JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 4 : 759~766 Apr. 2017

의료영상 보안을 위한 워터마크 인증 암호화 기법

조영복[1] · 우성희[2*] · 이상호[1]

Watermark Authentication Cryptography for Medical Image Security

Young-bok Cho[1] · Sung-Hee Woo[2*] · Sang-Ho Lee[1]

[1]Department of Computer Science, Chungbuk National University, Chungbuk 28644, Korea
[2*]Department of Medical Information&Engineering, Korea National University Transportation, Chnngbuk 27469, Korea

요 약

제안 논문에서는 의료영상의 다양한 공격에 안전하고 견고하도록 의료 영상을 일정기간 압축 저장해 디지털 콘텐츠에 투명성을 유지한다. 제안논문은 오리지널 영상의 특징 값을 추출하고 사용자의 정보와 결합해서 암호화된 영상 인증코드를 생성한다. 인증코드는 은닉된 데이터를 추출하기 위해 먼저 암호화된 의료영상을 복호화하고 영상의 공간 특성을 이용해 은닉데이터를 추출한다. 따라서 워터마킹을 통해 콘텐츠 자체에 직접 삽입 후 영상의 인증을 위해 추출된 인증코드와 새로 생성된 인증코드의 비교를 수행해 무결성을 보장하고 영상자료의 다양한 공격 안전함을 증명하고 인증률도 98.4%로 향상됨을 증명하였다.

ABSTRACT

In this paper, we preserve the transparency of digital contents by compressing and storing the medical image for a certain period so as to be safe and robust against various attacks of medical images. The proposed algorithm generates an encrypted image authentication code that extracts the feature value of the original image and combines it with the user's information. in order to extract hidden data, the authentication code is first decrypts the encrypted medical image and extracts the hidden data using the spatial characteristics of image. The proposed algorithm guarantees integrity when comparing extracted authentication code and newly generated authentication code for image authentication after directly inserting it into content itself through watermarking. We have proved various security of attack of image data and proved that the certification rate is improved to 98.4%.

키워드 : 인증코드, 무결성, 의료영상 이미지, 보안, 워터마크

Key word : Authentication Code, Integrity, Medical Image, Security, Watermark

Received 29 November 2016, **Revised** 01 December 2016, **Accepted** 08 December 2016

* **Corresponding Author** Sung-Hee Woo(E-mail:shwoo@ut.ac.kr, Tel:+82-43-820-5323)
Department of Medical Information&Engineering, Korea National University Transportation, Chnngbuk 27469, Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.4.759 print ISSN: 2234-4772 online ISSN: 2288-4165

ⓒThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/ by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

