Journal of the Korea Academia-Industrial cooperation Society
Vol. 20, No. 10 pp. 203-208, 2019

https://doi.org/10.5762/KAIS.2019.20.10.203
ISSN 1975-4701 / eISSN 2288-4688

디지털 영상의 무결성 검증과 변형 검출에 관한 연구

우찬일[1], 구은희[2*]
[1]서일대학교 정보통신공학과, [2]아주대학교 다산학부대학

A Study on Integrity Verification and Tamper Detection of Digital Image

Chan-Il Woo[1], Eun-Hee Goo[2*]
[1]Department of Information and Communication Engineering, Seoil University
[2]Dasan University College, Ajou University

요 약 디지털 워터마킹은 디지털 컨텐츠에 대한 불법적인 복제를 방지하기 위한 저작권 보호 용도로 개발 되었으나, 최근에는 의료 영상과 같은 디지털 컨텐츠에 대하여 무결성을 검증하고 불법적인 조작이나 변형 위치를 감지하기 위한 기술로도 활용하고 있다. 디지털 컨텐츠에 대한 불법적인 복제를 방지하기 위한 저작권 보호 기술에서는 디지털 컨텐츠에 삽입된 워터마크가 왜곡이나 필터링과 같은 다양한 공격에 대하여 강인해야 하는 특성이 있어야 한다. 그러나 디지털 컨텐츠에 대한 조작이나 변형을 감지하기 위한 기술에서는 컨텐츠에 대한 사소한 변형에 대해서도 삽입된 워터마크가 쉽게 제거되어야 하는 특성이 있어야 컨텐츠에 대한 변형 여부를 확인할 수 있다. 따라서 본 논문에서는 디지털 영상에 대한 변형이나 조작 여부를 쉽게 확인하기 위한 워터마킹 기술을 제안한다. 제안 방법에서는 영상에 대한 변형 유, 무를 확인하기 위해 전체 영상을 16×16 블록 단위로 변형 여부를 검사하고 변형이 발생 된 블록에 대해서는 4×4 블록 단위로 검사를 수행하여 변형이 발생 된 위치를 확인한다.

Abstract Digital watermarking was developed to protect copyright by discouraging the illegal copying of digital content. On the other hand, recently, watermarking has also been used to verify the integrity of digital content, such as medical images, and detect illegal manipulation or distortion locations. Watermarking should be tenacious so as to protect copyright from illegal copying and should remain firm to the content through a range of attacks, such as distortion or filtering. At the same time, however, it should be removed easily even in a slight transformation of the material to verify the integrity. Therefore, this paper proposes a watermarking technique that easily checks and verifies the deformation or manipulation of digital images. In the proposed method, the entire image was examined in 16×16 blocks to check for deformation of the image. When deformation was detected, further inspection proceeded in 4×4 blocks and the location where deformation occurred was identified.

Keywords : Digital Watermarking, Integrity, Tamper Detection, Fragile, Authentication

1. 서론

디지털로 제작된 영상이나 음성 데이터와 같은 컨텐츠는 아날로그 컨텐츠에 비하여 복사와 조작이 용이하여 이미지 합성이나 음성 데이터의 조작 같은 행위로 인하여 다양한 문제가 발생하고 있다. 또한, 유선뿐만 아니라 무선 인터넷이 광범위하게 사용되고 있는 상황에서 디지털 컨텐츠에 대한 저작권자의 허가 없이 임의로 배포되

본 논문은 2019년도 서일대학교 학술연구비에 의해 연구되었음
*Corresponding Author : Eun-Hee Goo(Ajou Univ.)
email: ehgoo@ajou.ac.kr
Received July 11, 2019 Revised July 30, 2019
Accepted October 4, 2019 Published October 31, 2019

거나 원래의 컨텐츠가 변형되어 유포되는 것은 사회적으로 커다란 문제가 되고 있다. 따라서 이러한 문제점들을 해결하기 위하여 다양한 기술들이 제안되고 있으며, 그 중 하나의 방법으로 디지털 워터마킹이 있다. 디지털 워터마킹은 디지털 영상과 같은 컨텐츠에 저작권자의 정보를 삽입하여 저작권에 대한 분쟁이 발생하였을 경우 이를 해결하기 위한 저작권 보호 기술과 디지털 컨텐츠에 대한 조작이나 변형 유, 무를 검증할 수 있는 기술로 개발되었다[1-3].

