論文 97-22-8-23

디지털 영상의 저작권 보호를 위한 새로운 서명 문양

正會員 서 정 일*, 우 석 훈*, 원 치 선*

A new watermark for copyright protection of digital images

Jung Il Seo*, Seock Hoon Woo*, Chee Sun Won* *Regular Members*

요 약

본 논문에서는 디지털 영상 정보의 저작권 보호를 위한 새로운 디지털 서명 문양(Watermark) 방법을 제안한다. 특히, 제안된 디지털 서명은 기존의 서명 방법과 비교하여 압축 환경에 대한 고려와 함께 불법적인 재서명 공격에 대응할 수 있도록 하였다. 또한, 서명 문양의 비화도를 증가시키기 위해서 기존의 난수 XOR의 방법을 사용하지 않고, 서명 문양을 원영상에 단순 연산하는 방법으로 원영상에 대한 서명 문양의 영향을 최대화하였다. 그리고, 문양의 검출시 발생되는 오차를 줄이기 위해 영상을 블록 단위로 특성을 분류한 후, 최소 압축 손실 블록을 선정하고, 그 블록에 대해서만 문양을 검출하므로써 압축 손실에 강한 서명 문양이 되도록 하였다. 또한, 극복할 수 없는 압축 손실은 가설 검증(Hypothesis Testing) 이론에 의한 확률적인 방법을 도입하였다. 이 밖에 서명 영상에 대한 제 3의 공격에 대해서도 원영상과 사용자 영상의 평균 자승 오차(MSE, Mean Square Error) 비교를 통해 확률적으로 문양을 검출하므로써 대비하였다. 제안된 서명 방법의 컴퓨터 시뮬레이션 결과 새로운 문양 방법은 양자화 에러와 제 3의 서명 공격에 더욱 강하다는 것을 확인하였다.

ABSTRACT

In this paper, we present a new digital signature for copyright protection of digital images. The proposed algorithm is designed to be more robust to both the compression (quantization) errors and the illegal signature attack by a third party. More specifically, to maximize the watermarking effect, we embed the watermark by randomly adding or subtracting a fixed number instead of executing the XORs. Also, to improve the reliability of the watermark detection, we extract the watermark only on some image blocks, which are less sensitive to the compression errors. Futhermore, the unrecovered compression errors are further detected by the Hypothesis testing. The illegal signature attack of a third party is also protected by using some probabilistic decisions of the MSE between the original image and the signed image. Experimental results show that the proposed algorithm is more robust to the quantization errors and illegal signature attack by a third party.

*동국대학교 전자공학과
論文番號:96391-1216
接受日字:1996年 12月 16日

Ⅰ. 서 론

디지털 영상은 기존의 아날로그 영상과 비교하여 영상 정보의 저장과 편집이 매우 간편한 장점을 갖는다. 하지만 영상을 디지털화함으로써 생기는 이러한 장점은 누구나 디지털 영상의 내용을 손쉽게 변형 및 복제할 수 있는 단점이 되기도 한다. 지금까지는 인증(authentication)을 위한 별도의 서명문(고전적인 의미)을 생성하여 이 서명문을 원정보와 함께 전송하므로써 사용자와 제공자의 권익을 동시에 보호하였다. 하지만 정보량이 매우 크고, 실시간 처리가 중요시되는 디지털 영상의 경우는 고전적 의미의 서명문을 이용할 경우 전송 정보량이 더욱 커지고 서명문 관리가 어렵다는 단점이 있다. 또한 점차 일반화되어 가는 멀티미디어와 네트워크 환경에서 어느 특정 이용자를 전제로 정보를 제공한다는 것은 무의미하다. 최근 대두되는 새로운 의미의 디지털 서명은 네트워크 상에 존재하는 모든 이용자들이 누구나 자유롭게 정보를 이용할 수 있도록 하면서 정보 제공자가 차후에 정보 이용에 대한 권리를 주장할 수 있도록 제안된 방법이다[1]. 새로운 의미의 디지털 서명 방법은 영상의 시각적인 특성을 이용하여 영상에 직접 임의의 변화를 주고, 저작권의 확인이 필요할 때는 서명 문양(watermark)이라고 불리는 이 변화를 검출하므로써 영상의 저작권 또는 소유권을 주장할 수 있는 근거를 마련할 수 있도록 하였다. 이 서명 문양 방법은 정보량이 증가하지 않고, 실시간 처리가 보다 용이한 장점을 갖는다. 서명 문양 방법은 인증을 위한 서명과는 달리 정보의 소유자와 이용자의 권리를 동시에 보호하는 차원이 아니고, 일반 대다수의 이용자를 전제로 정보의 소유권만을 보호하는 것이다. 즉, 서명 문양은 인증에 비해 협소한 의미를 가지는 디지털 서명의 한 방법이라고 할 수 있다[1]. 본 논문에서는 디지털 서명을 서명 문양을 이용한 저작권 보호책으로만 한정하여 사용한다.

