터마크

2.1 워터마크의 정의

워터마크란, 저작권 보호를 위해 영상 데이터에 표시한 보이지 않는 마크(Mark)를 말한다. 즉, 디지털 컨텐츠에 사용자의 ID(Identification)나 자신만을 나타낼 수 있는 정보를 넣음으로써 불법적인 복제를 막고, 데이터 소유자의 저작권과 소유권을 효율적으로 보호하기 위한 방법으로서 데이터에 일정한 암호를 숨겨서 부호화 하는 과정에 사용하는 부호를 워터마크(Watermark)라고 한다. 또한 영상이나 음성 등의 신호에 특정한 코드나 패턴 등을 삽입하는 것을 말하기도 한다. 미술품이나 책의 저자가 작품이 자신의 것임을 표시하기 위해 육안으로는 식별이 불가능한 특수한 형태의 표시를 해 두는 것을 말하기도 한다. 즉, 물이나 특별한 약품 등을 사용하여 보이지 않도록 표시해 두는 표식을 일컫는다.

디지털 워터마크(Digital Watermark)는 디지털 컨텐츠나 기존의 아날로그 데이터를 디지털화 할 때, 첨가하는 일종의 저작권 관리 정보로서 개인의 식별기호나 부호를 삽입할 때 삽입되는 표시라고 정의할 수 있다.

비디오 데이터를 예로 들어 좀 더 부연 설명하면, 주어진 영상 I에 레이블(Label) S = {S1, S2, ..., Sn}를 부호화 과정 E를 통해 삽입하면 워터마

크가 삽입된 영상 I′ = E(I, S)를 얻을 수 있게 된다. 이때 레이블 S는 영상에 숨겨진 워터마크라고 한다.

2.2 워터마크의 필수 요건

워터마크의 구비조건은 첫째, 인간이 시각적으로 감지하기 힘들어야 한다. 즉, 멀티미디어 영상의 경우 인간이 시각적으로 원본 멀티미디어 데이터와 워터마크가 삽입된 멀티미디어의 구분이 어려워야 한다는 것이다. 하지만, 이러한 조건을 만족시키려할 때 JPEG나 MPEG와 같은 손실 압축을 하는 경우에 삽입된 워터마크가 지워지는 문제가 발생할 수 있다. 둘째, 워터마크는 숨길 정보의 양을 고려하여야 한다. 즉, 워터마크를 필요로 하는 환경에 따라 삽입될 정보는 미리 정해진다. 영상에 대해서는 일반적으로 300~400 bit 가량의 정보를 삽입한다. 그러므로, 시스템 설계자는 이처럼 자료에 숨겨질 비트수를 고려해야만 한다. 셋째, 낮은 에러 확률(low error probability)을 가져야 한다. 즉, 고의적이거나 비고의적인 훼손과 손상이 없더라도 워터마크를 추출하는데 실패할 확률과 워터마크가 존재하지 않는데 존재할 확률이 아주 작아야 한다. 넷째, 워터마크는 다양한 손상 후에도 반드시 추출이 가능해야 한다. 이 기능이 디지털 워터마크 기능에서 가장 기술적으로 중요한 부분으로 디지털 형태의 Audio, Video 신호들은 일반적으로 다양한 형태의 변형이 있다. 이러한 변형에도 불구하고 워터마크는 반드시 추출되어야 한다. 만약 그렇지 못하다면 워터마크를 삽입할 이유가 없어지는 것이다. 다섯째, 원본이 없이도 워터마크의 추출이 가능해야 한다. 즉, 다양한 현실적인 멀티미디어 컨텐츠에 대한 오용행위는 너무도 다양하고 강력하다. 그러므로, 실세계에서는 원본이 없이도 워터마크의 추출이 가능해야 한다.