디지털 영상에 대한 저작권 보호 기술은 저작권 정보를 제거하기 위한 필터링, 왜곡과 같은 다양한 공격에 대해서 삽입된 저작권 정보가 검출될 수 있어야 하는데, 이러한 공격에 대하여 저작권 정보를 정확하게 검출하기에는 많은 기술적 한계가 발생하고 있다. 그러나 디지털 컨텐츠에 대한 조작이나 변형을 검출하기 위한 기술은 하나의 화소라도 변형이 발생 되었을 경우 삽입된 워터마크는 쉽게 부수어져야 하며, 변형이 발생된 위치도 쉽게 검출할 수 있어야 한다. 디지털 컨텐츠에 대한 무결성을 검증하기 위한 기술은 워터마크를 삽입한 후 컨텐츠에 대한 변형 여부를 확인하는 것으로 공간영역 및 주파수 영역에서 다양한 방법들이 제안되고 있다. 공간영역 방법은 영상의 화질 저하를 최소화하기 위해 주로 화소의 LSB에 워터마크를 삽입하여 영상의 변형 여부를 확인한다. 공간영역 방법에서는 워터마크가 삽입되는 화소를 일정 크기의 블록 단위로 구성하여 워터마크를 삽입하게 되면 워터마크의 검출과 영상의 변형 유무를 확인하는데 용이한 장점이 있으나 하나의 화소가 변형되더라도 화소가 속해있는 블록 단위로 변형 위치가 검출되는 단점이 있다[4-6].

본 논문에서는 디지털 영상을 특정 블록 단위로 분할하여 워터마크를 삽입한 후 변형 유, 무와 변형 위치를 최소의 블록 단위로 검출하기 위한 방법을 메시지 인증 코드를 이용하여 제안한다.

2. 관련 연구

2.1 워터마킹 기술 분석

워터마킹 기술의 목적을 살펴보면 먼저, 워터마킹은 영상의 저작권 보호를 위한 목적으로 기술이 개발 되었으며, 저작권 보호를 위해서는 워터마크가 삽입된 영상에 대하여 왜곡이나 필터링 그리고 압축과 같은 다양한 공격이 인가되더라도 삽입된 워터마크는 추출될 수 있어야 한다. 이와 같이 다양한 공격에 대하여 삽입된 워터마크가 파괴되지 않고 견뎌낼 수 있는 워터마킹 기술을 Robust Watermarking이라고 한다. 그러나 이러한 공격이 인가될 경우 삽입된 워터마크는 손실이 발생 될 수밖에 없으며, Robust Watermarking에서는 삽입된 워터마크의 손실을 최소화하기 위한 방법이 필요하며 이를 완벽하게 해결하기 위한 기술 개발은 현실적으로 매우 어렵다.

워터마킹 기술의 또 다른 응용 분야로, 워터마크가 삽입된 영상에 대하여 작은 변화라도 발생하였을 경우 변형된 위치를 효과적으로 검출하기 위한 방법이 제안되었다. 이 방법은 워터마크가 삽입된 영상에 대하여 사소한 변형이라도 발생되었을 경우 삽입된 워터마크가 쉽게 부수어져야 되는 특성을 가지고 있어야 하며 이것을 Fragile Watermarking이라고 한다[7,8]. Fragile Watermarking에서는 삽입된 워터마크가 원본과 다를 경우 워터마킹 된 영상의 조작 여부와 조작 위치를 확인할 수 있기 때문에 인증이나 무결성 검증용으로 활용할 수 있다.

