디지털 워터마크를 이용한 Semi-fingerprinting[1]

이한호° 이정수 김종원
㈜마크애니 연구소
{sslh2°, jwkim}@markany.com

Semi-fingerprinting System using The Digital Watermark

Hanho Lee° Jung Soo Lee Jong Weon Kim
MarkAny Research Institute

요 약

본 논문에서는 대역확산방식을 응용한 새로운 워터마킹 방법에 대해서 설명하고, 이를 이용하여 semi-fingerprinting을 구현할 수 있는 데이터 구조에 대해서 기술하였다. 본 논문은 저작권 보호에 주초점이 맞추어져 있는 워터마크 기술을 실질적으로 필요한 fingerprinting분야에 적용함으로써, 그 동안 학문연구에 그치고 있었던 워터마크 기술을 산업적 응용에까지 확대시키는데 큰 기여를 할 것으로 기대된다. 본 논문에서 제안한 워터마킹 방법은 난수이동(random number shift)방법을 이용하여 데이터 삽입량을 증가시켰다. 또한, semi-fingerprinting에 적용하기 위해 일본 내에서 진행중인 cIDf의 지침에 기반 하여 워터마크를 구성하였다.

1. 서론

최근 들어 유무선 디지털 콘텐츠 제공 업체들이 사용자들의 불법적인 콘텐츠 재배포와 관련하여 대책마련에 고심하고 있다. 디지털 콘텐츠는 serial number나 hard-lock을 사용하여 복사나 재배포 방지를 할 수 있는 컴퓨터 소프트웨어나 하드웨어와 달리 보호장치가 매우 미비하며, 기술적용도 매우 어렵다.

디지털 콘텐츠의 저작권 보호와 재배포 방지를 위해서 관심 있게 연구되고 있는 분야가 워터마킹과 암호화 기술이다. 암호화 기술은 이미 표준화가 진행되고 표준도 지정되었지만, 워터마킹 분야는 일부의 표준화 움직임[1][2]에도 불구하고, 표준이 채택되지 못했다. 워터마킹 기술이 아직까지 암호화기술만큼 인증 받지 못한 기술이지만, 높은 활용성 때문에 많은 사람들이 관심을 가지고 연구하는 분야이다. 그 활용분야[3]는 방송 모니터링, 소유자 정보 표시, 소유권자 증명, 인증, Fingerprint, 복사제어, 비밀정보전달등이 있다. 워터마크는 다양한 공격에 강인해 하지만, 특히 기하학적 변형에 강인해야 한다. 기하학적 변형에 강인한 워터마킹 방법은 기하학적 변형에 영향을 받지 않게 워터마크를 구성하는 방법[6,7,8]과 변형된 수치를 찾아내서 추출하는 방법[9,10]으로 구분할 수 있다.

Fingerprint는 워터마킹 기술응용의 한 분야이기는 하지만, 일반적인 워터마킹의 요구조건들보다 강인성과 데이터 삽입량에서 요구조건이 더욱 까다롭다. 워터마크는 일명 Key방식이라고 지칭하는 1bit워터마크로도 저작권 보호가 가능할 정도로 데이터 삽입량이 많이 요구되지 않는다. 그러나 fingerprint는 저작권자에서 중간 배포자 그리고 최종 소비자까지의 정보를 단계적으로 삽입하여야 한다. Fingerprint는 많은 데이터 삽입량이 요구되며, 특히 서로 다른 정보로 워터마킹 된 영상을 이용하여 평균을 취하는 평균공격과 여러 개로 쪼개서 붙이는 모자익공격에 매우 치명적이다(공모공격). 이 같은 공격에 강인하게 하기 위한 방법으로, 영상을 여러 영역으로 구분하여 거래가 발생할 때 마다 그 영역에 추가적으로 워터마크를 삽입하는 방법[11]과 특별한 주파수 대역 필터를 사용하여 정보를 삽입하는 방법[12], 그리고 Jpeg압축에 강인하게 하기 위해서 Jpeg의 Quality factor를 이용한 방법[4]등이 있다. 현재까지 연구된 fingerprint방법들은 아직까지 충돌공격에 대한 구체적인 대안을 제시하지 못하거나, 또는 원본의 필요성이 요구되는 등 많은 문제점을 가지고 있다.

앞의 내용을 정리해보면, fingerprint에는 높은 신뢰성, 낮은 프로세스, 견고성, 투명성, 부분보호 같은 필수항목들[5]이 추가되고 강화되어야 한다.

2. Semi-fingerprinting삽입 추출 방법 및 데이터 구조

본 논문에서는 정보 60bits와 CRC코드 20bits로 총 80bits의 정보가 삽입된다. 본 논문에서는 대역확산 방식을 사용하여 강인성을 유지함과 동시에, 워터마크 구성시 난수이동방법[6,13]을 응용한 새로운 정보 표시방법을 연구하였다.

