1999 年度 大韓電子工學會 夏季綜合學術大會 論文集 第 22 卷 第 1 號 99/6

디지털 영상의 저작권 보호와 기밀성을 위한 다중워터마킹 방법

이성우, 이형욱, 신재호
동국대학교 전자공학과

Multi-watermarking method for copyright protection and confidentiality for digital image

Sungwoo Lee, Hyoungwook Lee, Jaeho Shin
Dept. of Electronic Eng., Dongguk University
E-mail : niceisw@cakra.dongguk.ac.kr

Abstract

In this paper, we present a multi-watermarking method for a copyright protection and confidentiality for an original digital image. One watermark is used for a copyright protection and another for a confidentiality and a detection of unauthorized copies.

1. 서론

디지털 기술과 네트워크 기술의 급속한 발전으로 인해 디지털 영상을 손쉽게 이용할 수 있게 되었다. 그러나 디지털 영상은 디지털 속성으로 인해 복제가 용이하고 네트워크 상에서 쉽게 전송되고 또한 복제된 영상이 원 영상과 거의 화질이 동일하기 때문에 디지털 영상에 대한 저작권 분쟁이 자주 발생하고 있다. 그래서 최근에 디지털 영상의 저작권 분쟁의 해결책으로 워터마킹에 대한 많은 연구가 진행되고 있다 [1][2][3][4][5][6].

디지털 영상의 저작권 보호와 더불어 개인의 의료 정보가 담긴 영상이나 상업적 목적의 영상 또는 회사의 업무에 관련된 영상 등은 영상의 기밀성이 요구되는 경우가 있는데 실제로 이러한 기밀성을 제공하기 위해 암호화 방법이 사용되고 있다.

본 논문에서는 디지털 영상에 2개의 워터마크를 삽입함으로써 저작권 보호기능과 영상의 기밀성 및 복제물 추적 기능을 제공하는 방법을 고찰한다. 즉, 하나의 워터마크는 저작권 보호를 위한 것이고 다른 하나는 디지털 영상의 기밀성과 복제물 추적기능을 위한 것이다.

제안한 방법은 디지털 영상의 기밀성을 위해 별도의 암호화 방법을 사용하지 않고 직접 원 영상에 워터마크를 삽입함으로써 영상의 기밀성을 간편하게 처리할 수 있다. 디지털 영상의 저작권 보호를 위한 워터마크는 기존의 워터마크의 요구사항, 즉, 워터마크가 보이지 않아야 하고, 영상의 질을 떨어뜨리지 않아야 하고 디지털 영상처리, 압축 등에 견고해야 한다는 요구사항을 만족해야 한다.

디지털 영상의 기밀성과 복제물의 추적을 위해 원 영상의 소유자는 수신자의 정보를 바탕으로 워터마크를 생성한다. 이렇게 생성된 워터마크를 영상에 삽입하는 과정에 워터마크를 보이지 않게 하는 파라미터를 수신자의 공개키로 수정하여 영상에 삽입될 워터마크를 임의의 형태로 보이게 한다. 이렇게 함으로써 제3자는 임의의 형태의 워터마크로 덮여진 영상을 인식할 수 없게 된다. 영상의 허가된 수신자는 자신의 개인키로 파라미터를 복호화해서 워터마크를 보이지 않게 함으로써 원 영상을 볼 수 있게 된다. 그러나 무단으로 영상을 복제할 경우에 영상에 남아 있는 수신자 정보로 생성된 워터마크를 검출함으로써 복제자를 쉽게 식별할 수 있게 된다.

본 논문의 2장에서는 기존의 워터마킹 방법을 간략하게 소개하고 3장에서는 제안한 다중워터마킹 방법을 기존의 제안된 워터마킹 방법에 적용해서 알아보고 4장에서 결론을 맺는다.

2. 워터마킹 개요

워터마킹이란 디지털 영상 ,음성, 비디오 등 멀티미디

어 정보에 저작과 소유에 관한 정보를 넣음으로써 저작권을 보호하기 위한 방법이다. 즉 멀티디미어 정보에 외관상 드러나지 않는 정보를 삽입함으로써 저작권과 소유권을 보호하는 것이다.

2.1 워터마크의 요구사항

간략하게 워터마크의 요구사항을 정리해 보면 다음과 같다[1][3].

