Hash 함수를 이용한 디지털 영상의 내용기반 인증방법

임현[1], 박순영[2], 조완현[3]

Abstract

우리는 본 논문에서 디지털 영상에 대하여 Hash함수를 이용한 내용기반의 안전한 워터마킹 인증기술을 제시하려고 한다. 허가되지 않는 이미지의 내용변경을 막기 위해 안전한 워터마킹 시스템을 개발하기 위하여 비밀키를 가지고 있는 Hash 함수가 사용되었고, 각 블록의 워터마크신호는 Hash함수의 출력결과를 Seed로 사용하여 의사난수를 발생시킨 값에 따라 생성되어진다. 이미지 기술벡터들은 블록기반 에지 이미지로부터 측정되는데 이 값들은 해롭지 않는 조작 등에 대해서는 쉽게 변화하지 않지만 고의적인 내용변경 등의 조작에 대해서는 이들 값들이 바꾸어지는 성질을 갖고 있다. 워터마크신호의 삽입은 블록기반 스펙트럼 방법에 기초를 두고 있으며 워터마크신호의 크기는 인지성과 강인성이 조화를 이루도록 AC 부 밴드의 지그재그 스캔라인의 DCT 계수들의 지역적인 통계량에 따라 조정되어진다. 또한 저작권인증의 확인을 위한 경계 값의 선택은 통계학적으로 분석되어진다. 수치적인 실험의 결과는 제안된 기술이 강력한 저작권인증의 수행을 위해서 매우 효율적인 것을 보여주고 있다.

주요용어 : 워터마킹기법, 영상기술벡터, Hash 함수, 상관계수 탐색통계량, DCT계수

1. 서론

멀티미디어 매체 정보에 대한 급속한 저장기술과 인터넷 전달기술의 발달오 인하여 주어진 영상에 대한 내용인증 기술들이 요구되고 있다. 인증의 목적은 초기의 내용이 특별한 수준까지 수정되지 않았음을 입증하는 것이다. 최근에 다양한 디지털 워터마크기술들이 디지털 멀티미디어의 내용인증의 수단으로 제안되어 지고있다. 만족스러운 인증업무를 위해서는 이미지에서 발생되는 부분적인 내용변경이나 고의적인 조작 등과 해롭지 않는 영상의 조작 등을 구별할 수 있는 인증방법들이 필요하게 된다. 연기서 해롭지 않는 영상의 조작은 잡음의 첨가 및 높은 질의 압축 손실과 같은 합법적인 왜곡을 의미한다. 이와 반대로 고의적인 조작은 압축손실의

1) 목포대학교 전자공학과 박사과정
2) 목포대학교 전자공학과 교수
3) 전남대학교 통계학과 교수

낮은 질과 원래의 내용이 파괴 될 수 있는 이미지 객체의 제거 등을 의미한다.

이미지의 인증방법은 임의의 조작에 대하여 그들을 탐지하는 기술 등에 따라 넓게 2개의 영역으로 나눌 수 있다. 하나는 깨지기 쉬운(fragile) 워터마크의 접근방법과 다른 하나는 강건한(robust) 워터마크의 접근방법이다[1]. 깨지기 쉬운 워터마크의 접근방법은 영상에 대한 임의의 조작이 삽입된 워터마크를 파괴할 수 있다는 가정아래에서 시작되었다. Yeung et al.은 한 영상에 이진 워터마크가 삽입된 키-종속 함수에 의한 의사난수를 사용하여 이미지에 대한 어떠한 수정이 검출(탐색)되게 하였다[2].

최근에, 강력한 워터마킹 방법에 의한 이미지 저작권 보호는 깨지기 쉬운 워터마크기술과는 달리 해로운 조작과 해롭지 않는 조작 사이의 구별을 가능하게 할 수 있다는 면에서 점차적으로 각광을 받게 되었다. 이러한 경우 어떤 조작도 삽입된 워터마크 그 자체에 영향을 주지는 못한다. 그러나 Hash 함수의 개념을 사용하여 삽입된 워터마크와 관련이 없는 다른 워터마크에서는 영향을 받는다[1,4].

본 논문에서 우리는 Hash함수를 사용한 강력한 워터마킹 기반 인증기술을 제안하려고 한다. 이미지 기술 벡터는 블록 기반의 에지 이미지로부터 측정되어지며 이러한 값들은 해로운 조작에 대해서는 쉽게 변하지만 해롭지 않은 조작에서는 쉽게 바뀌지 않는다. 이미지 기술벡터를 삽입함에 따라 암호학적인 Hash 함수에 비밀키를 연결시키게 되며, 우리는 Hash 결과를 가지고 시드 값으로 하여 의사난수를 발생하여 각 블록의 워터 마크를 발생한다.