워터마크는 위의 5가지 사항을 반드시 만족시켜야 한다. 지금까지 워터마크에 대한 정의와 워터마크가 갖추어야 할 기본 요구조건들을 확인하였다. 그렇다면, 이러한 워터마크는 어떤 종류가 있을까?

2.3 워터마크의 구분

워터마크는 크게 2가지 종류로 나눌 수 있다. 즉, 공간 영역에서의 디지털 워터마크와 주파수 영역에서의 디지털 워터마크로 나뉜다.

첫째, 공간 영역에서의 워터마크는 물리적 픽셀 영역, 즉 공간 영역에서 워터마크를 삽입하는 것이다. 가장 간단한 방법은 픽셀들을 임의적으로 선택하여 그것의 밝기값의 LSB(Least Significant Bit)를 변형시키는 것이다. 이 방법은 잡음과 일반적인 신호처리(손실압축, 편집, 필터링)에 아주 약하다. 이러한 단점을 극복하기 위해 인간의 시각 특성을 이용할 수 있다. 즉, 인간 시각의 마스킹(Masking) 효과에 의해 영상 내의 결(Texture) 영역이나 윤곽선 둘레의 밝기 값의 변화를 육안으로 잘 구별할 수 없다는 점을 이용하여 워터마크를 삽입함으로서 단점을 보완할 수 있다.

둘째, 주파수 영역에서의 워터마크는 멀티미디어 영상 데이터를 FFT, DCT, Wavelet등과 같은 변환으로 주파수 공간으로 변환하여 그 주파수 영역들 중에서 시각적으로 덜 민감한 성분에 대하여 적응적으로 워터마크를 삽입하는 방법이다. 이 방법은 단일 주파수 성분을 변화시켜 변환 블록내의 밝기 값 전체에 영향을 미치는 방법이다. 그러므로, 불법적인 공격에 강한 워터마크를 만들 수 있다.

위의 2가지 디지털 워터마크 외에도 여러 가지 방법이 있기는 하지만 위의 두 가지 방법이 가장 일반적인 분류방법이다.

2.4 워터마크 삽입 과정

워터마크는 다음과 같이 멀티미디어 컨텐츠 내에 삽입, 추출된다. 먼저, 삽입 과정은 아날로그 신호 'S'를 디지털 신호 'D'로 나타낼 수 있다. 디지털 신호로부터 워터마크를 삽입할 수 있는 형태로 변환된

데이터를 'V', 삽입하고자 하는 정보를 'I'라고 하면, I가 V에 삽입될 수 있도록 변환된 정보를 'X'라고 할 때, 워터마크의 삽입 과정은 그림 2와 같다.

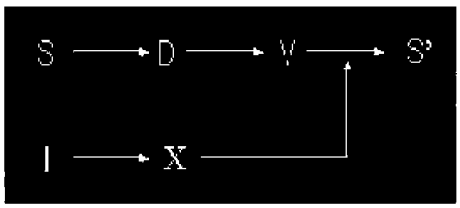

그림 2. 일반적인 워터마크 삽입과정

실제로, 워터마크의 삽입 동작을 상태흐름도로 표시하면 그림 3과 같다.