Ⅰ. 서 론

최근 급변하는 디지털 시대에 디지털 콘텐츠를 이용한 많은 서버가 개발되어지고 의료계에서도 환자진단 영상을 디지털 영상으로 저장하여 관리하는 PACS (Picture Archiving and Communications System)의 도입으로 디지털 의료영상으로서의 전환이 전체 의료계의 추세로 자리 잡아 가고 있다. 특히 HIS(Hospital Information System), RIS(Radiology Information System)의 텍스트 중심의 의료 전산시스템은 병원 업무의 효율성을 높여 주고 있다. 기존의 필름 중심 시스템에서의 물리적인 문제를 해결하고 환자에 관한 정보의 보안성 유지와 유용성을 확보하기 위해서 의료 영상의 통합적이고 효율적인 획득과 전송, 저장 관리할 수 있는 의료 영상 시스템인 PACS가 등장하였다. 또한 영상 자료의 무결성을 인증하기 위해서는 수신된 영상이 위변조되지 않았다는 것을 증명할 수 있어야만하고 인증의 처리과정은 거대한 분량의 멀티미디어 흐름에 지장이 없도록 실시간에 가깝게 처리되어져야만 한다[1,2]. 또한 공격자가 쉽게 유추하거나 복제할 수 없도록 보안성 조건도 만족하여야만 한다. 초창기의 인증 기술은 암호화 기법을 이용하여 정당한 수신자만이 영상을 볼 수 있도록 하는 방법이었다. 그러나 암호화 기술은 콘텐츠 배포과정에서의 보호만 보장할 뿐이며, 한 번 복호화된 콘텐츠는 더 이상 보호될 수 없기 때문에 콘텐츠의 무결성을 입증하기 위한 충분한 수단을 제공하기에는 부족하다[3]. 이와 같은 문제 해결을 위해 불법적인 사용의 제한과 환자정보 보안 및 인증을 위해 워터마킹(watermarking)기법이 제안되었고[3] 그중 디지털 워터마킹은 멀티미디어 데이터에 관련된 개인정보, 그리고 이진영상(Binary Image) 등의 워터마크를 사람이 청각이나 시각등으로 인지할 수 없도록 원본 데이터에 삽입하는 방식을 채택하고 있다[4,5]. 또한 기존의 암호화 방식과 비밀 통신의 장점을 혼용해 임의의 사용자에 의한 멀티미디어 데이터 변형, 복사, 위조 등의 불법적 행위와 일반적인 신호처리, 압축 등의 의도적이고 불법적인 다양한 상황에서도 디지털 콘텐츠를 보호할 수 있도록 하는 기술이다[5,6]. 디지털 워터마킹은 원본 콘텐츠에 대한 메타데이터 혹은 무결성 검증을 위한 인증코드 및 저작권 정보 등의 워터마크 정보를 비가시적으로 콘텐츠에 삽입하는 기술로 디지털 의료 영상은 의사의 진단 과정이 있기 전에는 어떠한 데이터 변형이나 손실도 허용하지 않고 있다. 이러한 의료 정보 영상의 특징을 기반으로 디지털 워터마킹을 PACS 환경 및 웹 기반 의료영상 시스템에 적용하여 의료 영상 정보에 대한 환자의 워터 마킹 방법은 압축, 필터링, 노이즈, 기하학적 변형 등에 대해서 여러 가지 알고리즘이 제안 되었다[7]. 그러나 의료영상 기록의 보안과 개인 사생활 보호, 진단의 정확성 및 저장 정보에 대한 데이터 인증 연구가 필요하다. 따라서 제안 논문에서는 의료 영상 정보에서 발생할 수 있는 기하학적 변환과 압축 등의 영상 변환에서도 워터마크의 견고성을 확인할 수 있는 워터마크 보안 알고리즘을 제안하고 실행하였다.

이 논문의 구성은 다음과 같다. 2장에서는 관련연구로 디지털영상 워터마킹 기법에 대해 설명한다. 3장에서는 이 논문에서 제안하는 의료영상 보안을 위한 워터마크 인증 암호화 기법에 대해 기술하고, 4장에서 실험 및 평가한다. 마지막으로 5장에서 논문의 결론과 향후 연구에 대해 기술한다.

Ⅱ. 관련연구

디지털 영상 콘텐츠의 인증과 무결성 검증을 위한 여러 데이터 은닉 기술들이 제안되어졌는데, 강인성 워터마킹보다는 주로 연성 워터마킹 기술들이 제안되었다. 연성 워터마킹으로 삽입된 은닉 데이터는 작은 조작에도 손상되기 쉬우므로 위변조 여부 판별에 쉽게 응용 가능하기 때문이다[4-6].

2.1. 디지털 의료영상 정보

디지털 의료 영상 정보는 대부분 환자의 신체를 투과하는 방사선과 몸속에 투여된 방사능 물질에서 방출되는 방사능 에너지를 측정하여 2차원 및 3차원 데이터를 나타낸다. 초음파 및 PET(Position Emission Topography)영상 일부는 칼라 영상이 사용되고 있으나 아직도 흑백 영상이 주종을 이루고 있다. 또한 명암 단계는 8비트에서 12비트까지이며 64×64bits의 핵의학 영상에서부터 2048×2560bits의 CR(Computed Radiography) 영상까지 다양한 데이터 용량을 가진다[8]. 의료 영상의 종류, 해상도, 비트 수 비교는 표 1과 같다.

