Fragile Watermarking 기법을 이용한 서명된 이미지의 유효성 검증 방식

박현철, 김광조

한국정보통신대학원대학교

Verification Method of Signed Image using Fragile Watermarking

Hyuncheol Park , Kwangjo Kim

Information and Communications University

요 약

멀티미디어 데이터의 사용이 증가함에 따라 이미지, 비디오, 오디오 데이터의 다양한 활용 및 보호 문제가 많이 논의되고 있다. 대표적인 예로 멀티미디어 데이터에 대한 저작권보호, 데이터 인증 등을 위한 Watermarking과 비밀 정보의 은닉 수단으로서 멀티미디어 데이터를 사용하는 Steganography를 들 수 있다. 암호학에 출발점을 둔 Steganography에 비해 신호 처리 이론을 기반으로 하는 Watermarking은 암호 이론의 적용에 많은 어려움을 갖는다. 본 논문에서는 주류를 이루는 Robust Watermarking과는 달리 약한 공격에도 쉽게 Watermark가 손상되도록 하는 Fragile Watermarking 개념을 바탕으로 이미지 Watermarking에 암호 알고리즘의 적용을 제안하고자 한다. 자필 서명, 인감 등의 스캔한 이진 이미지를 대상으로 디지털 서명 기법을 적용하여, 실세계에서와 동일한 서명의 유효성을 갖도록 하는 방식을 제안한다.

I. 서론

개인용 컴퓨터의 고속화, 대용량화로 기존의 텍스트 기반 데이터들이 이미지, 비디오, 오디오 등을 이용한 멀티미디어 데이터로 전환되는 것은 이미 보편화된 현실이다. 또한, 인터넷을 중심으로 한 네트워크 인프라의 보급과 성능 향상으로 웹을 기반으로 한 멀티미디어 데이터의 활용과 전송이 크게 증가하고 있다. 멀티미디어 데이터의 활용도와 중요성이 증가하면서, 데이터의 저작권을 보호하기 위한 방안들이 많이 연구되고 있다. JAVA 혹은 스트리밍 비디오 등을 이용한 웹 서비스에서 볼 수 있듯이 데이터의 시청은 가능하게 하면서도 다운로드를 방지하는 기술들이 개발, 적용되고 있지만, 최근에는 이러한 경우에도 다운로드를 가능케 하는 소프트웨어가 개발되어 저작권 문제에 대한 논쟁이 발생하고 있다.

Watermarking 기술도 이러한 저작권 문제에 대한 해결 방안으로 제안된 것으로 멀티미디어 데이터에 추출 가능한 Watermark, 즉 저작권 및 인증 정보를 삽입하여, 데이터에 대한 저작권(소유권)을 주장할 수 있도록 하는 방식이다. 나아가 불법 복사의 경로 추적이나, 복사 방지 장치, 영상 데이터 베이스의 인덱스 등으로도 활용이 가능한 기술이다.

Watermarking과 유사하면서 좀 더 포괄적인 개념으로, 비밀 정보를 멀티미디어 데이터에 은닉하여 정당한 사용자만이 확인할 수 있도록 하는 Steganography가 있다. 동일한 개념으로 생각되어질 수 있지만 Watermarking은 멀티미디어 데이터 자체가 보호 대상이 되어, 삽입되는 정보는 검출되었을 경우 누구나 인정할 수 있는 저작권 정보여야 하고, Steganography는 은닉되는 비밀 정보가 보호 대상이 되어, 정당한 수신자 이외에는 정보의 노출이 방지되어야 한다. Steganography의 기본적인 모델은 Simmons의 "prisoner's problem"에서 명확하게 설명되어진다[1].

