SIFT 를 이용한 방향성을 가진 원형반구 기반의 워터마킹 기법의 설계

성현승, 김성환
서울시립대학교 컴퓨터과학부
e-mail : wigman@uos.ac.kr, swkim7@gmail.com

Directional Circular Watermarking Scheme based on Feature Point Detection using SIFT

HyunSeong Sung and SeongWhan Kim
Dept. of Computer Science, University of Seoul

요 약

멀티미디어 컨텐츠에 가시적 혹은 비 가시적으로 정보를 삽입하는 기술을 워터마킹이라고 한다. 워터마크를 삽입한 컨텐츠는 일련의 공격에 강인하도록 설계되어야 하는데, 본 기법은 기하학적 공격에 강인하도록 설계하였다. Scale Invariant Feature Transform (SIFT) 을 이용하여 특징점을 찾고, 특징점 주변에 원형의 워터마크를 삽입하였다. SIFT 에서 구해지는 방향벡터를 사용하여, 워터마크를 삽입할 원형 반구를 설정하였으며, 기존의 원형 기반의 워터마킹 삽입기법보다 강인한 워터마크를 구성할 수 있는 장점을 가진다.

1. 서론

디지털 기술의 발전으로 많은 멀티미디어 컨텐츠들이 만들어지고 있다. 디지털 멀티미디어 컨텐츠의 경우 아날로그와는 다르게 컨텐츠의 복사와 이동이 쉽게 이루어진다. 이러한 디지털 컨텐츠의 장점이 있는 반면 멀티미디어 소유자나 판매자 에게는 컨텐츠를 안전하게 보관하고 유통시킬 수 있는 기술을 필요로 한다. 멀티미디어 컨텐츠의 저작권을 보호하는 기술 중 하나가 디지털 워터마킹이다. 디지털 워터마킹이란 가시적 혹은 비가시적으로 특정의 정보를 디지털 컨텐츠에 삽입/추출하는 과정을 말한다. 이러한 디지털 워터마킹은 소유권을 보호하는데 목적을 둔 저작권 보호, 뿐만 아니라 컨텐츠의 내용이 조작되었는지 판별하는데 사용하는 컨텐츠 인증, 방송의 횟수나 정보를 자동으로 감시하고자 하는 방송 모니터링, 불법적으로 유통되었을 때 출처를 알기 위한 핑거프린팅, 하드웨어 장비를 제어할 수 있는 기기 제어 등의 여러 분야에 응용되고 있다 [1].

2. 관련연구

워터마크가 삽입된 컨텐츠가 사용자에 의해 사용되다가 검출이 되기 전에 일련의 공격이 있을 수 있다. 정지영상을 예로 보았을 때, 영상의 압축이나 영상을 보정하기 위한 필터링 등과 같이 의도되지 않은 공격이 있고, 악의를 가진 공격자가 워터마크를 없애고자 의도적으로 공격 할 수 있다. 다양한 워터마크 공격 중 기하학적 공격은 워터마크가 삽입된 위치정보를 모두 파괴하기 때문에, 단순하면서도 매우 강력한 효과를 내는 공격중의 하나이다. 기하학적 공격에 강인하도록 워터마크를 삽입/추출하는 방법으로는 크게 네 가지로 나누어볼 수 있다. (1) Fourier-Mellin transform 과 같이 기하학적 변형에도 변함이 없는 Invariant transform 영역에 워터마크를 삽입/추출하는 Invariant transform 을 기반으로 한 워터마킹 기법, (2) 원형 혹은 십자형태의 미리 설정한 템플릿 (template)을 이용하는 기법, (3) 워터마크 삽입 시 주기적으로 워터마크를 삽입 한 후에 워터마크 검출 시 Auto-Correlation Function 을 이용하는 기법, (4) 에지(Edge) 혹은 코너(Conner) 등과 같이 영상의 두드러진 특징점(feature point)를 이용하는 기법이 있다 [2,3,4,5,6].

3. 제안하는 시스템

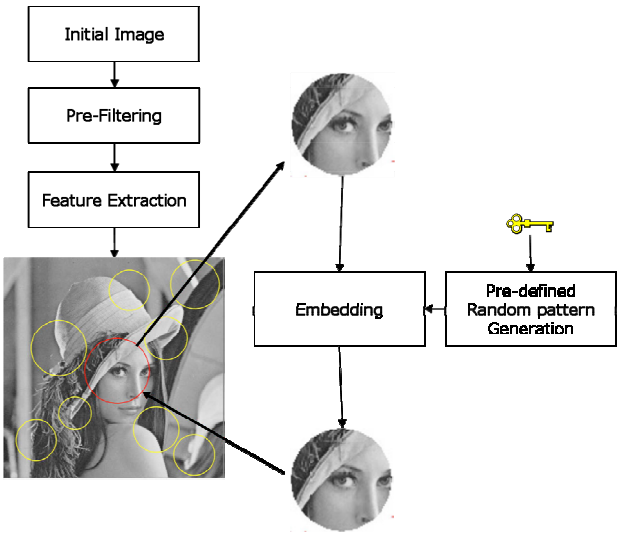
본 논문에서는 특징점을 기반으로 워터마크를 삽입한다. 그림 1 은 워터마크를 삽입하는 방법을 보여주고 있다. 기하학적 변형이 가해지더라도 추출할 수 있는 특징점을 Scale Invariant Feature Transform(SIFT)를 이용하여 특징점을 추출한다. 원본의 이미지의 Gaussian Filter 와 같은 Pre-filter 를 적용하여 필터링(Filtering), 압축(Compression)등의 강인하게 특징점을 추출한다. SIFT 를 수행하면 특징점의 위치 (x, y)와 크기(scale), 방향성(orientation), 방향의 세기(magnitude) 등이 추출된다. 원본의 이미지에서 추출된 특징들 중 수식 1 과 같이 특징점의 위치(x1, y1), 크기정보 (s)를 이용하여 특징점 주변에 원형의 워터마크가 삽입될 영역을 설정한다.