2.1 멀티비트 삽입방법

Joseph[6]은 난수를 이동시켜서 이동된 난수간의 거리를 측정하여 정보를 표현하였다. 본 논문에서는 Joseph의 논문을 응용하여 더 효율적인 정보표시 방법을 고안하였다. 그림 1과 같이 원본 영상을 여러 개의 워터마크 블록으로 나눈다. 여기서 워터마크 블록이란 cropping이 발생했을 경우 최소한 하나의 워터마

[1] 본 논문은 NRL과제번호 2000N-NL-01-C-286에 의해서 지원되었습니다.

크 블록이 살아 남게 하기 위해 구성한 것으로, 삽입하고자 하는 정보가 삽입되는 단위 블록이다

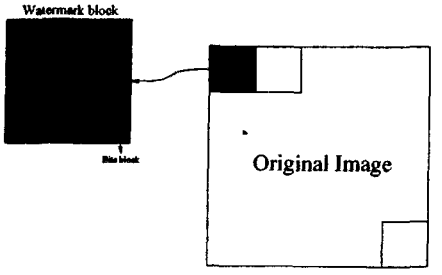

그림 1 정보를 삽입하기 위한 워터마크 블록과 비트블록

워터마크 블록은 여러 개의 비트블록으로 나뉜다. 비트블록은 실질적으로, 정보를 표현하기위해서 나뉘어지는 영역이다. 본 논문에서는 난수를 이동시킨 후, cross-correlation에 의해서 발생하는 최고 Peak의 위치를 표현하고자 하는 정보의 비트블록에서 발생하게 만든다. 다시 말해, 난수의 시작 위치를 원하는 비트블록으로 이동시킨다는 것이다. 그럼 이것을 사용하여 어떻게 정보를 표현할 수 있는지에 대해서 설명한다. 예를 들어, 워터마크 블록이 32×32 개의 비트블록으로 나뉘었다고 가정하자. 그럼 비트 블록의 개수는 총 1024개이다. 이것을 비트 정보로 변환하면, 2^{10} 으로 10bits가 된다. 이것을 식으로 표현하면 $N=2^x$ 이 되고, 여기서, N은 비트블록의 개수이고, x 는 삽입 가능한 비트수가 된다. 앞의 예제의 경우, 하나의 워터마크 블록에 삽입할 수 있는 정보의 양은 10bits가 되는 것이다. 또한, 만약 삽입하고자 하는 정보가 이진수 ' 1000000000' 이라면, 이것은 십진수로 ' 512' 가 되므로, 513번째(왜냐하면, 10bits가 표현할 수 있는 십진수의 범위는 0~1023이기 때문)비트블록에서 최고 Peak가 발생하게 난수를 이동시키면, ' 1000000000' 정보가 표현되는 것이다. 이제까지의 설명은 하나의 난수를 사용하였을 경우이다. 여러 개의 난수를 사용한다면 표현할 수 있는 정보량은 <식 1>과 같이 기하급수적으로 증가된다.

$$N_1\times N_2\times\cdots\times N_m=2^{x_1+x_2+\cdots+x_m} \quad \text{<식 1>}$$

따라서, 본 논문에서 삽입하고자 하는 80bits를 삽입하기 위해서는 1024개의 비트블록과 8개의 난수가 필요하다. 이상에서 확인할 수 있듯이, 정보 삽입량은 비트블록과 난수의 개수에 따라서 결정된다. 여기서, 사용되는 난수들은 서로 상관성이 없어야 하기 때문에, 의사난수를 사용하였다. 워터마크 블록의 크기는 128×128 로 설정하였으며, 비트블록의 크기는 4×4 로 결정하여, 하나의 워터마크 블록이 $32\times32=1024$ bits를 표현할 수 있게 구성하여 실험하였다.

비트블록의 크기는 특히, 크기변환공격(resizing)과 밀접한 관계를 가진다. 크기변환공격이 가해진 후에, 워터마크된 영상을 원래의 크기로 정확히 복원해낸다 하더라도 최고 Peak의 위치는 약간의 오차가 발생할 수 있다. 비트블록의 크기는 결국 최종적으로 추출되는 비트정보에 어느 정도의 오차 범위를 줄 것인가를 결정하는 요소가 된다. 그러나 이것을 크게 한다면 삽입할 수 있는 정보의 양이 줄어들게 되고, 만약 너무 작게 한다면 작은 공격에도 잘못된 정보를 추출하게 만들 수도 있다.

