2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

워터마킹 기술의 평가 기준에 관한 연구

임양규*, 국상진*, 전종민**, 원동호*
*성균관대학교 전기전자 및 컴퓨터 공학과
**(주) BCQRE
e-mail : yklim@dosan.skku.ac.kr

A Study on the Evaluation Criteria of Watermarking

Yang-Kyu Lim*, Sang-Jin Kook*, Jong-Min Jeon**, Dong-Ho Won*
*School of Electrical&Computer Eng., Sungkyunkwan University
**BCQRE Co., Ltd,.

요약

인터넷의 발달로 디지털화된 멀티미디어 데이터가 유통되기 시작하면서 저작권 보호에 대한 문제가 발생하였다. 저작권 보호를 위한 기술적인 대책으로 암호를 이용한 기법과 디지털 워터마킹 기술이 있다. 본 논문에서는 디지털 워터마킹 기술의 평가기준을 저작권 보호 제공 측면과 인증 및 무결성 제공 측면으로 분류하여 강인성, 안전성 및 효율성을 고려해서 도출하였다.

1. 서론

최근 인터넷, 전자출판 등 디지털 기술의 발전으로 문서, 음성, 사진, 비디오 데이터 등의 다양한 매체들이 디지털화 됨에 따라 인터넷과 통신망을 이용한 멀티미디어 데이터의 수요는 폭발적으로 증가하고 있다. 그러나, 이러한 디지털 데이터는 품질의 손상 없이 복제가 가능하기 때문에 디지털 데이터의 무단 복제 및 배포가 확산되고 있고, 이에 따라 저작권 및 소유권 보호에 대한 문제가 대두되고 있다.

이러한 추세에 따라, 멀티미디어 데이터의 전자상거래를 위해서 디지털 데이터에 대한 소유권 및 지적 재산권을 보호할 수 있는 방법이 요구되고 있으며, 이에 대한 해결책으로 암호기술을 이용한 방법과 디지털 워터마킹 기술이 제시되었다. 디지털 워터마킹 기술은 오디오, 이미지, 비디오 등의 다양한 매체에 대하여 강인성, 효율성, 기능성 등 여러 가지 측면을 고려해서 설계해야 한다.

단기간동안 많은 관심을 받아온 기술의 특성상 다양한 분야에서 제안된 많은 기술들이 존재하는 반면 기술의 안전성 및 평가에 관한 연구는 상대적으로 부족하기 때문에, 제안된 기술들에 대한 정형화된 평가가 어려운 실정이다.

본 논문에서는 저작권 보호기술 중의 하나로 주목받고 있는 워터마킹 기술을 강인성을 제공하는 robust watermarking과 인증 및 무결성을 제공하는 fragile watermarking 두 가지로 분류하여 워터마킹에 대한 평가 기준을 도출하였다.

논문의 구성은 다음과 같다. 2장에서는 디지털 데이터의 저작권 보호를 위한 기술적인 접근방법인 암호화 기법과 디지털 워터마킹에 관해서 개략적으로 살펴보고, 3장에서는 강인성, 안정성 및 효율성을 고려한 워터마킹의 평가기준을 제시하였으며, 4장에서 결론을 맺는다.

2. 저작권 보호기술

디지털 형태의 데이터가 네트워크 환경에서 전자적으로 거래됨에 따라 불법복제로 인한 저작권 침해 문제가 심각하게 대두되고 있다. 이를 해결하기 위한 여러 가지 기술적인 방안들이 제시되고 있는데, 가장 널리 사용되어온 암호화를 이용한 방법 외에도 최근, 디지털 워터마킹 기술이 저작권 보호를 위한 강력한 기술적 대안으로 떠오르고 있다. 그러나, 각각의 기술들은 아직까지 완벽한 저작권 보호를 제공하지 못하고 나름대로의 특징 및 장·단점들을 갖고

있다. 본 장에서는 저작권을 보호기술인 암호화 기법 및 워터마킹에 대해서 간략히 기술한다.

