Semi-fingerprinting을 위한 강인한 이미지 워터마킹 알고리즘 및 시스템 구조

정 길 호† · 이 한 호†† · 엄 영 익†††

요 약

본 논문에서는 대역확산 방식을 응용한 새로운 워터마킹 기법과 이를 이용한 semi-fingerprinting 시스템 구조를 제시하며, 특히, 저작권 보호에 주초점이 맞추어져 있는 워터마크 기술을 fingerprinting 분야에 적용함으로써 그 동안 학문연구에 그치고 있었던 워터마크 기술을 보다 현실적인 응용에까지 확대시키기 위한 방법을 제시한다. 본 논문에서 제안하는 워터마킹 기법은 대역확산 방식중 random number shift 방법을 이용하여 데이터 삽입량을 증가시키는 방법의 일종이며, 삽입되는 데이터량이 60-bits이고, 20-bits CRC 코드를 이용하여 추출된 정보의 신뢰도를 높였다. 또한, semi-fingerprinting에 적용하기 위해서 cIDf(content ID forum)의 지침을 기반으로 워터마크를 구성하였다.

A Robust Image Watermarking Algorithm and System Architecture for Semi-fingerprinting

Gil Ho Joung† · Han Ho Lee†† · Young Ik Eom†††

ABSTRACT

In this paper, we propose a new watermarking method based on spread spectrum and a semi- fingerprinting system architecture that can be built using our robust watermarking method. Especially, we describe a mothod that extends the application area of watermarking technology to more practical application domains by applying the watermarking technology that has been focused mainly on copyright protection to fingerprinting area. Our proposed watermarking scheme uses the method that inserts more data by using random number shifting method. We improved the reliability of acquired data with 20-bits CRC code and 60-bits inserted information. In addition, we designed the system architecture based on the recommendation of cIDf (content ID forum) in order to apply the system on the semi-fingerprinting area.

키워드 : 워터마크(Watermark), 핑거프린트(Fingerprint), 스테가노그래피(Steganography)

1. 서 론

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, 기술적용 또한 매우 어렵다. 디지털 콘텐츠의 저작권 보호와 재배포 방지를 위해서 관심 있게 연구되고 있는 분야가 워터마킹과 암호화 기술이다. 워터마킹의 활용분야로는 방송 모니터링, 소유자 정보 표시 및 증명, 인증, Fingerprinting, 복사제어 및 비밀정보 전달 등이 있다[1].

워터마킹 기술은 그 응용분야에 적용되기 위하여 다음과 같은 필수 요건들을 필요로 한다[1]. 첫째, 손실압축, A/D & D/A 변환, 기하학적 변환, Stirmark과 같은 공격에 대한 강인성을 제공해야 한다. 둘째, 임의의 공격에 대한 저항성을 제공해야 한다. 임의의 공격이라 함은, 워터마크에 대한 삭제 시도(능동적 공격), 워터마크의 오검지 유도(수동적 공격), 여러 개의 복사본을 이용하여 오검지 유도(충돌 공격), 다른 정보의 워터마크를 추가 삽입(충돌 공격), 다른 정보의 워터마크를 추가 삽입(위조 공격)을 들 수 있다. 세 번째, 워터마크가 삽입된 결과물은 인간이 감각기관으로 인식할 수 없게 만들어야 한다. 네 번째, 워터마킹 대상에 따른 삽입 및 추출 속도에 대한 계산량을 제공해야 한다. 마지막으로, 신뢰성을 위해서 ECC(Error Correcting Code) 또는 CRC (Cyclic Redundancy Check)를 사용하여 오검지율을 감소시켜야 한다.

앞서 언급된 워터마킹의 필수 요건들은 초기의 워터마킹 기술에 비해서 요구되는 조건들이 더욱 다양해지고 높은

† 준 회 원 : 성균관대학교 대학원 전기전자 및 컴퓨터공학과
†† 정 회 원 : (주)마크애니연구소 연구원
††† 종신회원 : 성균관대학교 정보통신공학부 교수
논문접수 : 2002년 10월 15일, 심사완료 : 2002년 12월 26일

견고성을 요구하고 있음을 알 수 있다. Fingerprinting은 워터마킹 기술 응용의한 분야이기는 하지만, 일반적인 워터마킹의 요구조건들보다 강인성과 데이터 삽입량에서의 요구조건이 더욱 까다롭다. 일반적으로 워터마크를 사용하여 저작권을 보호하기 위해서는 일명 키 방식이라고 지칭하는 1비트 워터마크로도 보호가 가능할 정도로 데이터 삽입량이 많이 요구되지 않는다. 또한 하나의 콘텐츠에는 한명 또는 하나의 그룹을 정보단위로 삽입하므로, fingerprinting에서 요구하는 평균공격이나 모자익 공격에도 강인하게 된다[2, 3]. 그러나 fingerprinting에서는 저작권자에서 중간 배포자 그리고 최종 소비자까지의 정보를 단계적으로 삽입하여야 하므로, 많은 데이터 삽입량이 요구되며, 여러 개의 다른 정보가 삽입된 콘텐츠는 평균공격이나 모자익 공격에 대해서 약점을 드러낼 수 밖에 없다.

