한국항행학회 논문지 제13권 제3호 2009년 6월

영상 인증과 변형 검출을 위한 Fragile 워터마킹

Fragile Watermarking for Image Authentication and Detecting Image Modification

우찬일*, 전세길**

Chan-Il Woo*, Se-Gil Jeon**

요 약

디지털 워터마킹은 소유권 검증이나 인증을 목적으로 시각적으로 인지할 수 없는 정보를 영상에 삽입하는 기술로, 연성 워터마킹과 강인한 워터마킹으로 분류될 수 있다. 강인한 워터마크는 저작권과 소유권 주장을 위한 목적으로 유용하며 삽입된 워터마크는 쉽게 제거되지 않아야 하고 회전, 크기변환, 크롭핑 등과 같은 일반적인 영상처리에 견뎌내야 한다. 반면에 연성 워터마크는 어떠한 영상처리 과정에 의해서도 삽입된 워터마크는 쉽게 훼손되어야 하며, 영상의 사소한 변경뿐만 아니라 국부적으로 변경된 영역도 검출할 수 있어야 한다. 본 논문에서는 계층구조를 이용하여 영상의 무결성 검증과 변형 위치를 검출할 수 있는 연성 워터마킹 방법을 제안한다. 제안 방법에서는 워터마크가 삽입되는 영상을 여러 레벨로 구성하여 각 레벨별로 영상을 여러 블록으로 나눈 후 각 블록에 대한 디지털 서명을 계산한다. 제안 방법은 cut-and-paste와 같은 공격에 강건하며, 실험 결과는 제안방법의 효율성을 나타내고 있다.

Abstract

Digital watermarking is a technique to insert a visually imperceptible information into an image so that the information can be extracted for the purposes of ownership verification or authentication. And watermarking techniques can be classified as either fragile or robust. Robust watermarks are useful for copyright and ownership assertion purposes. They cannot be easily removed and should resist common image manipulation procedures such as rotation, scaling, cropping, etc. On the other hand, fragile watermarks are easily corrupted by any image processing procedure, it can detect any change to an image as well as localizing the areas that have been changed. In this paper, we propose a fragile watermarking algorithm using a special hierarchical structure for integrity verification of image and detection of manipulated location. In the proposed method, the image to be watermarked is divided into blocks in a multi-level hierarchy and calculating block digital signatures in this hierarchy. The proposed method thwarts the cut-and-paste attack and the experimental results to demonstrate the effectiveness of the proposed method.

Key words : Fragile watermark, Authentication, Digital signature

* 서일대학 정보통신과(Dept. of Information and Communication Eng., Seoil University)
** 한국도로공사 도로교통연구원(Korea Highway Corporation ETRI(Expressway and Transportation Research Institute))
· 제1저자 (First Author) : 우찬일
· 투고일자 : 2009년 5월 11일
· 심사(수정)일자 : 2009년 5월 13일 (수정일자 : 2009년 6월 19일)
· 게재일자 : 2009년 6월 30일

I. 서 론

디지털 데이터는 저장과 편집이 용이한 장점이 있으나 불법적인 복사와 분배 그리고 변조 등이 가능하여 멀티미디어 데이터를 효율적으로 보호할 수 있는 기술이 요구되고 있다. 이러한 문제점을 해결하기 위해 데이터에 대한 접근을 제한하지 않으면서 인증(authentication)과 무결성(integrity)이나 저작권 보호(copyright protection)를 위한 목적으로 시각적으로 인지할 수 없는 정보를 디지털 데이터 내에 삽입 및 추출하는 디지털 워터마킹이 제안 되었으며, 디지털 워터마킹은 강인한 워터마킹과 연성 워터마킹 기술로 분류할 수 있다[1]-[5].