Steganography는 비밀 정보의 노출을 방지하기 위해 암호 이론을 도입하여 적용하지만, Watermarking은 데이터에 대한 여러 가지 공격에 대비하기 위해 신호처리 이론을 적용하고 있다. 하지만, 저작권 보호, 사용자 추적 등의 목적을 효과적으로 이루기 위해서는 여러 가지 암호 기법들의 적용이 요구된다. 공개키 기반구조를 바탕으로 한 판매자, 구매자, 저작권 인증기관간의 프로토콜 구성이나, DB를 활용하여 사용자 추적을 가능하게 하는 시스템의 구성, 구매자의 프라이버시를 고려한 구매 프로토콜 등이 그 예가 될 수 있다[2][3][4]. 그럼에도 불구하고 암호 기법을 Watermarking에 적용하는 데는 많은 어려움이 있다. 암호 알고리즘 및 프로토콜은 데이터의 무결성이 전제되어야 성립될 수 있는데, 신호 처리 이론은 일정 수준의 오차를 허용하기 때문에 암호 기법을 Watermarking에 적용하는 것은 접근이 쉽지 않은 연구이다. 이런 이유로 최근의 Watermarking에 관련한 연구는 Watermark 의 복원을 가능하게 하는 기법보다는 여러 가지 신호 처리 공격 이후에도 Watermark의 존재 유무를 파악할 수 있는 Robust Watermarking의 연구가 주류를 이루고 있다. 초기의 Watermarking 기법인 비트 영역의 Watermarking은 신호 처리 공격에 대해 매우 취약하다는 단점 때문에 최근에는 거의 고려되고 있지 않지만, 암호 기법의 적용은 훨씬 용이하다는 장점이 있다. 이러한 사실들에 비춰 볼 때, 아직은 연구의 진행이 미진한 Fragile Watermarking은 데이터 무결성을 위해 공격에 매우 약한 Watermark를 삽입하여 쉽게 깨지도록 하는 기법으로 암호 이론과의 결합이 고려될 여지가 많이 있다.

본 논문에서는 위에서 언급한 내용들을 바탕으로 Fragile Watermarking 개념을 이용한 암호 알고리즘의 적용을 제시하기 위해, 스캔한 자필 서명, 인감 등의 이진(binary) 이미지에 RSA 디지털 서명을 삽입하여 실세계의 자필 서명, 인감과 동일한 유효성을 갖는 서명 구성 방식을 제안한다.

논문의 구성은 관련 연구로서 2장에서 일반적인 Watermarking의 요구 조건과 Fragile Watermarking에 대해 알아보고, 3장에서 Watermark 구성에 사용할 RSA 디지털 서명에 대해 알아본다. 4장에서는 스캔한 이진 이미지를 이용한 서명의 유효성 검증 방식을 제안하고 5장에서 실험결과 및 안전성을 분석한 후 6장에서 결론을 맺는다.

II. Watermarking

1. Watermarking의 일반적인 요구사항

Watermarking의 목적을 만족시키려면 해당 응용에 따라 필요한 요구사항들을 검토해야 한다. 대부분의 응용에서 공통적으로 필요로 하는 Watermarking의 일반적인 요구사항들은 다음과 같다[5][6].

가. 지각적인 미 인식: Watermark에 의한 데이터 품질 저하는 인간의 지각능력으로 구별할 수 없

는 수준이어야 한다.

나. Watermark의 복잡성: 유사한 Watermark의 생성을 피하고, 제 3자가 같은 Watermark를 생성하는 것을 어렵게 한다.

다. Watermark 키: Watermark의 생성, 삽입, 검출에 사용되며, 디지털 데이터의 합법적인 소유자를 특징짓는 충분한 크기의 비밀키이다.

라. 통계적인 효율성: 특정한 Watermark를 검출하는 것은 적합한 키가 있을 때만 가능해야 한다.

마. 통계적인 미 인식: 제 3자의 Watermark 검출 및 위조를 불가능하게 하기위해 서로 다른 디지털 데이터는 같은 키 값을 갖는다 해도 각기 다른 Watermark를 생성해야 한다.

바. 다중 Watermarking: 같은 디지털 데이터에 각각 유일한 키를 갖는 충분한 수의 서로 다른 Watermark가 삽입될 수 있어야 한다.

사. 강인성: Watermark는 필터링 또는 JPEG, MPEG같은 압축 등의 수정에 대해서도 지각적으로 인식할 수 없고 검출이 가능한 강인성을 가져야 한다.

아. 알고리즘 공개에 기반한 보안성: 삽입, 검출 알고리즘이 공개되어도 Watermark의 제거나 검출이 적합한 경우에만 행해질 수 있도록 기밀성을 보장해야 한다.

