Journal of the Korea Academia-Industrial cooperation Society
Vol. 16, No. 7 pp. 4912-4917, 2015

http://dx.doi.org/10.5762/KAIS.2015.16.7.4912
ISSN 1975-4701 / eISSN 2288-4688

디지털 서명을 이용한 영상의 위변조 검출에 관한 연구

우찬일[1*]
[1]서일대학교 정보통신과

A Study on the Image Tamper Detection using Digital Signature

Chan-Il Woo[1*]
[1]**Dept. of Information and Communication Engineering, Seoil University**

요 약 연성 워터마킹은 인증이나 무결성 검증을 위한 목적으로 시각적인 화질저하 없이 워터마크를 영상에 삽입하는 기술로, 인증과 무결성 검증을 위한 워터마크는 필터링과 같은 영상 변형에 대하여 삽입된 워터마크가 쉽게 제거되어야한다. 본 논문에서는 디지털 서명을 이용하여 영상의 위변조 여부를 검출할 수 있는 블록기반 워터마킹 방법을 제안한다. 제안 방법에서는 초기화된 영상 블록의 해쉬 코드로부터 디지털 서명을 생성하고, 워터마킹 된 영상의 전체 블록을 검사하지 않고도 변형이 발생된 부분을 빠르게 검출할 수 있는 장점이 있다.

Abstract Fragile watermarking is a technique to insert a watermark into an image without significantly degrading its visual quality so that the watermark can be extracted for the purposes of authentication or integrity verification. And the watermark for authentication and integrity verification should be erased easily when the image is changed by filtering etc. In this paper, we propose a image block-wise watermarking method for image tamper proofing using digital signature. In the proposed method, a digital signature is generated from the hash code of the initialized image block. And The proposed method is able to detect the tampered parts of the image without testing the entire block of the watermarked image.

Keywords : Digital Signature, Encryption, Image Authentication, Tamper Detection

1. 서론

유, 무선 네트워크로 전송되는 데이터를 허가받지 않은 제3자로부터 보호하기 위해서는 암호화 방법이 널리 사용되어 왔다. 암호화 방법은 평문을 암호문으로 만들기 위해 사용되는 키에 따라 비밀키(대칭키) 암호와 공개키(비대칭 키) 암호로 구분된다[1]. 대칭키 암호는 암, 복호화 과정을 수행할 때 동일한 비밀키(secret key)를 사용하기 때문에 송신자와 수신자는 사전에 비밀키를 공유하고 있어야 한다. 대칭키 암호는 암호화와 복호화 속도가 빨라 데이터를 암호화하는데 효과적으로 사용할 수 있으나 송신자와 수신자가 공유하는 비밀키가 노출될 경우 암호화된 데이터는 더 이상 보호될 수 없게 된다. 이러한 대칭키 암호의 단점은 공개키 암호를 사용함으로써 극복할 수 있다. 공개키 암호에서는 공개키 분배 채널을 통해 공개된 수신자의 공개키(public key)로 데이터를 암호화 하여 전송하고 수신된 암호문은 수신자만이 알고 있는 개인키(private key)로 복호화하기 때문에 평문을 암호문으로 만드는 것은 누구나 가능하지만 암호문을 복호화하기 위해서는 비밀키를 소유하고 있는 사람만이 가능하기 때문에 대칭키 암호의 키 분배와 키 관리 문제를 해결할 수 있다. 그러나 공개키 암호는 암, 복호화 속도가 느려 대칭키 암호를 위한 키 분배와 디지털서명 등에 응용되고 있다[1-3]. 디지털서명(digital signature)은 일

본 논문은 2015년도 서일대학교 학술연구비에 의해 연구되었음.
*Corresponding Author : Chan-Il Woo(Seoil Univ.)
Tel: +82-2-490-7556 email: ciwoo@seoil.ac.kr
Received April 24, 2015 Revised July 15, 2015
Accepted July 16, 2015 Published July 31, 2015

