2002년 한국정보처리학회 춘계학술발표논문집 제 9 권 제 1 호

Active Networks 에서의 전자책 저작권 인증 시스템*

성순화*, 공은배**
*충남대학교 컴퓨터공학과
**충남대학교 컴퓨터공학과
e-mail : shsung@ce.cnu.ac.kr keb@ce.cnu.ac.kr

E-book copyright authentication system in Active Networks

Soon-Hwa Sung*, Eun-Bae Kong**
*Dept. of Computer Engineering, CHUNGNAM University
**Dept. of Computer Engineering, CHUNGNAM University

요 약

본 논문은 전자책 저작권과 소유권을 보호하기 위한 방법으로 워터마킹과 Proactive Pseudorandomness(PP) protocol 을 이용하여 secure multiparty 저작권 인증시스템을 제시한다. 그러므로 전자책 저자와 사용자와의 1 대 1 대응으로 제 3 의 인증기관없이 신속하고, 해킹에 능동적이며, 효율적인 인증시스템이 된다.

1.서론

웹브라우즈를 통한 디지털 정보의 유료화가 가속화 됨에 따라 전자책 저작권을 지속적으로 보장하고 관리하는 새로운 컴퓨팅 기술을 요구하고 있다. 이러한 새로운 컴퓨팅 기술이 안전한 통신으로써 여러가지 공격에 능동적이고 효율적으로 대처할 수 있는 방안이 절실하다.

그 방안으로 기존의 암호화 기법으로 전자책 저작권을 인증할 수 있는 방법보다 효과적인 워터마킹기법[1]과 능동적인 PP protocol[2]을 제시한다. 워터마킹기법에는 식별가능한(visible)것과 식별불가능한(invisible)것의 두가지가 있는데, 전자는 특별히 소유권에 대한 빠른 주장이 가능하며, 후자는 권리의 보호측면에서 강하게 입증할 수 있다는 특징을 지닌다. 따라서 본 논문은 전자책 저작권을 인증하기 위하여 식별불가능한 워터마크를 사용하여 전자책 저자의얼굴사진에 저자의 지문과 정보를 워터마크한다.

* 이 연구는 충남대학교 정보통신인력사업단의 RA 지원금에 의해 수행되었음

이때 워터마킹시의 비밀키는 안전한 형태로 유지되어야 한다. 워터마크 삽입알고리즘의 세부사항을 모두 알고 있는 공격자가 있을지라도 이 비밀키만 안전하게 보호된다면 워터마킹 특성에 의하여 안전한 전자책 저작권 보호를 할 수 있다. 그러므로 이 비밀키를 어떻게 하면 안전하게 보호할 수 있을지가 본 논문의 해결 방안이다. 따라서 전자책의 불법적 유통, 복제, 재생산, 조작, 분배가 됨으로써 발생하는 전자책 재산권 침해를 예방하고 탐지하는 저작권 인증방법으로 사용권한을 view, modify, copy, print, re-distribution 별로 나누어 전자책 저자와 분류별 서버와 상호대화로 인증할 수 있는 PP protocol 을 도입한다. 만약 제 3 자의 공격자로부터 비밀키가 해킹되면 reconstructible PP protocol[3]로 새로운 키가 생성되어 워터마킹시의 새로운 비밀키로서 저작자와 www server watermarking 사이의 상호대화로 저작권을 보호할 수 있다. 따라서 전자책 저작권을 모든 영역(view, modify, copy, print, re-distribution network)에서 지속적으로 보장할 수 있으며, 제 3 자의 공격으로 저작권의 침입을 받았을 때 이를 신속하고 능동적으로 해결할 수 있는 안전한 인증시스템을 구축할 수 있다. 본 논문의 구성은 2 장에서는

디지털 서명과 워터마크의 비교, 3장은 디지털 워터마킹, 4장에서는 Proactive Pseudorandomness(PP)protocol, 5장은 전자책 저작자와 www server watermarking 사이의 인증방법, 6장에서는 결론으로 맺는다.