Table. 1 Type of medical image, resolution and bit depth

Type	Resolution	Bit Dept
X-ray(CR,DR)	2048×2560	10
Remot(RF)	2048×2560	10
Digital subtraction(DS)	1024×1024	12
Culture Technology(CT)	512×512	12
Magnetic resonance	256×256	12
Ultrasound(US)	640×640	8
Nuclear Medical(NM)	64×64	8

기존 연구의 무손실 압축 기법을 이용하여 비트 평면을 압축한 후 빈 공간에 메시지를 삽입하거나[3], 주파수 영역에서의 변환계수에 삽입하였다[4,5]. 또는 원본 영상의 특성 값을 확장하여 삽입하는 차이 값 확장 방법을 사용하는 워터마크 기법들이 제안되었다[6,7]. 최근에는 계산 복잡도가 높지 않으며 높은 삽입용량을 얻을 수 있는 히스토그램 기반 방법들[9,10]에 관한 연구가 활발히 진행 중이며 알고리즘에 따라 영상의 밝기 값에 대한 히스토그램을 이용하거나 차이 값에 대한 히스토그램을 이용함으로 의료영상 이미지의 무결성을 보장하고 있다.

2.2. 의료영상의 워터마크 신호

의료영상의 대부분은 정지영상으로 기존 정지영상에 대한 워터마크 기법은 정지영상에서 워터마크를 삽입하는 기법과 동영상에서 워터마크를 삽입하는 기법으로 구분해 볼 수 있다[11]. 또한 정지영상에서 워터마크를 삽입하는 경우는 공간영역에서 워터 마크를 삽입, 주파수 영역의 변환계수를 워터마크 삽입하는 경우로 구분해 볼 수 있다. 또한 동영상에서는 화소영역에서 워터마크 삽입과 압축영역에서 워터마크 삽입으로 구분된다.

2.2.1. 정지 영상에서의 워터마크 기법

○ 공간 영역에서 워터마크를 삽입하는 기법

이 기법은 원 영상의 밝기의 세기를 변화시키거나 영상내의 임의 패턴을 삽입하는 방법을 사용한다[12]. 정지 영상의 경우 원영상의 내용과 질에 영향을 주지 않고 화소값을 LSB(Least Significant Bit)를 워터 마크로 바꾸는 방법과 화소들을 두 개씩 선택한 후 하나는 증가 시키고 하나는 감소시키는 방법 등이 있다.

○ 주파수 영역의 변환계수를 워터마크로 삽입

이 기법은 손실 압축을 수행한 후에도 워터마크가 존재할 수 있도록 DTC(Discrete Cosine Transform), DFT(Discrete Fourier Transform) 또는 DWT(Discrete Wavelet Transform) 등을 이용하여 주파수 영역으로 변환한 후 중간 주파수 대역에 워터마크를 삽입한다[13]. 그리고 LOGPolar mapping이라는 변환을 적용한 워터마크 기법이 있는데 이 변환은 회전, 이동, 크기변환에 불변한 공간으로 변환시키는 방법이다.

2.2.2.동영상에서 워터마크 기법

○ 화소영역에서 워터마크

동영상 워터마크 기법은 각각의 동영상 프레임에 정지 영상에서 사용한 워터마크 기법을 우선 적용한다. 워터마크의 일반적인 삽입 기법은 정지 영상에서 사용된 워터마크 기법을 각 프레임의 화소 영역에 워터마크를 삽입한다[13]. 그밖에 동영상 각 프레임의 DC-DCT계수에 워터마크를 삽입하는 방법과 각각의 프레임에서 객체를 구분해 객체에만 워터마크를 삽입하는 방법 등이 있다.

○ 압축 영역에서의 워터마크

압축 영역에서 워터마크 삽입 방법은 보호하고자하는 데이터가 이미 압축되어 있는 경우, 복원, 재압축의 과정 없이 워터마크 삽입이 가능하여 동영상등에 실시간으로 이용할 수 있다. MPEG의 표준 VLC에서 서로 바뀌어도 전체 비트 율이 변하지 않으며 화면의 질의 차이가 거의 없는 VLC 코드 쌍을 추출한다. 이를 Label-bit-carry VLC(lc-VLC)로 정의하고 lc-VLC를 서로 바꾸어 워터마크를 삽입하는 방법 등이 있다[14].