반적으로 해쉬 함수(hash function)와 공개키 암호를 이용하여 생성한다. 디지털서명은 전자문서를 암호화하지 않고 전자문서를 해쉬 함수의 입력으로 사용하여 생성된 해쉬 코드를 송신자의 개인키로 암호화하여 암호문을 생성하게 되는데 이것을 디지털서명이라고 한다. 디지털서명은 전자문서와 함께 수신자에게 전송되고, 수신자는 수신된 디지털서명을 송신자의 공개키로 복호화 하면 전자문서의 해쉬 코드를 얻을 수 있다. 그리고 수신된 전자문서는 디지털서명 생성에 사용된 해쉬 함수의 입력으로 사용하면 디지털서명으로부터 구한 해쉬 코드와 동일한 해쉬 코드를 생성할 수 있다. 따라서 이 두 개의 해쉬 코드를 비교하여 서로 같을 경우 전송된 전자문서는 변형이 발생하지 않았음을 나타내고, 만약, 다를 경우 전자문서에 어떠한 변형이 발생하였음을 알 수 있게 된다. 디지털서명 생성을 위해 사용되는 해쉬 함수는 다양한 크기의 데이터를 입력으로 사용할 수 있지만 해쉬 함수의 출력으로 생성되는 해쉬 코드는 입력 데이터가 서로 다르더라도 항상 일정한 크기를 가진다. 그리고 암호화 방법과는 달리 생성된 해쉬 코드로부터 원래의 데이터를 찾을 수 없는 특성과 해쉬 함수의 입력으로 동일한 데이터를 사용할 경우 항상 동일한 출력만 생성하는 특성이 있어 무결성 검증과 디지털서명에 효과적으로 사용될 수 있다[1,2].

이러한 디지털 서명은 디지털 영상에 대한 변형 여부와 변형 위치를 검출하기 위한 디지털 워터마킹 기술에 적용할 수 있다. 디지털 영상의 변형 여부와 변형 위치를 검출하기 위한 디지털 워터마킹 기술은 공간 영역과 주파수 영역에서 수행할 수 있으나 공간 영역에서 수행할 경우 변형 유무뿐만 아니라 미세한 조작에 대한 검출도 가능하다. 공간 영역에서 수행되는 워터마킹은 영상을 일정 블록들로 나누어 각 블록 내 화소의 LSB(least significant bit)에 워터마크를 삽입하여 영상의 변형 여부를 검출할 수 있는 Wong의 방법을 기반으로 연구되어 왔다[3]. 공간 영역에서 삽입되는 워터마크는 모든 화소들에 삽입하게 되는데 워터마크를 영상 블록 내 화소의 MSB(most significant bit) 부근에 삽입할 경우 화질 저하가 많이 발생할 수 있어 일반적으로 각 화소의 LSB에 삽입하고 있다[3-6].

공간 역역 기술은 일반적으로 일정 크기의 블록 단위로 수행되기 때문에 화소 단위의 변형 검출은 불가능하다. 따라서 블록 크기를 최소화하여 미세한 변형이 발생하여도 변형된 화소들만 효과적으로 검출할 수 있는 방법이 필요하다. 따라서 본 논문에서는 디지털서명과 대칭키 암호를 이용하여 디지털 영상의 변형 여부와 변형된 부분을 빠르고 효과적으로 검출하기 위한 방법을 제안한다.

2. 관련 연구

2.1 디지털 서명

2.1.1 공개키 암호

공개키 암호는 대칭키 암호에 비하여 느린 단점이 있으나 암호화에 사용되는 키와 복호화에 사용되는 키가 서로 달라 대칭키 암호에서 발생할 수 있는 키 관리와 키 분배 문제를 해결할 수 있는 장점이 있다. 공개키 암호는 암호화에 사용되는 키와 복호화에 사용되는 키가 서로 다른 특징이 있어 디지털 서명 등에 널리 응용되고 있다. 이와 같은 공개키 암호는 소인수 분해의 어려움을 기반으로 한 RSA, Rabin 암호와 이산대수 문제를 기반으로 한 타원곡선 암호로 나눌 수 있으며, RSA 공개키 암호의 키 생성 방법은 Table 1의 과정으로 수행된다[1].

