차분 이미지 히스토그램을 이용한 이중 레벨 블록단위 가역 데이터 은닉 기법

조성환[1], 윤은준[2], 유기영[3]

Twice Level Block-based Reversible Data Hiding Scheme using Difference Image Histogram

SungHwan Cho[1], Eun-Jun Yoon[2], Kee-Young Yoo[3]

요 약

가역 데이터 은닉 기법은 이미지에 비밀 데이터를 삽입 후, 이미지에서 삽입된 데이터를 추출한 후에 원본 이미지의 복원이 완벽하게 가능한 기법을 말하며 최근에 많은 관심을 받고 있는 분야이다. 이러한 복원 가능한 데이터 은닉 기법 중 기존의 히스토그램을 이용한 기법들은 데이터 처리를 비트 단위로 함으로서 은닉 데이터의 삽입량에 대한 효율성이 떨어지는 문제를 공유하고 있다. 본 논문에서는 이러한 문제점을 해결하기 위해 차분 이미지 히스토그램을 이용한 이중 레벨 블록단위 가역 데이터 은닉 기법을 제안한다. 본 논문에서 제안한 기법은 이미지 히스토그램의 역 S-순서를 블럭단위로 적용하고 은닉 데이터 삽입량을 향상하기 위해 이중 레벨 기법을 적용한다. 실험결과 본 논문에서 제안하는 기법이 데이터 삽입량 면에서 우수한 성능을 보였다.

핵심어 : 가역 데이터 은닉 기법, 차분 이미지, 블록단위 기법

Abstract

Reversible data hiding, which can recover the original image without any distortion after the extraction of the hidden data, has drawn considerable attention in recent years. However, the previous researches of histogram based data hiding scheme share the problem of the limit of the embedding capacity of secret data because they use bit level data processing. To overcome the problem, we propose a new twice level block-based reversible data hiding scheme using difference image histogram. The proposed scheme uses block-based inverse S-order image histogram and allows for dual-level data hiding to increase the hiding capacity. The simulation results demonstrate that the proposed scheme generates good performance in the embedding capacity.

Keywords : Reversible data hiding, Difference image, Block-based scheme

접수일(2013년03월01일), 심사의뢰일(2013년03월02일), 심사완료일(1차:2013년03월08일, 2차:2013년03월18일)

게재일(2013년04월30일)

[1]702-701 대구시 북구 복현동, 경북대학교 대학원 전자전기컴퓨터학부.
email: csh518@naver.com

[2]712-701 경상북도 경산시 하양읍, 경일대학교 사이버보안학과.
email: ejyoon@kiu.ac.kr

[3](교신저자)702-701 대구시 북구 복현동, 경북대학교 컴퓨터학부.
email: yook@knu.ac.kr

1. 서론

멀티미디어 기술과 인터넷 환경의 발달로 인해 현대 사회에서 디지털 콘텐츠의 이용이 지속적으로 증가하고 있다. 이러한 경향과 더불어 디지털 콘텐츠에 대한 소유권 및 저작권을 보호하기 위한 기술적 요구사항도 늘어나고 있다[1]. 특히, 디지털 콘텐츠(Digital Contents)는 불법적인 복사에 의해 손쉽고 빠르게 배포될 수 있으며 이에 따른 저작권 침해 문제가 대두되고 있다. 저작권 보호에 대한 이러한 문제를 해결하기 위해 콘텐츠의 불법 복제 및 유통을 차단할 수 있는 DRM (Digital Rights Management) 기술이 커다란 관심을 받고 있다[2].