- 비가시성(Invisibility) : 워터마크는 일반 사용자에게 보여지지 않아야 하고, 컨텐트의 질을 감퇴시키지 않아야 한다.
- 강인성(Robustness) : 워터마크는 제거가 어려워야 한다. 컨텐트에 변형을 가해도 저작권을 주장하기 위해 워터마크가 남아있어야 한다. 일반적인 변형에는 D/A, A/D변환, 재 양자화(requatization)등과 같은 일반적인 디지털 신호처리와 영상의 회전, 이동, 자르기, 확대/축소등과 같은 기하학적인 처리 등이 있다.
- 명확성(Unambiguity) : 워터마크를 검색함으로써 자신의 저작권을 분명히 주장할 수 있어야 한다.

2.2 워터마킹의 여러 가지 방법

기본적인 워터마킹 과정은 워터마크 삽입과 워터마크 검출로 나눌 수 있다.

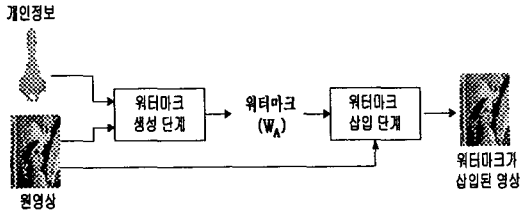

그림 1. 워터마크 삽입과정

워터마크는 그림 1에서와 같이 개인정보(개인키, 개인ID등)와 원 영상을 가지고 워터마크를 생성해서 원 영상에 삽입한다.

워터마크 검출과정은 그림 2에서와 같이 개인정보와 수신된 영상을 가지고 워터마크를 생성해서 주어진 임계치와 비교해서 워터마크를 판명한다. 또한 워터마크의 생성영역에 따라 공간영역에서의 워터마크와 주파수 영역에서의 워터마크로 나눌 수 있는데, 공간영역에서의 워터마크는 원 영상의 밝기의 세기를 변화시키거나 영상내 임의의 패턴을 삽입하는 방법으로 워터마

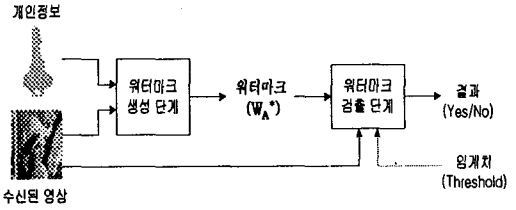

그림. 2 워터마크 검출과정

크를 생성하고, 주파수 영역에서의 워터마크는 주파수의 범위에 따른 인간시각의 서로 다른 특성을 이용하여 워터마크를 생성한다. 즉 DCT나 DFT, 혹은 wavelet 변환을 통해 얻은 주파수 성분의 계수에 워터마크를 삽입함으로써 영상내 텍스쳐 영역과 같이 시각적으로 덜 민감한 주파수 영역에 워터마크를 삽입하는 것이다.

3. 다중워터마킹 방법

앞장에서 언급한 워터마크 요구사항을 만족하는 두 개의 워터마크와 수신자 공개키로 저작권 보호와 영상의 기밀성과 복제물 추적이 가능한 다중워터마크 방법을 제안한다.

3.1 다중워터마킹 방법의 제안

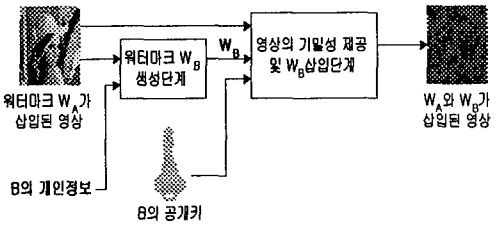

그림. 3 다중워터마크 삽입과정

제안한 다중워터마킹 방법은 그림 3에서 보는 바와 같이 원 영상 소유자의 저작권 보호를 위한 워터마크 W_A가 삽입된 영상과 수신자(B) 정보로 워터마크 W_B을 생성한다. 워터마크 W_A와 워터마크 W_B는 2장에서 기술한 워터마크의 요구사항을 만족한다고 가정한다. 영상의 기밀성을 제공하기 위해서 B의 공개키로 워터마크 W_B가 비가시성을 가지기 위해 사용했던 파라미터를 암호화해서 나온 결과를 이용해 미리 워터마크 W_A가 삽입된 영상에 삽입한다. 암호화해서 나온 결과가 랜덤하고 가시성을 가지도록 적합한 암호알고리즘을 선택했다고 가정한다. 그래서 워터마크 W_A와 워터마크 W_B가 삽입된 영상은 제 3자가 알아볼 수 없는

영상이 된다.