자. Watermark 크기: 삽입되는 Watermark의 크기(비트 수)는 미리 정의된 값을 사용하며, 데이터의 용량을 고려하여 결정되어야 한다.

차. 낮은 오류율: Watermark가 삽입된 데이터에 임의의 조작이 가해져도, Watermark 검출 시 오류율이 작아야 한다. 삽입된 Watermark를 찾지 못하는 경우나 존재하지 않는 Watermark를 잘못 찾아내는 경우가 없어야 한다.

카. Watermark 역변환성: 역변환성 첫 번째 의미는 정당한 사용자일 경우 삽입된 Watermark를 제거할 수 있도록 하는 것을 말한다. Watermark의 정당한 제거를 통해 원본 데이터를 획득할 수 있도록 하는 것이다. 그러나 이는 Watermark가 강인성 및 공격에 대한 내성을 가져야 한다는 특성과 맞서는 부분이 있어 쉽게 해결이 어려운 문제이다. 두 번째 의미는 거짓 데이터와 거짓 Watermark로 진짜와 동일하거나, 지각적으로 동일한 데이터를 생성해 낼 수 있는 특성을 나타낸다. Watermark의 위조 방지를 위해 이러한 의미의 역변환성을 방지할 수 있도록 알고리즘이 고려되어야 한다.

타. 알고리즘의 연산량: Watermark의 삽입, 검출 알고리즘은 실행할 실제 컴퓨터 시스템의 성능을 고려하여, 안전성이 보장되도록 적절하게 설계되어야 한다.

2. Fragile Watermarking

가. Fragile Watermarking 정의

일반적인 Watermarking 이라 하면, 앞 절에서 기술한 요구사항을 만족하면서 특히 강인성에 중점을 둔 Robust Watermarking을 의미한다. Fragile Watermarking은 데이터 인증을 위해 공격에 약한 인증 데이터로서 Watermark를 삽입하는 기법으로 데이터에 조작이 가해지면, 삽입된 Watermark가 쉽게 변경되어 데이터의 유효성 인증이 불가능하도록 하는 기법이다.

나. Fragile Watermarking 요구사항

이미지 데이터에 대한 Fragile Watermarking의 요구사항으로 다음의 다섯 가지가 제시되어있는데[7], ①,②,⑤ 항목을 별도로 고려한다면, 앞 절에서 언급한 요구사항 들도 대부분 동일하게

적용된다.

① 데이터의 변경 여부를 결정할 수 있어야 한다.
② 변경된 위치를 알 수 있어야 한다.
③ 인증 데이터는 별도의 파일이 아닌 이미지 데이터와 함께 결합되어야 한다.
④ 삽입되는 인증 데이터는 시각적으로 식별 불가능해야 한다.
⑤ 이미지에 대한 JPEG 등의 손실 압축은 허용해야 한다.

III. RSA 디지털 서명

RSA 디지털 서명은 RSA 공개키 암호 방식을 사용하며, 서명자 A가 검증자 B에게 메시지와 서명을 전송하는 경우 다음과 같이 서명과 검증이 이루어진다 [8].

키 생성 :

① 서명자 A는 충분히 큰 소수 p, q를 선택
② $n=p\cdot q$, $\varphi(n)=(p-1)(q-1)$ 을 계산
③ $1<e<\varphi(n)$, $\gcd(e,\varphi(n))=1$인 정수 e를 선택
④ 확장 유클리드 알고리즘을 이용하여 $1<d<\varphi(n)$, $e\cdot d\equiv 1(\bmod \varphi(n))$인 d를 계산
⑤ 서명자 A의 공개키 (n,e), 비밀키 d

서명 과정 :

① 메시지 M의 해쉬값 $H=h(M)$을 계산 (h는 해쉬 함수)
② 서명 $S=H^d \bmod n$ 을 계산
③ 서명자 A는 메시지 M과 서명 S를 검증자 B에게 전송

검증과정 :

① 검증자 B는 서명자 A로 부터 메시지 M과 서명 S를 수신
② 공개 목록에서 서명자 A의 공개키 (n,e)를 획득
③ $H=S^e \bmod n$, $H'=h(M)$을 계산
④ H와 H'을 비교하여 서로 같으면 서명의 정당성 확인