강인한 워터마킹은 저작권 보호나 불법 복제 추적 등의 용도로 사용되며 삽입된 워터마크는 워터마크를 제거하기 위한 다양한 공격에 대하여 제거되지 않는 특성을 가져야 한다. 그러나 인증이나 무결성 검증을 위한 연성 워터마킹은 삽입된 워터마크가 영상의 사소한 변화에도 쉽게 제거되어 워터마크가 검출되지 말아야 한다. 연성 워터마킹 방법은 법적 증거가 되는 영상이나 미세한 변조도 허용하지 않는 의료영상과 같은 영상에 워터마크를 삽입하여 변조 발생 시 워터마크가 쉽게 제거되어 영상의 변조 여부 및 변조 위치를 측정할 있는 방법을 제공하며, 일반적으로 인증을 위한 워터마킹에서는 해쉬 함수를 사용하여 원본 데이터로부터 워터마크를 생성한다[6]-[8]. 연성 워터마킹의 대표적인 기술인 Wong[4]의 방법은 디지털 서명을 기반으로 한 워터마킹 기술을 제안하였다. 이 방법에서는 원본 영상의 LSB를 제거한 후 8×8 블록으로 나누어 블록별로 해쉬 코드를 생성하여 삽입될 워터마크와 XOR 연산을 수행하여 비밀키로 암호화한 후 블록의 LSB에 삽입한다. 그리고 각 블록의 LSB에서 워터마크를 추출한 후 공개키로 복호화 하여 삽입된 워터마크의 검증을 수행한다. 만약 불법적인 변조가 발생할 경우, 블록의 서명이 달라지게 되므로 변조된 곳의 위치를 측정할 수 있게 된다. 그러나 블록마다 독립적으로 워터마크를 삽입하게 되어 블록 복사 또는 cut-and- paste와 같은 공격에 취약하다.

본 논문에서는 계층구조를 이용하여 영상의 변형 위치를 빠르게 검출할 수 있는 기존의 방법[2]에서 cut-and-paste 공격에 취약한 단점을 보완하고, 변형 위치를 효율적으로 검출할 수 있는 새로운 방법을 제안한다. 제안 방법의 기본적인 구성은 기존의 방법과 비슷한 방법으로 원 영상을 4등분한 후 계속하여 영상을 분할하여 여러 레벨로 나누어 각 레벨에서의 해쉬 코드를 구한다. 최하위 레벨을 제외한 상위 레벨들의 해쉬 코드들은 XOR 연산을 수행한 후 비밀키로 암호화하여 디지털 서명을 생성하여 최하위 레벨의 영상 블록들의 디지털 서명과 함께 최하위 레벨의 영상 블록에 삽입하여 워터마킹 된 영상의 변형 유, 무를 확인하고 변형이 발생한 영상 블록들과 블록 복사 또는 cut-and-paste 영상 블록들을 효과적으로 검출할 수 있다.

Ⅱ. 관련 연구

2-1 디지털 서명(Digital Signature)

디지털 서명은 복사가 용이하게 이루어질 수 있기 때문에 일반 서명에서처럼 항상 동일한 서명을 사용할 수는 없고, 문서의 내용에 따라 가변적인 디지털 서명의 생성이 요구된다. 따라서 디지털 문서를 작성한 사람만이 디지털 서명을 생성할 수 있어야 하기 때문에 그 사람만이 알고 있는 비밀정보가 적용되어야하고, 디지털 서명에 대한 확인은 공개된 방식으로 누구든지 수행할 수 있어야 한다[9].

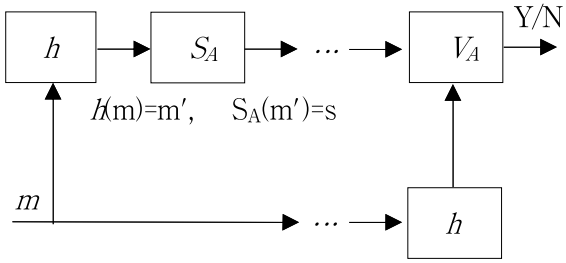


그림 1. 디지털 서명
Fig. 1. Digital signature.