2.3. 의료영상 인증 코드

블록 단위의 영상 인증에 관한 기존 연구들은 영상 블록에 대한 특징값을 유일하게 구분하기 위하여 여러 종류의 인증코드를 생성하여 사용하였는데, 일반적으로 평균값, 패리티 값, 체크섬, 해시값 등을 사용하여왔다. 그러나 이러한 값들은 그 크기가 작기 때문에 오탐지의 가능성이 존재한다. 예를 들어 평균값을 인증코드로 사용할 경우 일반적인 영상에서 8 비트의 크기를 가지므로, 인증코드의 경우의 수는 2^8가지(256)이다. 이것이 의미하는 것은 1/256의 확률로 우연에 의한 오탐지의 가

능성이 존재하는 것으로 만일 공격자의 위・변조 행위가 원영상과 매우 유사하도록 유지하며 미미하게 이루어질 경우에는 오탐지의 확률이 더욱 높아진다. 따라서 인증코드는 오탐지 확률을 최소화할 수 있을 정도의 길이를 가져야만 한다. 그러나 지나치게 큰 길이의 인증코드는 워터마킹 기법으로 메시지를 삽입하고자 할 때, 삽입 가능한 최대용량을 초과할 수 있으므로 워터마킹 알고리즘에 따라 알맞은 크기를 가져야 한다.

Ⅲ. 의료영상 보안을 위한 워터마크 인증 암호화 기법

3.1. 웨이블릿 변환을 이용한 의료영상 보안 알고리즘

웨이블릿(wavelet) 분석은 비교적 최근에 개발된 시계열 및 신호분석 도구이다. 웨이블릿 변환분석을 위해 Fourier Analysis의 의미를 파악하고 있어야 한다. 이 Fourier Analysis는 신호를 다른 진동수를 지닌 여러 개의 사인 함수로 쪼개어 그 신호를 구성하고 있는 성분을 분석하는 방법론이다. 그런데 이 방법론의 중대한 결점은 시간영역에서 진동수 영역으로 변환할 때 시간에 대한 정보가 사라진다는 점이다. 따라서 이와 같은 결점을 보안하기 위해서 Wavelet Analysis가 제안되었다. Fourier Analysis는 신호를 다양한 진동수의 사인파(sign)로 쪼개어 나타내는 반면, Wavelet Analysis는 신호가 기본이 되는 wavelet(mother wavelet)의 확장 또는 축소, 그리고 이동을 통해 생성된 wavelet(Daughter wavelet)을 이용하여 신호를 쪼개어 표현한다.

3.2. 웨이블릿 변환

웨이블릿은 단일 원형 함수에 기반을 둔 우수한 Scaling 특성으로 원 신호의 다중 해상도 표현 및 분석이 가능하다. 웨이블릿 변환은 식(1)에 의해서 저주파 측정에서는 기저 함수 신호 폭이 늘어나고 고주파의 경우 좁아지는 모양을 갖는다.

$$\psi_{a,b}(t) = \frac{1}{\sqrt{|a|}}\psi(\frac{t-b}{a}) \qquad (1)$$

그림 1는 일반적인 1차원 신호의 웨이블릿 분해와 복원이 이루어지는 과정을 나타낸 것이다. 그림 1에서 G0는 고역 여파기를, H0는 저역 여파기를 나타낸다. 2차원 신호인 영상 신호의 경우 수직과 수평 방향에 각각 저역여파기와 고역 여파기를 사용해 분해한다. 그 결과 서로 다른 4개의 대역이 생기게 되는데 수평 수직 저주파 대역인 LL-band, 수평방향으로 저주파수, 수직 방향으로 고주파수 대역인 HL-band, 수평방향으로 고주파수, 수직방향으로 저주파 대역인 HL-band, 수평 수직 고주파수 대역인 HH-band가 생긴다.

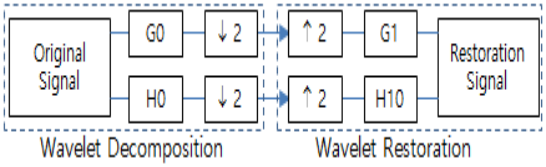

Fig. 1 Resolution & restoration of 1st degree signal

3.3. 워터마크 삽입 및 검출 알고리즘

○ 워터마크 삽입 알고리즘 설계

제안 알고리즘에서는 고주파 대역에 워터마크가 삽입되면 다양한 영상처리 과정에 의하여 워터마크의 견고성이 작아진다. 반대로 저주파 대역에 워터마크를 삽입하면 영상에 왜곡이 발생하는 현상 때문에 중간주파수 대역에 워터마크를 첨부하는 방안으로 삽입되는 워터마크를 삽입, 시각적으로 인지 가능한 의미 있는 이진(binary)영상을 사용하여 워터마크를 삽입한다. 워터마크 삽입은 다음과 같은 과정으로 이루어진다.

