쉬프팅 기법을 이용한 디지털 이미지 핑거프린팅 기술

Digital Image Fingerprinting Techniques Using Shifting Scheme

김광일*, 김종원**, 최종욱***
Kwang Il Kim*, Jong Weon Kim**, Jong Uk Choi***

Abstract - The wide use of digital media during the past few years, has led to an increase of digital piracy and tampering. To deal with these problems, the concept of digital fingerprinting has been introduced. Digital fingerprinting is an effective method to identify users who might try to redistribute multimedia content. In this paper, we propose new digital image fingerprinting techniques using watermark shifting scheme and concept of domain.

Key Words : fingerprinting, watermarking, digital piracy, collusion secure

1. 서 론

인터넷 환경이 급속도로 발전함에 따라 멀티미디어의 범람과 사용자들의 유료 콘텐츠 사용에 대한 인식 부족으로 디지털 콘텐츠의 지적재산권 침해가 빈번하게 발생하고 있으며, 이러한 불법콘텐츠들의 무분별한 공유는 디지털 콘텐츠 산업 발전을 저해하는 심각한 문제로 대두되고 있다. 이러한 지적재산권 침해로 인한 피해규모는 전 세계적으로 매우 크게 나타나고 있으며, 그로 인해 새로운 창작산업에 막대한 피해를 주고 있어 저작권 관련 이슈가 사회 문제로 대두되고 있다.

디지털 핑거프린팅(Digital Fingerprinting)은 기밀 정보를 디지털 콘텐츠에 삽입하는 측면에서는 디지털 워터마킹과 동일하다고 볼 수 있으나 저작권자나 판매자의 정보가 아닌 콘텐츠를 구매한 사용자의 정보를 삽입함으로써 콘텐츠 불법 배포자를 추적할 수 있도록 한다는 점에서 워터마킹과 차별화된 기술이다. 이러한 핑거프린팅 기술은 소유권에 대한 인증뿐만 아니라 개인 식별 기능까지 제공해야 하므로 기존의 워터마킹이 갖추어야 할 요구사항인 비가시성, 견고성, 유일성과 더불어 공모 허용, 비대칭성, 익명성, 조건부 추적성 등이 부가적으로 필요하다.

핑거프린팅 기술은 워터마킹의 확장된 형태의 기술로써 콘텐츠에 구매자 정보를 삽입하여 불법 배포된 콘텐츠에 대해서는 삽입한 구매자 정보를 추출함으로써 불법 배포가 이루어진 원천지(Source)를 추적할 수 있도록 해 준다.

워터마킹 방법은 한 개인의 단독적인 공격에는 강인하지만 저작권 정보만이 들어가기 때문에 디지털 콘텐츠가 불법 배포되었을 때는 배포자를 추적할 수 없다. 또한 워터마크로써 구매자 정보를 삽입한다고 할지라도 여러 사람이 공모공격(collusion attack)을 가했을 때는 삽입한 워터마크가 모두 손실되기 때문에 삽입한 구매자 정보 및 저작권 정보를 추출할 수 없게 된다.

공모공격은 주로 구매자 정보를 삽입할 때 사용되었던 워터마크와의 상관도 값이 작게 나오도록 하는 방법이 주를 이루고 있고, 다음과 같은 종류의 공모공격이 알려져 있다. 이 공모공격에는 평균(average)공격, 모자이크(mosaic)공격, 최대-최소(Max-Mix)공격[1], 상관계수 음수화(Negative Correlation)공격[1], 상관계수 제로화(Zero Correlation)공격법[2]이 있고, 각각의 공모공격은 하나의 콘텐츠를 서로 다른 ID를 가진 사람들이 내려 받고 각각 소유한 콘텐츠를 공모함으로써 수행된다.

핑거프린팅 기술에 대한 현재까지의 연구를 살펴보면 크게 기존의 워터마킹 기술을 이용하는 기법[3]과 삽입하는 코드 자체가 공모공격에 강인하도록 설계하는 공모보안 코드 방법[4~7]으로 분류할 수 있다.