2.디지털 서명과 워터마크의 비교

2.1 디지털 서명 기술의 현수준

디지털서명이란 메시지인증과 사용자인증기능을 합친 것으로 공개키 암호화기법과 일방향 해쉬함수(Oneway Hash Function)에 의한 요약추출물알고리즘(Message Digest Algorithm)을 결합하여, 일방향 해쉬함수[4]에 의한 요약추출물알고리즘을 통해 전자문서로부터 요약추출물을 생성한다. 그런후, 서명자의 개인키로 이 요약추출물을 암호화한 전자적 기록을 기존의 서명과 동일한 가치를 지닌 것으로 간주하는 것으로 암호화된 요약추출물이라는 전자적 기록을 의미하는 것에 불과하다. 다시 살펴보면 수신자가 서명자로부터 디지털서명이 첨부된 전자문서를 전달받아, 기밀성(confidentiality), 무결성(integrity)등을 확인하기 위하여는 서명자의 공개키를 획득할 수 있어야 하는데, 원칙적으로 그 획득방법에는 제한이 없다. 즉, 수신자는, 서명자로부터 서명자의 공개키를 건네받은 서명자의 지인을 통하여 디스켓에 담겨진 형태의 공개키를 전달받을 수도 있고, 서명자의 공개키가 컴퓨터통신의 게시판 또는 자료실에 올려진 경우라면, 이를 직접 다운로드받을 수도 있으며, 또한 1 대 1 통신을 통하여 서명자로부터 그의 공개키를 직접 전달받거나, 그가 운영하는 ftp 서버로부터도 다운로드받을 수 있는 것이다. 그러나, 어떠한 경우이든 서명자의 공개키가 서명자 자신의 것임이 객관적으로 보장되지 아니하는 상황에서는, 수신자가 서명자의 공개키를 이용하여 확인과정을 밟고, 무작정 그 결과를 믿는다는 것은 매우 위험한 일이 아닐 수 없다. 따라서 디지털서명은 직접적으로 자료의 내용에 신원을 결합시키지 않으므로 이용자의 신원과 자료를 결합시키기 위한 공유기밀에 있어서 그것들은 일부 다른 메커니즘과 결합시키는 방식으로 이용되지 않으면 안된다.

2.2 워터마킹의 장점

워터마킹은 콘텐츠의 의미를 변화하지 않고 어떤 코드를 삽입하여 멀티미디어 비트스트림을 수정한다. 삽입된 워터마크는 명백한 디지털 producer identification label(PIL)이나 명백한 규칙을 적용하여 일반화한 콘텐츠를 기반으로한 코드를 나타낸다. 압축되지 않은 멀티미디어 데이터의 완전한 증명을 위해 워터마크는 인증자가 편리하게 인증할 수 있는 데이터를 항상 모을 수 있다.

3. 디지털워터마킹 원리

디지털 워터마크란 디지털 콘텐츠에 사용자 ID(Identification)나 자신만의 정보를 넣음으로써 불법적인 복제를 막고, 데이터 소유자의 저작권과 소유권을 효율적으로 보호하기 위한 방법으로써 데이터에 일정한 암호를 숨겨서 부호화하는 과정으로 영상이나 음성 등의 신호에 특정한 코드나 패턴 등을 삽입하는 기술이다. 이때 워터마킹할 대상 안에 포함되며, 단지 파일 뒤에 첨가되는(append)것이 아니라 아예 파일의 내용안에 뒤섞이게 된다. 따라서 원래 파일 보다 크기가 늘어나지는 않는다[1]. 본인이 제시한 잉그마르 콕스의 워터마킹 방법은 워터마킹 시그널에 가중치 a 를 두고 w 에는 넣고자 하는 정보로 I' = I(1 + aw) 워터마킹을 수행하는 방법을 제시한다[5].

3.1 워터마킹 기법

디지털 워터마킹은 개념적으로 투명한 패턴으로 삽입된 이미지로서 워터마크 삽입알고리즘과 비밀키를 사용한다. 그 목적은 원 이미지에 대한 부가적인 정보를 이미지의 가시적인 수정없이 제공하여 파일 포맷의 변화와 같은 것이 필요 없이 음성적으로 날짜,시간, 일련번호 등을 워터마크로 남겨 이를 비교하여 인증하는 방법이다. 이미지에 정보가 가시적인 방법으로 삽입되거나 이미지 포맷과 유사한 헤더에 더해지는 방법은 쉽게 지워지거나 대체될 수 있다. 따라서 디지털 워터마크는 이미지에 지속적이고 견고한 방법으로 비가시적인 형태로 삽입되어야 한다. 그리고 워터마크의 중요한 특성은 데이터 왜곡에 대한 견고성이다. 이것은 워터마크가 일반적인 이미지 조작인 필터링,스케일링,노이즈 추가,크로핑 등을 받은 이미지로부터 읽을 수 있어야 한다. 또한 워터마크는 저작권 보호, 접근 조작에 대해 안전한 형태로 삽입되어야 한다. 이는 비밀키를 제외한 삽입알고리즘의 세부사항을 모두 알고 있는 공격자가 워터마크에 대한 공격을 하지 못하도록 해야 한다. 워터마크 알고리즘은 모든 멀티미디어 데이터에 적용이 가능하여야 하며, 내장된 워터마크가 제거되는 경우에는 반드시 화질의 저하가 이루어져 영상을 사용할 수 없게 함은 물론 재생된 워터마크는 원래의 워터마크와 동일한 코드를 가져야 한다[6].