원 영상의 소유자(A)는 자신의 저작권 보호를 위한 워터마크 W_A와 원 영상의 기밀성과 복제물의 추적을 위한 워터마크 W_B가 삽입된 영상을 사용자(B)에게 전송한다. 사용자(B)는 그림 4와 같이 자신의 개인키를 이용해서 공개키로 암호화된 가시성 파라미터를 복호화한 후 디지털 영상을 처리하여 가시성이 제거된 영상을 획득한다.

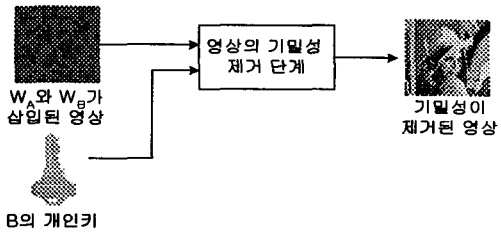

그림. 4 디지털 영상의 기밀성 제거과정

가시성이 제거된 후에도 영상에는 워터마크 W_A와 워터마크 W_B가 남아있기 때문에 만약 사용자(B)가 영상을 무단으로 복제하여 배포할 경우에 복제된 영상에 남아있는 워터마크 W_B를 원 영상 소유자가 검출함으로써 불법복제자(B)를 식별해 낼 수 있다.

3.2 제안한 다중워터마킹 방법 적용 예

Langelaar가 제안한 워터마킹 방법을 본 논문에서 제안한 다중워터마킹에 적용해 본다[1][7].

Langelaar가 제안한 워터마킹 방법은 영상의 밝기가 50%인 픽셀에 워터마크 삽입레벨인 상수 k를 더해서 영상에 워터마크를 삽입하는 방법이다.

워터마크를 삽입하는 과정은 다음과 같다.

① RGB 칼라 영상을 YUV 영역으로 변환한다.
U와 V(색차)값은 Y(luminance)값 보다 JPEG 압축 알고리즘에 의해 영향을 더 많이 받기 때문에 Y값만으로 워터마킹을 수행한다.

② 워터마크를 삽입하기 위해 Y영상을 일정한 크기의 블록 B로 나눈다.

③ 블록과 동일한 크기의 "0"과 "1"로 구성되어 있는 고정된 이진 가상 랜덤 패턴P를 생성한 후, 삽입레벨 k를 k_0로 놓는다.
여기서, P 블록의 "1"과 "0"의 비는 1 : 5로 한다.

④ 워터마크 비트 "0"을 삽입 할 경우, R=B-k*P.
워터마크 비트 "1"을 삽입 할 경우, R=B+k*P.

⑤ 랜덤 패턴 P=0에서의 블록 R의 밝기 값의 평균 I_0와 랜덤 패턴 P=1에서의 블록 R의 밝기 값의 평균 I_1 계산하여 high quality 차인 $D_{high} = I_1-I_0$을 계산한다.

⑥ 블록 R의 값들을 T에 임시로 저장하고, 블록 T의 품질을 8×8 DCT변환을 통해서 줄이고, 역 DCT 변환에 의한 특정 quality factor Q로 계수를 양자화 한다. 그리고 ⑤에서 했던 것과 마찬가지로 낮은 품질의 블록 T에 대한 low quality 차 $D_{low} = I_1-I_0$을 계산한다

⑦ 워터마크 비트 "0"이 삽입되어 있고 D_{high}, D_{low}중 하나라도 0보다 크면, 삽입 레벨 k를 1 증가시키고, D_{high}, D_{low} 값 모두가 0 이하이거나 k가 k_{max}일 때까지 과정 ④ ~ ⑦을 반복한다. 만약 워터마크 비트 "1"이 삽입되어 있고 D_{high}, D_{low}중 하나라도 특정 임계치 T보다 작으면, 삽입레벨 level k를 1 증가시키고, D_{high}, D_{low} 모두 T보다 크거나 k가 k_{max}일 때까지 과정 ④ ~ ⑦을 반복한다.

⑧ 블록 B를 블록 R로 대체한다.

⑨ 워터마트의 모든 비트들이 삽입될 때까지 과정 ②~⑧을 반복한다.

