논문 2006-43IE-2-14

국부적인 변형 검출을 위한 효율적인 워터마킹

(An Efficient Watermarking for Tamper Localization Proofing)

우 찬 일*, 전 세 길**

(Chan Il Woo and Se Gil Jeon)

요 약

최근 들어 지적 재산권 보호와 멀티미디어 데이터 인증을 위하여 다양한 워터마킹 방법들이 제안되어 왔다. 이미지 인증을 위한 워터마킹에서 워터마크는 영상의 부당한 변형 검출을 위해서 영상 내에 삽입된다. 따라서, 인증과 무결성을 위한 워터마킹은 스케일링 및 크롭핑 등과 같은 영상 변형에 대하여 삽입된 워터마크가 쉽게 지워져야 한다. 본 논문에서는 계층적 구조를 사용하여 영상의 무결성 검증과 변형 위치 검출을 위한 fragile 워터마킹 방법을 제안한다. 제안 방법에서는 워터마크가 삽입되는 영상을 여러 레벨로 구성하여 각 레벨별로 영상을 여러 블록으로 나눈 후 각 블록에 대한 디지털 서명을 계산한다. 디지털 서명은 블록 내 모든 화소의 상위 7개의 비트들(MSBs)을 사용하여 계산한 후 각 블록 내에서 선택된 화소의 LSB에 삽입된다. 본 논문에서 제안한 방법에 대한 실험 결과는 제안 방법의 효율성을 나타낸다.

Abstract

Many watermarking methods for protecting the intellectual property right and authentication multimedia data have been proposed in recent years. In image authentication watermarking, watermark is inserted into an image to detect any malicious alteration. So, watermark for authentication and integrity should be erased easily when the image is changed by scaling or cropping etc. We propose in this paper a fragile watermarking algorithm for image integrity verification and tamper localization proofing using special hierarchical structure. 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. At each level of the hierarchy, a digital signature for each block is calculated using the seven most significant bit(MSBs)-plane values of all pixels within the block. And the resulting signature is incorporated into the LSBs of selected pixels within the block. We provide experimental results to demonstrate the effectiveness of the proposed method.

Keywords : Fragile watermarking, Authentication, Digital signature.

Ⅰ. 서 론

최근 들어 통신망이 확대 보급되면서 정보교환이 신속하게 이루어지고 있으며 컴퓨터 네트워크와 멀티미디어 관련 기술의 발전으로 디지털 멀티미디어 데이터의 수요는 급격히 늘어나고 있다. 디지털 데이터는 아날로그 데이터에 비하여 저장 및 편집이 용이한 장점이 있으나 불법적인 복사 및 분배 그리고 변조 등이 가능하게 되어 멀티미디어 데이터를 효율적으로 보호할 수 있는 기술이 요구되고 있다[1-3]. 이러한 문제점을 해결하기 위해서 데이터에 대한 접근을 제한하지 않으면서 저작권 보호(copyright protection)나 인증(authentication)과 무결성(integrity)을 위한 목적으로 시각적으로 인지할 수 없는 정보를 디지털 데이터 내에 삽입, 추출하는 디지털 워터마킹이 제안되었다[4,5]. 저작권 보호를 위한 워터마킹은 정당한 사용자에 의해서는 삽입된 워터마크가 쉽게 검출 되어야 하지만 그 밖의 사용자에 대해서는 워터마크가 검출되거나 필터링, 왜곡 등과 같은 여러 후처리 과정에 의해서도 지워지지 않는 강인한

* 평생회원, 서일대학 정보통신전공
(Dept. of Information and Communication Engineering, Seoil College)
** 정회원, 한국도로공사 도로교통기술원
(Korea Highway Corporation HTTI(Highway & Transportation Technology Institute)
※ 본 논문은 2005년도 서일대학 학술연구비에 의해 연구되었음.
접수일자: 2006년3월27일, 수정완료일: 2006년6월9일