2.1 암호화 기법

암호기술을 이용하는 방법은 데이터를 항상 암호화된 형태로 유지하여 복호화 키를 가지고 있는 경우에만 컨텐츠를 사용할 수 있도록 함으로써, 저작권자에게 컨텐츠에 관한 사용권을 부여받은 후 복호화 키에 접근할 수 있도록 하는 방법이다. 이때, 복호화 키와 복호화된 컨텐츠는 사용자가 직접 접근할 수 없도록 관리하여야 하며, 복호화 키에 접근하는 별도의 인증메커니즘이 시스템의 매우 중요한 요소가 된다. 따라서, 컨텐츠를 사용하는데 필요한 특정 소프트웨어 혹은 하드웨어의 내부동작을 사용자가 분석하여 직접 조작할 수 없도록 하는 TRM (Tamper Resistance Module)기술은 암호화를 위한 저작권 보호를 위해 요구되는 중요한 요소이다. 그러나, 암호화를 이용한 저작권 보호는 적법한 사용자가 컨텐츠를 사용하기 위해서는 반드시 복호화 되어야 하며, 이때 복호화된 데이터 또는 복호화 키에 대한 접근을 막아야 한다는 문제점을 가지고 있다.

이밖에도 암호화를 이용한 저작권 보호기술로, 방송환경에서 암호화 기술을 이용하여 불법 디코더의 출처를 추적하는 tracing traitor기술 등이 있다[1].

2.2 디지털 워터마킹

저작권 보호문제를 해결할 수 있는 기술적인 접근은 아직 뚜렷한 해결방법이 마련되어 있지 않은 가운데, 디지털 워터마킹 기술이 문제해결의 실마리를 제공하게 되었다. 디지털 워터마킹과 관련된 연구는 해마다 매우 급격하게 증가하고 있다[2].

디지털 워터마킹은 컨텐츠로부터 분리할 수 없는 특정마크(저작권 정보 또는 구매자 정보)를 삽입하는 기술로서, 저작권 정보를 마크의 형태로서 삽입하게 된다. 따라서, 워터마킹 기술의 관건은 마크를 컨텐츠로부터 분리할 수 없도록 하는 강인성이며, 워터마킹시스템의 안전성과 관련된 가장 중요한 요소이다. 이외에도 마크 삽입전과 마크 삽입후의 데이터를 감각적으로 구별 불가능해야하는 비가시성, 저작권 정보 및 데이터 식별 정보를 표현할 수 있는 충분한 크기의 마크가 삽입될 수 있도록 하는 삽입 용량 등이 중요 요소이다.

또한, 워터마킹된 데이터는 소유권 증거의 기능뿐 아니라 전자상거래의 컨텐츠 거래 모델에서 재분배자를 식별할 수 있는 핑거프린팅 기능에 사용될 수 있다.

워터마킹 기술은 복사를 사전에 방지하는 것이 아니라, 불법복제가 발생했을 경우, 이를 검출 및 추적할 수 있는 기능을 제공하는 사후 검출 기술이라는 특징을 갖고있다. 그러나, 아직은 신뢰할 수 있는 강인성을 제공하는 기술적 수준에 이르지 못하였다는 안전성의 문제점도 갖고 있다.

3. 평가기준 도출

본 장에서는 저작권 보호 기능을 갖는 디지털 워터마킹 시스템을 평가하기 위한 기준을 도출하였다. 워터마킹 시스템의 요구사항에 대한 만족여부를 중심으로 시스템의 신뢰성, 효율성 등 시스템을 평가할 수 있는 다양한 측면들을 고려하여 워터마킹이 제공해 주는 기능을 저작권 보호 기능과 인증 및 무결성 검증 기능으로 분류하여 도출하였다.

3.1 저작권 보호를 위한 워터마킹 평가 기준

저작권 보호를 위한 워터마킹의 평가기준을 강인성, 안전성 등 다양한 기준으로 도출하였다[3],[4],[5],[6],[7],[8]. 또한, 오디오 및 비디오만이 갖는 시간성도 고려해서 도출하였다.

[평가 기준 1] Indistinguishability
- 워터마크 삽입 전의 컨텐츠와 삽입 후의 컨텐츠를 인간의 시각 및 청각으로 구별할 수 없어야 한다.

[평가 기준 2] Robustness
- 신호처리 변형 공격을 받았을 경우에도 컨텐츠에 삽입되어 있는 워터마크를 검출할 수 있어야 하며, 허가되지 않은 압축을 정확하게 검출할 수 있어야 한다.