현재까지 설명된 정보 표현방법은 동기(Synchronization)가 맞았다는 전제 하에 정보를 추출한 것이다. 만약 cropping이 발생한다면 정보를 정확히 추출해 내기 힘들기 때문에, 추가적으로 동기를 맞추기 위한 의사난수를 삽입하게 된다. 지금까지의 내용을 정리해 보면, 의사난수의 개수는 80bits의 정보를 삽입하기 위한 8개 와 동기신호까지 총 9개가 필요하다. 이 과정은 <식 2>와 같이 나타낼 수 있다.

$$W=\frac{(\sum_{k=1}^{k=n}RN_k+SW)}{\alpha} \quad \text{<식 2>}$$

여기서, RN은 정보를 표현하기 위한 의사난수, SW는 동기를 맞추기 위한 의사난수, n은 정보표현을 위해서 발생시킬 의사난수의 개수이고, α 는 삽입강도를 조절하기 위한 계수이며, W는 최종적으로 생성되는 워터마크 이다.

워터마크 추출은 삽입의 역 과정을 거쳐서 삽입된 모든 정보를 추출하게 된다.

2.2 Semi-fingerprinting을 위한 데이터 구조

본 절에서는 *semi-fingerprinting*를 구현하기 위해 삽입하는 정보의 데이터 구조에 대해서 설명한다. 삽입되는 정보의 데이터 구조는 그림 2에서와 같이 크게 Fingerprinting과 Transaction Information의 2개영역으로 구성되어 있다. 그림 2의 데이터 구조는 국내의 디지털 콘텐츠 관리를 위한 표준이 없기 때문에, 일본의 cIDf[2] 표준을 참고로 구성한 것이다.

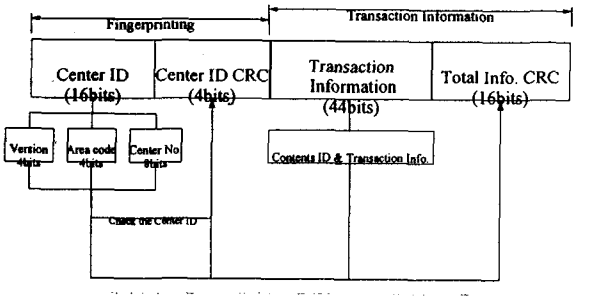

그림 2 Semi-fingerprinting을 위한 데이터 구조

그림 2에서 fingerprinting영역은 Center ID와 Center ID CRC로 구분된다. 여기서 Center ID는 다시 Version, Area Code, Center No.,로 세분화 된다. Fingerprinting영역은 앞서 설명했던 바와 같이, 충돌 공격에 강인하다. 단 반드시 하나의 콘텐츠에 하나의 고유한 정보가 부여된다는 가정이 전제 되어야 한다.

Transaction Information에는 Content ID와 Transaction Information이 삽입된다. 여기서 Content ID는 콘텐츠를 구분하기 위한 것이고, Transaction Info.는 어느 최종사용자가 언제 구매했는가를 정보로 가지고 있게 된다. 사용자를 추적하기에 가장 정확 데이터를 포함하고 있는 것이다. 그러나, 이 정보는 충돌 공격에 의해서 데이터간 중복이 발생될 수 있다. 모자익 공격이 가해질 때는 모자익 크기에 따라서 추출이 가능하지만, 평균 공격의 경우는 데이터 추출이 불가능할 수 있다. 그러나, 이 경우, Center ID를 추출해서 center를 찾아내고 center내의 Transaction정보와 비교해서 분석하면, 중복된 데이터를 분리해 낼 수 있고 불법 배포자를 찾아낼 수 있게 된다.

Semi-fingerprinting의 데이터 구조에는 2개의 CRC정보가 존

재한다. Center ID CRC는 Center ID의 진위여부를 판단하기 위한 정보이고, Total Info. CRC는 삽입된 정보가 모두 정확한가를 판단하기 위한 CRC이다. Total Info. CRC에 오류가 발생해도, Center ID CRC가 오류가 나지 않으면, Center ID정보로부터 사용자 추적을 시행하게 된다.

3. 실험결과

본 논문에서는 사용된 알고리즘의 우수성을 증명하기 위하여 stirmark4.0공격 및 공모공격에 대해서 실험하였다. 각 항목에 대한 실험결과는 그림2와 표1,2에 잘 나와있다.