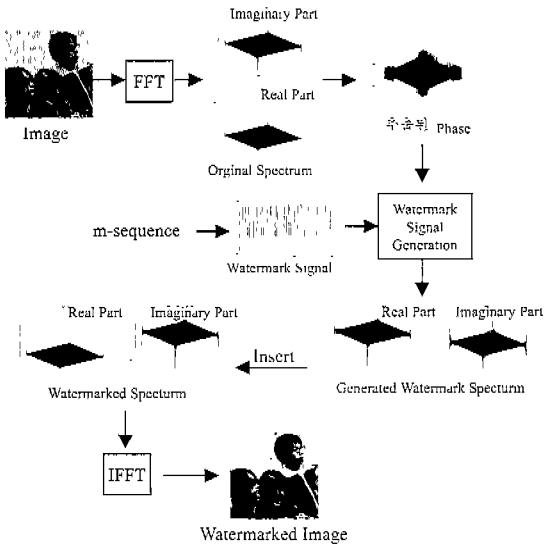

그림 3. 워터마크 삽입 동작

2.5 워터마크의 구성

영상 데이터를 주파수 형태로 변환했을 때 가질 수 있는 통신 채널이라고 가정한다면, 워터마크는 그 통신 채널로 통과하는 신호라고 볼 수 있다. 그 신호가 잡음, 필터링, 압축전송 등에 영향을 받지 않고 효과적으로 전송이 될 수 있도록 대역확산통신(Spread Spectrum Communication)방식을 도입한다. 즉, 워터마크(신호)를 영상(전송채널)이 갖고 있는 여러 주파수 영역으로 확산시킴으로써 특정 주파수 대역의 에너지는 감지하기 어렵게 한다. 영상의 변화를 감지 못하면서 시각적으로 중요한 영역에 정보를 삽입을 하기 위하여 워터마크는 M-Sequence를 사용한다.

워터마크를 I라고 하면 I는 {0,1} 또는 {-1,1}로 구성이 되는 Sequence이다. 워터마크를 삽입할 값은 크기 여부에 따라 정해진다.

워터마크를 **I**라고 하면 **I**는 **{0,1}** 또는 **{-1,1}**로 구성이 되는 Sequence이다. 워터마크를 삽입할 값은 크기 여부에 따라 정해진다.

$$V' = V + \alpha * I \qquad \text{(식 1)}$$

$$V' = V(1 + \alpha * I) \qquad \text{(식 2)}$$

(식 1)의 경우 V 에 단순히 값을 더하는 것이고, (식 2)는 V값에 비례하여 값을 더하는 경우이다. V 값에 따라 α는 다양한 값을 가질 수 있다.

2.6 워터마크 삽입 위치의 추출방법

워터마크를 삽입할 V를 추출할 때에는 블록 단위, 전체 영역, 라인 단위로 변환을 할 것인지, Frequency 영역이나, 물리적인 픽셀에 삽입할 것인지 고려해야 한다. 참고한 논문에서는 전체 영역에 대하여 FFT를 수행하여 Phase와 Magnitude의 변화 여부를 파악하여 Phase영역에서 워터마크를 삽입할 위치를 찾아내는 방법을 선택하였다.

워터마크 삽입 알고리즘은 다음과 같다.

D : 원본

D' : 워터마크가 삽입된 영상

I : 사용자의 워터마크

단계 1. 워터마크(M-Sequence)를 생성시킨다.

M : 워터마크의 크기

$I = \{I_k, / I_k \in \{-1, 1\}, k = 1..M\}$

단계 2. 영상(D)을 FFT를 한다. FFT후의 자료를 V라 한다.

N : 영상의 총 *pixel* 수 *(row x col)*

$D = \{D_k \mid D_k \in (0, 255), k = 1...N\}$

$V = \{V_k \mid V_k \in$ *Complex Number*, $k = 1...N\}$

$$V(u,v)=\frac{1}{col*row}\sum_{x=0}^{col-1}\sum_{y=0}^{row-1}D(x,y)\exp[-j2\pi(ux/col+vy/row)]$$

u = 0,1,..,col-1, v=0,1,....,row-1로 정의한다.

단계 3. V에서 추출된 Phase와 Magnitude를 조합하여 워터마크(W)를 삽입할 위치를 찾아낸다.