(robust) 워터마크를 영상 내에 삽입하는 과정이다. 영상에 대한 인증이나 변형 검출을 위한 워터마킹은 압축과 같은 영상의 변형에 대해서 삽입된 정보가 쉽게 제거되어야 하는데 이러한 방법을 fragile 또는 semi-fragile 워터마킹이라 한다[6]. 일반적으로 디지털 데이터의 인증이나 무결성을 증명하기 위한 방법은 디지털 서명에 의해 수행되는데 최근 들어 디지털 서명을 사용한 워터마킹 방법들이 제안되고 있다. 대부분의 fragile 워터마킹은 워터마크의 삽입과 추출 과정에 암호학적인 키를 사용하며 이러한 방법은 공개키(public key)와 개인키(private key) 방법으로 분류된다. 비밀키 워터마킹에서 워터마크 삽입과 추출에 사용하는 키는 서로 동일하며 이를 대칭키(symmetric key)라 한다. 공개키 워터마킹은 워터마크 삽입에는 비밀키(secret key)를 사용하고 추출에는 공개키를 사용하는 방법이다. 이 방법은 인증과 무결성 뿐만 아니라 영상의 변형 위치의 검출이 가능하여 대부분의 fragile 워터마킹에서 요구되는 방법이다[7-9]. 공개키 워터마킹 중 Wong[8]의 방법은 영상의 각 블록의 LSB를 제외한 나머지 부분에 대한 디지털 서명(digital signature)을 LSB에 삽입하는 방법을 제안하였다. 그리고 Celik[9]등은 Wong의 방법을 기반으로 하여 영상을 여러 단계의 레벨로 분할하여 각 레벨 블록별 워터마크를 삽입하는 계층적 구조의 워터마킹 방법을 제안하였다.

본 논문에서는 Celik 등이 제안한 방법을 변형하여 영상을 5 레벨로 구분하고 각 레벨에서의 영상 블록별 디지털 서명을 구한 후 마지막 레벨에 전체 레벨의 디지털 서명을 삽입하여 워터마킹 된 영상에 변형이 발생하였을 경우 변형 위치를 빠르게 검출할 수 있는 방법을 제안한다. 제안한 방법에 대한 실험 결과 워터마킹 된 영상에 변형이 발생하였을 경우 전체 영상에 대한 검사 없이 변형이 발생된 영상블록들만 검사할 수 있어 효과적으로 전체 영상에 대한 변형 여부를 확인할 수 있음을 알 수 있었다.

Ⅱ. 관련 기술

1. 보안 서비스

정보시스템 보급의 증가로 전자 정보가 종이 문서의 역할을 대신함에 따라 컴퓨터 및 네트워크 보안에 있어서 다음과 같은 사항들이 충족되어야 한다[10].

- 기밀성(confidentiality) : 송, 수신자만이 메시지를 읽을 수 있도록 하는 것.
- 인증(authentication) : 수신 받은 메시지가 정당한 사용자로부터 전송 되었고, 변경되지 않았다는 것을 확인하기 위한 절차.
- 무결성(integrity) : 메시지의 전송 도중 어떠한 변경도 없었음을 증명 하는 것.
- 부인봉쇄(non-repudiation) : 메시지에 대한 송신자와 수신자 모두 송,수신을 부인할 수 없도록 하는 것.

메시지의 기밀성은 암호화를 통해서 이루어지며 인증, 무결성 및 부인봉쇄는 디지털 서명을 통해서 이루어진다.

2. 해쉬 함수

해쉬 함수는 입력 데이터 스트링을 고정된 길이의 출력인 해쉬 코드로 대응시키는 함수를 말하며, 해쉬 코드는 다음 식과 같은 함수 H에 의해 만들어 진다.

$$h = H(M)$$

위 식에서 M은 가변 길이의 메시지이고, H(M)는 고정 길이의 해쉬 코드이다. 해쉬 함수는 입력 데이터의 한 비트가 바뀌어도 서로 다른 해쉬 코드를 생성한다. 해쉬 함수는 디지털 서명을 효율적으로 처리할 수 있는 방법을 제공한다.

3. 디지털 서명

디지털 정보는 동일한 내용으로 복제 및 위조 등이 용이하기 때문에 이러한 것들을 방지하기 위해 암호화 기법과 함께 디지털 서명 기술이 개발되었다.