[평가 기준 3] Malicious Attacks
- 워터마크 알고리즘은 악의적인 공격에 대하여 견딜 수 있어야 하며, 평가 방법은 워터마킹 알고리즘의 공개여부 및 공격을 가하는 집단을 기준으로 수행할 수 있다.

[평가 기준 4] Reliability
· 워터마크의 탐지에 있어서 completeness와 soundness를 만족해야 한다. 워터마크의 탐지 에러율을 측정할 때에는 다양한 미디어 및 형식으로 된 샘플을 가지고 측정한 평균 성능으로 한다.

[평가 기준 4-1] Completeness (완전성)
· 워터마크가 삽입된 컨텐츠에 대한 검출 에러율이 10^{-12}보다 작게 나타나야 한다.

[평가 기준 4-2] Soundness (건전성)
· 워터마크가 삽입되지 않은 컨텐츠는 검출 에러율이 10^{-2}보다 작게 나타나야 한다.

[평가 기준 5] Renewability
· 공격으로 인해 워터마크가 손상을 당했을 때에도 복구할 수 있는 적당한 방법을 제공해야 한다.

[평가 기준 6] Efficiency of Operation
· 워터마크의 삽입 및 검출에 걸리는 시간과 관련된 평가기준으로, 워터마크 삽입 및 탐지 시스템은 다양한 플랫폼, 기기, 통신 환경 등을 지원해야 하며, 적당한 효율성을 제공하여야 한다.

[평가 기준 7] Effect on Ability to Compress
· 제안된 기술로 워터마킹된 컨텐츠를 표준 압축 알고리즘으로 압축하였을 경우에 압축율에 영향을 미치지 않아야 한다.

[평가 기준 8] Wide Spread thorough the Content
· 워터마크는 음악파일 및 비디오의 전체에 고루 분포해야한다. 일반적으로 15초 분량을 잘라냈을 때 워터마크가 검출 가능해야 한다.

[평가 기준 9] Capacity
· 데이터에 관한 정보, 소유자 등 저작권에 관한 충분한 양의 정보가 삽입될 수 있어야 하며, 이때 지원되는 삽입 용량 내에서 이루어지는 워터마크의 삽입은 컨텐츠의 품질이 훼손되지 않는 범위 내에서 이루어져야 한다.

[평가 기준 10] Size and nature of contents
· 워터마킹 알고리즘은 워터마크를 삽입하고자하는 컨텐츠의 성질에 독립적이어야 한다. 또한, 데이터의 크기에 관계없이 일정 비트 이상의 워터마크 삽입이 가능해야 한다. 이때, 삽입 가능한 컨텐츠의 최소크기는 미리 정의되어야 한다.

[평가 기준 11] Secure key
· 삽입 및 검출에 사용되는 키는 전수공격으로 찾아낼 수 없도록 충분히 큰 공간에서 적절한 크기로 선택되어야 한다.

[평가 기준 12] Security should be dependent on secret key
· 워터마킹 방식의 안전성은 알고리즘에 의존하지 않고 반드시 키에 의존해야 한다. 즉, 알고리즘이 공개되어도 시스템의 안전성에는 아무런 영향을 미치지 않아야 한다.

[평가 기준 13] Digital domain detection
· 디지털 영역에서 워터마크된 데이터의 삽입 및 검출 연산이 가능해야 한다.

3.2 인증 및 무결성 제공을 위한 워터마킹 평가기준

컨텐츠의 인증 및 무결성 기능은 약간의 변형에도 쉽게 깨지는 fragile 워터마킹으로 제공될 수 있다. 공개키 방식을 이용함으로써 인증기능을 제공할 수 있으며, 워터마크가 깨진 위치로부터 컨텐츠 변형 위치 탐지기능도 제공할 수 있다. 다음은 fragile 워터마킹 시스템에 대한 평가 기준이다[1] [8],[9].

[평가 기준 1] Detect tampering
· Fragile 워터마킹시스템은 마크가 삽입된 컨텐츠에 어떠한 변경이 일어났는지를 검출 해낼 수 있어야 한다. 이 기준은 fragile 워터마크의 가장 기본적인 성질이다.

