Journal of the Korea Academia-Industrial cooperation Society
Vol. 15, No. 7 pp. 4516-4521, 2014

http://dx.doi.org/10.5762/KAIS.2014.15.7.4516
ISSN 1975-4701 / eISSN 2288-4688

해쉬 함수를 이용한 디지털 영상의 위변조 검출

우찬일[1*], 이승대[2]
[1]서일대학교 정보통신과, [2]남서울대학교 전자공학과

Tamper Detection of Digital Images using Hash Functions

Chan-Il Woo[1*], Seung-Dae Lee[2]
[1]Dept. of Information and Communication Engineering, Seoil University
[2]Dept. of Electronic Engineering, Namseoul University

요 약 디지털 영상의 인증과 무결성을 위한 워터마킹은 fragile 워터마킹을 기반으로 하고 있으며, 워터마크가 삽입된 영상에 대해 삽입된 워터마크와 조작에 의해 변형된 워터마크를 비교함으로써 영상의 변형 여부를 검출할 수 있다. 따라서 스케일링이나 필터링과 같은 영상처리에 의한 변형이 발생할 경우 영상의 인증과 무결성을 위한 워터마크는 쉽게 제거되어야 한다. 본 논문에서는 디지털 영상에 대하여 효과적인 변형 검출 방법을 제안한다. 제안 방법에서는 원 영상을 중첩되지 않은 2×2 크기의 블록으로 나누어 각 블록의 하위 2개의 LSB에 워터마크를 삽입하며, 워터마크 삽입으로 인한 영상의 왜곡은 사람의 눈으로 인지할 수 없다. 그리고 워터마크 추출 과정을 통해 워터마크가 삽입된 영상이 변형 되었는지의 여부를 결정할 수 있으며, 실험 결과는 제안 방법의 효율성을 나타내고 있다.

Abstract Digital watermarking for digital image authentication and integrity schemes are based on fragile watermarking and can detect any modifications in a watermark embedded image by comparing the embedded watermark with the regenerated watermark. Therefore, the digital watermark for image authentication and integrity should be erased easily when the image is changed by digital image processing, such as scaling or filtering etc. This paper proposes an effective tamper detection scheme for digital images. In the proposed scheme, the original image was divided into many non-overlapping 2×2 blocks. The digital watermark was divided into two LSB of each block and the image distortion was imperceptible to the human eye. The watermark extraction process can be used to determine if the watermarked image has been tampered. The experimental results successfully revealed the effectiveness of the proposed scheme.

Key Words : Fragile Watermarking, Spatial Domain, Tamper Detection

1. 서론

유, 무선 네트워크 기술의 발전은 정보를 보다 효과적으로 전송할 수 있는 환경을 제공하게 되어, 디지털 멀티미디어 데이터를 빠르고 효율적으로 전송할 수 있게 되었다. 그러나 사생활 정보와 같은 중요한 데이터를 네트워크를 통해 전송할 경우 제3자로부터 안전하게 보호할 수 있는 방법이 필요하다. 또한 디지털 영상 처리 기술의 발전은 영상 데이터를 보다 용이하게 편집할 수 있는 환경을 제공하고 있어 다양한 분야에서 널리 사용되고 있으나, 허가되지 않은 사용자로부터 디지털 영상 데이터를 불법적으로 조작하고 복제하는 것이 가능하여 이를 방지할 수 있는 방법이 필요하다[1,2].

일반적으로 중요한 데이터를 보호하기 위한 방법으로 암호화 기술을 사용하고 있다. 그러나 암호화 기술은 데이터를 보호하기 위한 효과적인 방법을 제공하고 있으나

본 논문은 2013년도 서일대학교 학술연구비에 의해 연구되었음.
*Corresponding Author : Chan-Il Woo(Seoil Univ.)
Tel: +82-2-490-7556 email: ciwoo@seoil.ac.kr
Received March 11, 2014 Revised April 10, 2014 Accepted July 10, 2014

정당한 사용자에 의해 복호화 된 데이터는 원본 데이터와 동일하기 때문에 복호화 된 데이터를 사용자가 임의로 조작하거나 불법적으로 배포를 할 수 있는 문제점이 발생할 수 있다. 따라서 정지영상이나 동영상과 같은 멀티미디어 데이터는 허가되지 않은 사용자로 부터 불법적인 조작이나 배포가 이루어질 수 있어 이를 해결할 수 있는 기술이 요구되고 있으며, 멀티미디어 데이터에 대한 불법적인 조작 여부를 확인하거나 저작권자의 소유권을 보호하기 위한 방법의 중요성은 점점 더 증가하고 있다. 이를 위해 시각적으로 인지할 수 없는 정보를 멀티미디어 데이터에 삽입하여 데이터의 조작 여부를 확인하거나 소유권을 증명할 수 있는 방법을 제공할 수 있는 디지털 워터마킹 기술이 대두 되었으며, 디지털 워터마킹 기술은 이러한 문제점들을 해결하기 위한 중요한 기술로 부각되고 있다[3].