Table 1. Key generation process for the RSA

stage	
1	Choose two distinct prime numbers p and q
2	Compute n = p×q
3	Compute $\varnothing(n) = (p-1)\times(q-1)$
4	Choose an integer e such that $1<e<\varnothing(n)$ and gcd(e, $\varnothing(n)$)=1, e and $\varnothing(n)$ are coprime e is released as the public key exponent
5	Determine d as $\equiv e^{-1} \bmod \varnothing(n)$ d is kept as the private key exponent

RSA 공개키 암호에서는 평문(M)과 암호문(C)에 대하여 다음의 형태를 따른다.

$$\text{암호화} : C = M^e \bmod n \quad (1)$$

$$\text{복호화} : D = C^d \bmod n \quad (2)$$

2.1.2 해쉬 함수

해쉬 함수는 디지털 서명에서 서명문 압축을 위해 사용하며, 임의의 메시지(M)를 해쉬 함수(h)의 입력으로 사용하면 고정된 크기의 해쉬 코드(H)가 생성된다[1,2].

$$H = h(M) \quad (3)$$

디지털 서명에 사용되는 해쉬 함수는 디지털 서명의 안전성을 보장하기 위해 다음과 같은 특성을 가지고 있어야 한다.

- 해쉬 함수의 계산 효율이 양호해야 한다.
- 해쉬 코드(H)로부터 해쉬 코드를 생성하기 위해 사용되는 서명문(M)을 찾는 것은 계산상 불가능 해야 한다.
- 임의의 서명문(M)과 그의 해쉬 코드 H = h(M)가 주어졌을 때, H = h(M')이 되는 서명문 M≠M'을 찾는 것이 계산상 불가능해야 한다.
- h(M)=h(M')이 되는 서명문 M≠M'을 찾는 것이 계산상 불가능해야 한다.

첫 번째 특성은 해쉬 함수의 조건에 해당하고 두 번째부터 네 번째까지의 특성은 해쉬 함수의 안전성에 관한 제약으로 두 번째와 세 번째 특성은 해쉬 함수의 역함수를 계산하는 것을 방지하는 것을 말한다. 네 번째 특성은 서명자가 서명문 M을 서명하여 전송한 후 나중에 M'을 서명하여 전송하였다고 주장하는 내부 부정을 방지하기 위한 기능이다.

2.1.3 디지털 서명

디지털 서명은 수기로 이루어지는 서명을 전자 문서에 적용한 것으로 RSA 공개키 암호를 이용한 디지털 서명과 SHA(secure hash algorithm)를 사용하는 미국 표준 전자서명 알고리즘인 DSA(digital signature algorithm) 그리고 국내 표준 전자서명 알고리즘인 KCDSA(korean certificate-based digital signature algorithm) 등 다양한 디지털 서명 알고리즘들이 개발되었다. Fig. 1은 인증서 기반 전자서명 알고리즘인 KCDSA의 서명 생성과 검증 과정을 나타내고 있다. KCDSA에서는 서명 검증을 위해 도메인 변수 *P*, *Q*, *G*와 공개 검증키(Y)를 인증서로부터 추출하여 사용한다 [1,2].

공개키 암호를 디지털 서명에 적용할 경우 디지털 서명 생성을 위해 전자 문서의 해쉬 코드를 비공개 서명키로 서명을 생성하고, 서명 검증을 위해서는 공개되는 검증키로 검증 과정을 수행한다.

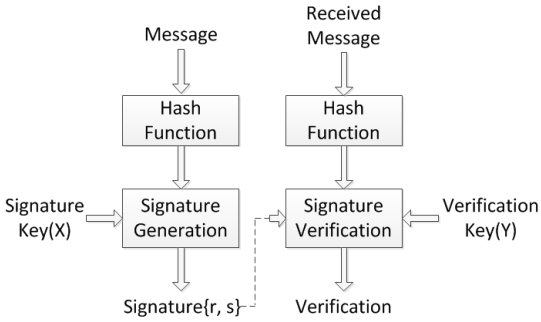

Fig. 1. Signature generation and verification process

2.1.4 블록 기반 공간 영역 워터마킹

블록 기반 워터마킹은 원 영상을 8×8 또는 16×16 화소 크기로 분할하여 워터마킹을 삽입하는 것으로 영상의 변형 검출은 워터마크 삽입에 사용된 블록 단위로 이루어지게 된다. 블록 기반 워터마킹의 대표적인 방법으로 Fig. 2의 Wong의 방법은 영상을 M×N 크기로 분할한 후 블록 내 각 화소의 LSB를 0으로 초기화하여 이미지 정보 등과 함께 MD5 해쉬 함수의 입력으로 사용한다. 이렇게 생성된 해쉬 코드는 워터마크와 XOR 연산을 수행한 후 RSA로 암호화하여 초기화된 LSB에 삽입한다 [3-6].