IV. 이진이미지를 이용한 서명의 유효성 검증 방식

Fragile Watermarking은 데이터의 무결성을 필요로 하는 응용에 적용되며, 데이터의 변경 사항을 쉽게 파악하여, 인증 여부를 결정한다. 여기서는 자필 서명이나 도장 등을 스캔하여 이진 이미지를 작성한 후, 실세계에서와 같이 디지털 문서에 대해서도 동일한 서명기능을 갖도록 RSA 디지털 서명기법을 이용하여 Watermark를 생성, 삽입한다. 이진 이미지의 이진 행렬, 즉, Bitmap 이미지 각 픽셀의 color 정보(black: 0, white: 1)로만 이루어진 행렬을 구한 후, 디지털 문서와 함께 RSA 서명에 적용하여 해당 문서에서만 유효하고 본인만이 작성 가능한 서명을 생성하여 Watermark로서

이진 이미지에 삽입한다.

데이터의 무결성을 전제로 하므로, 신호 처리 공격을 가정하지 않는다. 따라서 비트 영역에서의 Watermark 삽입을 통한 서명 구성이 가능하므로 Bitmap 이미지에 적용하는 방법을 먼저 제시하고, 이미지에 대해 보편적으로 적용되는 JPEG 압축에서도 가능하도록 DCT(Discrete Cosine Transform) 영역에서의 구성 방식을 함께 제시한다. 서명의 작성 및 검증 과정은 두 경우 모두 동일하며, 이진 행렬 추출, Watermark 삽입/추출에 사용되는 함수들을 각각 기술한다.

기호 정의 :

I_s : 스캔한 이진 이미지

I_w : Watermark삽입 이미지

M : 디지털 문서

b_{mat} : 이진 행렬

w : Watermark (디지털 서명)

h : 일방향 해쉬 함수

(n, e) : 서명자의 공개키

d : 서명자의 비밀키

F_{bi} : 이진 행렬 추출 함수

F_{ins} : Watermark 삽입 함수

F_{ext} : Watermark 추출 함수

$K_{i,j}$: X×Y이미지 K의 (i, j)위치 픽셀 비트값

Matrix : 이진 행렬

L_w : Watermark의 길이(비트)

B : DCT 적용 후의 8×8 이미지 블록

서명 작성 과정 :

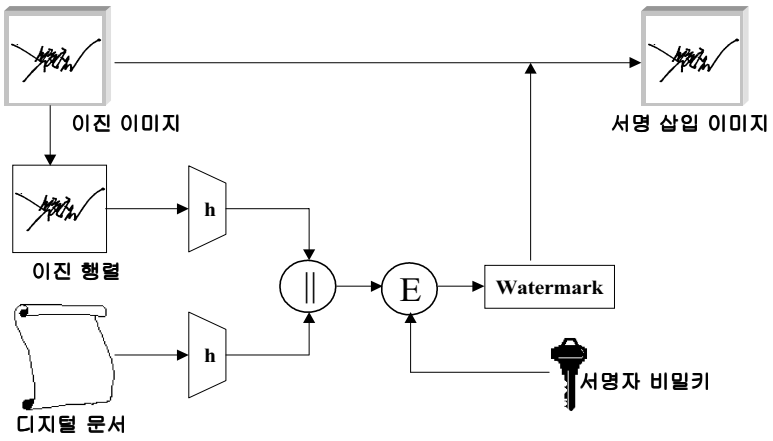
① 자필 서명, 도장 등을 스캔하여 I_s 생성

② $b_{mat} = F_{bi}(I_s)$, $H_1 = h(b_{mat})$ 를 계산

③ $H_2 = h(M)$, $m = H_1 || H_2$ 을 구한다.