서명 문양(watermark)[1]은 정보에 가해지는 임의의 변화 모두를 나타내지만, 대체로 두 가지의 형태로 나타난다. 그 중 하나는 서명값을 이용하는 것이고, 나머지 하나는 스탬프(seal or stamp)를 사용하는 것이다. 이 두 종류의 서명 문양은 모두 다음과 같은 전제 조건을 만족해야 한다[1][2].

- 삽입된 문양은 시각적으로 구별되지 않아야 한다.
- 영상의 저작권자 및 소유권자는 서명 문양을 쉽고 안전하게 검출할 수 있어야 한다.
- 손실 압축(Lossy compression)이나 필터링(Filtering)과 같은 디지털 영상 처리 기법 등에 대하여 서명 문양이 영향을 받지 않아야 한다.
- 서명 영상(Signed image)에 대해 제 3 의 디지털 서명 공격에 강해야 한다.

본 논문에서는 위의 디지털 서명을 위한 전제 조건에 모두 합당한 방법을 모색한다. 우선 서명값을 이용한 안정적인 검출과 서명 영상의 비화도를 높이는 방법을 연구한다. 본 논문의 구성은 다음과 같다. 제 Ⅱ절과 Ⅲ절에서는 서명 문양 검출시 발생되는 압축 손실 영향을 최소화하는 방법과 효과적인 디지털 서명의 삽입 방법, 그리고 서명 문양을 안정적으로 검출하는 기준(Detection Criteria)을 제안하며, 불법적인 재서명 공격에 대응책을 제안한다. 제 Ⅳ절에서는 제안된 디지털 서명 기법을 컴퓨터 시뮬레이션을 통해 실험적으로 검증하였다. 마지막으로 결론에서는 제안된 디지털 서명 기법의 장단점에 대하여 설명한다.

Ⅱ. 제안된 서명 문양 삽입 방법

N × N 2차원 픽셀의 집합 Ω내의 디지털 영상을 I, 픽셀 (n, m)에서의 영상의 밝기가 그레이 레블 L중의 하나인 x_{nm}이면,

$$I=\{x_{nm} | 0 \le x_{nm} \le L-1, (n, m) \in \Omega\} \quad (1)$$

$$\Omega=\{(n, m) | 0 \le n \le N-1, 0 \le m \le N-1\} \quad (2)$$

이다. 기존의 디지털 서명 방법[2][4][5]은 발생된 난수

1. 서명 문양(Watermark): 일반적으로 서명 문양(Watermark)은 두 가지의 형태로 구분된다. 서명값을 이용하는 경우와 또 다른 방법으로는 이진 영상을 이용하는 경우이다. 본 논문에서는 서명 문양을 이러한 관점에서 서명값(Signature value)과 스탬프(Signature stamps or seals)로 나누어 부르기로 한다.

비트를 원영상의 하위 비트에 XOR(Exclusive-OR)하므로 서명 대상 영상 면적의 픽셀 중에 평균적으로 약 50%의 픽셀만 분양이 삽입된다. 따라서 보안성과 불법적인 공격 및 압축이나 전송 에러에 그만큼 약하다는 단점이 있다. 이와 같은 단점을 극복하기 위해 본 논문에서는 서명 대상 영상 면적 전체의 픽셀에 분양이 삽입될 수 있도록 하였다. 본 논문에서 제안하는 디지털 서명을 위한 분양 삽입 과정은 다음과 같다. 분양의 삽입을 위한 서명 함수 S를 식 (3)과 같이 정의한다. 서명 함수 S는 원시 다항식(primitive polynomial)으로부터 발생되는 이진 난수의 집합이다.

$$S=\{s_{nm}|s_{nm}\in\{0,1\},(n,m)\in\Omega\} \tag{3}$$

본 논문에서 제안한 서명 알고리즘은 한정된 하위 비트에만 영향을 미치던 기존의 방법과는 달리 모든 비트에 영향을 미칠 수 있도록 하고, 영상내 서명값에 의해 변화되는 픽셀도 50%에서 영상의 전 픽셀로 확대시켰다. 즉, 식 (4)와 (5)에서와 같이 발생된 난수에 따라 서명값 k가 더해지거나 빼진다.

$$\begin{aligned}A&=\{x_{nm}|s_{nm}=1,(n,m)\in\Omega\}\\B&=\{x_{nm}|s_{nm}=0,(n,m)\in\Omega\}\end{aligned} \tag{4}$$