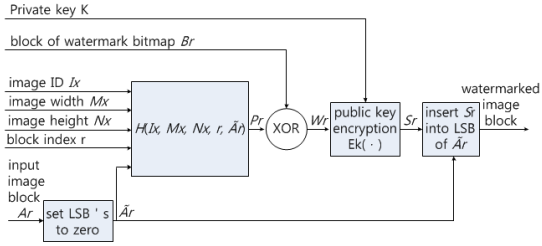

Fig. 2. Public key verification watermark insertion procedure

Fig. 2에서 영상 블록의 크기는 MD5 해쉬 함수의 출력인 128비트 크기의 해쉬 코드가 들어갈 수 있도록 12×12를 설정하고 있다. 그러나 128비트 해쉬 코드를 RSA로 암호화하여 12×12(144비트) 크기 이내의 암호문을 생성하기 위해서는 식 (1)에서 n이 144비트 이내의 값을 가져야한다. 또한 Table 1의 키 생성 알고리즘의 두 번째 단계에서 n이 144비트 이내의 크기를 가지기 위해서는 두 소수 p와 q의 최대 크기는 72비트를 넘을 수 없다. 따라서 두 소수 p와 q가 72비트의 크기일 경우 이때 생성될 수 있는 공개키는 작은 크기로 제한된다.

RSA 공개키 암호의 안전성은 소수 p, q의 크기에 의존하며 2048비트 이상의 키를 사용해야 암호문에 대한 안전성은 보장할 수 있지만 그렇지 않을 경우에는 RSA 암호의 안정성은 보장될 수 없는 문제점이 있다. 따라서 RSA 암호를 이용하여 워터마크를 삽입하기 위해서는 블록의 크기가 커야 되는 단점이 있다. 만약, 대칭키 암호를 적용할 경우 블록의 크기는 대칭키 암호에서 생성되는 암호문의 크기에 따라 블록의 크기는 조정할 수 있다. Triple DES의 경우 64비트의 암호문을 생성하기 때문에 8×8 크기의 블록이 가능하고, SEED의 경우 128비트의 암호문을 생성하므로 12×12 크기의 블록을 가질 수 있다. 그러나 대칭키 암호를 워터마크 생성에 적용할 경우 워터마크를 검증하는 사람은 자신만이 알고 있는 키를 이용하여 새로운 워터마크를 생성하여 삽입할 수 있는 문제가 있어 일반적으로 대칭키 암호는 사용하지 않는다. 따라서 공개키 암호를 사용할 경우 블록 크기와 공개키 암호의 안전성을 고려하여 워터마크를 삽입하여야 한다.

3. 제안 방법 및 분석

3.1 디지털 서명 기반 워터마킹

최근 들어 RSA 암호는 안전성을 보장하기 위해 2048비트 이상의 키를 요구하고 있으며, 2048 비트 이상의 키를 생성하기 위해서는 Table 1의 소수 p와 q가 매우 커야한다. 따라서 RSA를 이용하여 워터마크를 삽입할 경우에는 RSA 암호의 안전성을 보장하기 위해 소수 p와 q의 크기는 1024비트 이상이 요구되고 있다. 하나의 소수가 1024비트 크기를 가질 경우 식(1)의 암호화 과정에서 n의 값은 2048 비트의 크기를 가지며 이때 생성되는 암호문의 크기는 최대 2048비트 크기에 근접하게 된다. 따라서 암호화된 워터마크를 분할된 블록의 LSB에 삽입하기 위해서는 영상을 최소 46×46 단위로 분할해야 2048비트 개의 워터마크를 삽입할 수 있다. 그러나 영상을 46×46 크기의 화소 단위로 분할하여 워터마크를 삽입 할 경우 영상에 대한 변형 여부는 46×46 화소 단위로만 검증할 수 있어 워터마크가 삽입된 영상에 대하여 미세한 조작이 발생할 경우 작은 블록 단위로의 검출이 불가능한 단점이 있다.