디지털 영상에 대한 워터마킹 기술은 저작권 보호를 위한 워터마킹 기술과 영상의 인증과 무결성을 확인하기 위한 워터마킹 기술로 구분할 수 있다. 저작권 보호를 위한 워터마킹 기술은 워터마킹 된 영상에 대하여 필터링이나 이미지 왜곡과 같은 다양한 후처리 과정에도 삽입된 워터마크가 파괴되지 않아야 되는 강인한 특성을 가지고 있어야 한다. 그러나 인증과 무결성 확인을 위한 워터마킹 기술에서는 워터마킹 된 영상에 대하여 사소한 조작이 발생하더라도 삽입된 워터마크가 쉽게 파괴 되어야하는 특성을 가지고 있어야 한다.

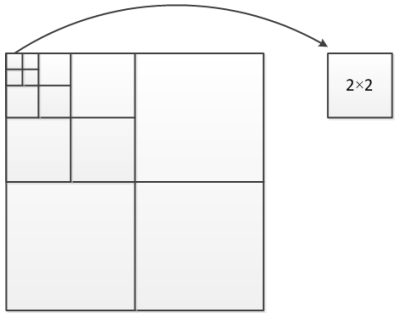
저작권 보호를 위한 워터마킹 기술에서는 워터마킹 된 영상의 불법적인 복제나 조작으로 부터 소유권자를 확인하기 위하여 법적인 근거 자료로 워터마크를 사용할 수 있으며, 인증과 무결성을 위한 워터마킹 기술에서는 수신자가 영상의 변형 여부와 송신자를 확인하기 위한 용도로 워터마크를 사용한다. 인증과 무결성을 위한 워터마킹 기술은 의료 영상이나 디지털 영상의 조작 여부를 확인하기 위하여 다양한 분야에서 광범위하게 연구되고 있다[4-6].

디지털 영상에 대한 인증과 무결성을 확인하기 위한 워터마킹 기술의 대표적인 방법으로, Wong[7]은 영상을 작은 크기의 블록으로 분할한 후 각 블록의 LSB에 워터마크를 삽입하는 방법을 공개키 암호를 이용하여 제안하였다. 그러나 Wong의 방법은 워터마크가 삽입된 영상의 LSB를 제거하게 되면 삽입된 워터마크가 모두 제거되어 공격자가 임의로 생성한 워터마크를 삽입할 수 있는 단점이 있다. Wong의 방법과 같이 블록을 기반으로 하여 공간영역에서 수행되는 워터마킹에서는 화소의 최상위 비트 부분에 워터마크를 삽입하게 되면 화질 저하가 많이 발생하게 되는 단점이 있고, 원 영상을 여러 블록으로 나눌 때 나누어진 블록의 크기가 커질 경우 워터마킹 된 영상에서 조작되는 부분이 미세하더라도 변형이 검출되는 영역은 커지게 되는 단점이 있어 블록 크기와 화질 저하를 고려하여 효율적으로 워터마크를 삽입할 수 있는 방법이 필요하다. 관련 연구로 Lin[8] 등이 제시한 방법에서는 디지털 영상 인증을 위하여 인증 데이터와 워터마크가 삽입된 영상에 조작이 발생하였을 경우 변형 된 영역을 복구할 수 있는 데이터를 워터마크로 사용하여 인증과 변형된 부분을 스스로 복구할 수 있는 방법을 제안하였다. 그러나 워터마크가 삽입된 영상에서 변형 부분이 많이 발생할 경우 복구 되는 영상의 품질은 좋지 않게 되는 단점이 있다. 본 논문에서는 디지털 영상에 대하여 미세한 조작이 발생하더라도 변형된 영역을 보다 효과적으로 검출하기 위한 방법을 제안한다. 제안 방법은 원 영상을 2×2 크기의 작은 블록들로 나눈 후 나누어진 각 블록 화소의 하위 두 개의 비트에 워터마크를 삽입하여 워터마크가 삽입된 영상에 변형이 발생할 경우 변형 위치를 2×2 블록 단위로 검출할 수 있는 장점이 있다.