⑩ 마지막으로 YUV 값을 RGB 영역으로 바꾼다.

사용자의 저작권 보호를 위한 워터마크 W_A를 위와 같은 방법으로 영상에 삽입하고 기밀성과 복제물 추적을 위한 워터마크 W_B을 영상에 삽입할 때 기밀성을 제공하기 위해서 가시성에 관련된 블록 R을 사용자(B)의 공개키를 암호화 해서 나온 결과(V)로 대체한다. 마찬가지로 사용자(B)가 가시성을 제거하기 위해서 자신의 개인키로 블록 V를 복호화 해서 원 블록 R로 대체한 후 YUV값을 RGB 영역으로 바꾸면 비가시성인 워터마크 W_A와 워터마크 W_B가 삽입된 영상을 얻게 된다.

워터마크를 검출하는 과정은 다음과 같다.

① RGB 칼라 영상을 YUV 영역으로 변환한다.

② 워터마크 비트를 읽기 위해 Y 이미지로부터 순서적으로 블록 B를 선택한다.

③ 블록과 동일한 크기의 "0"과 "1"로 구성되어 있는 고정된 이진 가상 랜덤 패턴P를 생성한다.

④ 랜덤 패턴 P=0에서의 블록 R의 밝기 값의 평균 I_0 계산하고 또한 랜덤 패턴 P=1에서의 블록 R의 밝기의 평균 I_1 계산하여 차 $D = I_1-I$ 계산해 낸다

⑤ 만약 D의 값이 0보다 크면, 블록에 삽입되어 있는 값은 1, 그렇지 않으면 0.

⑥ 워터마크의 모든 비트가 추출될 때까지 과정 ② ~ ⑤를 적용한다.

영상에 삽입된 워터마크 W_A와 워터마크 W_B를 ① ~ ⑥과정을 통해 검출할 수 있다.

본 논문에서 제안한 다중워터마킹 방법은 기존의 제시된 여러 워터마킹 기법에도 또한 적용할 수 있을 것이다.

그림. 5 원 영상

그림. 6 W_A가 삽입된 영상

그림. 7 W_A와 W_B가 삽입된 영상

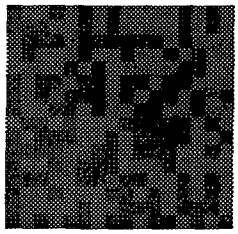

그림. 8 기밀성이 부여된 영상

4. 결론

본 논문에서는 저작권 보호기능과 영상의 기밀성 및 복제물 추적 기능을 제공하기 위한 다중워터마킹 방법을 제안했다. 제안한 다중워터마킹 방법은 워터마크가 삽입된 영상에 기밀성을 제공하기 위해 영상을 암호화하는 기존의 방법대신에 두 개의 워터마크와 수신자의 공개키를 가지고 간단하게 영상의 기밀성과 복제물 추적이 가능한 방법을 제시했다. 앞으로 음성이나 동영상등 모든 멀티미디어 서비스에도 적용 가능하도록 더 많은 연구가 진행되어야 할 것이다.

[* 본 연구는 '98 한국과학재단의 핵심전문연구비 (981-0928-155-2)지원으로 수행된 결과임]

참고문헌

[1] I. J. Cox, J. Kilian, T. Leighton, and T.Shamoon, "Secure spread spectrum - watermarking for images, audio and video", Proc ICIP'96, vol.3, pp.243-246, 1996.

[2] Nasir Memon, and Ping Wah Wong, "Protection Digital Media Content",Communications of ACM, vol.41, pp.35-43, July 1998.

[3] I. J. Cox, J. Kilian, T. Leighton, and T.Shamoon, "Secure spread spectrum watermarking for multimedia", Technical Report 95-10, NEC Research Institute, Princeton, NJ, USA, 1995.

[4] P. W. Wong, "A public key watermark for image verification and authentication", In Proceedings of ICIP, Oct 1998.

[5] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for Data Hiding", Technical Report, MIT Media Lab, 1994.

[6] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures", Proceeding of ICASSP'96, pp.2168-2171, Atlanta, Georgia, May 1996.

[7] G. Langelaar, J. C. A and J. Biemond, "Copy Protection for multimedia Data based on Labeling Techniques", Proc. of 17th Symposium on Information Theory in The Benelux, Enschede, The Netherlands, May 1996.