메시지 부가형 디지털 서명에서는 M을 서명자가 서명할 수 있는 메시지들의 집합, S를 모든 가능한

디지털 서명의 집합, S_A를 서명자의 비밀 서명함수라고 할 때 $s = S_A(m')$를 $m \in M$에 대한 서명자의 디지털 서명이라고 하며 {m, s}를 메시지가 부가된 디지털 서명이라고 부른다. 여기서, $m' = h(m)$으로 h는 해쉬 함수를 나타낸다.

디지털 서명에 대한 확인은 누구에 의해서도 수행될 수 있어야 하기 때문에 그림 1과 같이 공개된 서명 확인함수 V_A가 요구된다.

2-2 Wong의 방법

Wong의 방법은 $M \times N$ 크기의 화소를 갖는 그레이 레벨 영상 $\chi_{m,n}$을 $I \times J$ 크기의 여러 블록으로 나눈 후 각각의 블록별로 이진 워터마크 영상 $b_{m,n}$ 을 삽입한다. 여기서, 원 영상 $\chi_{m,n}$의 r번째 $I \times J$ 크기의 블록을 X_r이라 하고 LSB를 0으로 바꾼 블록을 $\widetilde{X}_r$이라고 한다. 그리고 $H(\cdot)$는 해쉬 함수를 나타내고 해쉬 코드는 다음과 같이 구한다.

$H(M, N, \widetilde{X}_r) = (p_1^r, p_2^r, \ldots, p_s^r)$. 여기서, P_r은 다음과 같이 나타낸다. $P_r \triangleq (p_1^r, p_2^r, \ldots, p_{I,J}^r)$. P_r과 워터마크 영상 블록 B_r은 $W_r = P_r \oplus B_r$ 연산을 수행하여 W_r을 생성하여 개인키(K')으로 W_r을 암호화하여 C_r을 생성한 후 $\widetilde{X}_r$의 LSB에 삽입하여 워터마크 블록 Y_r을 생성한다. 워터마크의 검증은 검증하려는 블록 Z_r에서 LSB 만을 추출한 G_r은 워터마크 삽입에 사용한 개인키(K')에 대응되는 공개키 K로 복호화 하여 U_r을 생성한 후 M, N과 검증하려는 영상 블록 Z_r에서 LSB를 제거한 $\widetilde{Z}_r$을 해쉬 함수의 입력으로 사용하여 Q_r을 얻고, $O_r = Q_r \oplus U_r$ 연산으로 최종 출력 블록을 계산한다.

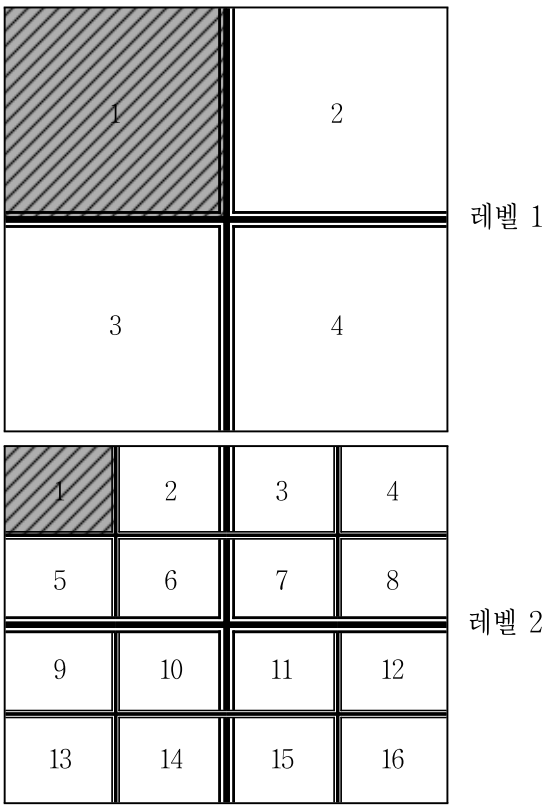
Wong의 방법은 블록 단위로 워터마크를 삽입하기 때문에 크기가 같은 영상에 동일한 워터마크가 삽입되었을 경우, 해당 이미지의 다른 블록이나 다른 이미지의 블록을 잘라 붙여 불법적인 조작을 하더라도 정상적인 워터마크가 추출되어 정상적인 인증이 이루어지는 cut-and-paste와 같은 공격에 취약하다.

