멀티미디어 컨텐츠 배포 시스템에서의 부정자 추적기법에 관한 고찰

신성한*, 박지환*, 허영**
부경대학교 전자계산학과* 한국전기연구소 영상응용그룹**

A Note on Traitor Traceable Techniques for Multimedia Contents Distribution System

Seong-Han Shin*, Ji-Hwan Park*, Young Huh**
Dept. of Computer Science, PuKyong National University*
Applied Imaging Research Group, Korea Electrotechnology Research Institute**

요 약

멀티미디어 컨텐츠의 저작권 보호에 대한 관심이 높아지면서 컨텐츠의 부정복제를 막는 예방 조치로서 여러 가지 기법이 제안되고 있지만, 한편으로는 이러한 부정을 저지른 사용자에 대한 추적 또한 여러 응용분야에서 다양하게 이루어지고 있다. 본 논문에서는 이러한 부정자 추적기법에 대한 연구동향을 살펴보고, 그에 상응하는 요구사항에 대해서 정의한다. 그리고, 실제로 제안된 기법을 검토하여 보다 안전성을 우선시하는 프로토콜에 대해서 논한다.

1. 서론

최근 정보의 디지털화와 아울러 인터넷을 통한 전자상거래가 활성화됨에 따라 다양한 형태의 멀티미디어 컨텐츠의 배포가 활발하게 이루어지고 있다. 그러나, 컨텐츠에 대한 저작권 보호가 되지 않을 경우, 제작자측면에서는 당연히 그에 따른 불이익을 보게 되며, 동시에 제작자의 창작의욕을 떨어뜨리게 된다. 따라서, 멀티미디어 컨텐츠의 건전한 유통을 촉진시키기 위해서는 컨텐츠에 대한 저작권 보호가 필수적이다.

이러한 저작권 보호의 일환으로 다양한 기법들이 제안되고 있다. 예를 들어, 디지털 워터마킹 기법이나 Fingerprinting 기법, 아울러 부정행위(예를 들어 컨텐츠의 무단배포, 혹은 불법복사)를 저지른 사용자에 대한 추적기법 등을 들 수 있다.

부정자 추적기법은 크게 2가지의 흐름으로 나누어 볼 수 있다. 처음으로 부정자 추적기법의 개념을 처음으로 소개한 B. Chor의 Pay-TV에 적합한 기법이고 [1], 다른 하나는 실제 응용분야에서 사용되는 기법이다. 결국 부정자 추적기법은 멀티미디어 컨텐츠의 저작권 보호에만 사용되는 것이 아니라, Digital Cash의 이중사용자(또는 부정행위자)에 대한 추적이라든지, Pay-TV를 부정으로 청취하는 사용자에 대한 추적, 키 복구시스템에서 결탁하여 부정통신을 하는 사용자에 대한 추적과 같은 요소기술의 하나로서 사용되고 있다.

본 논문의 목적은 이러한 부정자 추적기법의 흐름을 파악하고 요구되는 조건을 정의함으로써 향후의 응용분야에서 부정자 추적기법을 도입함에 있어서 보다 용이하게 하는데 있다.

본 논문의 구성은 다음과 같다. 2장에서는 부정자 추적기법의 개념에 대해서 설명하고, 3장에서는 최근 동향을 살펴봄으로써 부정자 추적기법에 필요한 요구사항을 정의한다. 4장에서는 실제 응용분야에서 제안된 기법을 사용한 프로토콜을 검토함으로써 요구사항의 타당성을 살펴본다. 마지막으로 5장에서는 결론으로 마무리한다.

본 연구는 2000년도 한국대학교육협의회 대학교수 국내교류 연구비 지원에 의한 것임

2. 부정자 추적기법

저작권 보호기법은 크게 디지털 워터마킹기법과

Fingerprinting기법의 2가지로 구분할 수 있다. 디지털 워터마킹기법은 어떤 컨텐츠에 워터마킹하는 기법으로 비가시성이나 공격에 대한 견고성등과 같은 일정한 조건을 만족하면서 컨텐츠 소유자(또는 제공자)의 신분을 확인할 수 있는 아이디 등을 삽입하는 것이다. 반면에 Fingerprinting기법은 컨텐츠에 소유자의 아이디 등을 삽입하는 대신에 구매자의 신분을 확인할 수 있는 것을 삽입함으로써 불법유통을 추적하는데 그 목적이 있다. 그림1은 저작권보호기법의 분류를 나타내고 있다. 부정자 추적기법은 그림에서 보는 바와 같이 Fingerprinting기법의 일종이지만, 구매자의 신분을 확인할 수 있는 아이디 대신에 구매(또는 거래) 당시에 사용된 키로서 부정자를 추출하는 기법이다.