앞의 내용을 정리해보면, fingerprinting에는 다음과 같은 필수항목들이 추가되고 강화되어야 한다[3]. 첫 번째, 합법적 사용자를 확실하게 가려낼 수 있어야 하며, 하나의 콘텐츠에서 사용자 중복을 최소화 할 수 있는 신뢰성을 제공해야 한다. 두 번째, fingerprinting 시스템은 다른 시스템의 부분으로 작동할 수 있도록 적은 자원으로도 수행 될 수 있는 경제성을 제공해야 한다. 세 번째, fingerprinting 기술에 대한 완벽한 지식이 없이는 이를 삭제하기 힘들어야 한다. 네 번째, fingerprint된 콘텐츠와 관련된 관련 S/W들에서도 사용될 수 있도록 투명성을 지녀야 한다. 마지막으로, 이상적인 면에서, 콘텐츠의 작은 부분으로도 배포자를 찾아낼 수 있어야 한다.

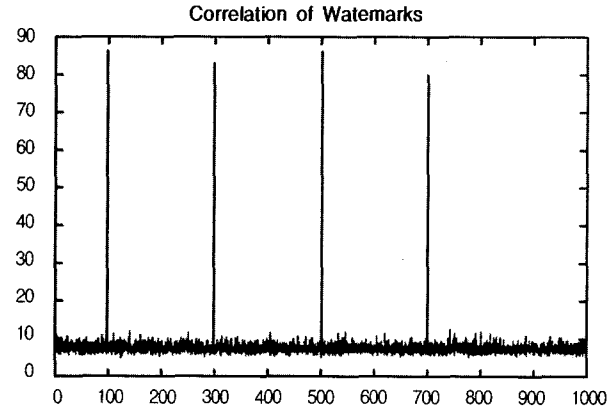
이상에서 설명된 바와 같이 fingerprinting 기술은 워터마킹 기술의 확장된 응용 분야이기도 하지만, 기술의 구현에 있어서는 높은 정밀성, 견고성 그리고 강인성을 요구하고 있다. 그러나 본 연구를 "semi-fingerprinting"이라고 정의한 이유는 위의 항목들을 모두 만족하기는 하지만, 5장 실험결과에서 알 수 있듯이 평균 공격에 대해서 높은 신뢰성에 문제를 가지고 있기 때문이다.

2. 관련 연구

본 절에서는 손실압축, 기하학적 변형과 같은 다양한 공격에 강인한 워터마킹 알고리즘들과 fingerprinting 기술들에 대해서 살펴보고, 본 논문의 목표를 기술한다.

2.1 강인한 워터마킹 방법

워터마킹 방법은 삽입 영역에 따라 공간영역 삽입 방법과 주파수 영역삽입 방법으로 구분할 수 있다. 그리고 워터마크에 대한 공격방법은 크게 손실압축 공격과 기하학적 변형공격으로 구분할 수 있다. 손실압축(대표적으로 Jpeg)에 대한 강인성 문제는 이미 워터마크 기술이 연구되던 초기부터 고려되어져 왔기 때문에, 필수요건이라고 볼 수 있다. 손실압축에 강인한 대표적인 워터마킹 방식은 I. J. Cox에 의해서 제안되었던 대역확산 방법이 있다. 대역확산 방법은 랜덤 수열의 특성이 Seed 값이 서로 다른 수열끼리는 상관도가 매우 낮은 직교특성을 이용하는 것으로 전 주파수 대역에 워터마크 정보가 분포되어 있기 때문에 특정 영역의 성분이 제거되더라도 복구할 수 있는 장점을 가지고 있다[13].



(그림 1) 랜덤 수열의 상관도

기하학적 변형에 강인한 워터마킹 방법에는 DFT 변환을 한 후에, log-log map을 사용하여 워터마크를 구성하는 방법과 log-polar mapping을 사용하는 방법 등이 있다[4-6]. 이중에서 log-polar를 사용하여 워터마크를 구성하는 방법은 회전과 크기변화에 영향을 적게 받기 때문에 많은 관심을 가지고 연구가 이루어졌다. 그러나 연산시간이 오래 걸리고, 작은 영상에서는 데이터의 손실이 발생하는 단점을 가지고 있다.

기하학적 변형의 수치를 찾아내는 방법은 영상에 임의의 특징을 삽입한 후 그 특징을 찾아내는 방법과 대역확산 방식으로 삽입한 워터마크를 자기상관(auto-correlation)을 이용하여 변형정도를 찾아내는 방법이 대표적이다[7, 8]. 특징을 삽입하는 방법은 쉽게 변형된 정보를 알아낼 수 있지만 손실압축에 약하고, 자기상관을 이용하는 방법은 손실압축에 강인하지만 변형된 정보를 찾아내는데 시간이 오래 걸리는 단점을 가지고 있다.

상기의 두 가지 방법은 필요에 따라서 복합적으로 사용되기도 하지만, 아직까지 처리속도와 정확한 워터마크 추출에서 많은 문제점들을 가지고 있으며 지속적으로 연구 중인 부분이다.