따라서 본 논문에서는 암호학적으로 안전성이 보장되면서 영상의 변형 여부를 8×8 화소 단위로 빠르게 검출하기 위해 디지털 서명을 이용한 방법을 제안한다. 제안 방법에서는 전체 영상을 64×64 블록으로 나누어 디지털 서명 s(256비트)와 r(256비트)을 생성하고, 64×64 블록을 다시 4개의 32×32 블록으로 나누어 상위 블록(64×64 블록)의 서명과 자신 블록(32×32)의 서명을 LSB에 삽입한다. 이와 같이 64×64 블록과 32×32 블록의 디지털 서명을 삽입하는 이유는 전체 영상에 대한 변형 검사를 64×64 블록 단위로 수행하여 64×64 블록에 대한 디지털 서명이 이상 없으면 변형이 발생하지 않은 것이므로 다음 64×64 블록을 검사한다. 그러나 변형이 발생하였을 경우에는 64×64 블록을 32×32 블록으로 분할하여 32×32 블록들을 검사하고, 변형이 발생된 32×32 블록은 다시 8×8 블록으로 분할하여 최종적으로 8×8 블록 단위로 변형된 부분을 검출할 수 있기 때문이다.

3.2 워터마크 생성 및 삽입 과정

Step 1 : 원 영상 전체 화소의 하위 2개의 LSB를 0으로 초기화한 한다.

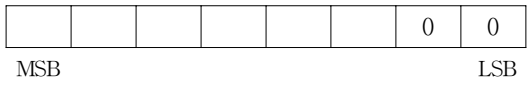

Fig. 3. Initialized pixel

Step 2 : 영상 분할 및 디지털서명 생성

① 초기화된 영상을 64×64 크기의 블록으로 분할하여 Fig. 1과 같이 디지털 서명 s와 r을 생성한다. Fig. 4의 경우 4개의 64×64 블록이 생성된다.

② 64×64 크기의 블록을 4개의 32×32 크기의 블록으로 분할하여 각 블록의 디지털 서명 s와 r을 생성한다.

③ 32×32 크기의 블록을 16개의 8×8 크기의 블록들로 분할하여 각 블록들을 MD5 해쉬 함수의 입력으로 사용하여 128비트의 해쉬 코드를 생성한다.

④ 각 블록 단위로 생성된 해쉬 코드는 상위 64비트와 하위 64비트를 XOR 연산하여 송,수신자가 공유하는 비밀키를 사용하여 Triple DES 등의 대칭키 암호로 암호화 한다. Triple DES로 암호화를 하는 이유는 8×8 블록에 삽입되는 정보는 64비트이므로 AES나 SEED와 같은 대칭키 암호알고리즘은 128비트 이상의 암호문을 생성하기 때문에

사용할 수 없고, DES의 경우 64비트의 암호문은 생성할 수 있지만 안전성을 보장할 수 없어 암호문 크기와 안정성을 고려하여 Triple DES를 사용한다.

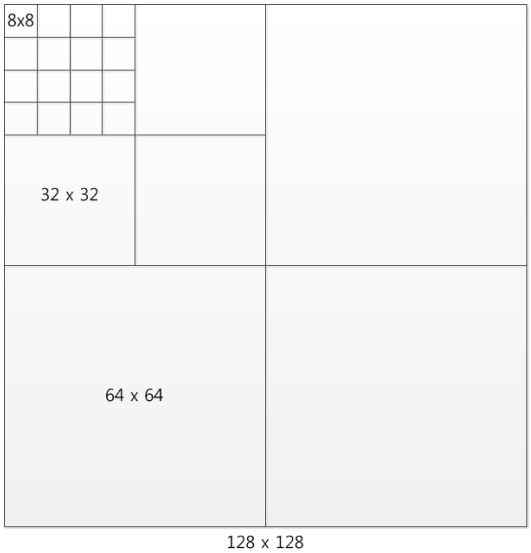

Fig. 4. The image block and its sub blocks

Step 3 : 워터마크 삽입

① Step 2의 ①에서 생성된 64×64 크기의 블록에 대한 디지털 서명(s, r) 512비트는 초기화된 32×32 블록의 LSB에 삽입한다. 32×32 블록의 화소는 총 1,024개로 구성되므로 상위 512개 화소에 삽입한다.