따라서 저작권 보호를 위한 워터마킹과 무결성 검증을 위한 워터마킹은 삽입된 워터마크의 손실 여부가 매우 다른 특성을 가지고 있다. 즉, 저작권 보호를 위한 Robust Watermarking에서는 저작권 정보를 확인하기 위하여 다양한 공격에 대하여 삽입된 워터마크에 대한 변형이 최소화 되는 것이 가장 중요하고 무결성 검증을 위한 Fragile Watermarking에서는 변형 여부를 쉽게 알 수 있도록 삽입된 워터마크가 쉽게 파괴되어야 하는 특성을 가지고 있어야 한다.

워터마크를 영상에 삽입하는 방법은 크게 두 가지로 나눌 수 있다. 첫 번째 방법은 영상을 구성하는 화소에 직접 워터마크를 삽입하는 공간영역 방법이 있다. 공간영역 워터마킹 방법은 영상을 구성하는 화소의 값을 변경하여 워터마크를 삽입하는 것으로 화질 저하를 최소화하기 위해 영상의 LSB 위주로 워터마크를 삽입하고 있다. 공간영역 워터마킹 방법에서는 암호 기술을 적용할 경우 인증과 무결성 검증이 가능한 장점이 있다.

두 번째 방법은 영상을 주파수 영역으로 나눈 후 특정 주파수 영역에 워터마크를 삽입하는 주파수 영역 워터마킹 방법이 있다. 주파수 영역에서 워터마크를 삽입하는 방법은 Wavelet Transform, Fourier Transform, Discrete Cosine Transform(DCT) 등을 사용하여 영상을 주파수 영역으로 변환하여 워터마크를 삽입하는 것으로 공간영역 방법보다 잡음이나 압축과 같은 공격에 강하여 저작권 보호를 위한 워터마킹 방법에서 주로 사용하고 있다.

2.2 무결성 검증 기술

무결성 검증은 데이터의 변형 여부를 확인하기 위한 것으로 암호학적으로 안전한 일방향 해쉬 함수(Hash Function)를 사용하여 구현할 수 있으며, 일방향 해쉬 함수의 특징은 다음과 같다.

- 임의 길이의 입력 데이터로부터 항상 고정된 길이의 출력을 생성한다.
- 동일한 입력에 대해서는 항상 동일한 출력을 생성하고, 입력 데이터가 다르면 출력 값도 다르게 생성된다.
- 해쉬 함수의 출력으로부터 입력 데이터를 찾는 것이 불가능해야 한다.
- 동일한 출력을 생성하는 서로 다른 입력 데이터를 발견하기 어려운 충돌 내성을 가지고 있어야 한다.

해쉬 함수는 소프트웨어의 변경과 패스워드 보안 등 메시지의 무결성 검증을 위해 사용할 수 있지만 거짓 행위는 검출할 수 없으며, 이러한 문제는 메시지 인증 코드를 통해 해결할 수 있다.

2.3 메시지 인증 코드

메시지 인증 코드(MAC : Message Authentication Code)는 데이터에 대한 무결성을 확인하고 송신자를 확인할 수 있는 기술로 데이터와 비밀키를 해쉬 함수의 입력으로 사용하여 생성되는 출력을 말한다. 메시지 인증 코드는 해쉬 함수의 특성을 이용하여 무결성을 검증하고 송, 수신자만이 가지고 있는 비밀키를 통해서 인증을 수행한다. 따라서 워터마크가 삽입된 이미지에 대하여 하나의 화소라도 변형이 발생 되었을 경우 이를 검출하기 위하여 메시지 인증 코드를 사용한다.

3. 워터마크 생성

본 논문에서는 전체 영상을 16×16 블록 단위로 분할한 후 하위 두 개의 LSB에 워터마크를 삽입하여 16×16 블록 단위로 변형 여부를 검사하고 만약, 변형이 발생된 블록이 있을 경우 변형이 발생된 16×16 블록에 대하여 4×4 블록 단위로 변형 화소를 검출하며, 제안 방법은 다음과 같은 과정으로 워터마크를 생성한다.