2.2 Fingerprinting 기법

서론에서 언급되었듯이 fingerprinting은 워터마킹보다 까다로운 조건들을 필요로 한다. 특히, 서로 다른 정보로 워터마킹 된 영상을 이용하여 평균을 취하는 평균공격과 여러 개로 분할하여 붙이는 모자익 공격은 일명 충돌공격(collu-

sion attack)이라 지칭되며, fingerprinting에 매우 치명적인 공격방법이다. 이 같은 공격에 강인하게 하기 위한 방법으로, 영상을 여러 영역으로 구분하여 거래가 발생할 때마다 그 영역에 추가적으로 워터마크를 삽입하는 방법과 특별한 주파수 대역 필터를 사용하여 정보를 삽입하는 방법, 그리고 Jpeg 압축에 강인하게 하기 위해서 Jpeg의 Quality factor를 이용한 방법 등이 있다[2, 9, 10]. 현재까지 연구된 fingerprinting 방법들은 아직까지 충돌공격에 대한 구체적인 대안을 제시하지 못하거나, 또는 원본의 필요성이 요구되는 등 많은 문제점을 가지고 있다. 그러나 본 논문에서는 원본을 필요로 하지 않고 로고방식과 같은 시각에 의존하는 방법이 아니다. 필요한 정보를 삽입하고 추출해 낼 수 있으며, Jpeg과 같은 압축에도 강인하다. 또한 논문[9]가 가질 수 있는 치명적인 약점인 Cropping 공격에도 강인성을 가지고 있다.

2.3 Semi-fingerprinting 기법

본 논문은 워터마킹 기술이 가져야 하는 기본적인 강인성을 만족시킴과 동시에 부분적으로 fingerprinting을 지원하는 semi-fingerprinting 기술에 관한 연구과정 및 결과에 관한 것이다. 본 논문에서 연구한 semi-fingerprinting 기술은 다음과 같은 특징을 가지며 4장에서 설명할 시스템에 적용함으로써, 그 실용성을 입증할 수 있다. 첫째로, 기존의 워터마킹 기술이 가지고 있던 강인성을 유지한다. 두 번째, 거래가 발생할 때, 사용자 정보를 삽입하는 기능을 가진다. 그러나 충돌공격에 의해서 사용자정보의 중복성이 나타난다. 세 번째, 저작권 정보와 합법적 배포자의 정보는 충돌공격에도 사라지지 않기 때문에, 사용자 정보가 사라져도 추적할 수 있다.

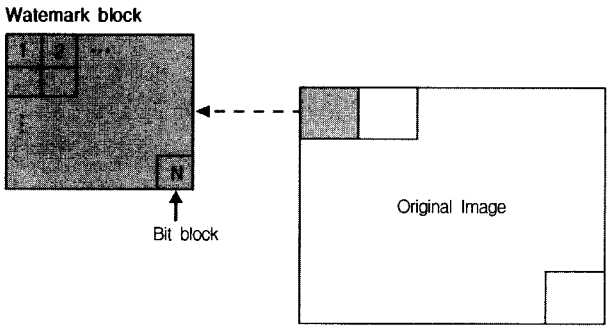
상기의 특징에서 알 수 있듯이, 본 논문에서 제안한 semi-fingerprinting 기술은 매우 강인한 워터마크 정보와 fingerprinting 정보가 공존함으로써, fingerprinting 정보가 중복이 되더라도 강인한 워터마크를 사용하여 역으로 배포자들을 추적할 수 있다. 아래의 3장에서는 본 논문에서 제안한 semi-fingerprinting 기술에 대하여 자세히 기술한다.

3. Semi-fingerprinting 정보 삽입 및 추출 방법

본 논문에서는 정보 60비트와 CRC코드 20비트로 총 80비트의 정보를 삽입한다. 본 논문에서는 대역확산 방식을 사용하여 강인성을 유지함과 동시에 난수 이동을 응용한 새로운 정보 표시방법을 연구하였다[4, 11].

3.1 변형된 대역확산 방식을 이용한 데이터 삽입량 증가 기법

Joseph의 논문에서는. 난수를 이동시킨 후, 이동된 난수간의 거리를 측정하여 정보를 표현하였다[4]. 본 논문에서는 Joseph의 논문을 응용하여 더 효율적인 정보표시 방법을 고안하였다. Joseph의 논문에서는 다양한 공격에 대비하기 위해서 워터마크가 삽입되지 않은 원본을 필요로 하고 있으며, 원본이 없을 경우에는 상대적으로 삽입할 수 있는 정보량이 제한될 수밖에 없다. 또한 회전이나 축소 확대, 이동(RST : Rotation, Scaling, Translation)과 같은 공격에 대비하기 위해서 주파수 평면에서의 진폭 스펙트럼 성분이 이동공격에 대해서 불변의 영역이고, 회전이나 축소 확대는 직교좌표를 극좌표 형태로 변환하고, 로그스케일을 사용함으로써 이동공격의 형태로 변환하여 RST 공격에 영향을 받지 않는 변환평면에서의 워터마크 삽입을 이용하였다. 그러나 이 방법은 극좌표 변환이나 주파수 변환을 위해서 상당히 많은 연산량을 요구하고 있으며, 극좌표 변환시와 로그 스케일에 의한 데이터의 표현시에 손실이 많이 발생하기 때문에 워터마크 정보를 삽입하더라도 효과적으로 복원하기가 어려움이 있다. 따라서 삽입할 수 있는 정보량에 한계를 가질 수밖에 없다. 본 연구에서는 원본 없이 많은 워터마크 정보를 삽입하기 위해서 (그림 2)와 같이 원본 영상을 여러 개의 워터마크 블록으로 나눈다. 여기서 워터마크 블록은 cropping이 발생했을 경우, 최소한 하나의 워터마크 블록이 살아남게 하기 위한 방법으로 많이 사용되고 있다. 워터마크 블록은 삽입하고자 하는 정보가 삽입되는 단위 블록이다. 따라서 본 논문에서는 언급된 바와 같이 총 80비트의 정보를 워터마크 블록에 삽입한다. 워터마크의 추출시에는 기하학적 공격이 가해지지 않았을 때는 워터마크가 한번에 검출이 가능하고, 워터마크 추출이 이루어지지 않았을 때는 기하학적 공격이 가해졌는지 여부를 판단한다. 기하학적 공격을 판단하기 위해서는 자기상관 계수를 구하여 워터마크가 삽입된 이미지의 기하학적 왜곡이나 축소 확대 정도를 파악할 수 있으며, 이는 워터마크 블록으로 데이터 설계가 되었기 때문에 가능한 방법이다.