N : 영상의 총 *pixel*수 *(row x col)*

$J \in (100 ,1000), \ J < N$

$P = \{P_1, \mid P_k = Phase(V_k), k = 1...N\}$

$M = \{M_k \mid M_k = Magnitude(V_k), k = 1...N\}$

$S = \{S_k\}$, S_k : P와 M의 조합에 의해서 구해진 V의 위치 인덱스, $k = 1...J$

단계 4. 선택된 P에 워터마크(W)를 더한다.

$$P'(S_k)=\sum_{k=1}^{J}(P(S_k)+\alpha\times X_k)$$

$\alpha \in$ 실수

$X_k = I(L_k), k = 1...J$

$L = \{L_k \mid L_k = M \bmod k , k = 1...J\}$, M은 I의 크기

단계 5. 워터마크가 삽입된 Phase(P')와 Magnitude를 조합하여 V'를 생성시킨다. V'를 IFFT를 하면 워터마크가 삽입된 D'가 생성된다.

N : 영상의 총 *pixel* 수 *(row x col)*

$D' = \{D'_k \mid D'_k \in (0, 255), k = 1...N\}$

V' = {V'k | V'k ∈ Complex Number, k = 1...N}

$$D'(x,y)=\sum_{u=0}^{col-1}\sum_{v=0}^{row-1}V'(u,v)\exp[j2\pi(ux/col+vy/row)]$$

x = 0,1,..,col-1, y=0,1,....,row-1 로 정의한다.

2.2.7 워터마크 추출방법

영상은 JPEG 압축과 잡음 등에 변형된 영상에서 워터마크를 효율적으로 추출하기 위하여 M-Sequence의 자기상관관계 특성과 원본과 워터마크가 삽입된 자료의 차이값을 이용하여 워터마크를 추출한다.

D : 원본

D' : 워터마크가 삽입된 영상

I : 사용자의 워터마크

단계 1. D와 D'를 FFT하여 V와 V'를 생성한다.

단계 2. V와 V'에서 Phase를 추출한다.

$P = \{P_k, \mid P_k = Phase(V_k) , k = 1...N\}$

$P' = \{P'_k, \mid P_k = Phase(V_k'), k = 1...N\}$

단계 3. V에서 추출된 Phase와 Magnitude를 조합하여 워터마크 가 삽입된 위치를 찾아낸다.

$J \in (100 ,1000), \ J < N$

$S = \{S_k\}$, S_k : P와 M의 조합에 의해서 구해진 V의 위치 인덱스, $k = 1...J$

단계 4. P와 P'의 차이를 구한 dP와 S를 이용하여 값(I')를 추출한다.

$$dP = P' - P$$

$$I'(S_k) = \sum_{k=1}^{J} dP(S_k)$$

단계 5. I′와 I 사이의 자기 상관 관계(Autocorrelation)를 구하여 워터마크가 있는지 없는지 판단한다.

위와 같은 과정에 의해 워터마크를 삽입하기 위한 삽입 위치를 추출하고 주파수 영역에 의한 워터마크 삽입 방법 중에서 FFT를 수행하여 삽입 위치를 결정하여 수행하는 예제를 보았다. 그리고, 이를 원본 없이 다시 추출하는 과정도 보았다.

그렇다면, 워터마크만 사용하여 멀티미디어 컨텐츠에 대한 소유권 주장의 법적인 효과를 보장할 수 있을까 ? 워터마크를 사용함으로서 워터마크를 적용하지 않았을 때 보다 분명히 소유권 보장을 받을 수 있을 확률이 높아졌음은 분명하다. 하지만, 참고논문에서의 워터마크도 별도의 워터마크를 삽입하여 위조를 하는 경우에는 위.변조 징후를 발견하기가 힘들고, 정당한 워터마크인가를 확인할 수 없는 단점을 가지고 있다. 또한, 위조 행위자가 이전에 발행된 워터마크를 추출하여 사용하는 경우에는 정당한 워터마크로 인식하게 된다는 단점도 지니고 있다. 마찬가지로 문서마다 서로 다른 워터마크를 채용하는 것도 불가능하다. 이와 같은 워터마크가 가지고 있는 단점들을 보안하기 위해서는 워터마크와 공개키 암호 알고리즘을 혼합적으로 적용하여 단점을 보안할 수 있을 것이다. 하지만, 단순히 워터마크를 암호화하여 추가하는 것은 좋은 생각이 아니다. 만약, 워터마크를 삽입한 후 이를 암호화하여 순차적으로 추가하는 경우라면 암호화 자체의 복잡성과 복호화 한 후에 워터마크 정보를 이용한 새로운 위조의 위험성을 가지게 된다. 또한, 복호화 한 순간부터 이미 멀티미디어 컨텐츠의 인증성은 손상되게 된다. 이는 비공개키 암호 알고리즘이 갖고 있는 구조적인 단점이기도 하다. 그러므로, 데이터를 암호화하는데 사용한 비밀키도 노출되게 되는 위험성을 지니고 있다.