DRM은 디지털 콘텐츠에 다양한 정보보호 기법을 적용함으로서 콘텐츠가 불법 유통되더라도 라이센스(License)가 없는 사용자는 콘텐츠를 사용할 수 없게 만드는 기술이다. DRM의 한 예로서 암호 기법을 통한 콘텐츠 보호 기법을 고려할 수 있다. 이 기법은 콘텐츠의 불법 복제를 사전에 차단할 수 있는 기능을 제공하지만 콘텐츠가 복호화 되어 이용되는 순간에는 무방비 상태가 되는 문제가 존재한다. 따라서 콘텐츠에 특별한 데이터를 숨김으로서 저작권을 보호할 수 있는 데이터 은닉(Data Hiding) 기법이 좋은 해결책이 될 수 있다. 데이터 은닉 기법은 디지털 워터마킹(Digital Watermarking) 기법으로 사용될 수 있는데 디지털 콘텐츠에 저작권 정보인 워터마크(Watermark)를 삽입함으로서 콘텐츠의 저작권을 보호할 수 있다. 기존의 디지털 워터마킹 기술에서는 비가시성을 만족하기 위해 디지털 콘텐츠 정보를 사람들이 인지할 수 없을 정도로 변형하여 저작권을 보호하였으므로, 디지털 콘텐츠의 원래 정보를 복원할 수 없는 문제점이 있었다. 하지만 의료나 군사 관련 이미지 등 원본 이미지에서의 조그만 정보 손실이 큰 영향을 미치는 응용 분야에서는 저작권 정보를 추출한 후 원본 이미지를 복원할 수 있는 기술이 필요하였다. 이러한 요구에 따라 최근 수년간 저작권 정보 추출 후 원래 정보를 복원할 수 있는 가역 데이터 은닉(Reversible Data Hiding) 기법에 대한 연구가 활발히 진행되고 있다[3-19].

가역 데이터 은닉 기법에는 크게 압축 이용 기법, 변환 계수 기법, 차이값 확장 기법, 그리고 히스토그램 수정 기법 등이 있다. 각 기법들의 장단점 및 관련 연구는 다음과 같다. Fridrich등은 가역 데이터 은닉 기법을 대표할 만한 무손실 압축기법을 이용한 기법을 제안하였다[3]. 이 기법은 데이터 은닉 공간을 만들기 위하여 이미지의 픽셀(Pixel)값을 비트 평면으로 나타낸 후, LSB(Least Significant Bit)부터 비트정보를 검사하면서 무손실 압축하여 비밀 데이터를 삽입하였다. Fridrich등의 기법에서는 하위 비트 평면은 노이즈 성분이 많아서 압축효율이 떨어지기 때문에 상대적으로 노이즈가 적은 상위 비트 평면에 메시지를 삽입하게 되어 시각적인 손상이 발생하는 문제가 존재한다. 변환 영역에서 이루어지는 알고리즘들의 경우 Yang등은 블록 단위의 정수형 DCT 계수에 기반하여 여러 AC 계수를 선택하여 메시지를 삽입하였다[4]. 그리고 Xuan등은 영상을 DWT로 변환 후 고주파 서브밴드에서 정수 웨이블릿 계수의 가운데 비트평면에 메시지 비트를 삽입했다[5]. Lee등은 영상의 블록에 정수대 정수 웨이블릿 변환을 적용하여 각 블록의 고주파 웨이블릿 계수에

비밀 데이터 비트를 삽입했다[6]. 이러한 방법들은 변환 영역에서 이루어지기 때문에 계산 복잡도가 높다.

차이값 확장 기법에서는 원본 영상의 특성을 포함할 수 있는 작은 값을 생성하고 그 값을 확장함으로써 확장된 공간에 정보를 삽입한다. Tian은 정수형 웨이블릿 변환을 이용하여 영상의 차이값과 평균값을 이용한 특성 값을 계산하고 이 특성 값을 확장하여 비밀 데이터를 삽입하였다[7]. 이러한 기법은 확장 가능한 모든 차이값들의 위치정보 맵을 워터마크와 함께 삽입해야하는 부담이 있다. Alattar는 임의의 정수 변환에 적용 가능한 정형화된 차이값 확장 방법을 제안하였다[8]. Kamstra와 Heijmans는 어느 위치가 확장 가능한지 예측하는 기법을 적용하여 성능을 향상시켰다[9]. Thodi와 Rodriguez는 위치정보 맵을 삽입하기 위해 히스토그램을 쉬프팅하는 방법과, 이웃하는 픽셀들의 공간적 유사도를 활용한 예측 오류 확장 방법을 제안하였다[10].