2. 영상의 기술벡터의 추출

내용기반 영상 인증단계에서 영상기술벡터를 사용하는 주된 생각은 이미지의 중요한 정보는 에지 요소에 존재한다는 사실이다. 시각적인 내용(항목)을 묘사하는 특징벡터가 그림1과 같이 추출된다.

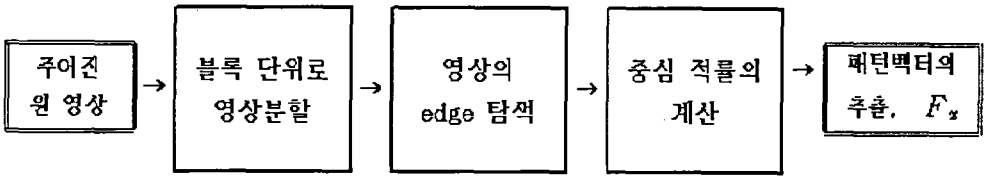

그림 1. 내용기반 패턴 벡터의 생성

우리는 이미지를 $I \times J$ 픽셀로 구성되는 블록으로 분할한 후 에지 연산자를 사용하여 각 블록으로부터 $I \times J$ 의 에지 이미지를 계산한다. 블록 이미지는 먼저 잡음을 제거하고, 고립된 요소를 제거하기 위해 메디안 필터를 사용하여 전처리 되어진다. 이때 우리는 이진 에지 요소를 찾기 위하여 경계값에 의한 Sobel 연산자를 이용하였다. 에지요소의 분포를 수량화하기 위하여 이들의 중앙모멘트들을 특징벡터로 계산하였다. 또한 특징벡터를 이용하여 각 블록의 이미지 기술벡터 F_k 를 얻을 수 있다. 이미지 기술벡터 F 는 차이가 있게 보이는 블록들에서 다른 결과를 가져오는 반면 유사하게 보이는 블록에서는 같은 비트의 결과를 보여준다.

암호학적인 Hash 함수는 임의의 길이를 갖는 비트열을 고정된 길이의 비트열로 바꾸어 준다. 우리는 Hash를 각 블록으로부터 다음과 같이 계산한다.

$$H(K \circ F_k \circ k) = (d_1 , \ldots , d_p) \quad (1)$$

여기서 K 는 비밀키이고, k 는 비트열에 대한 블록넘버이고, $\circ$ 은 연속연산자를 나타낸다. 여기서 Hash 함수는 K , F_k 그리고 k 의 입력을 사용하여 p 비트의 결과를 산출하게 된다. 본 논문에서, 우리는 p=128 일 때 Hash 함수로 흔히 잘 알려진 MD5 를 사용하였다.

3. 워터마크의 삽입과 검출절차

그림2는 이미지 인증을 위한 제안된 워터마크의 삽입과 검출을 위한 블록 다이어그램을 보여주고 있다. 원래의 이미지를 블록단위로 분할한 다음에 적절한 이미지의 내용을 기술하는 특징벡터의 집합을 추출하고, 이것을 Hash함수의 입력으로 사용한다. 저작권이 없는 영상의 무단복제를 탐지할 수 있는 안전한 워터마킹 시스템을 만들기 위해 비밀키를 가지고 있는 Hash 함수가 사용되어지며 각 블록의 워터마크의 결과는 Hash 함수의 출력결과를 가지고 의사난수를 발생시켜 산출한다. 워터마크 삽입과정은 스프레드 스펙트럼(Spread Spectrum) 방법과 유사하다[9,10]. 그러나 우리는 세밀함을 유지함과 동시에 강력한 워터마크를 삽입하기 위하여 어떤 고정된 상수 값을 사용하지 않고 부분적인 통계량을 적용하여 가변적인 α 값을 사용하는 방법을 이용한다.