그렇기 때문에 이를 보완하여 멀티미디어 컨텐츠에 대한 소유권 보장과 자료 인증을 위해서는 공개키 암호 알고리즘이 가지고 있는 장점과 워터마크 방법이 지니는 장점을 모두 수용하여 보완적으로 사용하는 것이 멀티미디어 컨텐츠 보호에 효율적이다.

Ⅲ. 워터마크와 공개키 암호 알고리즘을 이용한 멀티미디어 컨텐츠의 보호

워터마크를 사용하여 보호하고자 하는 멀티미디어 컨텐츠에 인지되지 않을 정도의 부가 잡음 정보를 추가하여 저작권 및 인증성을 제공할 수 있으나 이에 제한 조건이 있고, 위.변조의 위험성이 있으므로 공개키 암호 알고리즘과 혼합하여 저작권과 인증성 제공을 좀 더 보안하고자 한다. 그런데, 어째서 공개키 암호 알고리즘을 혼합하여 사용하려 하는가?

공개키 암호화 방식은 자신의 비밀키를 알려 줄 필요가 없으므로 비밀키에 의한 새로운 위.변조의 위험성이 적다. 또한 공개키를 제 3의 믿을 수 있는 인증기관이 관리하므로 위조에 대한 의혹을 제거할 있다.

워터마크에 대한 정의, 필수요건, 삽입, 삽입위치 추출, 추출에 대한 것들은 이미 앞의 장에서 살펴 보았으니 이번 장에서는 중복하여 언급하지 않기로 한다. 실제로 워터마크의 삽입과정까지 마친 단계의 멀티미디어 컨텐츠에 대하여 어떻게 암호화와 암호화된 데이터가 전송 과정후에 어떤 과정을 통하여 저작권에 대한 보장과 인증 서비스를 제공 받을 수 있는지에 초점을 맞추어 살펴보자.

첫 번째 방법으로, RSA공개키 암호 알고리즘을 적용하여 멀티미디어 컨텐츠의 저작권에 대한 보호와 인증 서비스를 제공하는 것을 보여준다. 우선, 멀티미디어에 워터마크를 삽입한 후 공개키 암호방식

의 키 생성 방식에 의해 난수 발생기에 의해 커다란 정수 x, y를 이용하여 비밀키와 공개키 X와 Y를 생성한다. 이렇게 생성한 자신의 비밀키 Y 를 사용하여 워터마크 처리된 멀티미디어 컨텐츠에 대하여 암호화를 수행한 후에 자신의 공개키 X와 멀티미디어 컨텐츠에 대한 정보를 인터넷에 공유한다. 멀티미디어 컨텐츠에 대한 필요성을 느끼는 사용자는 인터넷에서 문서와 공개키를 다운로드 받아 이를 사용할 때 제 3 의 인증기관에 저작권자의 공개키에 대한 정보를 확인함으로 인해서 문서의 저작권에 대한 보호와 인증 서비스가 이루어지게 된다. 또한 문서 자체에 대한 변형을 일으킨다고 하더라도 워터마크 처리가 된 상태이기 때문에 원본의 문서에 대한 완전 변조는 일으킬 수 없다.