② 32×32 블록의 화소 중 하위 512개 화소의 LSB에 Step 2의 ②에서 구한 디지털 서명(s, r)을 삽입한다.

③ Step 2의 ④에서 생성된 암호화 데이터는 Step 2에서 분할된 8×8 블록의 두 번째 LSB에 삽입한다. 이러한 과정은 32×32 블록에 포함되어 있는 모든 8×8 블록들에 대하여 수행한다.

Step 2에서 생성된 8×8 크기의 블록에는 대칭키로 암호화된 정보를 삽입하기 때문에 수신자는 삽입된 워터마크를 제거하고 새로운 대칭키를 사용하여 워터마크를 생성하고 삽입할 수 있다. 따라서 이러한 문제를 방지하기 위해 8×8 블록의 상위 블록인 32×32 블록의 LSB에 64×64 블록으로부터 생성된 디지털 서명과 32×32 블록으로부터 생성된 디지털 서명 을 삽입한다.

3.3 워터마크 추출 및 검증 과정

워터마크의 복원 과정은 Fig. 4와 같이 워터마크가 삽입된 영상을 64×64 블록 단위로 분할하여 다음과 같이 수행한다.

Step 1 : 워터마크가 삽입된 영상은 워터마크 추출과 변형 여부의 확인을 위해 2개의 LSB를 초기화한 영상과 구분하여 각각 64×64 블록으로 분할한다.

Step 2 : 분할된 64×64 블록은 다시 4개의 32×32 블록으로 분할한 후, 분할된 블록들 중 첫 번째 블록 내 상위 512개 화소의 LSB에 삽입된 64×64 블록(32×32 블록의 상위 블록)의 디지털 서명을 추출한다.

Step 3 : Step 2에서 추출된 디지털 서명은 Fig. 1에서와 같이 초기화된 영상의 상위 비트들을 메시지로 사용하여 검증키(Y)로 디지털 서명을 검증한다. 만약 디지털 서명이 성공적으로 검증될 경우 워터마크가 삽입된 영상에 변형이 없는 것을 의미하므로 Step 1에서 분할 된 64×64 블록들 중 검증되지 않은 다음 블록들에 대하여 Step 2를 반복한다. 만약 디지털 서명 검증이 실패할 경우 디지털 서명 검증을 수행한 64×64 블록에 변형이 발생한 것으로 판단하여 Step 4를 수행한다.

Step 4 : 변형이 발생된 64×64 블록 내 4개의 32×32 블록에서 하위 512개 화소의 LSB를 추출하여 Step 3에서와 같이 Fig. 2의 서명 검증 과정을 수행한다. 이 과정도 Step 3과 마찬가지로 검증이 성공하면 다음 블록을 검사하고 만약 검증이 실패할 경우 검증이 실패된 32×32 블록들을 16개의 8×8 블록들로 분할한다. 그리고 분할된 각 블록 내 화소의 두 번째 LSB에서 대칭키로 암호화된 해쉬 코드를 추출하여 복호화 하고, 초기화된 8×8 블록을 MD5 해쉬 함수의 입력으로 사용하여 생성된 해쉬 코드를 상위 64비트와 하위 64비트를 XOR 연산을 수행하여 복호화 된 데이터와 비교한다. 만약 두 값이 서로 다르면 그 블록에 변형이 발생한 것으로 판단하고 그렇지 않으면 변형이 발생하지 않은 것으로 판단하여 다음 블록에 대하여 위의 과정을 반복 수행한다.