첫째, 소유권자의 이미지 내용에 대한 정보를 포함한 워터마크를 생성한다.

둘째, 3단계 웨이블렛 변환을 통해 원본 이미지를 주파수 영역으로 변환하며, 고주파수 대역에서는 계수의 절대치 기준의 임계값을 설정한다.

셋째, 주파수 영역에서 워터마크를 삽입할 저주파 성분 영역과 수평 방향과 수직 방향과 대각선 방향의 에지 특성을 갖는 고주파 성분 영역에 임계값을 설정한다. 이 임계값은 이미지 워터마크를 시각적으로 삽입하기 위해 설정한다.

넷째, 설정된 임계값을 적용하여 (식2)에 따라 웨이블릿 변환에 따라 워터마크를 인코딩 한다.

$$\begin{aligned} &in\ case \quad D_c^{'} = D_c(1+\propto W_c) \subset |D_c > t_i| \\ &otherwise \quad D_c^{'} = D_c \end{aligned} \qquad (2)$$

여기서 D_c는 정해진 해상도 계층과 정해진 주파수방향에 따라 원본 이미지의 주파수 영역에서의 웨이블릿 계수의 값, $D_c^{'}$는 워터마크가 삽입된 이미지의 주파수 영역에서의 웨이블릿 계수의 값 , W는 워터마크 순서, 주파수 방향과 일치되는 t_i는 임계값을 각 각 나타낸다.

다섯째, 워터마크가 삽입된 계수의 시퀀스를 역 이산 웨이블릿 변환하여 워터마크가 삽입된 이미지를 생성한다.

3.4. 워터마크 인증 단계

워터마크의 추출은 삽입단계의 역 추적과정에 의해 처리되고 추출된 워터마크가 원소유자의 정보가 담긴 워터마크인지 아닌지, 통계학적 접근방법을 이용하여 인증한다. 워터마크가 삽입된 이미지 변형이나 삽입된 워터마크를 제거하기 위한다양한 공격 형태, 즉 손실 압축, 필터링, 잡음 첨가, 크로핑 리샘플링 등의 이미지 처리를 한 경우에 추출되는 워터마크를 인증할 필요가 있다. 제안 논문에서는 추출된 워터마크를 인증하기 위해서 통계학적인 접근방법을 이용하여 추출된 워터마크의 유사도를 판단하는 상관계수를 이용한다. 소유권에 대한 인증 절차는 그림 2와 같다.