위의 과정을 간략하게 나타내면 그림 4와 같다.

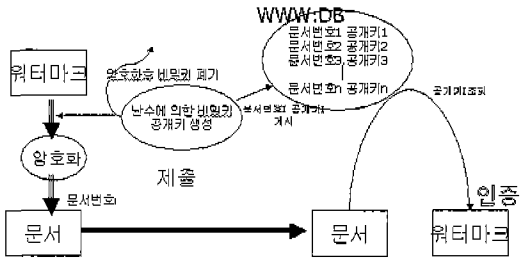

그림 4. 워터마크 + 암호화 동작방식 (RSA 적용)

두 번째로, 워터마크와 공개키 암호 알고리즘을 사용한 멀티미디어 컨텐츠의 저작권에 대한 보호와 인증 서비스 제공을 할 수 있는 방법으로 PGP (Pretty Good Privacy)를 적용하는 예이다. PGP 암호 알고리즘을 적용하는 방법은 워터마크 처리된 멀티미디어 컨텐츠에 대하여 PGP 키 값을 생성하여 지문정보를 WWW상에 지문정보를 공개함으로서 PGP 키 값을 사용하여 암호화된 문서를 상대방이 자신의 지문정보를 얻어 이를 지문 조회과정을 통해 멀티미디어 컨텐츠의 제작에 관한 저작권을 보호받고 인증 서비스도 제공 받을 수 있도록 하여 주는 방법이다.

이의 과정을 간략하게 그림 5와 같이 나타낼 수 있다.

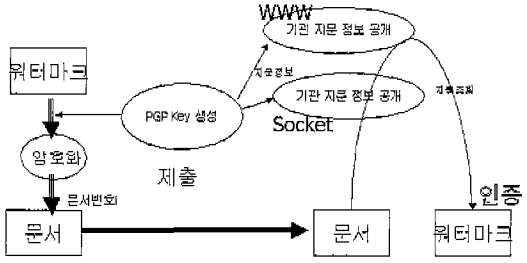

그림 5. 워터마크 + 암호화 동작방식 (PGP 적용)

Ⅳ. 결론 및 향후 연구과제

지금까지 멀티미디어 컨텐츠에 대한 저작권의 보호를 위한 수단으로 워터마크와 암호화 방식, 그리고 이를 보완하여 2가지 방법을 혼합한 방법에 대하여 보았다.

이 글에서 제안한 워터마크 + 공개키 암호 알고리즘 방식이 반드시 우수하다는 것은 아니다. 단지, 기존의 2가지 방식들의 보완된 형태로 위의 아이디어를 제안한 것이다. 또한 공개키 암호 알고리즘을 반드시 사용하여야 한다는 것은 아니지만 대칭키 암호 알고리즘을 사용하는 경우에 발생할 수 있는 비밀키의 노출에 대한 단점에 비해 우수하다는 것이다.

인터넷 접속의 기회 확대와 고도의 인터넷 관련 기술의 발달로 인하여 인터넷에 공유되어지는 멀티미디어에 대한 저작권 문제와 소유권 인증 서비스는 더욱 필요하게 될 것이다.

본 고에서 제안한 아이디어의 단점은 다음과 같다. 공개키 암호 알고리즘으로 사용한 RSA의 방식 같은 경우, 전통적인 워터마크 방식에 지나지 않는 제한 조건을 가지고 있다. 또한 PGP방식을 적용하는 경우에 있어서 아직까지는 텍스트 문서 처리에만

처리가 가능하다는 제한 조건이 있다. 화상 처리를 위해서는 PGP 방식을 적용하기 위한 구조적인 변경이 필요하다.