디지털 서명은 데이터가 암호화되어 있어도 데이터의 내용이 처음에 만들어진 내용과 동일하다는 것을 증명할 수 있는 메시지 인증과 메시지를 보낸 사람이 정당한 송신자 인지를 증명하는 사용자 인증 그리고 메시

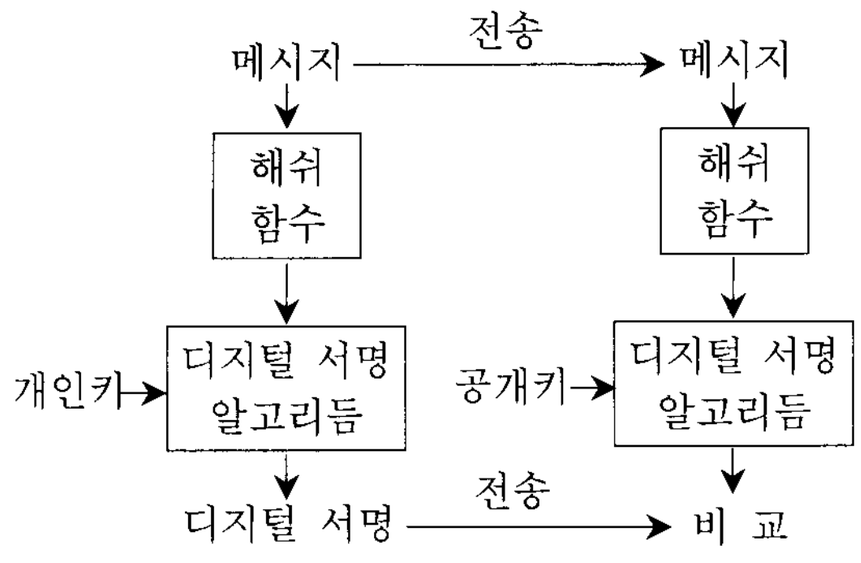


그림 1. 디지털 서명 생성 및 서명 확인
Fig. 1. Generation of digital signature and verify.

지를 수신한 사람이 수신 받지 않았다고 부인하는 것을 방지할 수 있는 기능을 제공한다. 디지털 서명은 공개키 및 대칭키 암호를 이용한 방법 등을 들 수 있다. 그림 1은 디지털 서명의 생성 및 서명 검증 과정을 나타낸다.

4. 영상 인증을 위한 워터마킹

저작권 보호를 위한 강인한(robustness)워터마킹은 압축, 필터링과 같은 영상에 대한 변형에도 삽입된 워터마크의 손실이 없어야 한다. 그러나 영상 인증을 위한 fragile 워터마킹은 송신자의 확인과 영상 데이터의 변형 여부를 확인하기 위한 목적으로 사용된다. 이 경우 영상에 대한 사소한 변형에 대하여도 삽입된 워터마크가 쉽게 파괴되어야 한다[6]. 비밀키 방식의 fragile 워터마킹은 영상의 LSB에 워터마크를 삽입하고 추출하는데 동일한 키가 사용되며, 영상의 사소한 조작을 감지할 수 있으며 조작 위치도 검출할 수 있다. 그러나 워터마크 삽입과 추출에 사용되는 키가 동일하여 수신자에 의해 삽입된 워터마크와 전혀 다른 워터마크가 삽입되어 유포될 수 있는 문제점이 있다. 이를 해결하기 위해 워터마크 삽입에는 송신자의 비밀키로 워터마크를 삽입하고 수신자는 공개키로 워터마크를 추출하는 공개키 방식의 워터마킹 방법이 제안되었다. 그림 2는 공개키 및 비밀 키를 사용하는 fragile 워터마킹을 나타낸다. 여기서 X는 원 영상, Xw는 워터마킹 된 영상을 그리고 W는 삽입된 워터마크를 나타낸다.

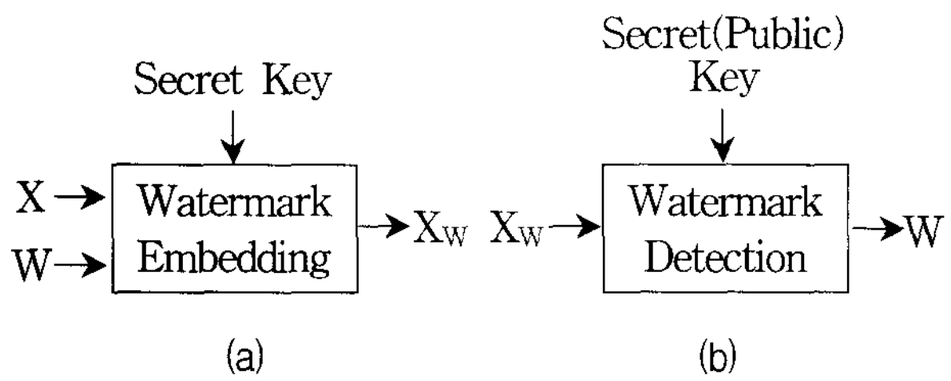


그림 2. Fragile 워터마킹: (a) 삽입 (b) 추출
Fig. 2. Fragile watermarking: (a) embedding (b) detection.