3.2 전저책저자의 얼굴사진에 전자책저자의 지문 워터마킹

e-book service web site 에서 www server watermarking 사이의 시스템은 생략되거나 혹은 미흡한 것이 현실이고 만약 부분적으로 적용한다고 하더라도 PPP 접속자에 대한 일체의 적용이 어려운 것이 현실적이다. 그러므로 본 논문은 접속시에 전자책 저작자인증에 대하여 항시 추적하면서 알려주며, DB 화하는 시스템으로 가능한 많은 Hacking 으로부터 보호하며 저작권 보호를 할 수 있는 시스템으로써 이러한 상태를 통한 등록, 확인, 요청, 공급, 반납을 신속하게 웹상에서 처

리 할 수 있는 인증시스템을 제시한다. 그러므로 제안한 이미지 삽입방법으로 잉그마르 콕스의 워터마킹 방법 I' = I(1 + aw)에 따라 a는 시그널 가중치로써 저작자의 지문을, w 는 넣고자하는 정보로써 제품의 일련번호와 저자의 신상정보 및 워터마크의 시각 날짜 등을 삽입한다.

4. Proactive Pseudorandomness(PP) protocol

3.1 에서 워터마킹한 전자책저자얼굴사진은 PP protocol에 의해 전자책 service web site와 www server watermarking 사이에서 전자책저작권으로 인증된다. 여기서 도입된 PP protocol에 대하여 알아본다.

암호는 외부의 악의있는 entities 에 대해 상호작용하는 parties 를 보호하는 것으로 insecure channels, authentication of parties, unforgetable siganatures, and general multiparty secure computation 에 대해 private communication 을 가능케 한다. 만약 상대방이 protocol 을 제어할 수 있다면 복구할 방법과 security 를 다시 얻는 것이 불가능하다. 따라서 안전한 proactive pseudorandomness(PP) protocol scheme 을 살펴보기로 한다. Parties 들은 계산의 시작에서만 randomness 를 사용하고, 한번 상호작용을 시작하면 더해진 randomness 는 무효하다. 이 scheme 은 각 round 에서 그전 round 에서 오류가 발생한 party 일지라도 상대방이 예측할 수 없는 fresh pseudorandom number 를 각 party 에 공급한다. 이러한 pseudorandom numbers 는 security 를 다시 얻는 fresh random numbers 로 party 를 복구하는데 사용될 수 있다. The parties 의 initial inputs 이 임의로 선택된다면 각 round 의 각 party 내에 generated value 은 모든 round 에서 모든 다른 paties 내에서 generate 될지라도 상대방의 random 과 구별할 수 없다. 이러한 protocol 을 Proactive pseudorandomness(PP) protocol 이라고 한다. 이러한 PP protocol 은 다음과 같은 조건을 만족해야만 한다. 상대방은 probabilistic polynominal time 에 제한되어 있고, 각 round 계산에서 적어도 한 개의 secure party 가 있어야 한다. secure party 는 round 에서 오류를 일으키지 않으며, 그전 round 에서 secure 했던 party 와 secure channel 을 가지고 이 channel 은 이 round 동안만 secure 해야만 한다[2][3].

5. 전자책 service web site 와 www server watermarking 사이의 인증방법

PP protocol 은 잉그마르 콕스의 워터마킹 방법으로 워터마킹한 전자책저작자의 얼굴사진이 있는 www server watermarking 과 전자책 service web site 를 연결한다. 이때 워터마킹시의 저작자의 비밀키를 안전하게 보호하는 방법으로 PP protocol 을 적용한다. 워터마킹 삽입 알고리즘의 세부사항을 알고 있는 공격자가 워터마크에 대한 공격을 하지 못하도록 하는 유일한 방법은 워터마킹시 비밀키를 안전하게 보호하는 방법이다. 따라서 전자책 저작자가 view 영역에서 저작자의 인증방법은 저작자의 비밀키로 저자얼굴사진에 지문과 정보(제품일련번호, 저자의 신상정보 및 워터마킹의 시각 날짜등)를 워터마킹한다. 이를 copy 영역에서 인증할 때는 view 영역에서의 비밀키를 입력으로한 PP protocol 의 출력을 비밀키로 한다. 이때 비밀키는 상호대화로 www server watermarking 으로 보내진다. 같은 방법으로 print, modify, re-distribution 분류별로 PP protocol 을 적용하여 인증한다. 만약 제 3 자의 공격으로 저작권의 침입을 받았을 때 reconstructible PP protocol 로 새로운 키를 생성한다. 이 새로운 키는 www server watermarking 에서 저자의 새로운 비밀키로 셋팅된다.