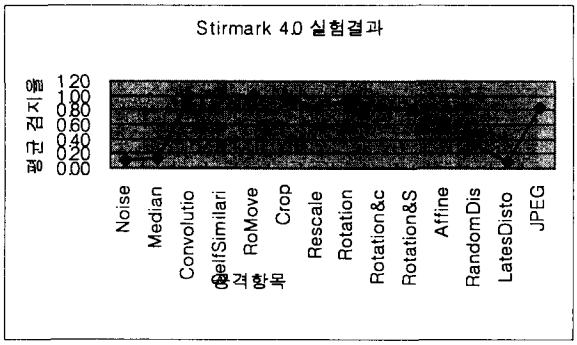

그림 2 Stirmark 실험결과

표 1 평균공격에 대한 강인성

영상개수	4	5	6	7	8	9	10
추출율%	100	100	100	100	100	100	100

표 2 모자익 공격에 대한 강인성

모자익 크기	128	96	64
추출율 %	100	100	98

4. 결론 및 향후과제

본 논문에서는 대영확산방식을 응용하여 삽입량을 증가시켰으며, 이 기술을 응용하여 semi-fingerprinting을 할 수 있는 방법에 대해서 제안하고 실험하였다. 실험결과에서 알 수 있듯이 제안된 워터마킹 기술의 강인성은 압축, RST공격, stirmark 테스트에서 매우 우수한 결과를 나타냈다. Fingerprinting에 응용하기 위해서 견뎌야 하는 공모공격에도 강인함을 보여줬다. 이와 같은 결과를 바탕으로 semi-fingerprinting시스템을 구축하여 운영할 경우, 콘텐츠의 무단 복제 방지에 큰 기여를 할 수 있을 것으로 여겨진다. 그러나, 본 논문에서 제안한 semi-fingerprinting 시스템이 완벽히 실효성을 거두기 위해서는 서로 다른 센터에 동일한 콘텐츠를 제공해서 안된다는 제약조건이 있다. 이것이 본 논문이 fingerprinting이 아닌 semi-fingerprinting기술로 정의될 수 밖에 없는 이유이다. 따라서 정책적인 지원 없이 콘텐츠 불법복제를 방지하고 예방하기 위해서는 semi가 아닌 좀더 완벽한 fingerprinting기술을 개발할 필요가 있다. 또한 실험된 워터마킹 기술이 median 필터 공격에 약점을 드러낸 만큼 이 부분에 대한 보완도 요구된다.

Reference

[1] http://www.sdmi.org

[2] http://www.cidf.org

[3] Ingemar J. Cox, Miller M. L. and Bloom J. A., " Watermarking applications and their properties" , *International Conference Information technology' 2000*, Las Vegas, 2000.

[4] Josep Domingo-Ferrer and Herrera-Joancomarti J., " Simple Collusion-Secure Fingerprinting Schemes for Images" , *IEEE ITCC' 2000*, pp.128-132, ISBN 0-7695-0540-6.

[5] Andrew E. Caldwell, Choi H. J. and Kahng A. B., " Effective Iterative Technique for Fingerprinting Design IP" , *36th ACM/IEEE Design Automation Conference Proceedings*, pp. 843-848, Jun. 1999.

[6] Joseph J.K. Rauanidh and Thierry Pun, " Rotation, Scale and Translation Invariant Digital Image Watermarking" , Signal processing journal, 1998.

[7] Ching-Yung Lin, " Public Watermarking Surviving General Scaling and Cropping: An Application for Print-and-Scan Process" , *ACM Multimedia 99*, Orlando, FL, USA, Oct 1999.

[8] Ching-Yung Lin and Shih-Fu Chang, " Distortion Modeling and Invariant Extraction for Digital Image Print-and-Scan Process" , *ISMIP 99*, Taipei, Taiwan, Dec. 1999.

[9] R. Caldelli, Barni M., Bartolini F. and Piva A., " GEOMETRIC-INVARIANT ROBUST WATERMARKING THROUGH CONSTELLATION MATCHING IN THE REQUQENCY DOMAIN" , *Proceedings of 7th IEEE ICIP' 2000*, Vol. II, pp 65-68, Vancouver, Canada, Sep. 10-13, 2000.

[10] Changryoul Choi and Jeong J., " Robust Image Watermarking Scheme Resilient to Desynchronization Attacks" , *SPIE 2002 Security and Watermarking of Multimedia Contents IV*, San Jose, USA, 21-24 Jan., 2002.

[11] Jana Dittmann, Behr A, Stabenau M., Schmitt P., Schwenk J. and Ueberberg J., " Combining digital Watermarks and collusion secure Fingerprints for digital Images" , *IS&T/SPIE Conference on Security and Watermarking of Multimedia Contents*, SPIE Vol. 3675, San Jose, California, Jan., 1999.

[12] Jonathan K. Su and Girod B., " On the Robustness and Imperceptibility of Digital Fingerprints" , *ICMCS' 99*, vol. 2, pp. 530-535, Florence, Italy, Jun. 1999.

[13] Ton Kalker, Depovere G., Haitsma J. and Maes M., " A Video Watermarking System for Broadcast Monitoring" , IS&T/SPIE Conference on Security and Watermarking of Multimedia Contents, SPIE Vol. 3675, San Jose, California, Jan., 1999.