Ⅲ. 제안 방법

3-1 분할 영상 구조

본 논문에서는 워터마크가 삽입된 영상에서 의도적인 변형이 발생하였을 경우, 변형이 발생된 블록들과 cut-and-paste와 같은 공격이 가해진 영상 블록들을 효과적으로 검출하기 위하여 워터마크가 삽입될 원 영상의 LSB를 “0”으로 초기화하여 여러 레벨로 분할한 후 최하위 레벨에 워터마크를 삽입한다.

본 논문에서는 분할되지 않은 영상을 레벨 0이라 하고, 그림 2와 같이 레벨 0의 영상을 1/4로 분할한 영상을 레벨 1이라 한다. 레벨 1의 영상은 총 4개의 영역으로 구분되는데 각각의 영역은 다시 1/4로 분할한다. 즉, 레벨 1 영상의 1-사분면을 1/4로 분할하여 4개의 영역으로 나누고, 2-사분면에서 4-사분면도 동일하게 각각 4개의 영역으로 분할하면 총 16개의 영역으로 나누어진 레벨 2 영상을 얻을 수 있다.



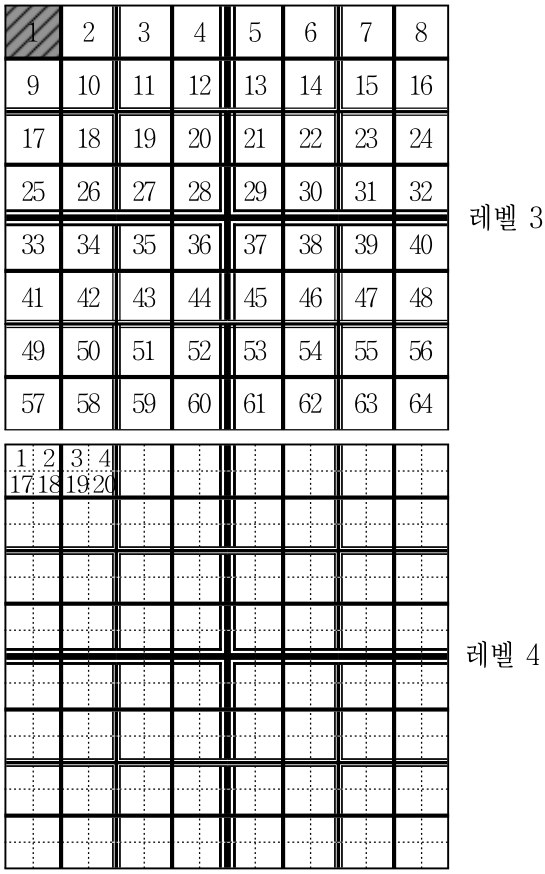


그림 2. 각 레벨의 블록 구성
Fig. 2. Block structure of each level.

이와 같은 방법으로 레벨 2 영상도 각각의 영역별로 1/4로 나누면 총 64개의 영역으로 나누어진 레벨 3 영상을 구할 수 있으며, 이와 마찬가지로 레벨 3 영상도 1/4로 분할하면 256개의 영역으로 나누어진 레벨 4 영상을 얻을 수 있다. 최종적으로 분할된 레벨 4 영상에서는 각 블록들이 16×16 크기로 이루어져 있으며, 그림 2는 위에서 설명한 방법으로 분할된 레벨 1에서 레벨 4까지의 영상을 나타내고 있으며, 각각의 레벨에서 분할된 블록들의 개수는 다음과 같이 나타낼 수 있다.