④ $w = m^d \bmod n$: RSA 비밀키 암호화를 통해 Watermark 작성

⑤ $I_w = F_{ins}(w, I_s)$: w를 I_s에 삽입하여 I_w 생성



(그림 1) 서명 작성 과정

서명 검증 과정 :

① 서명자로부터 M, I_w 수신

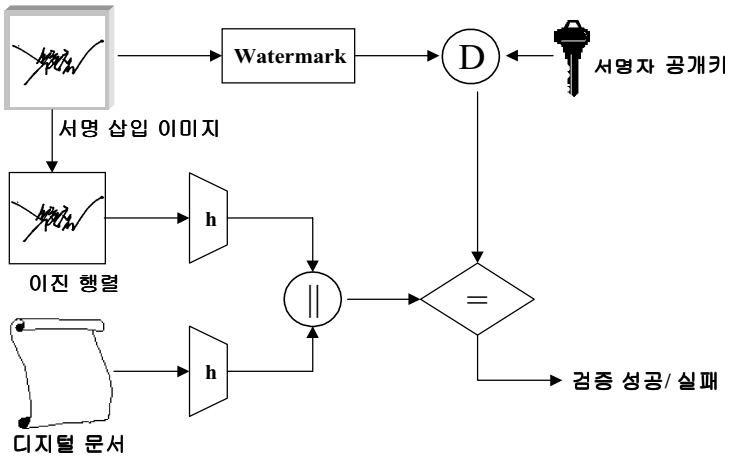
② 공개키 목록에서 서명자 공개키 (n, e) 획득

③ $b_{mat} = F_{bi}(I_w)$, $H_1 = h(b_{mat})$ 를 계산

④ $H_2 = h(M)$, $m = H_1 \| H_2$ 을 구한다.

⑤ $w = F_{ext}(I_w)$, $m' = w^e \bmod n$ 을 계산

⑥ m과 m'을 비교하여 서로 같으면 서명 확인



(그림 2) 서명 검증 과정

1. Bitmap 방식의 서명 구성

Bitmap이미지 픽셀의 LSB를 대상으로 서명 정보인 Watermark를 삽입한다. 이미지의 LSB 값들의 변경은 픽셀의 밝기 정보에 미미한 변화를 가하므로 시각적으로 Watermark의 존재를 식별하는 것이 불가능하다.

가. 서명 작성, 검증 시 필요한 함수 정의

F_{bi} : 이미지 각 픽셀의 LSB를 제외한 나머지 비트들의 값으로 흑,백 정보를 판별하여 이진 행렬을 구성한다.

F_{ins} : 이미지 LSB들의 약속된 위치에 Watermark를 삽입한다.

F_{ext} : 이미지 LSB들의 약속된 위치로부터 Watermark를 추출한다.

```
for  j= 0,…, Y  do
      for  i= 0,…, X  do
            if  K_{i,j} ≥ 0xFE  then
                  Matrix[i,j] = 1
            else if  K_{i,j} ≤ 0x01 then
                  Matrix[i,j] = 0
            else
                  Error
            end if
      end for
end for
```

(그림 3) Bitmap 방식의 F_{bi} 알고리즘

```
for  n= 0,…, L_w  do
      if  w_n == 1  then
            K_{i,j} = K_{i,j} | 0x01
      else
            K_{i,j} = K_{i,j} & 0xFE
      end if
      next  (i, j)
end for
```

(그림 4) Bitmap 방식의 F_{ins} 알고리즘

```
for  n= 0,…, L_w  do
      if  ( K_{i,j} & 0x01) == 1  then
            w_n = 1
      else
            w_n = 0
      end if
      next  (i, j)
end for
```

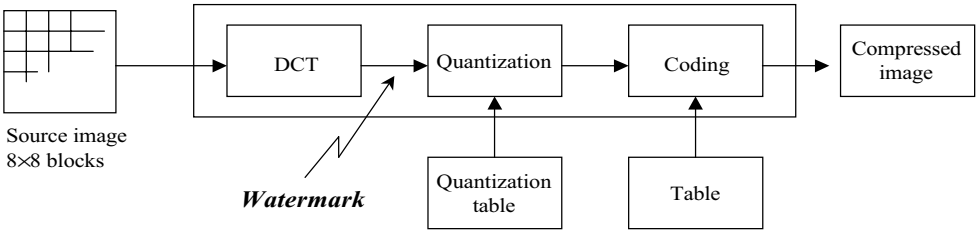
(그림 5) Bitmap 방식의 F_{ext} 알고리즘

2. JPEG 방식의 서명 구성

Bitmap 방식과는 달리 JPEG 압축을 적용하는 이미지는 이진 이미지의 비트 정보가 일부 손실되어 서명 삽입 이미지를 구성하므로 LSB를 이용한 Watermark의 삽입, 검출은 사용이 불가능하다. 따라서, JPEG 압축 후에도 Watermark를 검출할 수 있도록 DCT 영역에서 Watermark를 삽입, 검출한다.