3.1 영상 분할

공간영역에서 워터마크를 삽입하기 위하여 Fig. 1과 같이 원 영상을 여러 개의 16×16으로 분할하고 분할된 하나의 블록은 총 256개의 화소로 구성된다. 분할된 블록은 워터마크를 삽입하기 위해 블록 내의 모든 LSB와 256개의 화소 중 첫 번째부터 128번째까지 화소의 두 번째 LSB를 0으로 초기화한다.

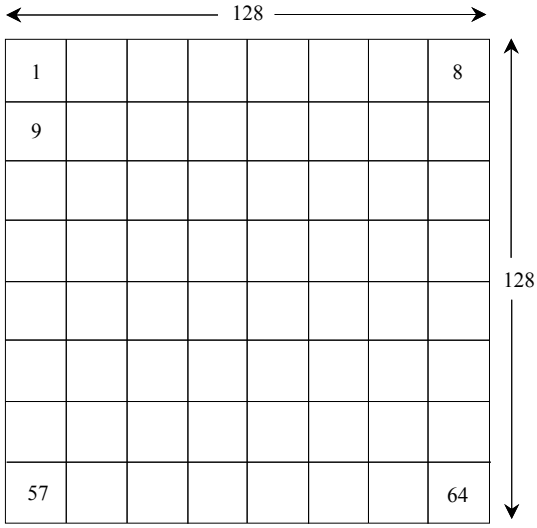

Fig. 1. Image segmentation

3.2 무결성 검사용 메시지 인증 코드

초기화된 16×16 블록에 대한 변형 여부를 검사하기 위해 사용되는 메시지 인증 코드는 Fig. 2의 정보를 메시지 인증 코드의 입력으로 사용하여 생성한다. 본 논문에서는 메시지 인증 코드 생성을 위해 MD5 해쉬 함수를 사용하므로 128비트의 메시지 인증 코드가 생성된다. 128비트의 메시지 인증 코드는 블록 내 256개 화소의 1/2인 128개 화소의 2번째 LSB에 삽입한다.

Initialized 16×16 block	Block Number	Unique Information

Fig. 2. MAC input information

16×16 블록은 총 256개의 화소를 가지므로 메시지 인증 코드는 256비트까지 생성하여 삽입할 수 있다. 따라서 16×16 블록에 삽입된 메시지 인증 코드를 검사하면 해당 블록에 대한 변형 여부를 알 수 있으며, 변형이 발생되었을 경우 블록 내에서 변형이 발생된 화소를 검

출하기 위해 16×16 블록을 다시 4×4 블록으로 분할하여 변형이 발생된 화소를 검출한다.

3.3 변형 화소 검사용 메시지 인증 코드

16×16 블록에 대한 변형이 발생하였을 경우 변형이 발생된 화소는 4×4 블록 단위로 검사한다. 이를 위해 16×16 블록은 Fig. 3과 같이 4×4 크기를 가지는 16개의 서브 블록으로 분할한다.

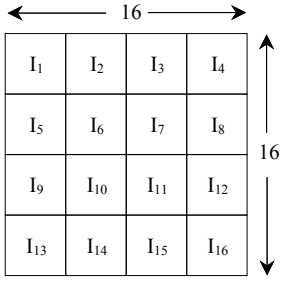

Fig. 3. 4x4 sub blocks of 16x16 block

Fig. 3의 서브 블록(I_1~I_{16})에서 각 블록은 16개의 화소로 구성되며 각 화소의 LSB에 16개의 워터마크를 삽입하여 4×4 블록에 대한 변형 여부를 확인한다. 4×4 블록에 대한 초기화는 16×16 블록을 초기화할 때 초기화 되며, 4×4 블록에 대한 변형 검사를 위한 워터마크는 다음과 같이 생성한다.