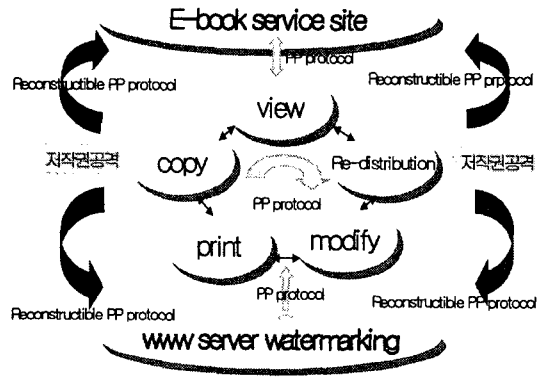

그림 1 능동적인 전자책저작권 인증시스템

이렇게 함으로써 PP protocol 은 전자책 service web site(client)와 www server watermarking(server)의 상호대화로 신속하고 능동적인 저작권 인증을 할 수 있다. 그리고 저작권을 view, copy, print, modify, re-distribution 용도별로 secure multiparty 저작권으로 인증할 수 있으므로 지속적인 저작권 인증과 전자책의 부적절한 사용에 대한 추적도 가능하다. 따라서 제시한 시스템은 제 3 자의 거짓 저작권 인증에 대하여 항상 추적하면서 hacking 으로부터 보호하며 전자책 저작권을 인증할 수 있다.

6. 결론

디지털 정보시대는 디지털 정보의 유료화에 따른 디지털 정보의 저작권 보호에 관심을 모으고 있다. 이에 따라 전자책 시장의 저작권을 보호하기 위한 방법이 가속화되고 있다. 따라서 현재의 전자책 인증방법의 단점을 보안할 수 있는 워터마크를 사용함과 동시에 저작권의 공격에 능동적으로 대처하는 PP protocol 을 사용함으로써 전자책의 사용 용도별 view, copy, print, modify, re-distribution 인 모든 network 에서 중앙집권적인 인증기관없이 전자책저자와 사용자가 1 대 1 대응으로 직접 인증할 수 있다. 뿐만 아니라 저작권의 공격이 있을 경우 스스로 능동적으로 대처를 할 수 있는 인증시스템이 된다. 따라서 중앙인증기관에

투자하는 비용을 줄일 수 있으며, 저작권의 공격에 신속하고 능동적으로 대처하는 효율적인인증시스템을 구축할 수 있다. 그리고 전자책의 영역별(view, copy, print, modify, re-distribution)로 저작권을 인증하지 않으므로 저작권 인증시스템의 traffic 을 줄일 수 있다. 따라서 저작권 공격에 스스로 능동적이고 효율적인 네트워크를 구축할 수 있으며, 제시한 방법을 생체정보형 IC(Intergrated Circuit)카드에 적용하여 안전한 사용자 인증(passport, 주민등록증 등), 국가간 이동의 비자 기능, 쇼핑몰의 안전한 회원인증 등에서도 이용할 수 있다.

그러나 제시한 전자책 저작권 인증시스템은 서버와 클라이언트 입장에서 인증만을 다루었다. 이를 확장하여 peer 와 peer 사이의 secure group system 일 때, 인증방안을 연구할 필요가 있다.

참고문헌

[1]R.B.Wolfgang and E.J.Delp, "A Watermark for Digital Images", IEEE International Conf. on Image Proccessing, Laussane, Switzerland, Oct 1996

[2]Ran Canetti, "Studies in Secure Multiparty Computation and Application", Thesis for the degree of Dr, pp. 131-134, 1996

[3]Ran Canetti, "Studies in Secure Multiparty Computation and Application", Thesis for the degree of Dr, pp. 12-15, 1996

[4]Alfred J. Menezes, Paul C.Van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", pp.327-331, 1997

[5]J.J.K. O'Ruanaidh, W.J.Dowling, and F.M. Boland, "Watermarking Digital Images for Copyright Protection", IEEE 1995

[6]R.G. Van Schyndel, A.Z. Trikel, and C.F. Osborne,"A Digital Watermark", IEEE International Conf. on Image Processing, Austin, Texas, Nov 1994