2. 연구 내용

본 논문에서는 워터마킹 기술을 핑거프린팅에 활용하기 위하여 2레벨 웨이블릿 변환 영역에 도메인 정보를 나타내는 쉬프트된 워터마크와 사용자 정보를 나타내는 인덱스 행렬을 삽입하게 된다. 그림 1은 2레벨 웨이블릿 변환을 수행 후 얻어진 주파수 성분의 데이터를 보여주는 것이다. 이 부대역 중에서 비가시성과 강인성을 모두 충족하는 대역을 선택하여 핑거프린트 정보를 각각 삽입하였다.

저자 소개
* 김광일 : 祥明大學 컴퓨터科學科 碩士課程
** 김종원: 祥明大學 컴퓨터科學科 硏究敎授
*** 최종욱: 祥明大學 소프트웨어學科 正敎授

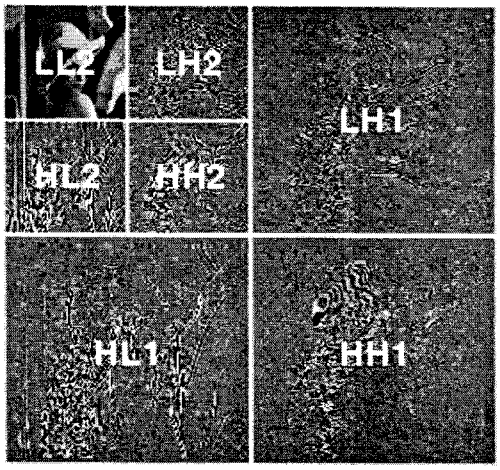

그림 1. 2레벨 웨이블릿 변환 영역

선택된 대역에 삽입할 쉬프트 워터마크는 삽입하고자 하는 도메인 정보를 식(1)에 의해 계산된 행과 열을 결정한다. 결정된 행과 열의 크기만큼 쉬프트하여 삽입하게 된다. 이렇게 쉬프트된 워터마크는 추출 시 그림 2와 같이 쉬프트된 워터마크 위치 만큼 이동하여 피크가 나타나므로 그 위치 점을 찾으므로 해서 도메인 정보를 얻을 수 있게 된다.

$$S_c = Mod(Domain, B_L/B_M)\times B_M + B_M/2$$
$$S_r = \left\lfloor \frac{Domain}{(B_L/B)} \right\rfloor \times B_M + B_M/2$$

(1)

S_c와 S_r은 각각 이동하게 될 행과 열을 나타내며, Domain은 삽입할 도메인 정보를 의미하고, B_L은 한 블록의 크기이다. B_M은 일종의 △성분으로 $B_M \times B_M$ 영역 안에 나타나는 모든 피크를 동일한 정보로 담고 있는 피크로 취급하기 위하여 설정한 것이다. ⌊ ⌋ 는 입력 값보다 작은 가장 가까운 정수 값을 계산한다.

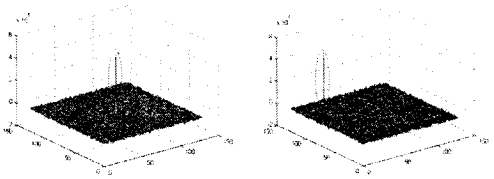

그림 2. 워터마크 쉬프트의 원리

위와 같은 방법으로 선택된 웨이블릿 영역에 쉬프트 워터마크를 삽입하고, 다시 동일한 영역에 인덱스 행렬을 재 삽입하게 된다.

2.1 핑거프린트 생성 및 삽입

본 논문에서 제안하는 핑거프린트 삽입 알고리즘은 웨이블릿을 통해 얻어진 주파수 영역 중 특정 부대역을 선택하여 핑거프린트 정보를 삽입하는 것이다. 그림 3은 제안된 핑거프린트 삽입 알고리즘 구조를 나타낸 것이다.

워터마크에 쉬프팅 기법을 사용하여 정보를 삽입하게 된다. 따라서 생성된 워터마크를 이용하여 부호화된 핑거프린트 정보는 다음 식 2와 같다

$$FP = IW_s + IM_i^s$$

(2)