$$\text{각 레벨의 블록 수} = 4^{l}, \quad l : \text{레벨}.$$

그림 2에서 하위 레벨이 상위 레벨에 포함 되는 관계를 살펴보면, 레벨 4의 1, 2, 17, 18번 블록은 레벨 3의 1번 블록에 포함되고 레벨 3의 1, 2, 9, 10번 블록은 레벨 2의 1번 블록에 포함되고 있다. 그리고 레벨 2의 1, 2, 5, 6번 블록은 레벨 1의 1번 블록에 포함되고 있다. 하위 레벨을 포함하는 상위 레벨 블록간의 이러한 관계는 본 논문에서 워터마크를 생성하는데 있어 매우 중요하며 이러한 특성을 이용하여 워터마킹 된 영상의 변형 유, 무 및 효율적인 변형 위치 검출 그리고 cut-and-paste 공격과 같이 복사된 블록을 검출할 수 있다. 본 논문에서는 레벨 3 영상 블록 단위로 레벨 3의 각 블록에 포함되는 4개의 레벨 4 영상 블록들에 디지털 서명을 삽입한다.

3-2 워터마크 생성 및 삽입

본 논문에서 삽입되는 워터마크는 영상의 특성을 이용하여 생성하며, 워터마크의 삽입 위치는 다음과 같이 구성한다. 워터마크는 레벨 3의 각 블록에 포함되는 레벨 4의 16×16 크기의 4개의 블록 단위로 삽입되며, 각 블록의 LSB에는 2개의 디지털 서명이 삽입된다. 첫 번째 디지털 서명은 레벨 4에서 서명이 삽입되는 블록 자신에 대한 디지털 서명이며, 두 번째 서명은 서명이 삽입되는 레벨 4 블록을 포함하는 상위 레벨들의 각 블록들에 대한 해쉬 코드를 XOR 연산 수행 결과로 생성된 디지털 서명이다. 즉, 그림 2에서 레벨 3의 1번 블록은 레벨 4의 1, 2, 17, 18번 블록을 포함하므로 레벨 4의 1번 블록은 자신의 블록인 16×16 크기의 영상 블록에 대한 해쉬 코드를 구한 후 비밀키로 암호화하여 첫 번째 서명을 생성하고, 1번 블록이 포함되는 상위 블록들은 그림 2에서 음영으로 표시된 레벨 3의 1번 블록, 레벨 2의 1번 블록, 레벨 1의 1번 블록 그리고 영상을 분할하지 않은 레벨 0이다.

따라서 각각의 상위 레벨 블록들에 대한 해쉬 코드를 구하고 XOR 연산을 수행한 후 두 번째 서명을 구한다. 레벨 4의 2번 블록도 1번 블록과 같은 방법으로 서명을 생성하나 차이점은 표 1과 같이 대응되는 최상위 블록(레벨 0)의 해쉬 코드 하나를 제거하고, 레벨 4의 17번 블록은 대응되는 최상위 블록을 포함한 상위 블록의 해쉬 코드 2개를 제거하며, 블록 18은 3개를 제거하여 디지털 서명을 구한다.

이와 동일하게 레벨 4의 3, 4, 19, 20번 블록은 레벨 3의 2번 블록, 레벨 2의 1번 블록, 레벨 1의 1번 블록에 포함되며, 각각의 블록에 삽입되는 디지털 서명은 레벨 4의 1, 2, 17, 18번 블록과 같이 두개의

디지털 서명을 생성하여 삽입한다. 따라서 레벨 4의 각 블록에는 항상 자신의 블록에 대한 서명과 상위 블록들에 대한 서명이 삽입되고, 상위 블록들에 대한 서명은 워터마킹 된 영상의 변형 유, 무의 판단과 변형 위치 검색 그리고 영상 블록을 복사 하였을 경우 이를 찾기 위한 방법으로 사용된다.