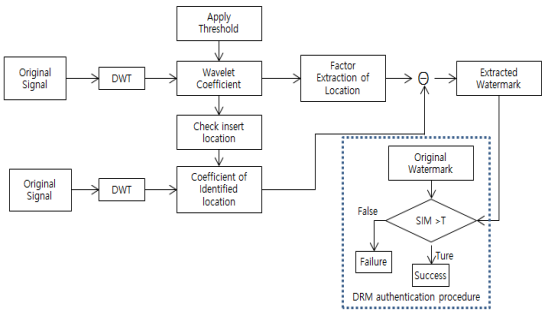

Fig. 2 DRM Authentication Procedure

3.5. 인증코드 생성 알고리즘

고성능의 인증률을 달성하기 위해서는 오탐지의 확률을 최소화하기 위한 충분한 길이의 인증코드를 사용하여야 하므로 각 블록에 대한 DCT 상위 계수들을 선택하여 인증을 위한 특징값으로 사용한다. 실험적으로 얻은 최적의 인증코드 길이는 8 Bytes로서 이것의 우연에 의한 오탐지 확률은 $1/2^{64}$가지 즉, $1/(1.84467E+19)=5.42101E-20$의 확률이므로 그 가능성은 거의 없다고 할 수 있을 것이다. 삽입해야 할 블록별 인증코드의 길이는 64 비트이므로 블록의 삽입 가능 용량이 충분한지 확인하여야 한다. 8x8 블록으로 영상을 분할할 경우에는 삽입공간이 많이 부족하여 적절하지 않다는 것을 실험을 통하여 알아내었다. 따라서 제안 논문에서는 그림 3과 같이 원영상을 16×16 크기의 블록으로 분할하고, 각 블록을 다시 8x8 크기로 평균값 샘플링을 한 뒤 DCT 및 양자화 과정을 수행하여 상위 8 Bytes의 계수를 선택하여 인증코드를 생성한다. 이때, 만일 공격자가 영상의 색상 정보를 일부 변화시키는 것이 아니라 블록보다 큰 크기의 영역을 완전히 잘라내기 공격을 하였을 때는 해당 블록에서 검출한 인증코드와 계산된 인증코드가 0으로 같아지게 되어 올바른 인증을 수행할 수 없게 된다. 이 문제를 방지하기 위하여, 선택된 DCT 인증코드를 영상의 수신측과 공유된 비밀키와 XOR 연산을 수행하여 최종적인 인증코드를 생성 한다. 비밀키는 인증기관을 통하여 발행된 키를 사용할 수도 있으며 또는 사용자 정보(user-specific code등을 사용 목적에 따라 유연하게 사용할 수 있다.

Ⅳ. 실험 및 결과

4.1. 실험환경

제안 논문에서 실험에 사용된 영상은 ㈜소노엠에서 운영되고 있는 스마트러닝 콘텐츠 이미지의 8-Bits 컬러 512x512 영상 8 개로 구성된다. 영상의 품질은 다음 수식(3)과 수식 (4)를 통하여 계산된 PSNR(dB)로 측정하였다.

$$MSE=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(p_{(i,j)}-p_{(i,j)}^{'})^2 \quad (3)$$

$$PSNR_{dB}=10\log_{10}\frac{(2^n-1)^2}{MSE} \quad (4)$$

M과 N은 각각 영상의 가로 및 세로 크기이며, $p_{(i,j)}$는 원본 영상의 픽셀값, $p^{'(i,j)}$은 마크가 삽입된 영상의 픽셀값이고, n은 한 픽셀을 표현할 때 필요한 비트의 수(Bit Depth)이다. 성능평가를 위하여 영상이미지의 대표적인 공격방법인 “Brightness”, “Darkness”,

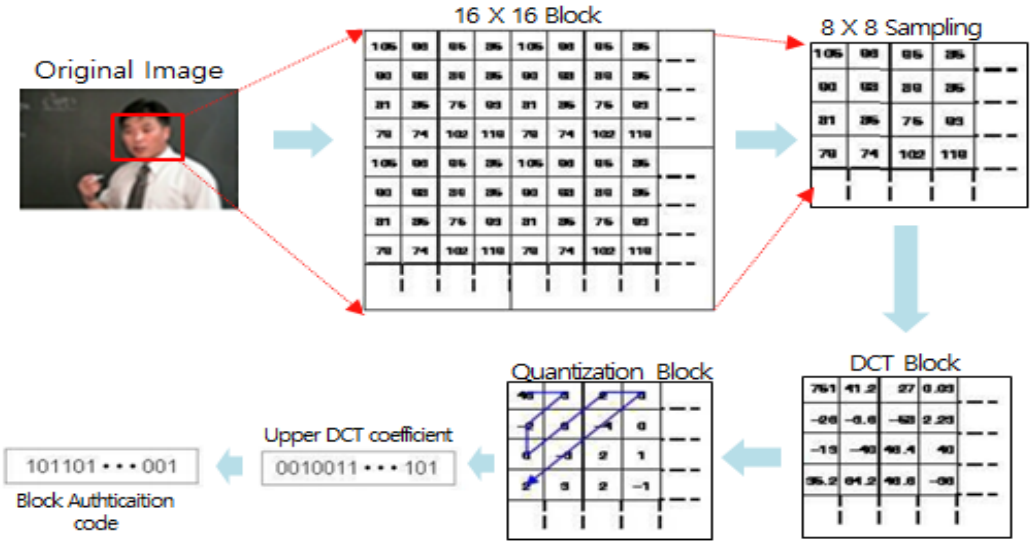

Fig. 3 Laplacian authentication code generation algorithm

"Manipulating", "Blurring" 과 "Copy&Paste"에 대하여 실험하였다. 알고리즘의 효율성을 알아보기 위한 실험 환경은 표 2와 같다.