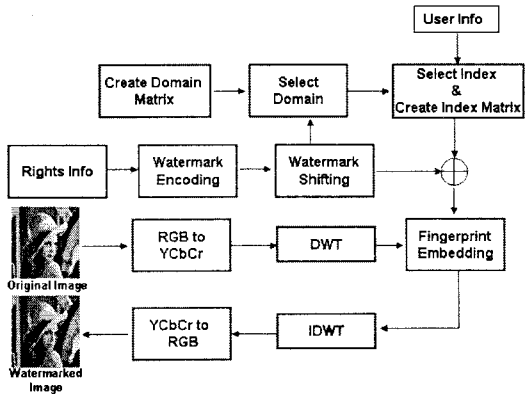

그림 3. 핑거프린트 삽입 알고리즘

IW는 기초 워터마크를, IM는 인덱스 행렬을 의미한다. s는 선택되어진 도메인 인덱스를 뜻하고, i는 s번째 도메인의 i번째 열을 나타내는 것이다. 이렇게 선택되어진 열을 행의 방향으로 차례로 기초 워터마크와 더하여 핑거프린트 정보를 생성하게 된다. 인덱스 행렬은 Malvar에 의해 제안된 듀얼 워터마킹/핑거프린팅(dual WM/FP)[3]에서 제안된 워터마크를 숨기는 반송 신호와 같은 방법으로 생성된 M×N의 2차원 행렬로, 표준편차가 B인 정규분포를 따른다(IM_i^s=N(0, B^2)). 이 인덱스 행렬을 여러 개 만들어서 각각의 행렬을 도메인으로 규정하고, 이 도메인에 인덱스를 부여하여 인덱스 정보를 기초 워터마크의 쉬프팅을 기법을 사용하여 기록하게 된다. 또한 인덱스 행렬의 각 열을 사용자 정보와 연관시켜 하나의 도메인 내에서 하나의 열이 한명의 사용자 정보와 연관되게 되는 것이다. 예를 들어 하나의 인덱스 행렬에 128개의 열이 존재하면, 하나의 도메인에 128명의 사용자 정보가 포함되는 것이다.

원 영상을 2레벨 웨이블릿 분해 후 LH2, HL2, HH2 영역에 앞서 설명한 핑거프린트를 삽입한다.

2.2 핑거프린트 정보 추출

핑거프린트 정보를 추출하는 단계에서 좀 더 높은 상관도를 얻기 위해 위너필터를 사용하였다. 위너 필터는 주로 잡음을 제거하기 위한 방법으로 많이 활용되고 있다. 워터마크된 이미지를 위너 필터링하고, 워터마크된 이미지와 이 필터링된 이미지와의 차 영상을 구하여 다음과 같은 삽입절차를 진행하게 된다.

차 영상을 2레벨 웨이블릿 분해하여 분해된 부대역중 LH2, HL2, HH2 영역의 계수들을 합한다. 이 계수들의 합과 기초 워터마크와의 상관도를 구하여 쉬프팅된 값을 추출하여 도메인 인덱스를 확인한다. 다음 확인된 인덱스 행렬의 각 열을 부대역 계수들의 합과 같은 크기의 행렬로 재조합하여, 이 부대역 계수들의 합과 다시 상관도를 구한다. 가장 높은 상관도 값이 나타나는 열의 인덱스를 확인하여 도메인 인덱스 s와 인덱스 행렬의 i 번째 열을 조합하여 사용자 정보 인덱스를 검출하게 된다.

3. 실험 결과

본 논문에서는 제안한 알고리즘의 성능을 측정을 위하여 512×512 영상 5개를 실험하였고, 공모 공격에 대한 강인성을 확인하기 위하여 평균 공모공격, 모자이크 공모공격을 실시하였다. 공모자의 수는 최대 10명으로 설정하였으며, 각 공모자 수에 따른 JPEG압축에의 강인성 성능측정도 함께 실시하였다.

3.1 평균 공모공격

표 1은 평균 공모공격에 대해 검출된 공모자의 수를 공격한 공모자의 수와 JPEG Quality Factor에 변화를 주면서 실시한 실험의 결과이다. 공모자의 수는 두 명에서 열 명까지 한 명씩 증가하였고, JPEG Quality Factor는 100에서 10까지 10%씩 감소하면서 실험을 하였다.

JPEG을 적용하지 않았을 때의 공격은 최대 10명의 공모자가 공격했을 시에도 10명의 공모자 모두를 검출하였다. Quality Factor 60%까지는 10명의 공모자 중 핑거프린팅 기술의 요구 조건중의 하나인 최소한 한명 이상의 공모자를 검출할 수 있었다.