가. DCT 영역의 Watermarking

DCT를 이용하는 JPEG 압축 과정은 아래 (그림 6)과 같으며, DCT 영역의 Watermarking은 DCT 변환 이후, Quantization이 적용되기 이전에 이뤄진다. DCT 변환이후, 블록의 좌측 상단에는 이미지의 저주파 영역이, 우측 하단에는 고주파 영역이 분포하며, 고주파 영역은 Quantization 과정에서 감소된다[9]. 따라서, Watermark는 가능한 한 저주파 영역과 근접한 계수에 삽입되어야 하며, 이미지의 중요한 정보가 손상되지 않도록 적절한 계수를 선택하여 삽입되어야 한다.



(그림 6) JPEG 압축 과정 및 Watermarking

나. 서명 작성, 검증 시 필요한 함수 정의

F_{bi} : 정해진 기준값(Threshold)을 이용하여 각 픽셀의 Black,White정보를 결정

F_{ins} : 두 DCT 계수의 크기 관계를 이용하여 하나의 8×8 블록에 1비트의 Watermark를 삽입[10]. 계수는 이진 정보의 손상 방지와 Quantization에 의한 손실을 감안하여 결정하여야 한다.

F_{ext} : 정해진 두 DCT 계수의 크기를 비교하여 1블록에서 1비트의 Watermark를 추출.

```
for  j= 0,…, Y  do
      for  i= 0,…, X  do
            if  K_{i,j} > Threshold  then
                  Matrix[i,j] = 1
            else if  K_{i,j} ≤ Threshold then
                  Matrix[i,j] = 0
            else
                  Error
            end if
      end for
end for
```

(그림 7) JPEG 방식의 F_{bi} 알고리즘

```
for  n= 0,…, L_w  do
      if   w_n == 1  then
            if  B_n( u_1, v_1) <  B_n( u_2, v_2) then
                  swap ( B_n( u_1, v_1),  B_n( u_2, v_2))
            end if
      else
            if  B_n( u_1, v_1) >  B_n( u_2, v_2) then
                  swap ( B_n( u_1, v_1),  B_n( u_2, v_2))
            end if
      end if
      adjust | B_n( u_1, v_1)- B_n( u_2, v_2)| > x
end for
```

(그림 8) JPEG 방식의 F_{ins} 알고리즘

```
for  n= 0,…, L_w  do
      if  B_n( u_1, v_1) >  B_n( u_2, v_2)  then
            w_n = 1
      else
            w_n = 0
      end if
end for
```

(그림 9) JPEG 방식의 F_{ext} 알고리즘

V. 실험 결과 및 분석

1. 실험 결과

서명, 즉, Watermark의 생성을 위해 SHA1 해쉬 알고리즘과 1024비트의 키 값을 갖는 RSA 암호 알고리즘 사용하였다. 1024비트의 Watermark를 삽입하기 위해 Bitmap 방식에서는 X×Y ≥ 1024이어야 하며, JPEG에서는 8×8 블록의 수가 1024개 이상 존재해야 한다. 여기서는 320×320 이미지를 사용하여 구현하였다.

Bitmap 방식의 서명 구현 및 결과는 손쉽게 얻을 수 있으며, (그림 10)에서 보는 바와 같이 스캔 이미지와 서명 삽입 이미지를 시각적으로 구별하기가 어렵다. 하지만, 삽입된 Watermark에 의해 (b)는 유효한 서명임을 확인할 수 있다.