Ⅲ. 제안 방법

1. 영역 분할

본 논문에서 제안하는 방법에서는 워터마크 삽입을 위하여 원 영상을 그림 3과 같이 여러 레벨로 분할하는 구조로 구성된다.

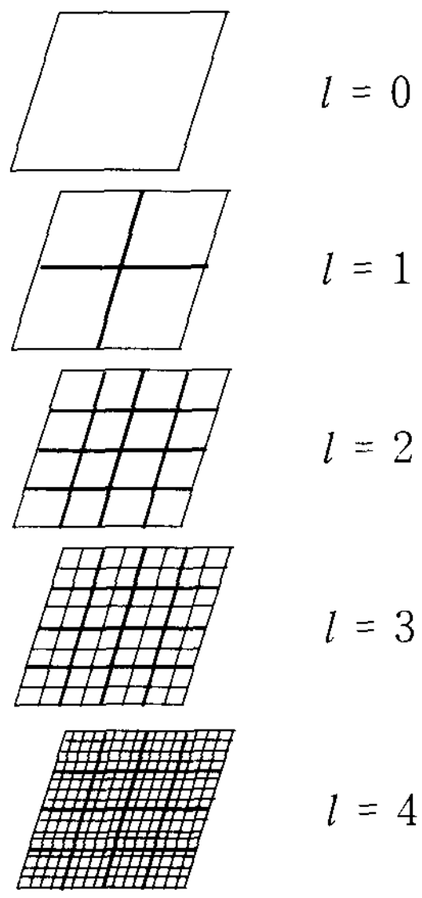


그림 3. 영상 분할
Fig. 3. Partitioning of an image.

그림 3에서 l = 0은 분할되지 않은 원 영상(256×256)을 나타내고 l = 1은 원 영상을 1/4 등분으로 1차 분할한 영상 블록을 나타낸다. 그리고 l = 2는 1차 분할된 영상의 각 블록을 1/4 등분으로 2차 분할한 영상 블록을 나타내고 l = 3은 2차 분할된 영상의 각 블록들을 분할한 영역들을 나타낸다. 본 논문에서는 영상을 4차 레벨(l = 4)로 분할한다. 이 경우 마지막 레벨에서의 각 블록들은 16×16의 크기를 갖는다.

이와 같은 과정으로 분할된 각 레벨에서의 영상 블록들은 LSB를 제거한 후 MD5 해쉬 함수를 사용하여 128비트의 해쉬 코드를 생성하고 공개키 암호 시스템의 비밀키로 암호화한다. 따라서 l = 0에서는 128비트의 해쉬 코드가 하나가 생성되고 1차 레벨에서는 4개의 128비트 해쉬 코드가 생성된다. 그리고 4-레벨에서는 256개의 해쉬 코드가 생성된다.

2. 워터마크 삽입

각 레벨에서 구한 암호화된 해쉬 코드는 4-레벨에서 각 블록들의 LSB에 삽입된다. 그림 4는 l = 4인 4차 분할된 영상 블록들과 분할된 영상 블록들의 번호를 나타낸다. 각 블록 들은 16×16의 크기를 가지고 있어 이러한 각 블록들에 l = 0에서부터 l = 4까지 영상을 분할하여 생성된 각각의 디지털 서명의 하나 또는 두개를 삽입한다. 이때 각 블록들에 삽입되는 디지털 서명은 표 1과 같이 구성된다. 표 1에서 마지막 레벨에 삽입되는 디지털 서명은 워터마킹 된 영상의 변형 부분을 찾기 위하여 마지막 레벨의 디지털 서명과 상위레벨(0~3 레