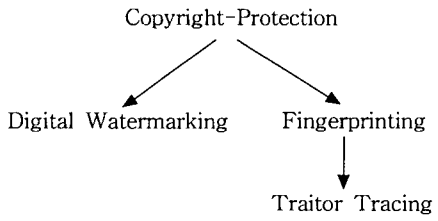

그림1. 저작권 보호기법의 분류

2.1.1 부정자 추적기법[1]

부정자 추적기법은 1994년 B. Chor et al.에 의해 처음으로 개념이 소개되었다. 이 절에서는 간략하게 부정자 추적기법의 개념을 살펴본다.

Pay-TV등에 적합한 부정자 추적기법으로 부정자라 함은 정당한 사용자들 중에서 임의의 k명이 결탁하여 Pirate decoder를 구성하여 허가되지 않은 사용자(비인가자)에게 넘겨주는 자들을 말한다. 여기에서 제안된 기법은 아래의 조건을 만족한다.

(1) k명 사용자의 결탁없이는 정당한 사용자를 부정자로 오인할 수 없다.

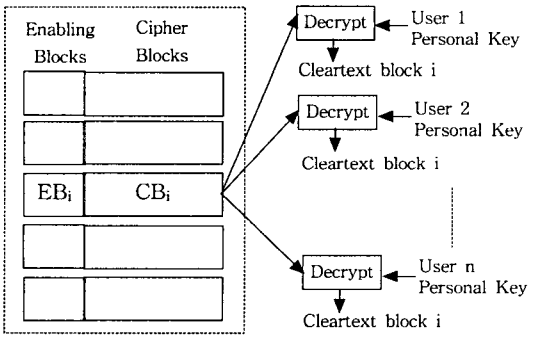

그림2. 부정자 추적기법의 개념도

(2) Pirate decoder가 복호할 수 있다면, Traitor tracing algorithm을 통해서 결탁한 사용자중 적어도 한 명을 정확하게 identify할 수 있다.

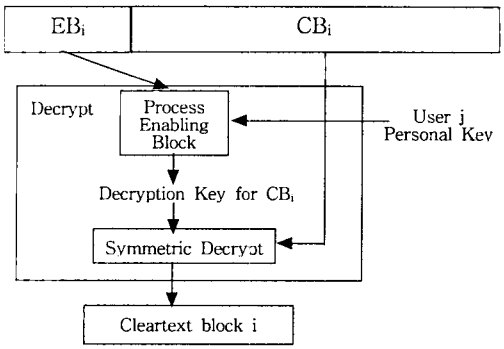

그림3. Decoding Box의 내부연산과정

[초기화]

n명의 사용자중에 k명의 부정자가 있다고 가정한다. 우선, 컨텐츠 제공자는 랜덤하게 해쉬함수들을 선택한다($h_1, \cdots, h_l$). 이 때, 각각의 해쉬함수 h_i는 $\{1, \cdots, n\}$을 $\{S_{i,1}, \cdots, S_{i,2k^2}\}$의 $2k^2$개의 독립적인 집합으로 매핑시킨다. 각 사용자에 대한 Personal Key는 l개의 키로 다음과 같이 구성된다.

$$\{h_1(u), \cdots, h_i(u), \cdots, h_l(u)\}$$

$$\begin{matrix} S_{1,1}, & \cdots & , S_{i,1}, & \cdots & , S_{l,1} \\ S_{1,2}, & \cdots & , S_{i,2}, & \cdots & , S_{l,2} \\ \vdots & & \vdots & & \vdots \\ S_{1,2k^2}, & \cdots & , S_{i,2k^2}, & \cdots, & S_{l,2k^2} \end{matrix}$$

[키 분배]

컨텐츠 제공자는 $\{S_{i,1}, \cdots, S_{i,2k^2}\}$에서 $2k^2$개의 키 각각에 대해서 키 s_i를 암호화한다(여기에서 s_i는 복호키 s를 l개로 분할한 것이다). 실제 데이터는 Final Key s에 의해서 암호화된다.

$$s = s_1 \oplus \cdots \oplus s_l \text{ (bitwise XOR)}$$

각각의 정당한 사용자는 $\{S_{i,1}, \cdots, S_{i,2k^2}\}$중에서 하나의 키를 가지고, 모든 s_i를 복호할 수 있으므로 s를 계산할 수 있다.