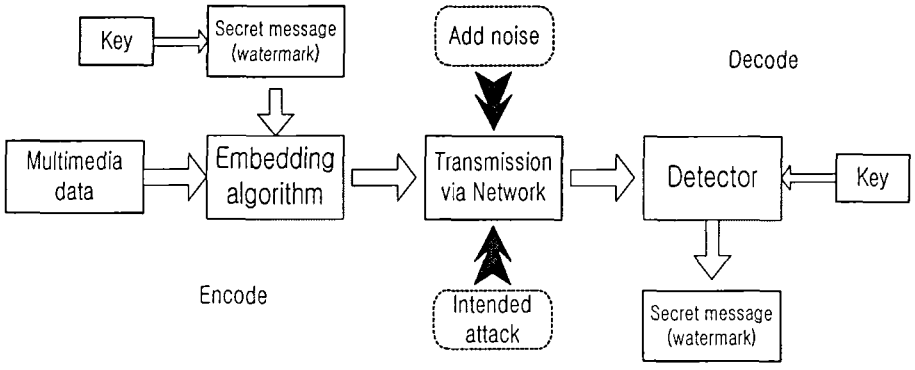

그림 2. 제안된 워터마크 시스템의 구조에 대한 블록그림

워터마크를 삽입을 위해서 그레이스케일 이미지를 $I \times J$ 픽셀 크기의 블록으로 분할한 후 각 블록에 대한 $I \times J$ DCT 계수를 계산한다. 우리는 v_{ij}^k 는 이러한 k 번째 블록의 (i, j) 위치의 DCT 계수이고, Ω_i 는 i 번째 지그재그로 읽어지는 DCT 계수들의 집합이다. 예를 들어 $\Omega_0 = \{(0,0)\}$, $\Omega_1 = \{(0,1) , (1,0)\}$ 등으로 주어진다.

워터마크 신호는 평균이 0 이고 분산이 1인 표준정규분포를 따르는 의사난수에 의해서 얻어진다.

$$W = \{w_0 , \ldots , w_{m-1}\} , \; w_j \sim N(0,1) \quad (2)$$

기호를 단순화하기 위하여 $X = \{x_0, \ldots x_{m-1}\}$ 는 블록 k 의 2차원 DCT $\{v_{ij}^k\}$ 의 AC 계수 부 밴드의 지그재그로 선택된 순서에서 길이가 m 인 DCT 계수의 결과이다. 워터마크가 삽입되는 계수는 다음과 같이 워터마크를 DCT 계수에 첨가함으로써 얻어진다.

$$x_i^w = x_i + \alpha |x_i| w_i, \; i=0, \ldots, m-1 \tag{3}$$

여기서 α는 워터마크의 이점에 맞게 선택되어진 파라메터이다. 워터마크에서 보다 더 큰 α 를 선택함으로서 워터마크가 더 시각적일 때 더욱 강력해 진다. 예전에 자주사용 되었던 고정된 경험적인 값들 대신에, 우리는 다음과 같은 DCT 계수의 부분적인 통계량에 따라 적응적으로 파라메터의 값을 추정하여 사용한다.

$$\alpha_i = \frac{s}{\log\left(\sum_{v_{ij}^k \in \Omega_i} |v_{ij}^k|\right)} \tag{9}$$

여기서 s는 곡선의 편차를 조절하는 척도요인이며 $v_{00}^k / \overline{v_{00}}$ 의 비율이다. 워터마크를 각 DCT 계수에 삽입한 후에 각 블록에 대한 역 DCT 변환을 취한 후 워터마크된 이미지 I^w 를 얻게된다.

4. 워터마크 탐색통계량의 성질

인증을 주장하는 한 가지 방법은 이미지를 몇 개의 블록으로 나누어서 각 블록에 따른 워터마크를 삽입하는 것이다. 그러면 우리는 이러한 워터마크들이 관측된 이미지 속에 존재하는지 존재하지 않는지 증명할 수 있을 것이다. 통계학적으로 이러한 문제를 풀기 위해서 우리는 다음의 두 가지 가설을 고려한다.

H_0 : 주어진 이미지의 각 블록의 내용에는 어떠한 변화도 발생되지 않는다.

H_1 : 주어진 이미지의 각 블록에 특정한 조작이 일어났다.

이때 우리는 주어진 영상을 크기가 $(l \times l)$ 인의 L 개의 블록으로 나누고, DCT 변환을 이용하여 각각 나누어진 블록영상에 대하여 DCT 계수를 계산한다. 이때 우리는 관측된 영상의 어떤 블록에 대하여 위조나 어떠한 조작이 일어났을 때 이것을 탐지할 수 있는 통계량으로 다음의 상관계수 탐색통계량을 사용할 수 있다.

$$R_k = \frac{1}{m} \sum_{i=0}^{m-1} x_i^* w_i^* \tag{4}$$

여기서 m은 워터마크가 삽입된 각 블록의 DCT 계수의 전체 수이다.