① 초기화된 4×4 블록에 포함된 화소들에 대한 밝기 값의 평균을 식 (1)과 같이 계산한다.
밝기 평균 = (화소$_1$ + ⋯ + 화소$_{16}$) / 16 (1)

② 각 화소에 대해 다음 값을 구한다
1 : 초기화된 화소 값 ≥ 밝기 평균 값
0 : 그 밖의 경우

120	120	118	116
120	122	118	110
116	118	120	120
122	120	120	118

(a) 4×4 Image block

1	1	0	0
1	1	0	0
0	0	1	1
1	1	1	0

(b) Binary pattern

Fig. 4. Binary pattern generating process

Fig. 4의 경우 밝기 평균은 118.63이므로 118.63보다 크거나 같은 값을 가지는 화소는 1, 작은 값을 가지는 화소는 0으로 한다.

③ 16×16 블록에 대한 메시지 인증 코드를 생성하는 Fig. 2의 입력과 유사한 방법으로 초기화된 4×4 블록과 Fig. 5와 같은 서브 블록 번호 그리고 영상에 대한 고유정보를 입력으로 사용하여 128비트 메시지 인증 코드를 생성한다.

Fig. 5는 Fig. 1의 57번 블록에 대한 서브 블록(4×4)들을 나타낸다. 블록 번호는 블록 단위로 복사 할 경우 이를 방지하기 위한 용도로 사용되기 때문에 블록 번호는 다른 블록과 중복되지 않게 설정한다. 또한 고유정보는 영상에 대한 일련번호와 같이 워터마크가 삽입된 영상을 구분하기 위한 정보로써 고유한 값을 가지는 정보를 사용한다.

57-1	57-2	57-3	57-4
57-5	57-6	57-7	57-8
57-9	57-10	57-11	57-12
57-13	57-14	57-15	57-16

Fig. 5. 4×4 sub-block number

④ 128비트 메시지 인증 코드는 Fig. 6과 같이 16비트씩 분할하여 8개의 16비트 블록을 생성하고 이 블록들에 대하여 XOR 연산을 수행하여 16비트 결과를 생성한다.

⑤ ②에서 구한 16비트와 ④에서 구한 16비트에 대해 XOR 연산을 수행하여 생성된 16비트를 4×4 블록 내 모든 화소의 LSB에 삽입한다. 이러한 과정은 모든 4×4 블록들에 대해 수행한다.

16×16 블록에 대한 변형 여부를 검사하기 위한 정보는 128비트로 구성되기 때문에 블록 내 모든 256개의 화소에 삽입할 필요가 없다. 그러나 4×4 블록을 검사하기 위한 정보는 16비트로 구성되기 때문에 블록 내의 전체 화소에 삽입되어야 한다. 따라서 화질 저하를 최소화하기 위하여 16×16 블록 검사를 위한 정보는 블록 내

256개의 화소 중 128개 화소의 두 번째 LSB에 삽입하고 4×4 블록을 검사하기 위한 정보는 4×4 블록 내 모든 화소의 LSB에 삽입한다.