2. 제안 방법

2.1 영상 분할

워터마크 생성과 삽입을 위해 원 영상을 2×2 크기의 작은 블록들로 분할한다.



[Fig. 1] 2×2 blocks of original image

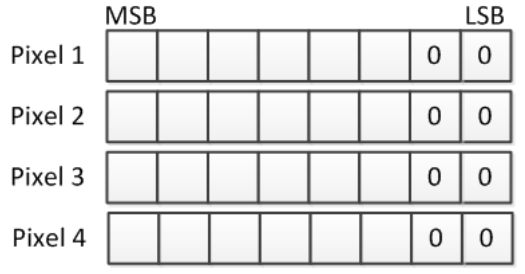
Fig. 1과 같이 분할된 영상 블록들은 1~n까지의 번호

를 부여한다. 만약, 원 영상의 크기가 32×32일 경우, (32×32)/(2×2)=256개의 블록들로 분할되고 각 블록들은 1~256까지의 번호가 주어진다. 이와 마찬가지로 원 영상의 크기가 256×256일 경우 16,384개의 블록들로 분할되고 각 블록들은 1~16,384까지의 번호가 주어진다.

이와 같이 영상을 2×2 크기의 블록들로 분할하는 이유는 워터마크가 삽입되는 영상에 대하여 미세한 조작이 발생하였을 경우, 변형이 발생된 화소를 보다 정밀하게 검출하기 위해서이다. 만약, 분할되는 영상 블록이 8×8 크기를 가지게 될 경우 블록 내에서 하나의 화소만 조작되더라도 변형된 화소의 위치는 8×8 블록 단위로 검출되기 때문에 보다 작은 블록들로 나눌 수 있다면 조작되는 위치 또한 보다 정밀하게 검출할 수 있게 된다.

2.2 워터마크 생성

분할된 2×2 크기의 영상 블록들 내의 화소들의 하위 2비트는 워터마크 생성과 삽입을 위해 "0"으로 초기화한다.



[Fig. 2] Pixels of block

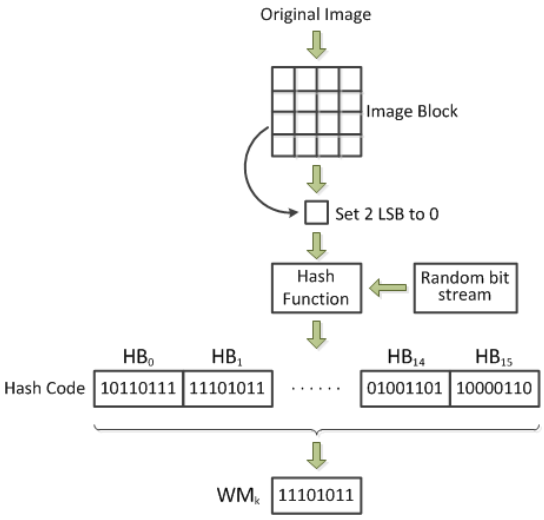
Fig. 2와 같이 초기화된 4개의 화소들은 임의의 비트 스트림과 함께 해쉬 함수의 입력으로 사용하여 해쉬 코드를 생성한다. 해쉬 함수는 입력으로 사용되는 데이터 스트림이 한 개의 비트라도 다르게 될 경우 생성되는 해쉬 코드는 매우 달라지게 되는 특성이 있다. 또한 해쉬 함수는 생성된 해쉬 코드로부터 동일한 해쉬 코드를 생성하는 서로 다른 입력 쌍을 찾는 것이 어려운 특징을 가지고 있는 일방향 함수로 일반적으로 디지털 서명에 사용된다.

본 논문에서는 MD5 해쉬 함수를 사용하여 128비트 해쉬 코드를 생성하며, MD5 해쉬 함수로 부터 생성된 128비트의 해쉬 코드는 8개의 비트 단위로 분할하여 총 16(블록번호 0~15)개의 해쉬 코드 블록들을 생성한다. 해쉬 코드를 8개의 비트 단위로 분할하는 이유는 2×2 화소로 분할된 영상 블록에 속해있는 화소들의 하위 2개의 비트에 해쉬 코드 비트 블록으로 부터 생성되는 워터마크(8개의 비트로 구성)를 삽입하기 때문이다.