Table. 2 Simulation Environments

System Type	64bit OS
Processer	Inter(R) Core i7 3.4GHz
OS	Windows 10
Memory	8GB
Progrmming	Visual Studio 2015
Image Size	16×16
Resolrution	8bit RGB
File Format	BMP

전체 인증코드를 삽입한 영상을 나타낸 그림 4를 통해 알 수 있듯이 영상의 변화를 인간의 시각적 능력으로 감지 할 수 없다. 실험영상에 대하여 인증코드를 워터마킹 한 결과를 표 3에 나타내었다. 표 3에서 나타나듯이 평균 인증률은 98.4%로 나타냈으며 인증 시간은 평균 0.64sec로 기존 영상 암호화 방식과 거의 유사한 결과를 보였다.

Table. 3 Simulation Result

Images	PSNR (dB)	Payload (bpp)	Insert time (sec)	Auth Time (sec)	Cert rate (%)
Img1	38.08	0.57	0.571	0.640	98.38
Img2	28.56	0.57	0.633	0.640	98.78
Img3	34.80	0.57	0.586	0.639	97.04
Img4	34.54	0.57	0.587	0.656	98.89
Img5	36.17	0.57	0.582	0.655	98.42
Img6	31.74	0.57	0.618	0.640	98.47
Img7	40.17	0.57	0.555	0.640	98.76
Img8	30.47	0.57	0.586	0.640	98.47
Avg	34.32	0.57	0.59	0.64	98.40

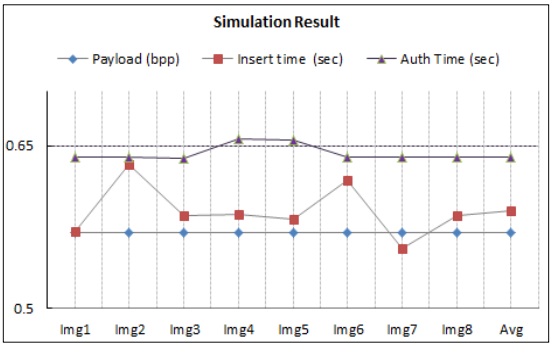

Fig. 4 Simulation Result

Ⅴ. 결 론

제안 논문에서 영상 콘텐츠의 무결성을 검증하기 위한 알고리즘으로서, 원본 영상을 16x16 크기의 블록단위로 분할하여 각 블록에 DCT 계수를 통한 인증코드를 삽입함으로써 공격자에 의한 손상여부를 인증할 수 있는 기법을 제안하였다. 디지털 워터마킹 기법은 지적재산권보호를 목적으로 제안되었지만 현재는 다양한 분야에서 활용되고 있다.

불법적인 사용자에 의한 의료 영상의 변형, 의도적인 공격에 따른 의료 영상의 훼손, 데이터 진위 여부 판단, 환자 정보의 보안 등이 문제점으로 제기되고 있다. 이와 같은 문제들을 해결하기 위한 방법으로 디지털 콘텐츠에 소유자의 정보를 삽입하는 워터마크 방법이 제안되었다. 시각적 품질인 PSNR은 평균 36dB로 양호한 상태이다. 이 결과를 통해 알 수 있듯이, 제안한 영상 인증 가역 워터마킹 알고리즘의 성능은 영상 특성에 따라 조금씩 달라진다. Splash처럼 저주파 성분을 더 많이 포함하고 있는 영상이 품질을 좋게 유지하면서도 높은 삽입용량을 얻을 수 있지만 Baboon처럼 고주파 성분이 많은 영상은 상대적으로 품질이 낮아진다는 것을 알 수 있다.

16x16 블록에 8Bytes씩 RGB 채널 각각에 삽입되었으므로 삽입용량은 0.57 bpp로 동일하다. 단일 채널에 대한 삽입용량은 0.25 bpp가 된다. 삽입과정에 걸린 시간은 평균 0.59초이며, 검출 및 인증에 걸린 시간은 평균 0.64초이다. 인증률은 98.4%로서 대부분의 손상 블록을 탐지할 수 있었다.

ACKNOWLEDGMENTS

This work (No.C0422615) was supported by Business for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Small and Medium Business Administration in 2017

REFERENCES

[1] G. T. Oh, Y. B. Lee and S. J. Yeon, “Security Mechanism for Medical Image Information on PACS Using Invisible Watermark,” in *Proceedings of the International Conference on High Performance Computing for Computational Science 2004*, pp. 315-324, 2004.