[평가 기준 2] Perceptual Transparency
· 삽입된 워터마크는 감각적으로 인지할 수 없어야 하며 컨텐츠의 기능성을 방해하지 말아야 한다.

[평가 기준 3] Don't require original image
· 원본 이미지가 존재하지 않거나, 검출 과정에서 원본이 노출될 우려가 있기 때문에, 원본 없이 워터마크 추출이 가능해야 한다.

1) [평가기준4], [평가기준5], [평가기준6], [평가기준7]은 robust watermarking에도 적용될 수 있다.

[평가 기준 4] Key space
- 삽입 및 검출에 사용되는 키는 전수공격으로 찾아낼 수 없도록 충분히 큰 공간에서 적절한 크기로 선택되어야 한다.

[평가 기준 5] Impossible to deduce marking key
- 검출된 정보로부터 마킹한 키를 추론하는 것이 불가능해야 한다.

[평가 기준 6] Insertion difficulty
- 마킹된 컨텐츠에서 워터마크를 제거하는 것과 제거하여 얻은 워터마크를 다른 이미지에 삽입하는 것은 어려워야 한다.

[평가 기준 7] Embedding in compressed domain
- 압축된 영역에 마크를 삽입 할 수 있어야 한다는 기준으로, 다양한 응용프로그램 등에 사용되어 보관 및 전송 시에 장점을 가질 수 있다.

[표 1]은 도출한 평가기준을 기능별 요구사항으로 정리한 것이다.

[표 1] 기능별/요구사항 분류

	저작권 보호	인증 및 무결성
비가시성	[평가기준1]	[평가기준2]
강인성	[평가기준2], [평가기준3], [평가기준5], [평가기준9]	[평가기준1], [평가기준6]
안전성	[평가기준4], [평가기준8], [평가기준11], [평가기준12]	[평가기준3], [평가기준4], [평가기준5]
효율성	[평가기준6], [평가기준7], [평가기준10], [평가기준13]	[평가기준7]

4. 결론

인터넷을 통한 디지털 데이터의 유통 및 공유는 심각한 저작권 문제를 야기하였다. 본 논문에서는 이를 해결하기 위한 기술적 방안인 디지털 워터마킹의 평가기준에 대해서 저작권 보호기능과 인증 및 무결성 제공의 두 가지 기능성을 고려해서 도출하였다.

도출된 기준은 오디오 및 이미지 워터마킹 제품 개발시에 유용하게 활용될 수 있을 것이다.

참고문헌

[1] Chor, B., A. Fiat, and M. Naor, "Tracing Traitors," in Advances in Cryptology, Proceeding of CRYPTO '94, vol. 839 of LNCS, Springer-Verlag, pp. 257-270, 1994

[2] Ross J. Anderson, "Information Hiding - A Survey," in Proceedings of the IEEE, special issue on protection of multimedia content, May 1999, Invited paper.

[3] http://www.SDMI.org

[4] L. Boney, A. H. Tewfik, K. N. Hamdy, "Digital Watermarks for Audio Signals," in International Conference on Multimedia[4] Computing and Systems, Hiroshima, Japan, 17 23 June 1996, IEEE, pp. 473 480.

[5] J. Zhao, E. Koch, " A Digital Watermarking System for Multimedia Copyright Protection," in Fourth ACM International Multimedia Conference, Boston, Massachussetts, 18 22 Nov. 1996, pp. 443 444, ACM.

[6] Petitcolas, F. A. P., R.J. Anderson, and M. G. Kuhn, "Information Hiding - A Survey," Proceedings of the IEEE, vol. 87, no. 7, 1999m pp. 1062-1078.

[7] Kutter, M., and F. A. P. Petitcolas, "Fair Benchmarking for Image Watermarking Systems," in Proceedings of the SPIE 3657, Security and Watermarking of Multimedia Contents, 1999, pp. 226-239.

[8] Petitcolas, F. A. P., R. J. Anderson, "Evaluation of copyright marking systems," in IEEE Multimedia Systems, Florence, Italy, 7-11 Jun. 1999.

[9] E. T. Lin and E. J. Delp, "A Review of Fragile Image Watermarks," Proceedings of the Multimedia and Security Workshop (ACM Multimedia '99) Multimedia Contents, October 1999, Orlando, pp. 25-29