따라서 k번째 영상 블록의 워터마크는 임의의 비트 스트림과 함께 초기화된 k번째 영상 블록을 해쉬 함수의 입력으로 사용하여 128 비트의 출력을 생성한다. 그리고 생성된 해쉬 코드는 8 비트 단위로 분할하여 16개의 해쉬 코드 블록들을 생성하고 그 중 하나의 해쉬 코드 블록(8비트)을 선택하여 k번째 영상 블록에 삽입할 워터마크(WM_k)로 사용한다. 본 논문에서 사용하는 해쉬 코드 블록(HB_i)은 다음의 연산을 통해 선택한다.

$$HB_i = k \bmod 16,\ i = 0 \sim 15 \quad (1)$$

여기서, k는 워터마크가 삽입되는 2×2 크기의 블록 번호를 나타낸다.



[Fig. 3] Generation of 8-bit watermark

Fig. 3은 k번째 2×2 블록에 삽입되는 워터마크(WM_k)의 생성 과정을 나타내고 있으며, 워터마크 생성에 사용되는 Random bit stream은 임의의 정보 또는 로고와 같은 이미지를 사용할 수 있으며, 블록 복사를 방지하기 위하여 각 블록마다 서로 다른 bit stream을 사용할 수 있다. 이미지를 Random bit stream으로 사용할 경우 이미지 데이터를 초기화된 2×2 영상 블록과 함께 해쉬 함수의 입력으로 사용하여 해쉬 코드를 생성한다. 그리고 8비트 단위로 나누어진 해쉬 코드 블록들은 식 (1)을 사용하

여 하나의 해쉬 코드 블록을 선택하여 워터마크로 사용한다. 예를 들어, 128번째 영상 블록에 워터마크를 삽입할 경우, 임의의 비트 스트림과 128번째 영상 블록으로부터 생성된 해쉬 코드 블록들 중 0번째(128 mod 16) 해쉬 코드 블록이 워터마크로 사용된다. Fig. 3의 워터마크 생성 과정은 원 영상을 2×2 블록으로 분할한 후 분할 된 모든 블록들에 대하여 반복적으로 수행하여 워터마크를 생성하고 삽입한다.

2.3 워터마크 추출

삽입된 워터마크는 다음과 같은 과정으로 추출하여 워터마크가 삽입된 영상에 대한 조작 유무를 판단한다.

2.3.1 영상 분할

워터마크 삽입 과정과 동일하게 워터마크가 삽입된 영상을 2×2 크기로 분할하고, 분할된 영상은 1~n까지의 블록 번호를 부여한다.

2.3.2 워터마크 추출 및 생성

워터마크를 추출하기 위하여 워터마크가 삽입된 영상은 워터마크 삽입 과정과 동일하게 2×2 크기의 블록으로 나눈다. 그리고 각 블록에 포함된 4개의 화소에서 하위 2개의 LSB에 삽입된 워터마크를 추출하고 “0”으로 초기화한다. 초기화된 블록은 워터마크 삽입에 사용한 임의의 비트 스트림과 함께 해쉬 함수의 입력으로 사용하여 128 비트의 해쉬 코드를 생성한다. 이와 같은 과정으로 생성된 해쉬 코드는 16개의 블록으로 나눈 후, 워터마크 생성을 위해 사용된 식 (1)을 사용하여 하나의 8비트 해쉬 코드 블록을 선택한다.

2.3.3 변형 유무 검사

워터마킹 된 영상에서 추출된 워터마크는 워터마크 삽입과정과 동일한 과정으로 생성된 워터마크와 비교하는데 만약, 생성된 워터마크와 추출된 워터마크가 서로 다르게 될 경우, 워터마크가 삽입된 영상에 대하여 조작이 발생한 것으로 판단하여 해당 영상 블록이 변형되었음을 체크한다.