이와 같은 과정을 수행하면 워터마크가 삽입된 영상에 대하여 미세한 변형이 발생하였을 경우 4개의 32×32 블록 중 하나의 블록에서 상위 블록인 64×64 블록의 디

지털 서명을 추출하여 검증한 후 이상이 없으면 다른 64×64 블록들을 검증하면 되므로 결과적으로 64×64 블록 단위로 빠르게 전체 영상의 변형 여부를 확인할 수 있다. 그리고 변형이 발생한 부분은 8×8 블록 단위로 검출이 가능하므로 미세한 변형이 발생할 경우에도 효율적으로 변형 부분을 검출할 수 있는 장점이 있다. 본 논문에서는 DSA나 KCDSA 등의 디지털 서명 알고리즘을 사용할 수 있기 때문에 디지털 서명의 안전성은 보장할 수 있다.

4. 결론

본 논문에서는 블록을 기반으로 영상의 변형 여부를 확인할 수 있는 방법을 디지털 서명을 이용하여 제안하였다. 블록을 기반으로 한 영상의 인증과 무결성 방법은 공개키 또는 대칭키 암호를 사용하여 인증하고 영상의 무결성 검증은 분할된 영상의 블록 단위로 수행된다. 만약, 대칭키 암호만으로 워터마크를 삽입할 경우 정당한 수신자에 의해 삽입된 워터마크를 제거한 후 새로운 워터마크를 삽입할 수 있기 때문에 일반적으로 공개키 암호를 사용한 방법들이 제안되고 있다.

그러나 RSA 공개키 암호를 사용할 경우 공개키 암호의 안정성 확보를 위해 소수의 크기를 1,024 비트 이상으로 사용해야 된다. 따라서 큰 소수를 사용하여 워터마크를 생성할 경우 워터마크 삽입을 위한 블록의 크기는 46×46이 되어야 되기 때문에 미세한 변형이 발생할 경우에도 46×46 블록 단위로만 변형된 부분을 검출되는 되는 단점이 있다.

따라서 본 논문에서는 공개키 암호 또는 대칭키 암호를 사용했을 경우의 문제점들을 해결하기 위해 디지털 서명을 이용한 방법을 제안하였다. 제안 방법에서는 안전성이 검증된 알고리즘들을 사용하기 때문에 삽입된 워터마크의 안정성을 보장할 수 있고, 전체 영상을 검사하지 않고 큰 블록 단위로 변형 여부를 검사하기 때문에 변형이 발생된 부분을 빠르게 검출할 수 있는 장점이 있다. 향후 연구과제로는 보다 작은 블록으로의 영상 분할과 워터마크 생성 방법에 대한 연구가 필요할 것으로 생각된다.

References

[1] Dongho Won, *Modern Cryptology*, Green Press, 2006.

[2] *Digital Signature Mechanism with Appendix - Part2:Korean Certificate-based Digital Signature Algorithm KCDSA*, TTA Standard, 2014.

[3] P. W. Wong, “A Public Key Watermark for Image Verification and Authentication,” in Proc. of IEEE Conf. on Image Processing, pp. 425-429, 1998.
DOI: http://dx.doi.org/10.1109/ICIP.1998.723526

[4] Chanil Woo, Seungdae Lee, “Digital Watermarking for Image Tamper Detection using Block-Wise Technique” International Journal of Smart Home, Vol, 7, no. 5, pp. 115-124, 2013.
DOI: http://dx.doi.org/10.14257/ijsh.2013.7.5.12

[5] G. Kaur, K. Kaur, "Image Watermarking using LSB," International Journal of Advanced Research in Computer Science and Sofrware Engineering, Vol. 3, no. 4, pp. 858-861, April 2013.

[6] C. M. Wu, Y. S. Shin, "A Simple Image Tamper Detection and Recovery Based on Fragile Watermark with One Parity Section and Two Restoration Sections," Optics and Photonics Journal 3, pp. 103-107, 2013.
DOI: http://dx.doi.org/10.4236/opj.2013.32B026

우 찬 일(Chan-Il Woo) **[정회원]**

- 1995년 2월 : 단국대학교 대학원 전자공학과 (공학석사)
- 2003년 2월 : 단국대학교 대학원 전자공학과 (공학박사)
- 1995년 11월 ~ 1997년 2월 : LG 이노텍(주) 연구원
- 2004년 3월 ~ 현재 : 서일대학교 정보통신과 교수

<관심분야>
정보보호, 암호 프로토콜, 디지털워터마킹