Enabling Block은 다음과 같이 구성된다.

$$\begin{matrix} Enc(s_1, S_{1,1}), & \cdots & , Enc(s_i, S_{i,1}), & \cdots & , Enc(s_l, S_{l,1}) \\ Enc(s_1, S_{1,2}), & \cdots & , Enc(s_i, S_{i,2}), & \cdots & , Enc(s_l, S_{l,2}) \\ \vdots & & \vdots & & \vdots \\ Enc(s_1, S_{1,2k^2}), & \cdots, & Enc(s_i, S_{i,2k^2}), & \cdots, & Enc(s_l, S_{l,2k^2}) \end{matrix}$$

[부정자 발견]

f_i는 Pirate Decoder에서의 키로 정의된다. 이 때, $f_i \in \{S_{i,1}, \cdots, S_{i,2k^2}\}$. 압수된 Pirate decoder의

블랙박스에서 $h_i^{-1}(f_i)$로 사용자를 identify할 수 있으므로 부정자를 추적(mark)할 수 있다(실제로 l/k 보다 많이 mark된 사용자가 부정자이다).

3. 부정자 추적기법의 요구사항

B. Chor[1]의 기법에서는 사용자 n의 수가 많아짐에 따라 배포되어야 하는 정보도 그만큼 증가하게 된다. 아울러 결탁하는 사용자의 수 k를 적게 하면 안정성이 떨어지게 된다. 그리고, 컨텐츠 제공자를 신뢰할 수 있다라는 가정을 두고 있기 때문에 악의를 가진 제공자에 의해서 정당한 사용자가 부정자로 오인받을 수 있는 여지가 있다. 그 이후로 Naor[2]는 임계치를 두어 어떤 decoder의 성공확률이 q보다 클 때 키의 소스를 추적할 수 있는 (k, n) threshold tracing schemes기법을 제안하였다. B. Pfitzmann[3]은 컨텐츠 제공자의 부정 행위를 방지하기 위해 Asymmetric Fingerprinting기법을 제안하였고, K. Kurosawa[4]는 효율적인 Asymmetric 기법을 제안하였다. 최근에는 컨텐츠 제공자 뿐만이 아니라 사용자의 부정행위를 막기 위한 기법, 디지털 워터마킹과 결합한 기법들이 제안되고 있다[5,6]. 본 장에서는 지금까지 제안된 부정자 추적기법을 바탕으로 요구사항을 새롭게 정의한다.

[요구사항1]

컨텐츠 자체에 부정복사가 행해져도 추적할 수 있는 기능이 필요하다(Fingerprinting과의 결합)

B. Chor에 의해 제안된 기법에서는 Pay-TV의 적용에 주안점을 두고 있으므로 복호된 컨텐츠의 부정 행위에 대해서는 다루고 있지 않다. 하지만, 전자상거래에 적용하기 위해서는 부정자 추적기법 이외에도 Fingerprinting과의 결합을 통해서 거래 이후의 부정 행위를 추적할 수 있어야 한다.

[요구사항2]

정당한 사용자를 부정자로 오인하는 경우가 없이 부정자를 정확하게 검출할 수 있어야 한다

부정자를 특정한다는 것은 결국 법정판결로 이어질 수 있으므로 부정자 검출이 정확해야 한다.

[요구사항3]

Piracy를 증명할 수 있는 명백한 증거를 확보할 수 있어야 한다

부정자 추적기법 자체가 거래 당시에 사용된 키로서 특정되기 때문에 거래에 사용되는 키의 안정성이 보장되어야 한다.

[요구사항4]

거래를 행하는 사용자나 컨텐츠 제공자의 입장에서 계산량이 적어야 한다

부정자 추적기법은 하나의 요소기술이기 때문에 컨텐츠 자체의 거래에 따른 계산량을 초과해서는 안 된다.

[요구사항5]

Data redundancy overhead(Cryptographic security parameter)와 Communication overhead가 적어야 한다

웹을 통한 거래가 활성화되고 있는 시점에서 통신량 뿐만 아니라 데이터의 오버헤드도 최소화 되어야 한다.

[요구사항6]

컨텐츠 제공자와 사용자 이외에도 중재기관(Arbiter)가 존재하여야 하며, 그 역할은 최소화되어야 한다

어떤 분쟁이 발생했을 시에 그 분쟁을 해결할 수 있는 제3자가 필요하며, 제3자가 컨텐츠 제공자나 사용자의 정보를 남용할 수 없어야 한다.

[요구사항7]

컨텐츠 제공자와 사용자 사이에는 상호인증이 필수적이다(인증서 도입)

Entity에 대한 인증만이 아니라 거래에 사용될 키에 대한 인증도 이루어져야 한다.

[요구사항8]

사용자의 프라이버시가 보호되어야 한다

제3자에 의해 분쟁이 해결되었을 때에도 사용자의 프라이버시(즉, 사용자의 비밀키에 대한 정보등)가 노출되지 않아야 한다.

4. 부정자 추적기법에 대한 고찰

부정자 추적기법은 크게 2가지 흐름으로 나누어 볼 수 있다. 하나는 B. Chor에 의해 제안된 기법을 기반으로 효율적인 측면이라든지, 안전성의 측면에서 다루는 것이고, 다른 하나는 응용분야에서의 부정자 추적기법이다.