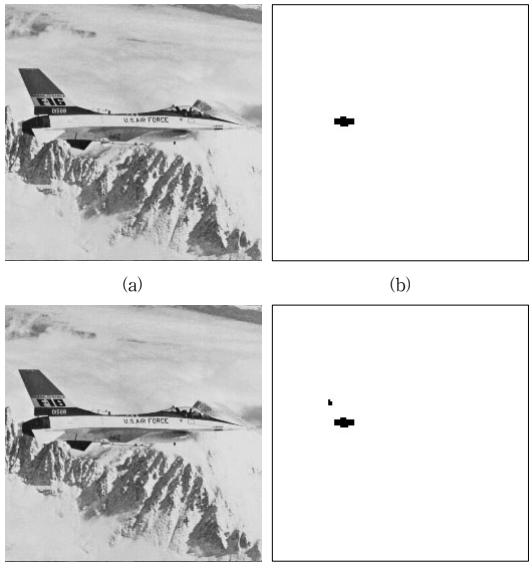
3. 실험 및 결과

본 논문에서는 256×256 크기의 영상을 대상으로 실험하였으며, 원 영상은 16,384개의 블록들로 분할되고 각 블록들은 1~16,384까지의 번호가 부여된다.

(a) (b)

(c) (d)

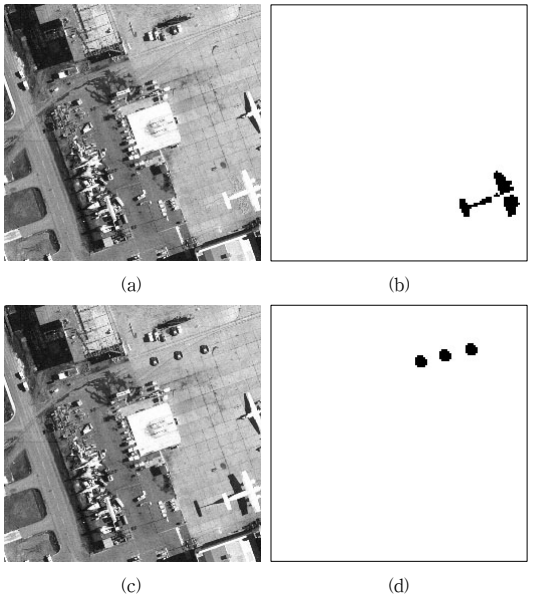
[Fig. 4] The image used for an experiment
(a) AIRPLANE (b) AIRFIELD
(c) CAMERA (d) HOUSE



(a) (b)

(c) (d)

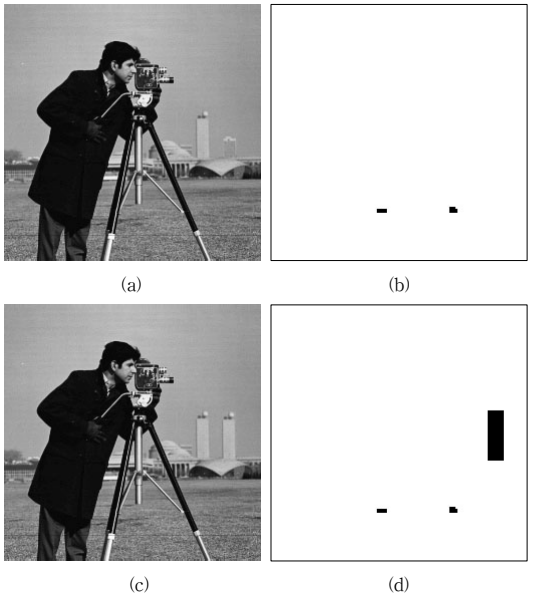
[Fig. 5] Tampered image and tamper detection result
(a), (c) Tampered image
(b), (d) Tamper detection result



(a) (b)

(c) (d)

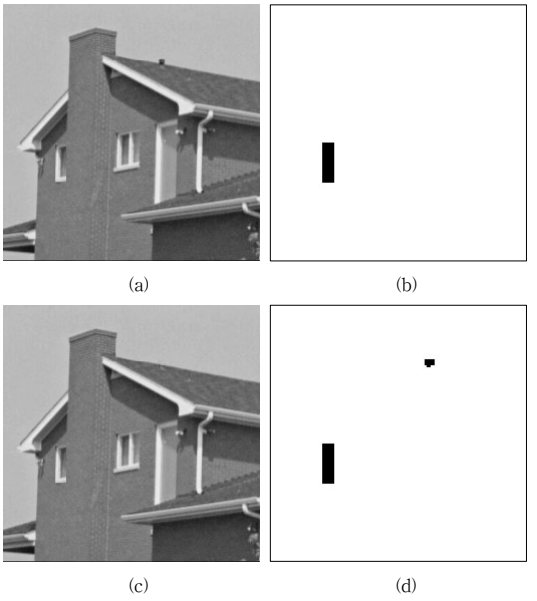
[Fig. 6] Tampered image and tamper detection result
(a), (c) Tampered image
(b), (d) Tamper detection result