표 1. 디지털 서명 생성
Table 1.
Generation of digital signature.

두 번째 서명 삽입 블록	서명생성
레벨 4의 1번	E^e(L0⊕L11⊕L21⊕L31)
레벨 4의 2번	E^e(L11⊕L21⊕L31)
레벨 4의 17번	E^e(L21⊕L31)
레벨 4의 18번	E^e(L31)

여기서, L0 : 레벨 0의 해쉬 코드
L11 : 레벨 1의 1번 블록의 해쉬 코드
L21 : 레벨 2의 1번 블록의 해쉬 코드
L31 : 레벨 3의 1번 블록의 해쉬 코드

3-3 워터마크 검출

워터마크의 검출은 워터마크의 삽입과 같이 그림 2의 레벨 3 영상 블록 단위로 수행된다. 레벨 3의 1번 블록은 레벨 4의 1, 2, 17, 18번 블록을 포함하고 있어, 레벨 4의 1번 블록의 LSB에서 두 번째 서명을 추출한 후 워터마크 삽입에 사용된 비밀키에 대응되는 공개키로 복호화한 후, 워터마크 생성과 동일한 방법으로 워터마킹 된 영상의 LSB를 제거하여 상위 레벨들의 해쉬 코드를 계산한 후 각각의 해쉬 코드들의 XOR 연산을 수행한 결과와 비교한다. 여기서, 두개의 값이 같으면 전체 영상에 변화가 없음을 나타내고 서로 다른 값이 나타나면 워터마킹 된 영상에 변형이 있음을 나타낸다.

워터마킹 된 영상에 변형이 발생 하였을 경우, 레벨 4의 2번 블록에서 두 번째 서명을 추출하여 복호화한 후 계산된 해쉬 코드의 XOR 값과 비교하고, 만약 같은 값을 가지면 레벨 1의 1번 블록에는 변형이 없는 것으로 판단하여 레벨 1의 2번 블록에 해당하는 레벨 3 블록을 검사한다. 이러한 이유는 각 블록에 삽입되는 두 번째 서명은 표 1에 나타낸 것처럼 4개의 레벨 4 블록들이 포함되는 상위 블록들의 해쉬 코드의 XOR 연산에 의한 값이기 때문에 상위 레벨 블록의 변형이 확인될 경우에 하위 레벨의 변형 블록을 찾을 수 있도록 구성되었기 때문이다.

즉, 레벨 3의 1번 블록에 대응되는 레벨 4의 첫 번째 블록(1번 블록)에서 추출한 서명을 복호화 한 L0⊕L11⊕L21⊕L31 값이 워터마킹 된 영상에서 LSB를 제거하고 계산된 L0′⊕L11′⊕L21′⊕L31′ 값과 동일하면, L0 = L0′라는 의미로 전체영상의 해쉬 코드인 레벨 0의 해쉬 코드가 원 영상 전체의 해쉬 코드와 변함이 없기 때문에 전체 영상에 아무런 변형이 없음을 나타낸다. 그러나 변형이 발생하였을 경우, 레벨 4의 두 번째 블록(2번 블록)에 삽입된 서명을 복호화 한 L11⊕L21⊕L31의 값을 계산된 L11′⊕L21′⊕L31′과 비교한다. 마찬가지로 두개의 값이 같으면 L11 = L11′으로 레벨 1의 첫 번째 블록에는 변형이 없음을 나타낸다. 따라서 이러한 경우, 레벨 1의 2~4번 블록에 해당하는 레벨 3의 블록들을 위와 같은 방법으로 검사한다.

그러나 다른 값이 나타나면 레벨 3에 포함되는 레벨 4의 세 번째 블록(17번 블록)의 두 번째 서명을 복호화 하여 계산된 해쉬 코드 연산 결과인 L21′⊕L31′와 비교한다. 이 경우도 위와 마찬가지로 값이 같으면 L21 = L21′으로 레벨 2의 1번 블록에는 변형이 없는 것을 의미하여 레벨 2의 2~16번 블록에 해당되는 레벨 3 블록들을 검사한다.