(a) 스캔 이미지　　(b) 서명 삽입 이미지

(그림 10) Bitmap 방식의 서명 작성 결과

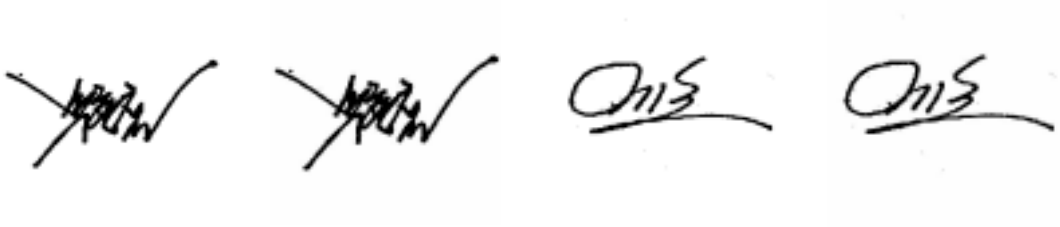
JPEG 방식의 구현은 몇 가지 사항들에 유념해서 Watermark의 삽입 대상 계수, Quantization 테이블, 이진 행렬 추출을 위한 기준값 등을 결정해야 한다.

- 계수는 고주파 영역에서 Quantization에 의해 소거되지 않는 것을 선택한다.
- Quantization 테이블은 이진 정보의 손상 방지를 고려하여 선택하여야 한다.
- 이진 행렬 추출의 기준값은 JPEG 압축 과정의 오류를 고려하여 정확한 이진 정보가 복원될 수 있도록 결정해야 한다.

위의 사항에 준하여 구현 및 실험에 사용한 데이터를 [표 1]에 보였으며, JPEG 방식의 서명 이미지 생성 결과는 (그림 11)에 제시하였다.

[표 1] 구현에 사용 한 데이터

선택 계수	Quantization Table	이진행렬 추출 기준값
$B_n(4,5)$ $B_n(5,4)$	1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 1, 1, 1, 2, 2, 2, 2, 3, 1, 1, 2, 2, 2, 2, 3, 8, 1, 2, 2, 2, 2, 3, 8, 64, 1, 2, 2, 2, 3, 8, 64, 128, 1, 2, 2, 3, 8, 64, 128, 128, 1, 2, 3, 8, 64, 128, 128, 128	$K_{i,j} > 128 \rightarrow 1$ $K_{i,j} \leq 128 \rightarrow 0$



(a) 스캔 이미지 (b) 서명삽입이미지 (c) 스캔 이미지 (d) 서명삽입이미지

(그림 11) JPEG 방식의 서명 작성 결과

2. Watermarking 요구사항에 대한 만족도 분석

가. 일반적인 요구사항

[표 2] 일반적인 요구사항 만족도

요구사항	만족여부	요구사항	만족여부	요구사항	만족여부
지각적인 미인식	○	통계적 미인식	○	Watermark 크기	○
Watermark복잡성	○	다중 Watermarking	△	낮은 오류율	△
Watermark 키	×	강인성	×	역변환성	○
통계적 효율성	×	알고리즘 공개	○	알고리즘 연산량	○

○ : 만족, △ : 조건부 만족, × : 불만족

[표 2]에서 기술한 바와 같이, Watermark의 삽입과 추출 시에는 별도의 비밀키를 필요로 하지 않으며, 서명자의 비밀키, 공개키는 서명의 유효성 검증을 위한 키이므로, Watermark 키와는 구별된다. 다중 Watermarking은 알고리즘 구조상 가능하지만, 본 논문의 서명 유효성 검증에서는 필요로 하지 않으므로, 조건부 만족으로 기입하였다. Fragile Watermarking에 기반하므로 강인성은 JPEG에 한해서만 만족하고, 오류율 또한 고려하지 않는다. Watermark 복잡성과 크기는 RSA 암호문의 안전성에 기반하고, RSA 비밀키가 비공개이므로 서명 위조, 차용이 불가능하여 역변환성도 만족한다. 연산량은 비밀키 암, 복호화 과정의 지수연산이 문제가 될 수 있으나, 서명 생성/ 검증 시 1회씩만 수행하므로 최근의 컴퓨터의 연산속도를 고려하면 별 문제가 되지 않는다.

나. Fragile Watermarking 요구사항

[표 3] Fragile Watermarking 요구사항 만족도

요구사항	만족여부	요구사항	만족여부	요구사항	만족여부
변경 여부 결정	△	인증데이터 결합	○	JPEG 허용	○
변경 위치	×	시각적 식별 불능	○		

○ : 만족, △ : 조건부 만족, × : 불만족

[표 3]에서 제시한 바와 같이, 서명 삽입 이미지의 작성, 검증에는 영향이 없지만 JPEG 데이터의 경우 사소한 변경은 감지하지 못할 경우도 있으며, 전체 데이터에 대해 해쉬 함수를 적용하므로 변경 위치를 파악하는 것은 불가능하다.