(a) (b)

(c) (d)

[Fig. 7] Tampered image and tamper detection result
(a), (c) Tampered image
(b), (d) Tamper detection result



(a) (b)

(c) (d)

[Fig. 8] Tampered image and tamper detection result
(a), (c) Tampered image
(b), (d) Tamper detection result

실험 결과를 살펴보면, Fig. 5의 (a)와 같이 특정 영역을 제거하거나 (c)와 같이 특정 영역 제거와 조작이 동시에 이루어질 경우에도 변형된 위치를 정확하게 검출할 수 있었다. Fig. 6에서는 (a)와 같이 비행기의 그림자를 제거하거나 (c)와 같이 영상내의 특정 영역을 복사하여 붙여 넣었을 경우에도 변형된 부분을 2×2 블록 단위로 검출할 수 있음을 확인할 수 있다.

4. 결론

영상의 변형 여부를 검출하기 위해 영상을 작은 영역으로 나눈 후, 나누어진 블록을 기반으로 워터마크가 삽입되는 워터마킹 방법에서는 8×8 또는 16×16과 같이 여러 화소로 구성된 블록들에 워터마크가 삽입된다. 그러나 블록의 크기가 커지게 되면 블록 내에서 하나의 화소만 조작 하더라도 변형된 영역은 전체 블록 단위로만 검출되게 된다. 따라서 본 논문에서는 이러한 문제를 해결하기 위하여 영상을 2×2 크기의 작은 블록으로 나누어 워터마크를 삽입하고, 워터마킹 된 영상에 대하여 미세한 조작이 발생하더라도 변형된 부분을 보다 세밀하게 검출할 수 있는 방법을 제안하였다.

제안 방법에서는 워터마킹 된 영상의 일부분만을 제거하였을 경우에도 조작된 영역을 2×2 화소 블록 단위로 검출할 수 있음을 실험을 통하여 확인하였다. 또한, 워터마크가 삽입된 영상 블록들의 위치를 서로 바꾸거나 특정 블록을 다른 블록으로 복사할 경우에도 위, 변조된 영역을 효과적으로 검출할 수 있는 장점이 있어, 의료 영상과 같이 영상의 조작 여부를 확인하기 위한 분야에 효과적으로 활용할 수 있을 것으로 생각된다. 향후 연구 과제로는 정지영상 뿐만 아니라 음성이나 텍스트 그리고 동영상과 같은 다양한 데이터에도 제안 방법을 효과적으로 적용할 수 있는 방법에 대한 연구가 필요할 것이다.

References

[1] R. M. Rad, A. Attar and R. E. Atani, "A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR," International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 6, no. 5, pp. 275-290, 2013.
DOI: http://dx.doi.org/10.14257/ijsip.2013.6.5.25

[2] 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.

[3] M. Wu, B. Liu, "Watermarking for image authentication," ICIP 98, Vol. 2, pp. 437-441, October 1998.

[4] http://140.127.82.166/handle/987654321/15174

[5] 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

[6] H. Nyeem, W. Boles and C. Boyd, "Counterfeiting Attacks on Block-Wise Dependent Fragile Watermarking Schemes" in Proc. of the 6th International Conference on Security of Information and Networks, ACM Press and Digital Library, 2013.
DOI: http://dx.doi.org/10.1145/2523514.2523530

[7] 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

[8] P. L. Lin, C. K. Hsieh and P. W. Huang, "A Hierarchical Digital Watermarking Method for Image Tamper Detection and Recovery," Pattern Recognition, Vol. 38, no. 12, pp. 2519-2529, 2005.
DOI: http://dx.doi.org/10.1016/j.patcog.2005.02.007

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

이 승 대(Seung-Dae Lee) **[정회원]**

- 1992년 2월 : 단국대학교 대학원 전자공학과 (공학석사)
- 1999년 8월 : 단국대학교 대학원 전자공학과 (공학박사)
- 1995년 4월 ~ 현재 : 남서울대학교 전자공학과 교수

<관심분야>
정보통신, 유무선통신, 정보보호