(그림 2) 정보 삽입을 위한 워터마크 블록과 비트블록

워터마크 블록은 여러 개의 비트블록으로 나뉜다. 비트블록은 실질적으로, 정보를 표현하기 위해서 나누어지는 영역이다. 본 논문에서는 난수를 이동시킨 후, 상호상관에 의해

서 발생하는 최고점을 표현하고자 하는 정보의 비트블록에서 발생하게 만든다. 다시 말해, 난수의 시작 위치를 원하는 비트블록으로 이동시킨다는 것이다.

예를 들어, 워터마크 블록이 32×32개의 비트블록으로 나뉘었다고 가정하자. 그럼 비트 블록의 개수는 총 1024개이다. 이것을 비트 정보로 변환하면, 2^{10}으로 10비트가 된다. 이것을 식으로 표현하면 $N = 2^x$이 되고, 여기서, N은 비트블록의 개수이고, x는 삽입 가능한 비트수가 된다. 앞의 예제의 경우, 하나의 워터마크 블록에 삽입할 수 있는 정보의 양은 10비트가 되는 것이다. 또한, 만약 삽입하고자 하는 정보가 이진수 '1000000000'이라면, 이것은 십진수로 '512'가 되므로, 513번째(왜냐하면, 10비트가 표현할 수 있는 십진수의 범위는 0~1023이기 때문) 비트블록에서 최고점에 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.

$$N_1 \times N_2 \times \Lambda \times N_m = 2^{x_1 + x_2 + \Lambda + x_m} \quad (1)$$

따라서, 본 논문에서 삽입하고자 하는 80비트를 삽입하기 위해서는 1024개의 비트블록으로 워터마크 블록을 나누고 8개의 난수를 사용한다면, 총 80비트를 삽입할 수 있는 것이다.

이상에서 확인할 수 있듯이, 정보 삽입량은 비트블록과 난수의 개수에 따라서 결정된다. 여기서, 사용되는 난수들은 서로 상관성이 없어야 하기 때문에, 의사난수를 사용하였다. 워터마크 블록의 크기는 128×128로 설정하였으며, 비트블록의 크기는 4×4로 결정하여, 하나의 워터마크 블록이 32×32 = 1024비트를 표현할 수 있게 구성하여 실험하였다.

비트블록의 크기는 특히, 크기변환 공격(Resizing)과 밀접한 관계를 가진다. 크기변환 공격이 가해진 후에, 워터마크된 영상을 원래의 크기로 정확히 복원해내지 못한다면 결국 최고점의 위치는 약간의 오차가 발생할 수 있다. 비트블록의 크기는 결국 최종적으로 추출되는 비트정보에 어느 정도의 오차 범위를 줄 것인가를 결정하는 요소가 된다. 그러나 이것을 무작정 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 전제하에 정보를 추출한 것이다. Cropping이 발생할 경우 정보를 정확히 추출해 내기 힘들기 때문에, 추가적으로 동기를 맞추기 위한 의사난수를 삽입하게 된다. 지금까지의 내용을 정리해 볼 때, 80비트의 정보를 삽입하기 위한 8개의 의사난수와 동기신호까지 총 9개의 의사난수가 필요하다. 이 과정은 식 (2)와 같이 나타낼 수 있다.

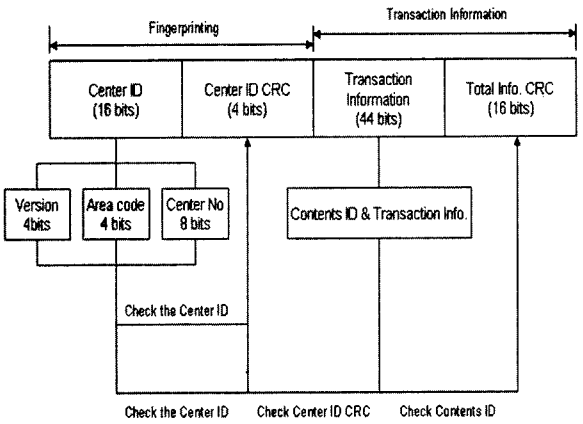
$$W = \frac{(\sum_{k=1}^{k=n} RN_k + SW)}{\alpha} \quad (2)$$

여기서, RN은 정보를 표현하기 위한 의사난수, SW는 동기를 맞추기 위한 의사난수, n은 정보표현을 위해서 발생시킬 의사 난수의 개수이고, α는 삽입강도를 조절하기 위한 계수이며, W는 최종적으로 생성되는 워터마크이다. 워터마크 추출은 삽입의 역 과정을 거쳐서 삽입된 모든 정보를 추출하게 된다.