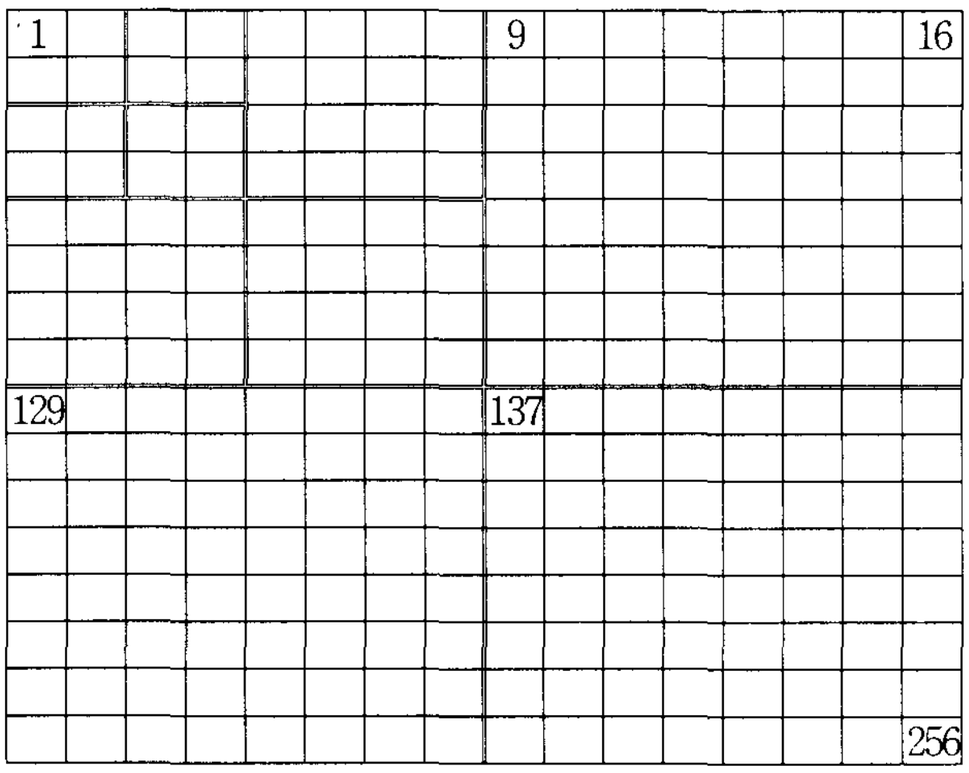


그림 4. 4차 레벨 영상 블록
Fig. 4. 4-Level hierarchical image block structure.

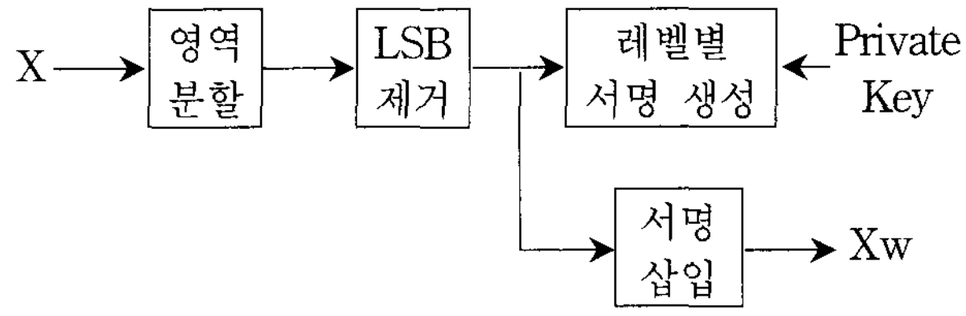
표 1. 삽입되는 디지털 서명
Table 1. Embedded digital signature.

블록 번호	삽입되는 디지털 서명 (레벨-블록번호)	4-레벨에 대응되는 상위레벨 블록 번호
1	0-1, 4-1	3-1, 2-1, 1-1
2	1-1, 4-2	
17	2-1, 4-17	
18	3-1, 4-18	
9	1-2, 4-9	3-5, 2-3, 1-2
10	2-4, 4-10	
25	3-5, 4-25	
26	4-26	
129	1-3, 4-129	3-33, 2-9, 1-3
130	2-9, 4-130	
145	3-33, 4-145	
146	4-146	

벨)의 디지털 서명이 같이 삽입되며 4-레벨의 4개의 블록(예:1,2,17,18)은 상위 레벨인 3-레벨의 1번 블록을 1/4로 분할한 것을 나타낸다.