$$(x-x_1)^2+(y-y_1)^2=(ks)^2 \qquad (1)$$

특징 key 를 이용하여 정해놓은 패턴을 워터마크로 하여 각 특징점 주위의 원형의 조작에 삽입이 된다. 워터마크를 삽입할 때, 인지시각적 특성을 고려하여 weighting 값을 결정하는데 본 논문에서는 수식 2, 3 과 같이 noise visibility function(NVF) [7]을 사용하였다.

$$strength=\alpha\cdot(1-NVF)+\beta\cdot NVF \qquad (2)$$

$$NVF(i,j)=\frac{1}{1+\theta\cdot\sigma_x^2(i,j)},\quad \theta=\frac{D}{\sigma_x^2\max} \qquad (3)$$

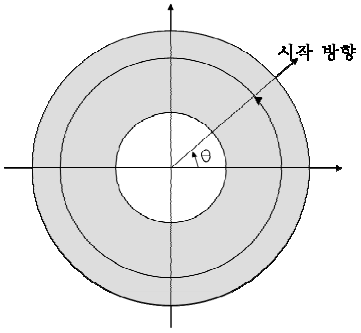


(그림 1) 워터마크 삽입 시스템

삽입된 워터마크가 회전(rotation) 공격에 강인하도록 설계하기 위하여 원형의 워터마크 조각에 시작 위치를 설정한다. 그림 2 에서와 같이 원형의 워터마크에서 시작을 알리는 방향 (θ)는 SIFT 에서 추출한 특징점의 방향성을 이용하였고 반 시계 방향으로 워터마크가 삽입되도록 설계하였다. 또한 원형의 중심부에서는 오류의 확률이 높아지기 때문에 원형의 중심부에는 삽입하지 않도록 하였다.

4. 결론

본 논문에서는 SIFT 를 이용하여 영상의 특징점을 추출하고 특징점을 중심으로 원형의 워터마크를 삽입하는 방법에 대해 제안하였다. 기존의 특징점을 이용하는 Bas 방법 [2]에서는 특징점을 기준으로 Delaunay tessellation 을 수행하여 삼각형 형태의 워터마크를 삽입하였으나 이 방식의 경우 하나의 특징점이 제대로 추출되지 않았을 경우에 많은 수의 삼각형에 영향을 미치게 되어 성능 저하를 불러온다. 본 논문에서 제안한 방식은 이러한 단점을 극복하여 하나의 특징점이 제대로 추출되지 않았더라도 다른 특징점에는 영향을 미치지 않아 전체적 워터마크 성능 향상을 모색하였다. 또한 SIFT 에서 추출된 방향성 특징을 고려하여 워터마크를 삽입함으로써 회전 공격에 강인하도록 설계하였으며, SIFT 고유의 스케일 변화에 강한 특징을 살려 크기변화 공격에도 강인하도록 설계하였다.



(그림 2) 워터마크 시작 방향 설정

참고문헌

[1] I. J. Cox, M. L. Miller, J. A. Bloom, "Digital Watermarking, " Morgan Kaufmann Publishers, 2001.

[2] P. Bas, JM Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," IEEE Trans. Image Proc., vol. 11, no. 9, pp. 1014–1028, Sept. 2002.

[3] J.J. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking," Proc. IEEE Int. Conf. Image Proc., pp. 536 -539, 1997.

[4] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," IEEE Trans. Image Proc., vol. 9, no. 6, June, 2000.

[5] M. Kutter, "Watermarking resisting to translation, rotation, and scaling," Proc. of SPIE Int. Conf. on Multimedia Systems and Applications, vol. 3528, 1998, pp. 423-431.

[6] P.-C. Su and C.-C. J. Kuo, "Synchronized detection of the block-based watermark with invisible grid embedding," Proc. SPIE Electronic imaging (Security and Watermarking of Multimedia Contents III), 2001.

[7] S. Voloshynovskiy, A. Herrige, N. Baumgaertner, and T. Pun, "A stochastic approach to content adaptive digital image watermarking," Lect. Notes in Comp. Sci.: 3rd Int. Workshop on Info. Hiding, vol. 1768, pp. 211-236, Sept. 1999.