3.2 Semi-fingerprinting을 위한 데이터 구조

본 절에서는 semi-fingerprinting을 구현하기 위해 삽입하는 정보의 데이터 구조에 대해서 설명한다. 삽입되는 정보의 데이터 구조는 (그림 3)에서와 같이 크게 Fingerprinting과 Transaction Information의 2개 영역으로 구성되어 있다. (그림 3)의 데이터 구조는 국내의 디지털 콘텐츠 관리를 위한 표준이 없기 때문에, 워터마크 표준 중 하나인 cIDf 표준을 참고로 구성한 것이다.

(그림 3)에서 fingerprinting 영역은 Center ID와 Center ID CRC로 구분된다. 여기서 Center ID는 다시 Version, Area Code, Center No.로 세분화 된다. Version은 삽입된 워터마킹 기술의 버전을 확인하기 위한 것으로, 시간이 흐름에 따라서 변화된 버전에 맞추어 정보를 추출하기 위한 것이다. Area Code는 콘텐츠 제공 센터가 속해있는 지역 또는 분야로 구분하기 위한 것이고, Center No.는 Center를 구분하기 위한 고유의 번호이다. 이상의 3가지 항목이 Center ID가 되며, Center ID의 진위여부를 판단하기 위해서 Center ID CRC가 추가된다. Fingerprinting 영역은 앞서 설명했던 바와 같이, 충돌 공격에 강인하다. 단 반드시 하나의 콘텐츠에 하나의 고유한 Center ID가 부여된다는 가정이 전제되어야 한다. 따라서 본 데이터 구조는 이런 전제를 뒷받침해 주는 데이터 할당 정책이 수립되어 있어야 한다.



(그림 3) Semi-fingerprinting을 위한 데이터 구조

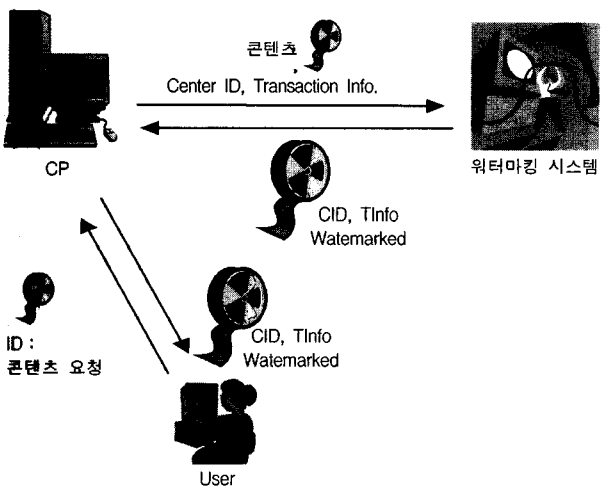
Transaction Information에는 Content ID와 Transaction Information이 삽입된다. 여기서 Content ID는 콘텐츠를 구분하기 위한 것이고, Transaction Information은 어느 최종 사용자가 언제 구매했는가를 정보로 가지고 있게 된다. 사용자를 추적하기에 가장 정확 데이터를 포함하고 있는 것이다. 그러나 이 정보는 충돌 공격에 의해서 중복될 수 있다. 모자익 공격이 가해질 때, 모자익의 크기가 최소 96×96 이하가 될 경우 중복 데이터를 추출 할 수 있으며, 평균 공격의 경우는 중복 데이터 추출을 피해갈 수 없다. 그러나 이 경우, Center ID의 추출 통해서 center를 찾아내고 center 내의 Transaction정보와 비교해서 분석하면, 중복데이터를 분리해 낼 수 있고, 불법 배포자를 찾아낼 수 있게 된다.

이상에서 설명된 바와 같이, Semi-fingerprinting의 데이터 구조는 2개의 CRC 정보를 포함한다. 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 ID 정보로부터 사용자 추적을 시행하게 된다.

4. Semi-fingerprinting 시스템 구성

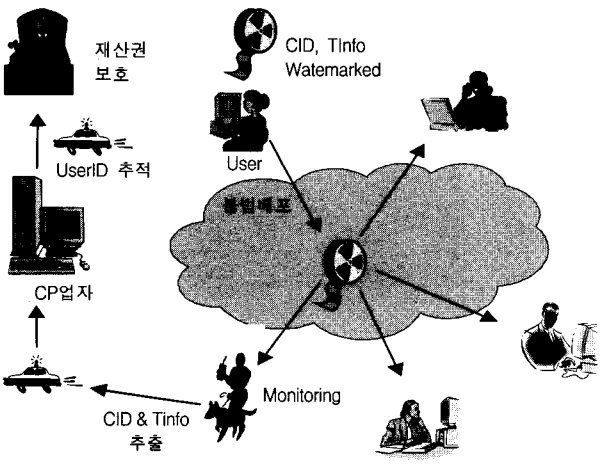
3장에서 설명된 바와 같이 구성된 semi-fingerprinting 데이터를 구성하고 삽입하여 서비스하는 과정은 (그림 4)에 나타나 있다.