$$C=\{c_{nm}|c_{nm}=\min(x_{nm}+k,L-1),x_{nm}\in A\}$$

$$D=\{d_{nm}|d_{nm}=\max(x_{nm}-k,0),x_{nm}\in B\} \tag{5}$$

$$I_s=C\cup D$$

여기서 I_s는 원영상 I에 대해 제안된 서명 기법으로 서명된 영상을 나타낸다. 식 (5)에서 보는 바와 같이 서명값 k를 삽입할 때, 기존 방법과 같은 논리적 연산이 아니고 단순 연산을 이용한다. 이 방법을 사용하기 위해 연산의 결과 그레이 레벨값이 L-1보다 크거나 0보다 작아질 수 있으므로 연산 결과의 최대값은 L-1, 최소값은 0으로 정의한다. 제안된 서명 삽입 방법은 논리적인 연산과 비교하여 서명값이 영상에 미치는 영향을 최대화하는 장점이 있다. 이것은 곧 서명값의 비화도가 증가하는 것을 의미한다. 동일한 2비트 서명값을 각각 XOR 방법과 제안된 방법으로 서명을 삽입하고 서명된 영상을 비교하면, XOR 방법을 이용한 경우 서명 영상의 각 픽셀마다 일정수의 LSB만이 변화하고, 전체 영상에서는 전 픽셀의 약 50% 정도만이 변화한다. 하지만, 본 논문에서 제안된 방법을 이용하면, 십진수로 나타낸 서명값이 직접 각 픽셀의 그레이 레벨값에 더해지거나 빼지므로 서명된 각 픽셀의 변화된 비트수는 일정 LSB로 한정되지 않고, 최소 1비트에서 최대 8비트(그레이 레벨이 256인 영상의 경우)까지 변화된다. 즉, 서명 영상의 변화 비트수가 일정한 것이 아니고 각 픽셀값마다 다르므로 서명값을 발견하기는 기존의 XOR 방법을 이용하

(a) 원영상 (b) 제안 서명 영상 (c) XOR 서명 방법

그림 1. 서명 영상과 원영상의 비교
Fig. 1 Original image vs. Signed image

는 것보다 어렵다. 한편, 서명 문양 k가 삽입된 서명 영상 I_s는 시각적으로 원영상 I와 구별되지 않아야 한다. 그림 1은 k = 3의 문양이 기존의 방법과 본 논문에서 제안된 방법으로 각각 서명된 영상과 원영상을 보여주고 있다. 그림에서 보듯이 서명 문양은 시각적으로 원영상과 구별되지 않는다. 그러나 서명값이 커지면 본 논문에서 제안한 방법의 경우는 영상 열화정도가 심해진다. 지나친 영상열화를 방지하기 위해서는 서명값의 범위를 한정해야 한다. 영상마다 제한되는 크기는 다르지만 일반적으로 서명값의 크기를 6이하로 하는 것이 적당하다[2]. 서명값의 제한으로 생길 수 있는 서명 비도는 주기가 매우 큰 의사 난수를 이용하여 극복할 수 있다. 그리고 본 논문에서는 서명 검출에서 블록 특성을 이용하기 때문에 이것 역시 서명값 제한의 단점을 보완할 수 있다. 결론적으로, 본 논문에서 제안하는 서명 문양의 삽입 방법은 기존의 서명 방법[2][4][5][6]과 비교하여 원영상의 시각적인 화질 열화를 일정 수준 유지하면서도, 픽셀의 한정 비트만 변화하는 것이 아니고 원영상 각 픽셀에 따라 변화되는 비트수가 다르므로 원영상에 미치는 서명 문양의 영향을 최대화하고 불법적인 공격에 대해서도 보다 강한 장점을 갖는다.

Ⅲ. 서명 문양 검출 기준

3.1 압축 환경에서의 서명 문양 검출

디지털 영상은 그 정보량이 매우 크므로 영상의 저장이나 전송을 위해서는 반드시 압축 과정을 거친다. 압축 방법은 사용자의 목적과 정보의 중요도에 따라 다양한 방법을 이용할 수 있지만, 일반적으로 압축률이 높은 손실 압축(Lossy compression)의 방법을 가장 널리 이용한다. 손실 압축 방법은 영상을 압축(Compression)/신장(Decompression) 과정에서 원영상 정보에 필연적인 손실을 준다. 그러나, 기존의 여러 디지털 서명 방법[2][5][6]은 압축 환경에 대한 고려가 거의 없었다. 본 절에서 제안하는 서명 기법은 실제 통신 시스템이나 멀티미디어 환경에서도 사용될 수 있도록 압축에 대한 영향을 고려하였다.

대부분의 영상 압축 방법들이 DCT를 기반으로 하는 압축 방법이므로 본 논문에서는 DCT를 기반으로 하는 JPEG 압축 표준안을 압축 환경의 예로 사용하였다. 본 논문에서 압축 방법으로 이용하는 JPEG 표준 압축의 압축 과정은 다음과 같다. 영상을 8×8의 블록으로 분할하여, 각각의 블록에 대해 식 (6)을 이용하여 영상을 DCT변환(Discrete Cosine Transform)한다.

$$X_{uv} = \frac{1}{4} C(u)C(v) \sum_{n=0}^{7} \sum_{m=0}^{7} x_{nm} \cos\left(\frac{(2n+1)u\pi}{16}\right) \cos\left(\frac{(2m+1)v\pi}{16}\right) \quad (6)$$

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{for } u = 0 \\ 1, & \text{for } u \neq 0 \end{cases}, \ (u, v) \in \Omega$$