표 1. 평균 공격에 대한 공모자 검출 실험

lena, airplane, girl, milk, pepper (PSNR:38.65db)										
JPEG / 공모자수	100	90	80	70	60	50	40	30	20	10
2	2	2	2	2	2	2	2	2	1.6	0
3	3	3	3	3	3	3	3	2.4	0	0
4	4	4	4	4	4	4	2.8	0.8	0	0
5	5	5	5	5	5	4	2	0.2	0	0
6	6	6	6	5.6	4.8	2.8	1.4	0	0	0
7	7	7	6.8	6	3.8	2.2	0.8	0	0	0
8	8	8	6	3.8	1.6	0.2	0	0	0	0
9	9	8.8	5.8	2.8	1.2	0	0	0	0	0
10	10	9.8	6	3	1	0.4	0	0	0	0

3.2 모자이크 공격

표 2는 모자이크 공격에 대해서 검출된 공모자의 수를 공격한 공모자의 수와 JPEG Quality Factor에 변화를 주면서 실시한 실험의 결과이다. 압축을 하지 않았을 시는 최대 8명의 공모자를 모두 검출할 수 있었으며, 50%이상의 JPEG Quality Factor에서도 8명의 공모자중 최소한 1명 이상의 공모자를 검출할 수 있었다.

표 2. 평균 공격에 대한 공모자 검출 실험

lena, airplane, girl, milk, pepper (PSNR:38.65db)										
JPEG / 공모자수	100	90	80	70	60	50	40	30	20	10
2	2	2	2	2	2	2	2	2	1.6	0
4	4	4	4	4	4	4	3.4	1.4	0	0
6	6	6	6	5.4	3.6	2.4	1	0	0	0
8	8	8	5.8	3.8	2.4	1	0.2	0	0	0

4. 결 론

본 논문에서는 저작권 정보를 부호화한 기초 워터마크의 쉬프팅 기법과 인덱스 행렬의 한 열을 선택하여 사용자 정보로 조합하여 핑거프린트를 생성하였다. 이렇게 생성된 핑거프린트 정보를 2레벨 웨이블릿 변환 영역 중 LH2, HL2, HH2 부대역에 삽입하였다. 추출과정에서는 기초 워터마크의 쉬프팅 정보를 기초로 도메인 인덱스를 먼저 검출하고, 이 인덱스 행렬의 열에 해당하는 인덱스를 다시 검출하여 사용자 정보 인덱스를 검출하게 된다. 쉬프팅 정보와 도메인 개념을 사용하여 보다 많은 사용자에게 핑거프린트 정보를 삽입할 수 있으며, 최대 10명까지의 공모 공격에 대해 JPEG Quality Factor 60% 이상 까지는 최소한 1명 이상의 공모자를 검출할 수 있는 핑거프린팅의 기본 조건을 만족 하였다.

참 고 문 헌

[1] H. S. Stone, "Analysis of Attacks On Image Watermarks with Randomized Coefficients, " NEC Res. Inst., Tech. Rep. 96-045, 1996

[2] V. Wahadaniah, Y. L. Guan, and H. C. Chua, "A New Collusion Attack and Its Performance Evaluation, "Proceedings of IWDW, 2002, pp. 88-103. 2002.

[3] D. Kirovski, H. S. Malvar, and Y. Yacobi, "Multimedia Content Screening Using a Dual Watermarking and Fingerprinting System, " ACM Multimedia, 2002.

[4] D. Boneh and J. Shaw, "Collusion-Secure Fingerprinting for Digital Data," IEEE Trans. Inf. Theory, vol. 44, no. 5, pp. 1897-1905, Sept., 1998.

[5] J. Dittmann, "Combining Digital Watermarks and Collusion Secure Fingerprints for customer Copy Monitoring," Proc. IEE Seminar Sec. Image & Image Auth, pp. 128-132, Mar., 2000.

[6] J. Domingo-Ferrer and J. Herrera-Joancomart, "Simple Collusion-secure Fingerprinting Schemes for Images," in IEEE International Conference on Information Technology: Coding and Computing, ISBN -7695-0540-6, pp. 128-132. 2000.

[7] W. Trappe, M. Wu, and K. J. R. Liu, "Collusion Resistant Fingerprinting for Multimedia," Proc, of IEEE Int. Conf. on Acoustics, Speech, and Signal Processing(ICASSP. 02), vol. IV, pp. 3309-3312. May, 2002.