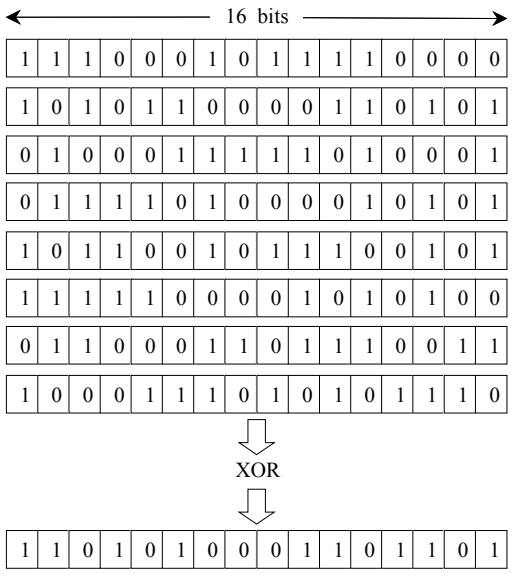

Fig. 6. Watermark generating process

4. 워터마크 추출 및 변형 검출

본 논문에서는 전체 영상을 16×16 블록으로 분할하여 분할된 블록 단위로 영상의 변형 여부에 대한 검사를 수행한 후 변형이 발생 된 블록이라고 판단될 경우 해당 블록을 4×4 블록으로 분할한 후 변형 위치를 4×4 블록 단위로 검출한다. 이를 위해 각 블록에서 메시지 인증 코드를 추출한 후 메시지 인증 코드를 생성하는 방법과 동일한 과정으로 메시지 인증 코드를 생성하고 추출된 메시지 인증 코드와 비교하여 블록의 변형 유무를 검사한다.

4.1 영상 변형 검출

영상에 삽입된 워터마크를 추출하고 변형 유무를 확인하기 위해서는 Fig. 1과 같이 워터마크가 삽입된 영상을 16×16 블록 단위로 나누어 검사를 수행한다. 워터마크는 각 블록을 구성하는 블록 내 화소의 LSB와 두 번째 LSB에 삽입되며 두 번째 LSB에 삽입된 워터마크는 16×16 블록에 대한 변형 여부를 검사하기 위한 정보이고 LSB에 삽입된 워터마크는 변형이 발생된 16×16 블록 내에서 변형이 발생 된 화소를 4×4 블록 단위로 검출하기 위한 정보이다. 따라서 각 블록의 LSB와 두 번째 LSB에 삽입된 워터마크를 추출한 후, 워터마크를 삽입하는 과정과 동일하게 Fig. 2를 기반으로 메시지 인증 코드를 생성하여 두 번째 LSB에서 추출된 메시지 인증 코드와 비교한다. 만약 두 개의 메시지 인증 코드가 서로 다르면 해당 16×16 블록은 변형이 발생된 블록에 해당하여 블록을 다시 4×4 단위로 분할하여 Fig. 3~Fig. 6의 과정으로 4×4 블록 검사용 메시지 인증 코드를 생성하고 4×4 블록의 LSB에서 추출한 값과 비교하여 변형 위치를 확인한다. 이와 같은 과정으로 변형 위치를 확인하면 블록 내 화소중 하나의 화소에서만 변형이 발생 되더라도 4×4 블록 단위로 변형 부분이 검출된다. 블록 내에서 변형이 발생 된 화소를 최소의 영역으로 검출하기 위해서는 하나의 화소 또는 최소의 블록 단위로 워타마크를 삽입해야 되는데 블록의 크기가 작을수록 삽입되는 워터마크의 조작이 비교적 용이할 수 있다. 따라서 본 논문에서는 암호학적으로 안전한 메시지 인증 코드를 워터마크로 사용하여 4×4 블록에 대한 변형 위치를 확인한다.

제안 방법은 비밀키를 사용하는 메시지 인증 코드를 사용하기 때문에 비밀키가 노출될 경우 삽입되는 워터마크가 조작될 수 있는 단점이 있다. 이와 같은 문제는 공개키 암호를 적용하면 해결이 가능하나 공개키 암호는 암호문의 크기가 일정하지 않고 암호문이 평문 블록보다 커질 수 있는 단점이 있다. RSA 공개키 암호를 사용하여 작은 크기의 블록 단위로 워터마크를 삽입할 경우, 공개키를 생성하기 위한 두 소수(p, q)의 크기는 작아야 되는데 두 소수의 크기가 작아질 경우 공개키 암호에 사용되는 키 사이즈가 작아져서 암호문의 안전성에 문제가 발생할 수 있다.

5. 결론

디지털 워터마킹 기술은 저작권 보호를 위해 개발 되었으나 인증과 변형 검출을 위한 용도로도 활용되고 있다. 디지털 워터마킹의 저작권 보호를 위한 기술에서는 삽입된 정보가 다양한 공격에 대하여 강인해야 되는 특성이 있어야 되는 반면, 변형 검출을 위한 워터마킹에서는 영상에 대한 사소한 조작에 대해서도 조작여부를 확인하고 조작 위치를 검출할 수 있어야 한다.