식 (6)과 같이 얻은 DCT 계수 X_{uv}를 식 (7)과 같이 8×8 크기의 양자화(quantization) 테이블로 나누어 부호화하는 것이 JPEG 압축의 기본 알고리즘이다[7].

$$q_{uv} = \left\lfloor \frac{X_{uv}}{Q_{uv}} \right\rfloor \quad (7)$$

이때, u, v는 8×8 블록내 DCT 계수의 위치를 나타내며, 각각 $0 \le u \le 7$, $0 \le v \le 7$이다. 또, Q_{uv}는 양자화 테이블 (i, j)의 양자화 계수이다. 신장 과정에서는 역으로 다음의 식 (8)과 식 (9)를 사용한다. X_{uv}^{DQ}를 신장 과정에서 얻은 역양자화된 데이터이고, X_{nm}^{DQ}는 역 DCT변환(IDCT, Inverse DCT)된 픽셀의 그레이 레블값이라고 하면,

$$X_{uv}^{DQ} = q_{uv} \times Q_{uv} \quad (8)$$

$$X_{nm}^{DQ} = \frac{1}{4} \sum_{u=0}^{7} \sum_{v=0}^{7} C(u)C(v) X_{uv}^{DQ} \cos\frac{(2n+1)u\pi}{16} \cos\frac{(2m+1)v\pi}{16} \quad (9)$$

이때, JPEG에서 발생되는 압축 손실은 양자화 단계에서 발생되는 손실로 식 (10)과 같다.

$$\varepsilon_Q = |x_{nm} - X_{nm}^{DQ}| \quad (10)$$

식 (10)에서와 같이 발생되는 압축 손실은 영상 데이터 자체에는 많은 변화를 가져오지만 낮은 압축률에서는 실제 시각적으로 구별되지 않는다. 하지만, 영

상 데이터의 미세한 변화를 이용하는 서명 문양 방법에서는 매우 치명적인 약점이 된다. 이런 압축 손실을 극복하기 위해 다음절에서 영상의 압축 손실을 최소화할 수 있는 방안을 모색한다.

3.2 블록 특성별 압축 손실 비교

본 절에서는 압축 손실 계산을 각 특성 블록의 평균과 표본 분산(sample variance)을 구해 식 (11)과 같이 나타낸다. 영상을 블록 단위로 특성을 분류한 후 [3], 단순 블록(monotone block), 질감 블록(texture block), 및 에지 블록(edge block)으로 분류된 특성 블록의 픽셀들의 집합을 각각 M, T, E라 할 때, z 특성을 갖는 블록의 압축 손실은 아래와 같다.

$$\varepsilon_z \triangleq \frac{1}{|Z|} \sum_{(n,m)\in\Omega} (x_{nm} - x_{nm}^{rcv})^2 \qquad (11)$$

여기서, ε_z는 z 특성 블록(z는 M, T, 또는 E 중의 하나)의 압축 손실이고, |Z|는 z 블록의 픽셀수이며, x_{nm}^{rcv}는 복원 영상에서 z 특성 블록의 픽셀 그레이 레벨값이다. 식 (11)을 이용하여 Lena256, Baboon256 영상과 Couple256 영상을 실험한 결과 블록별 압축 손실은 표 1과 같이 단순 블록이 압축 손실에 가장 강하다는 것을 알 수 있다. 그러나, 압축 손실에 강한 단순 블록에 대해서만 서명 문양을 삽입하여도 실제로 압축 손실을 완벽하게 극복하기는 어렵다. 따라서, 본 논문에서는 영상에 삽입된 서명 문양을 검출하기 위해 가설 검증 (Hypothesis Testing) 이론에 근거한 t-percentile $t_{1-\alpha}$도 이용하였다. 가설 검증 이론은 가설 H_0와 H_1을 설정한 후에, test statistic q와 t-percentile $t_{1-\alpha}$를 비교하여 그 진위 여부를 판정한다. 판정 과정에서는 에러가 발생될 수 있는데, 이 에러를 Type Ⅰ과 Type Ⅱ 에러라고 한다. 각 표본 집단의 분산이 중첩되는 부분에서 Type Ⅰ과 Type Ⅱ 에러가 발생되고 만약 이 중첩 부분이 없거나 작다면, Type Ⅰ과 Type Ⅱ 에러의 상대적인 발생 확률도 작아질 수 있다. 결국, 본 논문에서 제안하는 서명 문양 방법은 표본 분산이 가장 작은 단순(monotone) 블록에서만 서명 문양을 검출한다. 에지(edge) 블록의 경우도 압축 손실은 작지만, 표본 분산이 가장 크기 때문에 Type Ⅰ과 Ⅱ 에러에 대해서는 매우 약하다. 즉, 압축 손실의 영향을 최소화하는 것도 중요한 관점이지만, 서명 문양 검출 시 발생될 수 있는 Type Ⅰ과 Ⅱ 에러를 최소화하는 것도 상당히 중요하다.