만약 귀무가설 H_0 가 사실이면 DCT 계수들은 삽입된 워터마크와 동일한 워터마크를 포함한다. 따라서 이들은 관측된 블록 이미지로부터 다음과 같이 계산되어진다.

$$x_i^* = x_i + \alpha |x_i| w_i + \varepsilon_i \tag{5}$$

여기서 w_i는 삽입된 워터마크 신호를 나타내며 ε_i 는 추정오차를 나타낸다. 만약 관측 이미지가 주어진 원 영상과 일치한다면 두 종류의 워터마크가 정확히 같다. 따라서

$$w_i^* = w_i \;, \quad i=0, \cdots, m-1$$

이고, 탐색통계량은 다음과 같이 주어진다.

$$R_k = \frac{1}{m}\sum_{i=0}^{m-1}(x_i + \alpha|x_i|\,w_i + \varepsilon_i)w_i \tag{6}$$

이때 주어진 탐색통계량의 평균과 분산을 계산할 수 있고, 이들은 각각 다음과 같이 주어진다.

$$\mu_k = E[\frac{1}{m}\sum_{i=0}^{m-1}(x_i + \alpha|x_i|\,w_i + \varepsilon_i)w_i] = \frac{1}{m}\sum_{i=0}^{m}\alpha E[|x_i|] \tag{7}$$

$$\sigma_k^2 = \frac{1}{m^2}E(\sum_{i=0}^{m-1}(X_i + \alpha|X_i|\,W_i + \varepsilon_i)W_i)^2 - (\frac{1}{m}\sum_{i=0}^{m-1}\alpha E[|X_i|])^2$$

$$= \frac{1}{m^2}\sum_{i=0}^{m-1}((1+3\alpha^2)E(|x_i|^2) + N\cdot\sigma_\varepsilon{}^2) - \frac{1}{m^2}\sum_{i=0}^{m-1}\alpha^2 E[|x_i|]^2 \tag{8}$$

또한 중심 극한정리를 사용하면 탐색통계량의 분포는 대략적으로 정규분포에 근사하며 따라서 귀무가설을 기각하는 영역은 유의수준 γ 에서 다음과 같이 주어진다.

$$R_k \le \mu_k - z_\gamma \frac{\sigma_k}{\sqrt{m}}\ ,\ k=1,\cdots L.$$

5. 실험결과

제안된 워터마크방법을 평가하고 이론적인 결과를 입증하기 위해 우리는 그림3(왼쪽)에 보여지는 512 ×512 크기의 Girls 영상을 64 ×64 크기의 블록영상으로 분할하고, DCT 변환을 적용하였다. 각 블록의 DCT 계수들로부터 우리는 이미지 기술벡터 F_k 와 워터마크를 삽입하기 위한 강한 α 값을 계산하였다. 그림3 (오른쪽)은 블록기반 스프레드스펙트럼과 Hash 함수를 사용하여 원 영상에 보이지 않는 워터마크를 삽입한 결과를 보여준다. 우리는 이미지 기술벡터 F_k 는 압축손실과 첨가된 잡음이 있는 영상에서 더 잘 반응한다. 반면에, 만약 워터마크된 이미지의 어떤 부분들이 편집들에 의해서 수정이 된다면 그때 이미지 기술벡터의 값도 또한 변하게 된다.

그림3 원영상

다음으로 우리는 워터마크가 존재하지 않는 경우와 워터마크가 삽입된 경우에 대한 상관계수 탐색 통계량을 계산한다. 우리가 그림4 에서 볼 수 있듯이 삽입된 워터마크에 대한 탐색통계량은 항상 워터마크가 삽입되지 않은 경우의 탐색통계량보다 항상 더 높고 넓게 나타난다. 워터마크가 삽입된 이미지의 상관계수의 평균값과 워터마크가 삽입되지 않은 이미지의 상관계

수의 평균값은 각각 2.0과 0.0이다. 따라서 워터마크의 존재는 저작권의 보호를 입증하는데 쉽게 이용될 수 있다..