3. 안전성 분석

서명, 즉, Watermark의 안전성은 RSA 디지털 서명의 안전성과 동일한 의미를 가지며, 서명 삽입 이미지의 이진 행렬이나 Watermark가 손상되면 서명 자체가 무효화되므로 이 경우 Fragile Watermarking과 마찬가지로 이미지 무결성을 전제로 한다. 이진 행렬과 문서의 해쉬값을 동시에 비밀키로 암호화하여 서명을 생성하므로 타인에 의한 서명 생성이 불가능하고, 해당 문서이외의 다른 문서에 서명을 차용하는 것도 불가능하다.

JPEG 방식의 경우, 서명 삽입 이미지에 변경이 가해져도, DCT 변환의 특성상 검증과정에서 변경 사실을 감지하지 못할 수도 있지만, 감지되지 않는 변경은 실제 이미지에 미미한 영향을 주며, 변경 내용이 서명의 위조, 차용을 가능하게 하지 못하므로 이 응용에서는 무시해도 될만한 요소이다.

VI. 결론

본 논문에서는 신호 처리 이론에 기반 한 Watermarking과 암호 이론의 상호 필요성 및 결합의 난해함을 바탕으로 서명의 유효성 검증 방식 제시를 통한 Watermarking에의 암호 이론 적용을 고려해 보았다. 암호 이론이 요구하는 데이터의 무결성 보장을 위해 Fragile Watermarking의 개념을 적용하였으며, 이진 정보를 갖는 Bitmap 이미지와 JPEG 이미지에 RSA 디지털 서명을 삽입하여 서명의 유효성을 검증하는 방식을 구현하였다. 제안한 방식은 그룹웨어의 결재 시스템이나, 웹 상에서 자필 서명이나 인감 등의 시각적인 정보를 필요로 할 때 적용 가능하다.

Watermarking에 대한 연구는 앞서 기술한 어려움 때문에, Watermark의 존재 여부 검출을 기반

으로 DVD 혹은 MP3 player 등 하드웨어 상에서의 적용이 많이 연구되고, 표준화 논의가 이뤄지고 있다. 향후 암호 이론을 단순한 이진 이미지만이 아니라 일반적인 멀티미디어 데이터에 대해 적용하는 연구가 지속적으로 이뤄진다면 Watermarking의 다양하고, 효과적인 활용이 가능할 것이다.

참고문헌

[1] Simmons, G. J., "The Prisoner's Problem and the Subliminal Channel", Proc. of Crypto'83, Plenum Press, 1984, pp.51-67

[2] A.herrigel, J.Ruanaidh, H.Petersen, S.Pereira, T.Pun, "Secure Copyright Protection Techniques for Digital images", Proc. of the Workshop on Information Hiding, April, 1998

[3] Hideyuki Kakuno, Hirouki Inaba, Masao Kasahara, "Notes on the Performance of Digital Watermark for MPEG Video", Proc. of SCIS'99, Kobe, Japan, January, 1999

[4] Hiroyuki Inaba, Masao Kasahara, "Notes on Privacy Enhanced Protocol for Digital Watermark" , Proc. of SCIS'99, Kobe, Japan, January, 1999

[5] "Watermarking Technology for Copyright Protection: General Requirements and Interoperability", http://www.imprimatur.alcs.co.uk/ download.htm, 18 May, 1998

[6] "Research on digital watermarking at Aristotle university of Thessaloniki", http://poseidon.csd.auth.gr/signatures/report.html, 1997

[7] Min Wu, Bede Liu, "Watermarking for Image Authentication", proc. of ICIP'98, vol.2, 1998, pp.437-441

[8] "PKCS #1 v2.1 : RSA Cryptography Standard", http://www.rsalabs.com/pkcs/pkcs-1/ index.html, September 17, 1999

[9] C.W.Brown, B.J.Shepherd, "Graphics File Formats", Manning, 1995, pp.220-229

[10] S.Katzenbeisser, F.A.P.Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, 2000, pp.58-61