표 1. 256 × 256 영상별 압축 손실 비교
Table 1. The comparison of compression errors with 256 × 256 digital image

특성 블록	각 특성 블록별 압축 손실 비교		
	Lena	Baboon	Couple
Edge	62	101	24
Monotone	24	58	19
Texture	166	379	66

표 2. 256 × 256 영상별 분산 비교
Table 2. The comparison of variance with 256 × 256 digital image

특성 블록	각 특성 블록별 분산 비교		
	Lena	Baboon	Couple
Edge	1049	990	417
Monotone	58	118	59
Texture	1030	1038	822

3.3 서명 문양 검출

3.2절에서 언급하였듯이, 손실 압축 환경에서 디지털 영상은 압축 손실의 영향을 반드시 받는다. 이 압축 손실은 원영상과 비교하여 시각적인 차이는 별로 크지 않지만, 원영상의 변화를 검출하는 디지털 서명에는 매우 치명적인 약점이 될 수 있다. 따라서 본 논문에서는 3.2절의 실험 결과에 근거하여 일반적으로 압축 손실이 작은 단순 블록에서만 서명 문양을 검출하고자 한다. 일반적인 검출 기준(Detection criteria)을 찾기 위해 다음과 같이 가정할 수 있다. Hypothesis Testing 이론에서 test statistic q는 일반적으로 student distribution을 갖으며, 이것은 표본의 수가 30보다 큰 경우에는 근사화된 정규 분포를 이루는 특성을 갖는다[2][4][5]. 논문에서 제안하는 test statistic q는 최소한 블록에서 계산되므로 표본 픽셀의 수는 64개이므로 이 성질에 따라 충분히 정규 분포를 이룬다고 가정할 수 있다. 이 경우 표본의 평균과 분산은 모집단의 평균, 분산의 신뢰 구간 내에 존재한다[9]. 따라서

가설 검증(Hypothesis Testing)이론[8][9]을 이용하여 서명 영상에서 서명 문양 k를 찾을 수 있다.

$$\bar{\omega} = \bar{a} - \bar{b} \tag{12}$$

$$\bar{a} = \frac{1}{\alpha} \sum_{(n,\,m)\in C_{sign}} x_{nm} \tag{13}$$

$$b = \frac{1}{\beta} \sum_{(n,\,m)\in D_{sign}} x_{nm} \tag{14}$$

여기서, C_{sign}과 D_{sign}은 식 (15)에 의해 정의된다.

$$\begin{aligned} C_{sign} &= \{(n, m) \mid (n, m) \in M,\ s_{nm} = 1\} \\ D_{sign} &= \{(n, m) \mid (n, m) \in M,\ s_{nm} = 0\} \\ |C_{sign}| &= \alpha,\ |D_{sign}| = \beta \end{aligned} \tag{15}$$

식 (12)는 두 평균값의 오차를 결정하여 본 논문에서 검출 기준으로 이용할 다음의 test statistic q를 얻기 위한 것이다.

$$q = \frac{\bar{\omega}}{\sigma_{\bar{\omega}}} \tag{16}$$

여기서,

$$\sigma_{\bar{\omega}}^2 = \frac{s_a^2}{\alpha} + \frac{s_b^2}{\beta} \tag{17}$$

$$s_a^2 = \frac{1}{\alpha - 1} \sum_{(n,\,m)\in C_{sign}} (x_{nm} - \bar{a})^2 \tag{18}$$

$$s_b^2 = \frac{1}{\beta - 1} \sum_{(n,\,m)\in D_{sign}} (x_{nm} - \bar{b})^2 \tag{19}$$

이다. 이렇게 구해진 q를 가설 검증 이론에 적용하기 위해서 다음과 같은 가설을 세운다.

H_0: 서명 문양이 존재하지 않는다.
H_1: 서명 문양이 존재한다.

각 가설에 대해서 Type Ⅰ과 Type Ⅱ 에러가 각각 발생할 수 있다. Type Ⅰ과 Type Ⅱ 에러는 다음과 같다.

Type Ⅰ : 실제 문양이 없는데 문양이 있다고 판정
Type Ⅱ : 실제 문양이 있는데 문양이 없다고 판정

이때, Type Ⅰ과 Type Ⅱ 에러를 모두 최소화하기 위해 t-percentile를 사용한다[2][8][9].

$$t_{1-\alpha} = \frac{k}{\sigma_{\bar{\omega}}} \tag{20}$$

식 (20)은 test statistic q를 판단하기 위한 기준으로, 서명 영상에서 서명 문양 k의 분포도를 나타낸다. 즉, $q < t_{1-\alpha}$이면 가설 H_0를 만족하고, $q > t_{1-\alpha}$이면 가설 H_1을 만족한다. 그런데, 이와 같은 t-percentile의 방법만을 이용하는 경우는 test statistic q를 판별하는 기준의 범위가 너무나 커서 판정의 신뢰도가 낮은 단점이 있다. 판정의 신뢰도가 낮아질 경우 영상의 저작권을 주장하기 위한 근거 마련에 어려움이 있다. 이 단점을 보완하기 위해 다음과 같이 새로운 검출 기준을 사용한다.