(그림 4)에서와 같이 임의의 사용자가 특정 콘텐츠를 요청할 경우, 사용자에게 다운로딩 서비스를 해주기 전에 콘텐츠에 Center ID와 Transaction 정보를 삽입한다. 이렇게 다운로딩 된 콘텐츠가 불법적으로 사용될 경우는 (그림 5)와 같은 시나리오에 의해서 사용자 추적이 가능해진다. 그림에서 CID는 Center ID이고, TInfo는 Transaction Information이다.



(그림 4) 서비스 흐름도

(그림 5)는 불법 사용자를 추적하는 시나리오에 대해서 설명해주는 그림이다. (그림 4)에서 워터마크가 삽입된 콘텐츠가 불법적으로 배포될 경우, CID와 TInfo를 통해서 불법 배포자를 추적하게 된다.



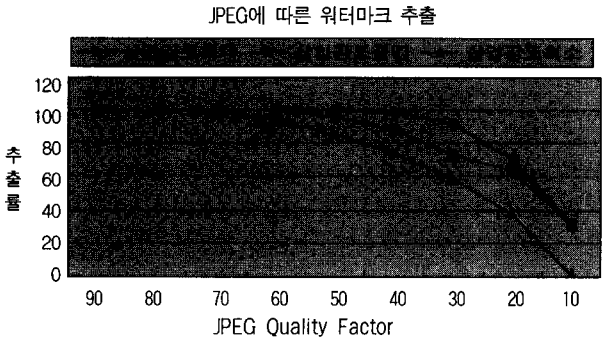
(그림 5) 불법사용자 추적 시나리오

5. 실험 결과

연구된 정보 삽입 기술의 강인성과 신뢰성을 입증하기 위해서 본 논문에서는 워터마크 된 752개의 영상을 대상으로 압축, 기하학적 변형 그리고 stirmark 실험을 수행하였다. stirmark 실험의 경우, 버전 4.0으로 실험하였으며 stirmark 실험 항목에 포함되어 있는 압축과 RST(Rotation, Scaling, Translation) 공격에 대해서는 별도항목으로 분류하고 세분하여 정밀하게 실험하였다.

5.1 JPEG에 대한 강인성

(그림 6)과 <표 1>은 압축에 대한 강인성테스트 결과이다. 일반적으로 이미지를 인터넷상에서 사용하기 위해서 Jpeg 압축을 많이 사용한다. Jpeg은 손실 압축방법으로 QF(Quality Factor)를 압축의 척도로 사용한다. QF가 높을수록 압축이 적게된 이미지로 화질이 좋으며, QF가 낮을수록 압축이 많이된 영상으로 화질이 떨어진다.



(그림 6) 압축률에 따른 워터마크 추출률의 변화

〈표 1〉 압축률에 따른 워터마크 추출 상세 결과

Quality Factor	삽입강도 최대	삽입강도 중간	삽입강도 최소
90%	100.0%	100.0%	100.0%
80%	100.0%	100.0%	100.0%
70%	100.0%	100.0%	99.1%
60%	100.0%	99.2%	94.0%
50%	99.9%	95.9%	84.8%
40%	98.4%	87.7%	74.1%
30%	92.0%	72.1%	59.2%
20%	69.6%	63.4%	38.4%
10%	31.6%	34.8%	0.8%
SNR	31dB	33dB	35dB

실험 결과를 보면 삽입 강도에 따라서 차이가 있지만, QF 30%까지 추출율이 50% 이상이 됨을 확인할 수 있다. 또한, SNR은 삽입 강도에 따라 31~35dB의 분포를 나타냈다.

5.2 RST 공격에 대한 강인성

RST 공격은 이미지 툴(photoshop, paintshop 등)을 이용하면 누구나 쉽게 가할 수 있는 공격 방법으로 간단하면서도 워터마크에는 치명적인 공격이다. 그러나 본 연구의 실험결과는 <표 2>에서 알 수 있듯이 우수한 결과를 보였다.

〈표 2〉 RST 공격에 따른 워터마크 추출 결과

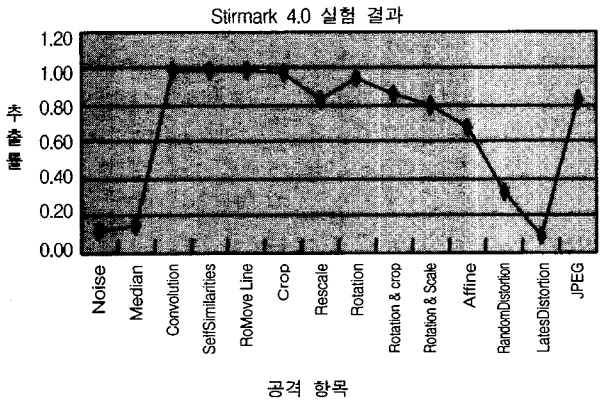
삽입강도 중간	Resizing	Rotation	Cropping
Bitmap	71.3%	100.0%	98.0%
Jpeg 90%	52.2%	99.7%	96.5%

본 논문에서는 자기상관을 측정해서 RST 공격이 가해진 정도를 찾아내어 역으로 영상을 복원한 후에 데이터를 추출하는 알고리즘을 사용하였다[8]. <표 2>의 첫 번째 행에서 Bitmap은 압축이 가해지지 않은 이미지로서 순수하게 RST 공격이 가해졌을 때, 워터마크 추출률 나타내고 있으며, 두 번째 행에서 Jpeg은 앞에서 설명되었던 압축 공격으로, 압축과 RST, 두 가지 공격이 모두 가해졌을 경우, 추출률을 나타내고 있다.