이 글에서 사용한 연구 방안은 1 bit 흑백문서 화상 처리를 할 때 좁은 대역폭 때문에 비트 플레인 처리가 불가능하다. 그러므로, 주파수 방식이나 DCT 방식을 적용해 보는 것과 같은 대안이 있을 수도 있다. 또한 웹 서버에 조회하지 않고 자기 증명을 하기 위한 방법으로 위조 방지를 위한 자기 증명 알고리즘이나 PGP 키 값을 적용할 때 특정 키에 의해 관리가 가능하다는 단점도 지니고 있다. 또한, 화상 전달시에 데이터 크기가 크다. 이를 완화하기 위하여 다른 압축 방식을 사용하게 되면 위, 변조 행위와 식별이 불가능하거나 오인하는 경우가 발생한다.

마지막으로, 위와 같은 단점들에 대해 고려한 좀 더 발전적인 방안들이 연구되어 멀티미디어 컨텐츠 저작권에 대한 보호와 인증 서비스가 원활하게 이루어 질 수 있기를 바란다.

※ 참고문헌

[1] L. F. Turner, "Digital data security system", patent IPN WO 89/08915, 1989.

[2] M. D. Swanson, Bin Zhu, A. H. Tewfik, "Transparent Robust Image Watermarking", proc. IEEE ICIP, vol.3, sep., pp.211-214, 1996.

[3] R. B. Wolfgang, E. J. Delp, "A Watermark for Digital Image", proc. IEEE ICIP, vol3, pp. 219-222, 1996.

[4] I.J. Cox and M. L. Miller, "A Review of Watermarking and the Importanc of Perceptual Modeling", proc. SPIE Conf. on Human Vision and Electronic Imaging II, vol.3016, pp.92-99, Feb., 1997.

[4] 김덕령, 박성한, "디지털 영상의 소유권을 위한 적응 워터마킹 기법", 제10회 신호처리합동학술대회 논문집 제10권 1호, pp.1133-1136, 1997.

[5] 김태성, 이정수, 김회율, "영상 데이터의 소유권 보호를 위한 강인한 워터마킹 알고리즘", 제10회 신호처리합동학술대회 논문집 제10권 1호 pp.1129-1132, 1997

[6] 박정빈, 황재문, 정성환, "웨이브릿 변환을 이용한 디지털 칼라 영상의 정보 보호", 한국멀티미디어학회 춘계학술발표 논문집, pp.187-192, 1998

[7] 배익성, 김강석, 차의영, "디지털 영상의 보호를 위한 워터마킹에 관한 연구", 한국정보과학회 논문집 10, 1998

[8] 원치선, "디지탈 영상의 저작권 보호", 정보과학회지 제15권 제12호, pp.22-27, 1997.

[9] 최은주, 서정희, 양황규, 차의영, "영상의 변형에 강인한 적응적 디지털 워터마킹에 관한 연구",

[10] 최은주, 서정희, 차의영, "오류 역전파 학습 알고리즘을 이용한 디지털 워터마킹에 대한 소유권 인증",

[11] 배익성, "워터마킹 알고리즘에 관한 연구" http://harmony.cs.pusan.ac.kr/~isbae/semian/watermark1.html

[12] 김윤명, "디지털 컨텐츠 보호를 위한 디지털 워터마크", http://www.orizine.net/oz/9907/digitalwatermark.html

유 황 빈

1975년　인하대학교 전자공학과(학사)
1977년　연세대학교 대학원(공학석사)
1989년　경희대학교 대학원(공학박사)
1981년~현재 : 광운대학교 컴퓨터과학과 교수
1994년~1995년　미 UCSD 교환교수
1995년~1997년　광운대학교 전자계산소장
1997년~1999년　광운대학교 중앙도서관장
2000년~현재　광운대학교 정보지원처장
관심분야: 멀티미디어통신 및 응용, 네트워크 보안

김 진 묵

1998년　배재대학교 컴퓨터공학과(학사)
2000년　배재대학교 대학원(공학석사)
2000년~현재　광운대학교 대학원 박사과정
관심분야: 네트워크 보안, 웹 보안, 인증 시스템