$$t_{1-\alpha} < q < \frac{\bar{\varepsilon}_Q}{\sigma_{\bar{\omega}}} + t_{1-\alpha} \tag{21}$$

식 (21)은 test statistic q의 상위 조건이 없기 때문에 발생되는 검출 에러를 보완하기 위한 것이다. 식 (21)의 test statistic q의 상위 기준은 실험적으로 얻은 값인데, 표본 분산 $\sigma_{\bar{\omega}}$가 일정하다고 가정하면 서명값 k가 표본 집단의 평균에 미치는 영향보다 압축 손실 ε_Q가 평균에 미치는 영향이 더 크다. 즉, 만약 test statistic q가 변화되었다면 그 원인은 압축 손실 ε_Q 때문이다. 이런 가정에서 실험을 한 결과, 식 (21)에서 $\bar{\varepsilon}_Q/\sigma_{\bar{\omega}} + t_{1-\alpha}$은 test statistic q의 상위 기준으로 사용하기에 적합했다.

3.4 유사 서명 공격 대비

지금까지 본 논문에서는 서명된 문양을 검출하기 위해 공격받지 않은 서명 영상을 검출 대상 영상으로 하였다. 그러나, 사용자 수신 서명 영상이 어떤 불법적인 공격을 받았다고 가정하면 식 (21)에 의한 검출은 확률적인 판단이라는 제약 때문에 검출 오류가 발생될 수 있다. 예를 들어, 만약 영상의 소유자가 서명값 k로 서명한 영상에 제 3자에 의해 $k \pm 1$의 새로운 서명값으로 서명을 하는(이때, 서명을 위한 방법은 그레이 레블 밝기값의 연산 방법, 즉 본 논문의 방법이나 XOR 방법 등) 유사 서명 공격을 하였다면, 식 (21)에 의한 검출은 이러한 유사 서명 공격에 대해서는 서명값의 검출 신뢰도가 떨어진다. 표 4는 Lena256

영상에 k=3의 서명값을 삽입한 후, 다시 k′=2와 k′=4로 재서명하여 식 (21)에 의해 얻어진 검출 신뢰도를 보여주고 있다. 표 4의 결과처럼 유사 서명 공격을 받지 않은 경우 검출 신뢰도가 0.95인데 비해 유사 서명 공격을 받은 경우에는 상당히 검출 신뢰도가 떨어졌음을 알 수 있다. 이것은 식 (21)에서 test statistic q의 하위 조건과 상위 조건이 확률적 범위이기 때문이다. 따라서 유사 서명 공격에 대해서는 검출 신뢰도를 신뢰할 수 없는 단점이 발생된다. 이 단점을 극복하기 위해서 본 논문에서는 서명 검출 범위를 조절하기 위해 다음과 같은 식을 사용한다.

$$|MSE(I-I_{sign})-MSE(I-I_{user})| \le \tau \qquad (22)$$

표 3. 제안 서명 방법에 의한 분양 검출 신뢰도
Table 3. The fidelity of detection watermark with proposed digital signature

원영상 \ 서명영상	k=1	k=2	k=3	k=4	k=5	k=6
Lena	0.93	0.95	0.95	0.95	0.98	0.98
Baboon	0.85	0.88	0.90	0.97	0.92	0.94
Couple	0.90	0.92	0.94	0.94	0.97	0.98

표 4. Lena256 영상에서의 유사 서명 공격에 대한 분양 검출 신뢰도
Table 4. The fidelity of detection watermark against illegal signature attack

실험 방법 / 검출신뢰도	k=3			
	XOR 서명 방법		제안 서명 방법	
	k′=2	k′=4	k′=2	k′=4
검출 신뢰도 (k=3, 0.95)	0.89	0.86	0.85	0.83
유사 서명 판정 여부	Yes	Yes	Yes	Yes

식 (22)에서 τ는 임의의 허용 오차이고 I_{user}는 압축 과정을 거친 사용자 수신 서명 영상이다. 원영상 I와 서명된 영상 I_{sign}의 MSE를 비교하고, 원영상과 사용자 영상, 다시 말해 서명 영상이 압축 환경을 거쳐 실제 사용자가 소유 또는 이용하는 영상의 MSE 차를 서로 비교한다. 이론적으로 전송이나 저장중의 에러가 발생하지 않는다면, τ는 식 (10)에서 얻은 압축 손실만의 영향을 받을 것이다. 그러나 만약, 사용자 영상 I_{user}가 제3자에 의한 서명 재공격을 받았다면 식 (21)의 결과는 달라지며, 이런 변화를 τ를 이용하여 검출하고자 한다. τ는 실험적으로 얻어낸 허용 오차로서, τ는 원영상과 부서명 복원 영상(서명되지 않은 원영상이 압축/신장 과정을 거쳐 얻어진 영상)과의 압축 손실로서 영상의 소유자는 쉽게 얻을 수 있지만, 서명 복원 영상만을 가지고 있는 영상 사용자가 계산하기에는 어려운 값이다. τ의 값은 식 (11)을 이용하여 원영상과 부서명 복원영상에서 동일하게 단순영역으로 분할된 블록에서만 계산된다. 또, 영상마다 압축 손실이 다르므로 τ 역시 영상마다 그 특성에 따라 다른 값을 갖는다. 본 논문에서 이용한 τ의 값은 Lena 256 영상에서 얻은 값 0.30542와 Baboon 영상에서 얻은 값 0.44712이다. 표 4에서 유사판정 여부를 위한 τ 값은 0.30542를 이용하였다.