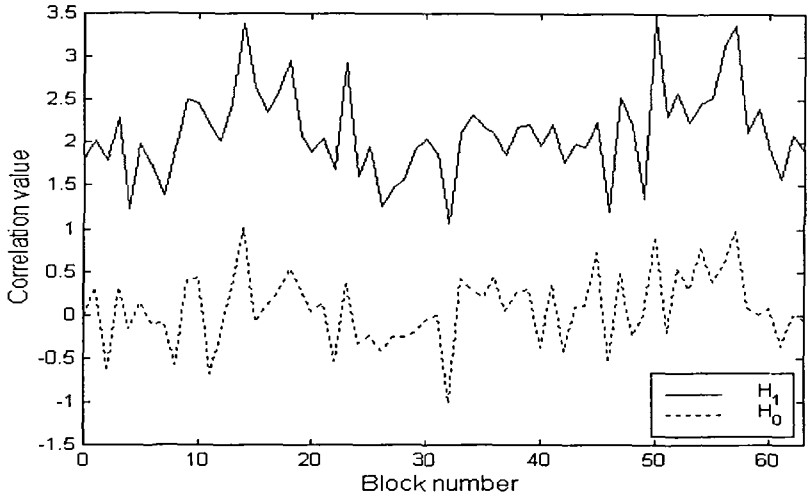

그림4 워터마크가 삽입된 영상에 대한 탐색통계량의 결과
(solid line : 워터마크가 삽입된 영상, dotted line : 워터마크가 없는 영상)).

다음 그림5 는 내용인증 이미지로서 워터마크가 삽입된 이미지에 대한 탐색통계량의 결과를 보여주고 있다. 원 영상이 의도된 조작에 의하여 수정되었을 때 이 부분영상에 대한 탐색통계량의 값은 $Z_\gamma = 0.1$ 정도로 이것은 가설을 기각하는 경계 값보다 더 작게 주어진다. 그러므로 우리는 미리 정의 된 경계 값을 각 블록의 상관계수와 비교하여 내용인증을 증명할 수 있다.

그림5 (a) 변형된 워터마크 영상(앞이 부분), (b) 변형된 영상에 대한 블록부분

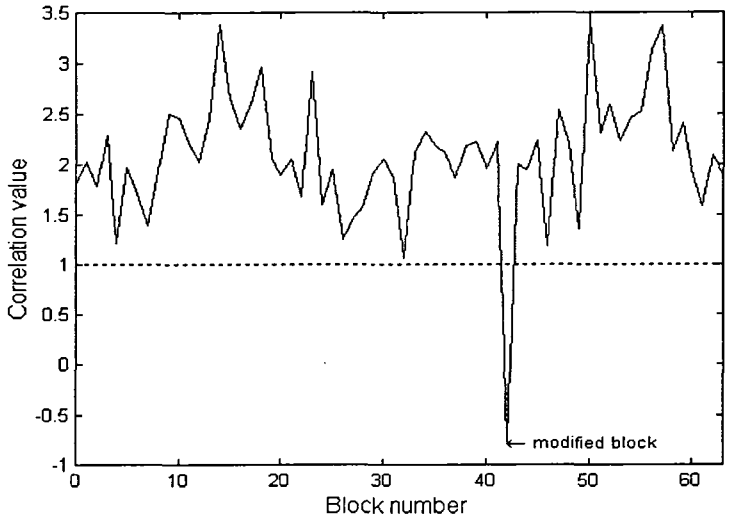

그림5(c) 변화가 일어난 각 블록에 대한 탐색통계량의 값

6. 결론

본 논문에서 우리는 Hash 함수를 사용한 강력한 워터마킹 기반의 인증기술을 제시하였다. 이미지 기술벡터는 블록기반의 에지 이미지로부터 추정되어지며 이 값은 해로운 조작에 의해서는 쉽게 바뀌지는 반면 해롭지 않는 조작에 대해서는 쉽게 바뀌지 않는다. 암호학적인 Hash 함수들에 연속적인 비밀키를 이미지 기술벡터에 입력함으로서 우리는 Hash 결과를 가지고 의사난수를 발생시켜 각 블럭 기반의 삽입된 워터마크를 생성하였다. 우리는 또한 부분적인 통계량을 사용함으로써 워터마크의 장점에 의해 강력한 워터마크를 보여줄 수 있다. 워터마크 탐지의 통계학적인 분석에 있어서 일반화 가우시안 분포가 사용되었으며 경계 값은 적절한 유의수준에서 결정되었다. 이 실험은 제안된 기술이 저작권의 입증과 내용인증의 수행에 매우 효과적이라는 사실을 보여주고 있다.

참고문헌

[1] F. Barrolini, A. Tefas, M. Barni and I. Pitas, "image Authentication Techniques fir Surveillance Applications," Proceedings of IEEE Trans. On Image Processing , 89(10), Oct.2001, 1403-1418.

[2] M. M. Yeung and F. Minzer, "An invisible watermarking technique for image verification", Proc. ICIP97, Santa Barbara, CA, Oct. 1997, 680-683.

[3] P. W. Wong and N. Memon, "Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification", Proceedings of IEEE Trans. On Image Processing, Oct. 2001, 1593-1601.