본 논문에서는 영상의 변형 검출을 위한 워터마킹 방법을 제안하였으며, 제안 방법에서는 공간영역에서 각 화소의 하위 2개의 LSB에 워터마크를 삽입하고 변형 여부

를 16×16 블록 단위로 확인한다. 그리고 변형이 발생된 16×16 블록에 대해서는 4×4 블록 단위로 검사를 수행하여 변형 위치를 확인한다. 메시지 인증코드를 사용한 제안 방법은 영상의 변형 여부를 확인하기 위한 다양한 응용 분야에 적용할 수 있으나 비밀키를 사용하는 메시지 인증 코드의 한계로 키가 노출될 경우 삽입된 워터마크의 조작이 가능한 단점이 있다. 따라서 이러한 문제를 해결하기 위한 연구가 필요하다.

References

[1] 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

[2] Yoo, Heung-Ryol, Son, Yung-Deug, "Fragile Watermark System using Quantization and DC Coefficients", Journal of IKEEE, Vol. 22, No. 3, pp. 774-779, 2018.
DOI: https://doi.org/10.7471/ikeee.2018.22.3.774

[3] P. MeenakshiDevi, M. Venkatesan and K. Duraiswamy, "A Fragile Watermarking Scheme for Image Authentication with Tamper Localization Using Integer Wavelet Transform", Journal of Computer Science, Vol. 5, No. 11, pp. 831-837, 2009.
DOI: https://doi.org/10.3844/jcssp.2009.831.837

[4] A.Kannammal, S.Subha Rani, "Authentication of DICOM Medical Images using Multiple fragile watermarking Techniques in Wavelet Transform Domain", International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, pp. 181-189, 2011.

[5] S. Dadkhah, A. Abd Manaf and S. Sadeghi, "Efficient Digital Image Authentication and Tamper Localization Technique Using 3Lsb Watermarking", International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, pp. 1-8, 2012.

[6] Heng Zhang, Chengyou Wang, and Xiao Zhou, "Fragile Watermarking Based on LBP for Blind Tamper Detection in Images", Journal of Information Processing Systems, Vol. 13, No. 2, pp. 385-399, 2017.
DOI: https://doi.org/10.3745/JIPS.03.0070

[7] M. A. Hajjaji, S. Ajili, A. Mtibaa, E. Bourennane, "Fragile Method for Watermarking of Medical Image: Method Based LSBs", International Journal of Sciences and Techniques of Automatic control & computer engineering IJ-STA, Vol. 6, No. 1, pp. 1764-1781, 2012.

[8] P. Rahmati, A. Adler, T. Tran, " Watermarking in E-commerce", International Journal of Advanced Computer Science and Applications, Vol. 4, No. 6, pp. 256-265, 2013
DOI: https://doi.org/10.14569/ijacsa.2013.040634

우 찬 일(Chan-Il Woo) [종신회원]

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

〈관심분야〉
정보보호, 암호 프로토콜, 디지털워터마킹, 소프트웨어 공학

구 은 희(Eun-Hee Goo) [정회원]

- 2004년 8월 : 단국대학교 대학원 전자컴퓨터공학과 (공학석사)
- 2009년 8월 : 단국대학교 대학원 전자컴퓨터공학과 (공학박사)
- 2013년 3월 ~ 2014년 9월 : ㈜도넛시스템 LSI 책임연구원
- 2014년 10월 ~ 2016년 8월 : ㈜이너트론 이동통신연구소 수석연구원
- 2016년 9월 ~ 현재 : 아주대학교 다산학부대학 교수

〈관심분야〉
정보보호, 암호 알고리즘, 서비스로서의 보안(ASCaaS), 소프트웨어 공학