Ⅳ. 전산 모의 실험

제안된 디지털 서명 기법의 컴퓨터 시뮬레이션은 12:1의 압축률을 갖는 JPEG 압축 환경에서 실험되었다. 실험 방법은 서명 분양의 값을 1~6의 자연수로서 변화를 주어 원영상에 서명을 한 후, JPEG 표준 압축 방법에 의해 압축/신장되어 복원된 서명 영상을 각각 단순 블록에서만 서명 분양을 검출하였다. 서명 분양값을 6이하로 한 것은 6이상의 서명 분양은 서명

표 5. 서명값에 따른 원영상과 비교(PSNR)
Table 5. The comparison of PSNR between original and signed image

원영상 \ 서명복원영상	부서명 복원영상	k=1	k=2	k=3	k=4	k=5	k=6
Lena	30.0447	30.0767	30.0454	30.4660	30.0071	29.9946	29.9911
Baboon	23.4931	23.4979	23.4883	23.4842	23.4768	23.4653	23.4739

된 후에 영상의 변화가 시각적으로 확연히 드러났기 때문이다. 본 논문에서 제안한 서명 방법의 장점은 서명값에 변화비트수가 기존의 방법과 비교하여 크다는 점이다. 그런데 이런 방법에서는 서명값에 의한 영상의 열화정도가 기존의 방법보다는 심하다. 논문에서 서명값의 범위를 제한하는 것도 이와 같은 영상 열화의 단점을 보완하기 위해서이다. 그리고, 서명값의 제한으로 발생되는 서명 비도는 의사 난수를 이용하여 극복하였다. 주기가 매우 큰 의사 난수를 발생하고 의사 난수의 초기치를 적당히 변화함으로써 극복한다. 서명값에 따른 영상의 열화정도는 표 5에 나타내었다. 실험 결과 Lena 영상은 모든 서명 문양을 검출하는데 성공하였고, Baboon 영상의 경우는 k=2 이상에서 서명 문양을 찾았다. k=1인 경우에는 85%의 신뢰도로 서명 여부를 판정할 수 있다. 표 3과 그림 2는 각 서명 문양에 대한 검출 결과의 신뢰도를 나타낸 것이다. 검출 신뢰도는 제안된 방법에 의해 연산된 test statistic q가 신뢰 구간내에서 존재하는 확률을 나타낸다[8]. 그림 2에서 보듯이, k=3 이상의 서명 문양은 평균 95%의 신뢰도로 검출할 수 있다. 참고 문헌 [2]에서는 Lena 영상에 k=1로 서명하고 90.96%의 신뢰도로 서명값을 확인하였는데, 본 논문에서는 Lena의 경우 k=1에서 93%의 신뢰도를 나타냄으로서 약 3% 정도의 신뢰도 향상을 가져왔다. Baboon 영상의 경우는 서명값이 커질수록 검출 신뢰도가 증가하는 특성은 Lena와 유사하게 나타나지만, k=4에서 최대 검출 신뢰도를 나타낸다. 이러한 결과는 본 논문에서 제안된 검출 방식이 영상의 블록 특성을 이용하기 때문이다. 삽입된 watermark를 검출하기 위해서 원영상과 서명 영상에서 동시에 단순 영역으로 판정 받은 블록만을 계산의 정의역으로 한다. 서명값의 변화에 따라 판정을 위한 정의역의 범위가 변화되고, Baboon영상의 경우는 다른 실험 영상보다 단순영역의 표본 분산과 압축 손실이 비교적 크기 때문에 계산과정상의 결과로 Baboon 영상에서 k=4일 때 검출 신뢰도가 최대로 발생할 수 있다. 한편, 식 (21)에 의해 주어진 신뢰도를 검출된 영상에 대해 유사 서명 공격의 여부를 판단하기 위해 식 (22)를 사용하여 실험해본 결과 실험 대상의 영상에서 유사 서명 공격을 발견할 수 있었다. 그림 3은 본 논문에서 제안한 서명 시스템의 서명 삽입 과정을 그림 4는 서명 검출 과정을 보여 주고 있다.