만약, 서로 다른 값이 나타나면 레벨 2의 1번 블록에 변형이 발생된 것으로 판단하여, 레벨 2의 1번 블록에 포함되는 레벨 3의 블록(1, 2, 9, 10번)에서 이들 블록들에 포함되는 레벨 4의 네 번째 블록들(18, 20, 50, 52번)의 두 번째 서명을 복호화 한 후 계산된 해쉬 코드 L31′, L32′, L39′, L310′과 비교하여 서로 같지 않은 값을 가지는 블록을 검사한다. 즉, L31 ≠ L31′, L32 ≠ L32′, L39 ≠ L39′, L310 ≠ L310′인 것을 찾는다.

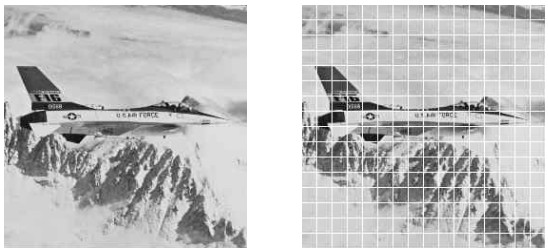
여기서, 서로 다른 값을 나타내는 블록이 발견되면 그 블록이 포함되는 레벨 3 블록에 속하는 모든 레벨 4 블록(만약, L31 ≠ L31′이면 1, 2, 17, 18번)들의 첫 번째 서명을 복호화 한 후, 서명을 추출한 해당 블록의 해쉬 코드와 비교하여 값이 서로 다른 블

록을 찾는다. 이때, 의도적인 변형이 발생되었을 경우 해당 블록을 검출할 수 있으나 복사된 블록은 계산된 해쉬 코드와 복호화 된 해쉬 코드가 같기 때문에 검출이 불가능하다. 따라서 이러한 경우 4개의 레벨 4 블록에 삽입된 두개의 서명을 복호화 하여 전체 영상 블록에서 같은 값을 가지는 블록을 추출하여 복사 여부를 판단한다.

Ⅳ. 실험 및 결과

본 논문에서 제안한 방법에 대한 영상의 변형 유, 무 및 변형 위치 검출은 256×256 크기의 그림 3의 영상을 사용하였다. 그림 3에서 격자 형태로 표시된 분할 영상은 16×16 크기의 블록들을 가진다.

(a) Lena 및 분할 영상



(b) Airplane 및 분할 영상

그림 3. 실험 영상

Fig. 3. Test images.

그림 4는 제안 방법으로 워터마크를 삽입한 후 인위적인 조작 및 블록 복사 후의 영상과 검출 결과를 나타내고 있다.

그림 4에서 인위적으로 변형이 발생된 블록의 검출은 흰색으로 채워진 사각형으로 표시하였으며, 복사된 블록의 검출은 그림 4의 (b)와 같이 원본 블록과 함께 흰 테두리의 사각형으로 표시하였다.

(a) 블록 복사 (b) 블록 복사 검출

(c) 복사 및 변형 (d) 복사 및 변형 검출

(e) 블록 복사 (f) 블록 복사 검출

(g) 복사 및 변형 (h) 복사 및 변형 검출

(i) 원 영상 블록 (j) 변형 영상 블록

그림 4. 인위적 조작과 워터마크 검출

Fig. 4. Manipulation and watermark detection.

실험 결과 워터마크가 삽입된 영상 내의 블록이 변형 되었거나 영상내의 다른 블록을 복사하였을 경우, 레벨 4의 블록만으로는 변형 여부를 판단하기 어려울 수 있으나 상위 레벨의 서명을 확인함으로써 해당 블록의 변형 여부를 알 수 있음을 확인할 수 있었다.