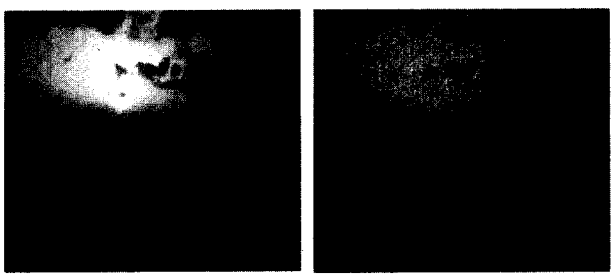
5.3 Stirmark 공격에 대한 강인성

Stirmark 4.0의 공격항목은 Noise 첨가, Median 필터링, Convolution, SelfSimilarities, Remove Lines, Cropping, JPEG 압축 공격, Rescale, Rotation 공격 항목이 존재한다.

(그림 7)의 실험결과 항목에서 실험결과가 안 좋은 항목은, 노이즈 첨가와 Median 필터링, 그리고 Lates Distortion이다. 이들 결과의 특징을 살펴보면, 노이즈 첨가의 경우 20~60% 까지의 노이즈가 첨가되는데, 영상은 (그림 8)과 같이 원본 영상에 매우 많은 손실을 주기 때문에, 20%를 제외한 나머지 noise 첨가의 결과가 나쁘게 나왔다. Median 필터링의 경우는 3×3 ~ 7×7까지 공격이 발생하는데, 3×3 외의 필터링에는 약점을 드러냈다. 그 이유는 median 필터가 저주파 또는 고주파 필터들과 달리 주파수공간에서 필터링이 이루어지는 것이 아니라 공간영역의 픽셀 값 자체를 변화시키기 때문인 것으로 생각되며, 구체적으로는 본 논문의 정보 삽입 방법이 공간영역에서 이루어지기 때문이다. Lates Distortion의 경우는 공격자체가 영상에 많은 왜곡을 주기 때문에 사실상 추출이 거의 불가능했다.



(그림 7) Stirmark 4.0에 대한 실험 결과



(a) (b)

(그림 8) 워터마크된 영상(a)과 noise 20%가 첨가된 영상(b)

5.4 충돌 공격에 대한 강인성

충돌 공격이란 서로 다른 정보가 삽입된 이미지들을 이용하여 평균을 취하거나 또는 모자익 공격을 행함으로써 삽입되어 있는 정보를 추출하는데 혼선을 야기하기 위한 공격 방법이다. (그림 9)은 평균 공격과 모자익 공격의 일예이다. 3.2절에서 제안한 데이터 구조로 삽입 정보를 구성하여 삽입 후 충돌 공격에 대한 실험을 한 결과는 <표 3>과 <표 4>에 잘 나와 있다. 여기서 추출정보는 Center ID(16비트)로 국한한다.

〈표 3〉 평균 공격에 대한 강인성

영상개수	6	7	8	9	10
추출율(%)	100	100	100	100	100

〈표 4〉 모자익 공격에 대한 강인성

모자익 크기	128	96	64
추출율(%)	100	100	100

<표 3>과 <표 4>의 결과에서 알 수 있듯이 Center ID의 경우는 100% 추출되었다. 이것은 3.2절에서 설명한 데이터 구조로 구성되었기 때문에 당연한 결과이다. 평균 공격의 경우는 60비트(Center ID + Transaction Information)의 정보를 정확히 추출해내는데 문제점을 가지고 있다. 이것이 본 논문에서 제안한 알고리즘을 "semi"라고 정의한 이유이다. 정확하게 불법 배포자를 추적해내기 위해서는 삽입한 60비트의 정보가 모두 추출되어야만 한다. 그러나 언급된 바와 같이 평균공격에 대해서는 60비트 정보를 모두 추출해내지 못하고, Center ID를 추출하여 불법 배포자를 찾아내기 위한 조사 범위를 좁혀주는 기능을 한다. 반면, 모자익 공격의 경우는 Cropping 공격의 확장으로 볼 수 있다. 따라서 모자익 공격의 경우는 <표 2>에서 확인할 수 있듯이 96×96 이상의 크기로 모자익 될 경우 98% 정도의 추출율을 보인다.

5.5 워터마킹 성능 평가

최근 워터마킹 시스템에 대한 체계적인 성능평가를 둘러싼 많은 움직임을 엿볼 수 있다. 본 논문에서는 앞서 얻은 실험 결과에 더불어 기존의 워터마킹 시스템과 비교하였으며, 이는 본 논문의 성격이 단순 워터마킹 알고리즘 제안이 아닌 특정 시스템을 위한 여러 가지 공격 대안을 제시하고 있기 때문이다. 다음의 결과는 Digimarc의 BATCH EMBEDDING TOOL 1.00.13/READMARC 1.5.8, GENAVA 대학의 워터마킹 툴 그리고 SIGNUM Technologies의 SureSign Server 1.94를 각 조건에 맞도록 실험한 성능 비교이다[12].