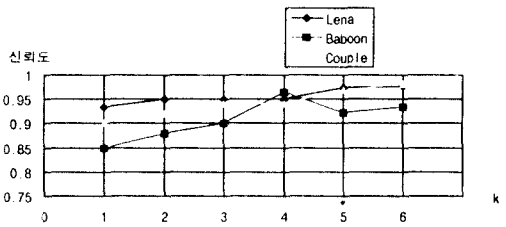

그림 2. 문양 검출 신뢰도
Fig. 2 The fidelity of detection watermark

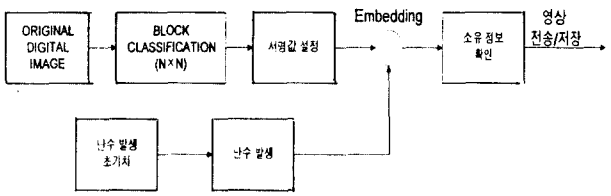

그림 3. 서명 문양 삽입 과정
Fig. 3 The Flowchart of embedding watermarks

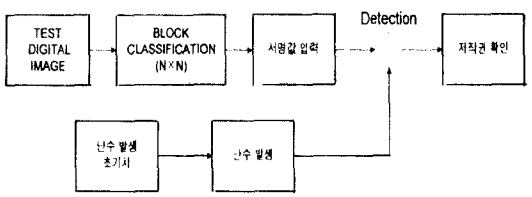

그림 4. 서명 문양 검출 과정
Fig. 4 Flowchart of detection watermarks

V. 결 론

본 논문에서 제안된 디지털 서명 기법은 기존의 서명 방법[2]과 비교하여, 삽입되는 서명 문양이 원영상에 미치는 영향을 극대화하여 서명 문양이 상당히 안정적이며, 압축 환경 하에서 서명 문양의 검출 능력이 훨씬 더 뛰어났다. 즉, [2]의 검출이 서명 문양의 검출이 아닌 단순 서명 여부만의 판정을 하는 것인데 비해, 제안된 방법은 삽입된 서명값을 찾을 수 있다. 이 결과 저작권자는 보다 정확하게 저작권에 대한 정보를 검출하므로써, 확실한 저작권의 증거를 제시할 수 있다. 그리고, 유사 서명 공격에 대해서도 대비책

을 마련하였다. 제안된 서명 방법은 서명 분양의 영상에 대한 영향을 최대화하여 서명 영상에서 서명값을 불법적으로 찾기는 매우 힘들며, 서명 검출에서 압축 손실을 고려하여 실제 서명값을 확률적으로 발견하므로써 압축 손실에 상당히 강하며, 저작권 주장에 근거를 제시할 수 있다. 또 마지막으로 유사 서명 공격에 대해서도 어느 정도의 보완책을 마련하였다.

참 고 문 헌

1. B.M. Macq, J.J. Quisquater, "Cryptology for digital TV broadcasting", *Proceedings of the IEEE*, pp. 944-957, June, 1995.
2. N. Nikolaidis, I.Pitas, "Copyright protection of images using robust digital signatures", *Proc. of ICASSP-96*, pp.2168-2171, May 7-10, Atlanta, GA, 1996.
3. C. S. Won, "Variable block size segmentation for image compression using stochastic models", *Proc. of ICIP '96, Vol.* Ⅲ, pp.975-978, 1996.
4. S. Walton, "Image authentication for a slippery new age", *Dr. Dobb's Journal*, pp.18-26, April, 1995.
5. I. Pitas, T. Kaskalis, "Applying signatures on digital images", *Proc. of IEEE Workshop on Nonlinear Signal and Image Processing*, pp.460-463, 1995.
6. F.M. Boland, J.J.K. O Ruanaidh, and C. Dautzenberg, "Watermarking digital images for copyright protection", *Image Processing And Its Applications*, pp.326-330, 1995.
7. V. Bhaskaran, K. Konstantinides, "Image and Video Compression Standards", *KLUWER ACADEMIC Pub.*, 1995.
8. A. Papoulis, "Probability, Random Variables, and Stochastic Process", *McGRAW-HILL*, 1991.
9. E.L. Lehmann, "Testing Statistical Hypotheses", *WILEY*, 1986.

서 정 일(Jung Il Seo) 정회원

1996년 2월 : 동국대학교 전자공학과 학사

1996년 3월~현재 : 동국대학교 전자공학과(석사 과정)

※주관심분야 : 영상 정보 보호, 암호화, 디지털 방송 등.

우 석 훈(Seock Hoon Woo) 정회원

1995년 2월 : 동국대학교 전자공학과 학사

1996년 3월~현재 : 동국대학교 전자공학과(석사 과정)

※주관심분야 : 영상 분할 기반 비디오 정보 검색, 영상 정보 보호, 디지털 방송 등.

원 치 선(Chee Sun Won) 정회원

1982년 2월 : 고려대학교 전자공학과 학사

1986년 2월 : Univ. of Massachusetts/Amherst(석사)

1990년 2월 : Univ. of Massachusetts/Amherst(박사)

1989년 11월~1992년 8월 : 금성사 선임연구원

1992년 9월~현재 : 동국대학교 전자공학과 조교수, 부교수

※주관심분야 : 영상 분할 기반 영상 압축, 비디오 정보 검색 및 비디오 정보 보호