[2] E. T. Lin, C. I. Podilchuk, and E. J. Delp, “Detection of image alterations using semi-fragile watermarks,” *in Proceedings of the Electronic Imaging. International Society for Optics and Photonics*, pp. 152-163, 2003.

[3] M. Awrangjeb, “An Overview of Reversible Data Hiding,” *in Proceedings of the Sixth International Conference on Computer and Information Technology*, pp.75-79, 2003.

[4] X. Q. Zhou, H. K. Huang and S. L. Lou, “Authenticity and integrity of digital mammography images,” *IEEE Transactions on Medical Imaging*, vol. 20, no. 8, pp. 784-791, Aug. 2001.

[5] K. F. Li, T. S. Chen and S. C. Wu, “Image tamper detection and recovery system based on discrete wavelet transform,” *in Proceedings of the IEEE Pacific Rim Conference*, vol. 1, no. 8, pp.164-167, 2001.

[6] I. J. Cox, M. l. Miller and J. A. Bloom, “Watermarking applications and their Properties,” *in Proceedings of the Information Technology:Coding and Computing 2000*, pp. 6-10, 2000.

[7] J. J. Eggers, J. K. Su, and B. Girod, “Performance of a practical blind watermarking scheme,” *in Proceedings of the Photonics West 2001-Electronic Imaging*, vol. 4314, pp. 594-605, 2001.

[8] S. Milani, M, Fontani., P. Bestagini, M. Barni, A. Piva, M. Tagliasacchi, and S. Tubaro, “An overview on video forensics,” *in Proceeding of Signal Proceedings Conference*, pp. 1229-1233, 2012.

[9] S.Y Tak, J.M Ban, S Lew, W.J Lee, B.R Lee and H.CKang, “A Study on an Image Stabilization in Moving Vehicle,” *International Journal of The Institute of Electronics Engineers*, vol. 49, no. 4, pp. 95-104, Jun. 2012.

[10] S. D. Lin, and Z. L Yang, “Hierarchical Fragile Watermarking Scheme for Image Authentication,” *International Journal of Intelligent Automation & Soft Computing*, vol. 17, no.2 , pp. 245-255, Mar. 2011.

[11] R. Amirtharajan, and J. B. B. Rayappan, “Brownian motion of binary and gray-binary and gray bits in image for stego,” *International Journal of Applied Sciences*, vol.12,

no.5, pp. 428-439, May. 2012.

[12] M. U. Celik, G. Sharma, A. M. Tekalp and E. Saber, “Lossless generalized-LSB data embedding,” *IEEE Transactions on Image Processing*, vol.14, no.2, pp.253-266, Feb. 2005.

[13] S. Lee, C. D. Yoo and T. Kalker, “Reversible image watermarking based on integer-to-integer wavelet transform,” *IEEE Transactions on Information Forensics and Security*, vol.2, no.3, pp.321- 330, Sept. 2007.

[14] H. J. Kim, S. Xiang and I. K. Yeo. “Robustness analysis of patchwork watermarking schemes,” *in Digital Audio Watermarking Techniques and Technologies:Applications and Benchmarks.* IGI Global, pp. 172-186, 2008.

조영복(Young-Bok Cho)

2005: 충북대학교 전자계산학과 공학석사.
2012: 충북대학교 전자계산학과 공학박사
2016: 충북대학교 의학과 박사과정수료
현재: 충북대학교 초빙교수
※관심분야: 의료영상처리, 정보보안, 의료정보보호
Email : bogicho@cbnu.ac.kr

우성희(Sung-Hee Woo)

1993: 충북대학교 전자계산학과 이학석사.
1999: 충북대학교 전자계산학과 이학박사
현재: 한국교통대학교 의료정보공학과 교수
※관심분야: 침입차단 및 방지, 의료정보보호, 정보보안, 컴퓨터네트워크
Email : shwoo@ut.ac.kr

이상호(Sang-Ho Lee)

1989: 숭실대학교 전자계산학과 공학박사.
현재: 충북대학교 소프트웨어학과 교수
※관심분야: 컴퓨터네트워크, 정보보호, 데이터통신
Email : shlee@cbnu.ac.kr