Ⅴ. 결 론

영상의 인증과 무결성 검증을 위한 연성 워터마킹 방법은 수신된 영상에 대한 인증과 변형이 발생하지 않았음을 증명할 수 있어야 하며, Wong의 방법과 같이 블록 단위로 수행되는 대부분의 연성 워터마킹 방법은 인증과 무결성 증명을 위해 다양한 방법으로 연구가 이루어져 왔다. 그러나 블록 단위로 워터마크가 삽입 되는 특성으로 인해 cut-and-paste와 같은 공격에 취약한 단점을 가지고 있어 이를 극복하기 위한 새로운 방법들이 제안되고 있다.

본 논문에서는 블록 단위로 워터마크를 삽입하여 빠르게 변형 위치를 찾을 수 있는 기존의 방법에서 cut-and-paste와 같은 공격에 취약한 문제를 해결하기 위한 새로운 방법을 제안하였다. 제안된 방법에서는 인위적으로 발생된 영상의 변형과 영상 블록 간의 복사 영역을 검출할 수 있음을 실험을 통하여 확인하였으며, 군사용이나 의료용 등과 같이 민감한 분야에서 위, 변조 등을 판별할 수 있는 기술로 활용이 가능할 것으로 생각된다. 향후 연구 과제로는 어떠한 영상 처리 방법에서도 워터마킹 된 영상의 인증과 변형 위치를 찾을 수 있는 방법에 대한 연구가 필요할 것이다.

감사의 글

본 논문은 2008년도 서일대학 학술연구비에 의해 연구되었음.

참 고 문 헌

[1] 박재연, 임재혁, 원치선, “MPEG-2 비트열에서의 인증 및 조작위치 검출을 위한 디지털 워터마킹 기법,” *전자공학회논문지* 제40권 SP편 제2호, pp. 76-85, 9, 2003.

[2] 우찬일, 전세길, “국부적인 변형 검출을 위한 효율적인 워터마킹,” *전자공학회논문지* 제43권 IE편 제2호, pp. 87-92, 6, 2006.

[3] L. Qian and K. Nahrstedt, “Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer's Rights,” *Pre-print*, 1998.

[4] P.W.Wong, “A Public Key Watermark for Image Verification and Authentication,” *in Proc. IEEE Int. Conf.* Image Processing, pp. 425-429, 1998.

[5] M.P.Queluz, “Content-based integrity protection of digital images,” *Proc. of SPIE*, vol. 3657, Jan, pp. 85-93, 1999.

[6] C.C.Chien, K.C.Fan, and S.W.Wang, “A wavelet-based public key image authentication watermarking,” *Proc. of IEEE 37th Annual 2003 Int*., pp. 321-324, 2003.

[7] Katzenbeisser, Petitcolas, Information Hiding techniques for steganography and digital watermarking, Artech House, 1999.

[8] M.U.Celik, G.Sharma, A.M.Tekalp, E.Saber, “Localized Lossless Authentication Watermark (LAW),” *Proc. of SPIE-IS&T Electronic Imaging,* Vol. 5020, pp. 689-698, 2003.

[9] 박창섭, *암호이론과 보안,* 대영사, 1999.

우 찬 일 (禹讚溢)

1993년 2월 : 단국대학교 전자공학과(공학사)
1995년 2월 : 단국대학교 전자공학과(공학석사)
2003년 2월 : 단국대학교 전자공학과(공학박사)
2004년 3월~현재 : 서일대학 정보통신과 교수
관심분야 : 정보보호, 디지털 워터마킹, 데이터베이스 보안

전 세 길 (全世拮)

1998년 2월 : 단국대학교 컴퓨터공학과(공학사)
2000년 2월 : 단국대학교 컴퓨터공학과(공학석사)
2004년 8월 : 단국대학교 전자컴퓨터공학과(공학박사)
2006년 3월~현재 : 한국도로공사 도로교통연구원 책임연구원
관심분야 : 정보보호, 데이터베이스 보안, 시공간 데이터베이스, 디지털 워터마킹