표 1에서 4-레벨의 첫 번째 블록(4-1)은 상위레벨 중 0-레벨의 디지털 서명과 4-레벨 1번(자신의 블록)에 대한 디지털 서명이 삽입되고 2번 블록은 1-레벨의 1번 블록의 디지털 서명과 4-레벨 2번의 디지털 서명이 삽입된다. 여기서, 0-레벨은 분할되기 전의 전체 원 영상을 나타내기 때문에 128비트 1개의 디지털 서명이 생성되고 1-레벨의 경우 원 영상이 4개의 블록으로 분할되기 때문에 4개의 디지털 서명이 생성된다. 마찬가지로 2-레벨에서는 16개의 디지털 서명이 생성된다. 따라서 마지막 레벨의 각 블록에는 자신에 대한 디지털 서명과 상위 레벨 중 자신의 블록이 속해있는 상위 블록들의 디지털 서명이 삽입된다.

이와 같은 과정으로 디지털 서명을 삽입하는 이유는



X : 원 영상, Xw : 워터마킹 된 영상

그림 5. 워터마크 삽입 과정
Fig. 5. Watermark insertion process.

워터마킹 된 영상에 대한 변형 유,무와 변형 위치를 빠르게 검출하기 위함이다. 예를 들어 마지막 4-레벨 1번 블록에서 0-레벨의 디지털 서명을 검사하면 전체 영상에 대한 변형 유무를 알 수 있다. 이때 전체 영상의 디지털 서명과 4-레벨의 1번 블록에서 검출된 0-레벨 디지털 서명을 비교하여 만약 같은 값을 가지면 워터마킹 된 영상에 어떠한 변형도 발생하지 않은 것을 알 수 있으며 이 경우 다른 블록들에 대한 변형 검사를 생략하여도 워터마킹 된 전체 영상에 어떠한 변형도 발생하지 않았음을 알 수 있다.

만약 서로 다른 값이 검출되면 워터마킹 된 전체 영상 중에서 일부분이 변형된 것임을 알 수 있어 이 경우 워터마킹 된 영상을 1-레벨로 분할하여 1번 블록의 디지털 서명과 마지막 4-레벨의 2번 블록에서 추출된 디지털 서명을 비교하여 같은 값을 가지면 1-레벨의 1번 블록에 해당하는 전체 영역에 대한 변형이 발생하지 않은 것을 알 수 있다. 이 경우 1-레벨 블록에 대응되는 4-레벨의 각 블록들에 대한 디지털 서명의 비교는 생략할 수 있어 1-레벨 2번 블록에 대한 검사를 수행하면 된다. 따라서 4-레벨의 9번 블록에서 추출된 1-레벨의 2번 블록의 디지털 서명과 계산된 1-레벨의 2번 디지털 서명을 비교하여 만약 서로 다른 결과가 발생하면 1-레벨의 2번 블록내의 화소에서 변형이 발생한 것을 알 수 있어 이 블록을 2차 레벨로 분할하여 2차 레벨 중 변형 블록을 찾아 마지막 레벨에서 구체적인 변형 위치를 알 수 있게 된다.

이와 같은 과정을 수행하면 전체 영상에 대한 검사 없이 실질적으로 변형이 발생된 블록들만 검사하면 되므로 효과적으로 변형 위치를 찾을 수 있는 장점이 있다. 그림 5는 워터마크 삽입의 전체 과정을 나타낸다.

3. 워터마크 추출

워터마크 추출 및 검증 과정은 그림 6과 같이 4-레벨에서 각 레벨별 디지털 서명을 추출하여 워터마크 삽입에 사용된 비밀키에 대응되는 공개키로 복호화 한다.

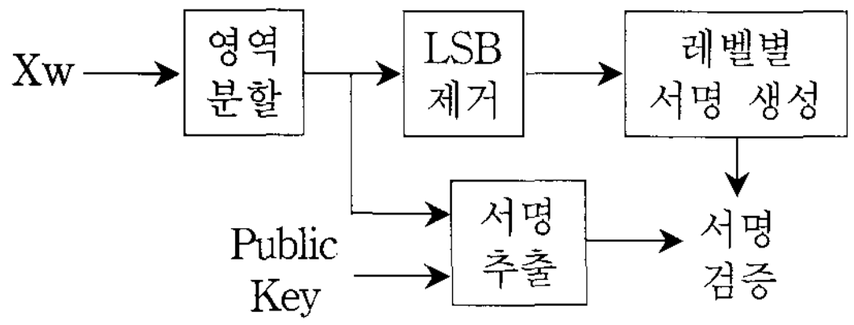


그림 6. 워터마크 검증 과정
Fig. 6. Watermark verification process.