Pay-TV에서는 초당 30프레임으로 보내어지는 데이터에 대해서 부정자를 특정하고 있지만, 실제 전자상거래의 경우에서는 한시적 거래가 주류를 이루고 있다. 한시적 거래에서 세션키를 이용하는 기법은 부적절하며 실제로 응용분야에서는 다른 기법을 도입하고 있다.

여기에서는 Digital Cash에서 사용되고 있는 이중사용자(부정 사용자)의 추적기법을 도입하여 디지털 서명으로 구현한 프로토콜[7]을 분석함으로써 부정자 추적기법에 대해서 고찰한다.

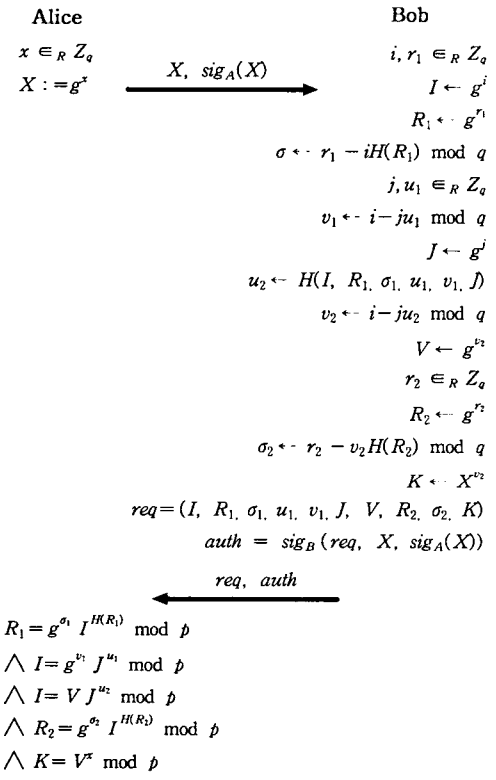

그림4. 부정자 추적 서명

이 프로토콜은 부정자를 특정하기 위해서 사용자의 비밀키를 증거로 사용하고 있으며, 상호인증과 동시에 프라이버시를 보호하기 위해서 Schnorr의 인증기법을 도입하고 있다. 동시에 중재기관의 역할은 최소화되면서 암호학적 안전성에 기반을 두고 있다.

그러나, 사용자(Bob)의 비밀키를 컨텐츠에 삽입하는 과정을 가정으로 두고 있다. 요구사항1을 만족하기 위해서 Black box로 구현하는 것은 한시적 거래에서 고비용이므로 Fingerprinting의 결합이 필요하겠다. 또한 다중 사용자의 결탁에 대해서는 고려하고 있지 않기 때문에 요구사항7에서 상호인증하기 위해 인증서를 활용하면서 보다 안전한 인증기법을 사용해야 할 것이다.

앞으로의 연구는 이러한 요구사항을 만족하면서 각 응용분야에 적합한 프로토콜의 개발이 필요하겠다.

5. 결론

부정자 추적기법은 앞에서 논한 바와 같이 2가지의 흐름으로 나눌 수 있다. 그러나, Pay-TV에 적합한 부정자 추적기법은 각 프레임마다 세션키를 삽입해야 하기 때문에 당연히 계산량이 커지게 되고, 한시적인 전자상거래에는 적합하지 않게 된다.

본 논문은 부정자 추적기법의 개념과 동향을 소개하고, 요구사항을 정의함으로써 앞으로 응용분야에 적합한 프로토콜의 개발에 도움이 되리라 본다.

[참고문헌]

[1] B. Chor, A. Fiat, M. Naor, "Tracing Traitors", in Proc. Advances in Cryptology-Crypto'94: Springer-Verlag, 1994, LNCS 839, pp.257-270

[2] M. Naor, B. Pinkas, "Threshold traitor tracing", in Workshop on Information Hiding, LNCS 1174, Cambridge, U.K., 1996, pp.49-64

[3] B. Pfitzmann, M. Waidner, "Asymmetric Fingerprinting for Larger Collusions", 4th ACM Conf. on Computer and Communications Security, 1997

[4] K. Kurosawa, Y. Desmedt, "Optimum Traitor Tracing and Asymmetric Schemes", in Proc. Advances in Cryptology-Eurocrypt'98

[5] K. Baba, H. Imai, "An Asymmetric Traceability Scheme without Agents", The 21st Symposium on Information Theory and Its Application(SITA98), 1998 (Japanese)

[6] S. Yamamoto, T. Horioka, T. Nakamura, Y. Takashima, "A Privacy Enhanced Content Distribution System with Blind Watermarking", The 2000 Symposium on Cryptography and Information Security(SCIS2000-C13), 2000 (Japanese)

[7] Y. Watanabe, Y. Zheng, H. Imai, "Traitor Traceable Signature Scheme", Proc. of ISIT2000