〈표 5〉 Stirmark 3.0에서의 워터마킹 벤치마크

	Digimarc	Unige	SureSign	Semi-F
Signal enhancement				
Gaussian	100	100	100	100
Median	100	100	100	16
Sharpening	100	100	100	97
FMLR	100	67	100	100
Compression(JPEG)	65	52	87	87
Scaling(Without JPEG 90)	81	81	97	81
Cropping(Without JPEG 90)	100	81	94	98
Shearing				
X	50	13	42	50
Y	50	4	42	50
Rotation				
Auto-crop	95	74	37	96
Auto-scale	97	77	51	96
Other geometric trans.				
Col. & line removal	100	69	89	100
Horizontal flip	100	100	100	100
Random geometric dist.	17	0	0	32

<표 5>의 결과에서 볼 수 있듯이 Signal enhancement를 제외한 대부분의 평가 항목에서 우위를 보이고 있는 것으로 나타났다. 이는 앞서 평가한 Stirmark 4.0 실험에서도 잘 드러나 있다.

6. 결론 및 향후 과제

본 논문에서는 대영확산 방식을 응용한 강력한 워터마킹 기술과 이 기술을 응용하여 semi-fingerprinting을 할 수 있는 방법에 대해서 제안하고 실험하였다. 실험결과에서 알 수 있듯이 제안된 워터마킹 기술의 강인성은 압축, RST 공격, Stirmark 테스트에서 매우 우수한 결과를 나타냈다. Fingerprinting에 응용하기 위해서 견뎌야 하는 충돌공격에도 매운 강인함을 보여줬다. 이와 같은 결과를 바탕으로 4장에서 제안한 semi-fingerprinting 시스템을 응용할 경우, 콘텐츠의 무단 복제 방지에 큰 기여를 할 수 있을 것으로 여겨진다. 또한 기존의 fingerprinting에 관한 논문들은 본 논문에서와 같이 구체적이고 상세한 실험결과를 첨부한 연구를 찾아보기 힘들었다. 따라서 본 논문은 앞으로 다른 논문들의 참고대상이 될 수 있을 것으로 기대된다.

그러나 본 논문에서 제안한 semi-fingerprinting 시스템이 실효성을 거두기 위해서는 서로 다른 센터에 동일한 콘텐츠를 제공해서 안 된다. 이것이 본 논문에서 제안된 semi-fingerprinting 기술의 한계라고 여겨진다. 따라서 시스템이나 정책적인 지원 없이 콘텐츠 불법복제를 방지하고 예방하기 위해서는 semi가 아닌 좀 더 완벽한 fingerprinting 기술을 개발할 필요가 있다. 또한 실험된 워터마킹 기술이 median 필터 공격에 약점을 드러낸 만큼 이 부분에 대한 보완이 요구된다.

참 고 문 헌

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

[2] D. F. Josep and H. J. Jordi, "Simple Collusion-Secure Fingerprinting Schemes for Images," *IEEE ITCC '2000*, pp. 128-132, 2000.

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

[4] J. J. K. O'Ruanaidh and T. Pun, "Rotation, Scale and Tran-

slation Invariant Digital Image Watermarking," *Signal Processing Journal*, 1998.

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

[6] C. Y. Lin and S. F Chang, "Distortion Modeling and Invariant Extraction for Digital Image Print-and-Scan Process," *ISMIP '99*, Taipei, Taiwan, Dec., 1999.

[7] R. Caldelli, M. Barni, F. Bartolini and A. Piva, "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., 2000.

[8] C. R. Choi and J. Jeong, "Robust Image Watermarking Scheme Resilient to Desynchronization Attacks," *SPIE 2002 Security and Watermarking of Multimedia Contents IV*, San Jose, USA, Jan., 2002.

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

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

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

[12] F. A. P. Petitcolas and R. J. Anderson, "Evaluation of copyright marking systems," In proceedings of *IEEE Multimedia Systems '99*, Florene, Italy, Vol.1, pp.574 - 579, June, 1999.

[13] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," NEC Res. Insti., Princeton, NJ, Tech. Rep.95-10, 1995.

정 길 호

e-mail : horizon@ece.skku.ac.kr
2000년 상명대학교 정보과학과(학사)
현재 성균관대학교 전기전자 및 컴퓨터 공학과 석사과정
관심분야 : DRM, 멀티미디어 저작권 보호 등

이 한 호

e-mail : sslh2@markany.com
1998년 경희대학교 우주과학과(학사)
2001년 한국외대 경영정보대학원(이학석사)
현재 (주)마크애니연구소 연구원
관심분야 : 디지털 워터마킹, 멀티미디어 저작권 보호 등

엄 영 익

e-mail : yieom@ece.skku.ac.kr
1983년 서울대학교 계산통계학과(학사)
1985년 서울대학교 대학원 전산과학전공 (공학석사)
1991년 서울대학교 대학원 전산과학전공 (공학박사)
현재 성균관대학교 정보통신공학부 교수
관심분야 : 분산 시스템, 이동 컴퓨팅 시스템, 분산 객체 시스템