그리고 워터마킹 된 영상의 LSB를 제거 한 후 각 레벨별로 해쉬 코드를 생성한 후 복호화 된 디지털 서명을 비교하여 워터마킹 된 영상의 변형 유,무와 변형 위치를 찾아 나간다.

워터마크 추출 과정에서 워터마크 삽입에 대응되는 올바른 공개키를 사용하지 않으면 워터마크를 추출할 수 없게 된다.

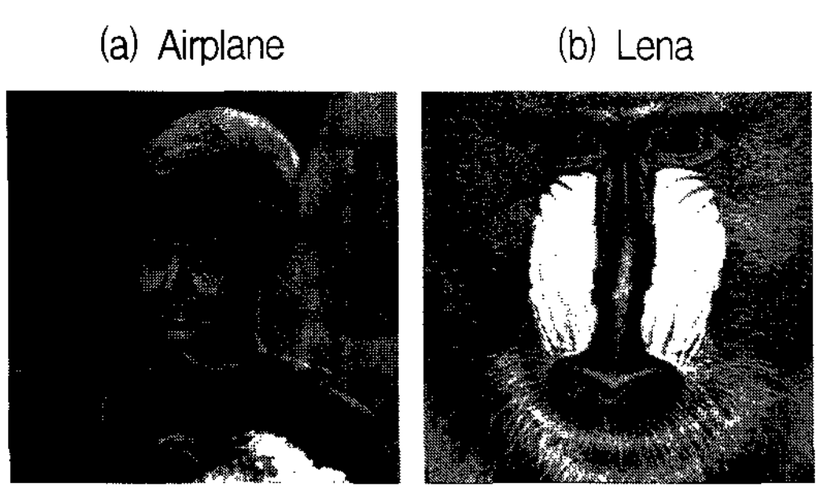
Ⅳ. 실험 결과 및 성능 분석

제안 방법에 대하여 워터마크를 삽입한 후 영상의 변형 유,무 및 변형 위치의 검출은 256×256 크기의 그림 7의 4가지 영상을 대상으로 실험하였다.

본 논문에서의 실험 결과는 그림 7의 (a)Airplane에 대해서만 나타내었으며 이의 결과로 그림 8은 4-레벨에서 16×16 크기로 분할된 각 블록들을 나타내고 있다.

그림 9의 (a)는 그림 7의 Airplane 원 영상을 변형한 것을 나타내고 (b)는 변형된 부분을 검출한 영상으로

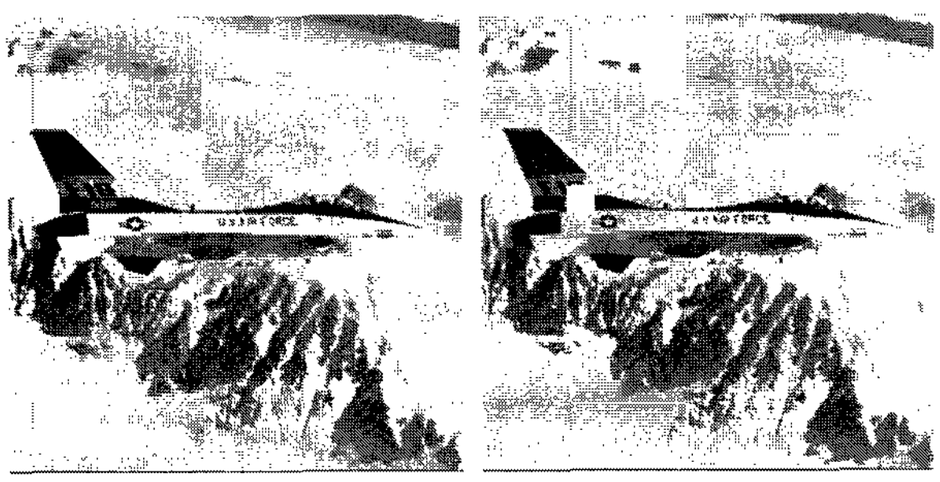
(a) Airplane (b) Lena



(c) Girl (d) Baboon

그림 7. 실험 영상
Fig. 7. Test Images.

그림 8. 4-레벨 영상 블록
Fig. 8. 4-level blocks of the Image.



(a) 변형된 영상 (b) 변형부분 검출 영상

(c) 원 영상 블록 (d) 변형 영상 블록

(e) 변형 부분 검출 블록

그림 9. 변형된 영상과 워터마크 검출 영상
Fig. 9. Manipulated image and Watermark detection image.

변형이 발생된 부분을 흰색 블록으로 나타내고 있다. (c)는 변형이 발생되기 전의 원 영상 블록을 나타내고 (d)는 변형된 영상의 블록을 나타내고 있다. (e)는 변형된 부분을 검출한 세부 영상을 나타낸다.

Ⅴ. 결 론

본 논문에서는 워터마킹 된 영상의 국부적인 변형이 발생하였을 경우 워터마킹 된 영상의 전체를 검사하지 않고 변형이 예측 되는 부분만을 검사하여 변형 유,무와 변형 위치를 효과적으로 검색할 수 있는 워터마킹 방법을 제안하였다. 제안된 방법은 워터마크 삽입을 위하여 원 영상을 5계층의 레벨로 구분하여 영상을 분할

한 후 각 레벨의 영상 블록들에 대한 디지털 서명을 구한다. 이와 같은 과정으로 얻어진 레벨별 영상 블록들에 대한 디지털 서명은 4-레벨의 각 영상 블록들에 삽입된다. 워터마킹 된 영상의 변형 유,무의 검출은 워터마크 삽입과 같은 방법으로 각 레벨의 영상블록 들의 디지털 서명을 구한 후 4-레벨의 영상 블록에서 검출된 디지털 서명을 비교하여 확인한다.

제안 방법에 대한 검증은 256×256 크기의 4가지 영상들을 대상으로 실험하였으며 실험 결과 워터마킹 된 영상에 변형이 발생하였을 경우 전체 영상에 대한 검사 없이 변형이 발생된 영상블록들만 검사할 수 있어 효과적으로 전체 영상에 대한 변형 여부를 확인할 수 있었다. 향후 연구과제로는 분할되는 레벨을 줄일 수 있는 방법과 정지영상 뿐만 아니라 음성, 동화상 등의 멀티미디어 데이터에 적용할 수 있는 방법에 대한 연구가 필요할 것이다.

참 고 문 헌

[1] D.Kundur, D.Hatzinakos, "A Robust Digital Image Watermarking Method using Wavelet-Based Fusion," Proc. IEEE ICIP, Santa Barbara, California, Vol.1, pp. 544-547, Oct, 1997.

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

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

[4] K.S.NG and L.M.CHENG "Selective block assignment approach for robust digital image watermarking," Proc. of SPIE, Vol. 3657, Jan, pp. 14-20, 1999.

[5] R.B.Wolfgang, J.D.Edward, "Fragile Watermarking Using VW2D Watermark," Proc. of SPIE, Vol. 3657, Jan, pp. 204-213, 1999.

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

[7] 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.

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

[9] M.U.Celik, G.Sharma, E.Saber, A.M.Tekalp, "Hierarchical Watermarking for Secure Image Authentication with Localization," IEEE Trans. on Image Processing, Vol. 11, No. 6, pp. 585-595, June, 2002.

[10] William Stallings, *Network and Internetwork Security*, Prentice Hall, 1995.

저 자 소 개

우 찬 일(평생회원)

1993년 단국대학교 전자공학과 공학사.
1995년 단국대학교 전자공학과 공학석사.
2003년 단국대학교 전자공학과 공학박사.
2004년~현재 서일대학 정보통신전공 교수.
<주관심분야: 디지털 워터마킹, 정보보호 시스템, 스마트카드 보안, 데이터베이스 보안>

전 세 길(정회원)

1998년 단국대학교 컴퓨터공학과 공학사.
2000년 단국대학교 컴퓨터공학과 공학석사.
2004년 단국대학교 전자컴퓨터공학과 공학박사.
2006년~현재 한국도로공사 도로교통기술원 책임연구원
<주관심분야: 시공간데이터베이스, 데이터 모델링메타데이터, 데이터베이스보안>