히스토그램 수정 기법은 영상의 히스토그램을 이용한다. 대부분의 히스토그램 기반 방법들은 모든 처리과정이 공간 영역에서 수행되어지기 때문에 변환 영역에서의 기법에 비해 계산 복잡도가 훨씬 낮다. 이 방법은 알고리즘에 따라서 원 영상의 픽셀값 히스토그램이나 차분 영상의 히스토그램을 이용한다. Ni등과 Versaki등의 방법은 히스토그램의 최소값과 최대값을 이용하는데 삽입용량은 최대값에 속한 픽셀의 빈도수에 의해 정해진다[11-12]. Hwang등과 Kuo등은 Ni의 방법을 확장하여 최소값과 최대값에 대한 정보를 저장하는 위치정보 맵을 이용하였다[13-14]. Lin등은 영상을 서로 겹치지 않는 블록으로 나누고 각 블록에서의 차분 영상을 생성한 후, 각각의 차분 영상에 대한 히스토그램을 수정하여 비밀 데이터를 삽입하였다[15]. Tsai등은 각 블록에서 기준 픽셀과 나머지 픽셀과의 차분으로 구성된 차분 영상을 이용하였다[16]. Li등은 원래 정보를 복원할 수 있는 인접 픽셀들간의 유사도에 기반한 데이터 은닉 기법을 제안하였다[17]. Li등의 기법은 인접 픽셀 차이 값을 역 S-순서(Inverse S-order)로 읽어 히스토그램을 생성하고, 그 히스토그램에서 최대값 2개를 선택한다. 이후 서로 중복되지 않는 범위 내에서 최소값 2개를 선택하고, 각각의 최대값과 최소값을 이용하여 히스토그램 이동한 후, 비어있는 최대값에 비밀 데이터를 비트열로 삽입한다. 이러한 히스토그램 이동을 이용한 기존의 가역 데이터 은닉기법들이 데이터를 숨기기 위한 충분한 공간을 만들 수 있다 하더라도, 데이터가 은닉된 영상에서는 히스토그램 이동 때문에 언더플로우와 오버플로우의 문제가 발생되고 화질저하의 문제가 유발된다. 이 문제를 해결하기 위해 위치정보와 같은 부가 정보를 가지고 있어야 한다.

본 논문에서는 기존의 가역 워터마킹 기법들 중 히스토그램 수정 기법들에 존재하는 공통적인 문제점을 효율적으로 해결하기 위한 이중 블록단위 차분 이미지 히스토그램을 이용한 가역 데이터 은닉 기법을 제안한다. 기존의 가역 데이터 은닉 기법들은 역 S-순서를 사용하고 데이터 처리를 비트단위로 함으로서 은닉 데이터의 삽입량에 대한 효율성이 떨어지는 문제를 공유하고 있다. 본 논문에서는 이러한 기존 연구의 문제점을 해결하기 위해서 이미지 히스토그램의 역 S-순서를 블록단위로 적용하는 이중 레벨 블록단위 가역 데이터 은닉 기법을 제안한다.

본 논문의 구성은 다음과 같다. 먼저, 2장에서는 제안한 가역 데이터 은닉 기법과 연계된 기본

적인 개념에 대해서 살펴본다. 3장에서는 제안한 가역 데이터 은닉 기법에 대해서 비밀 데이터 삽입 및 추출 기법에 대해서 살펴본다. 그리고 4장에서는 실험 및 성능 분석을 제시하고, 5장에서 결론을 맺는다.

2. 가역 데이터 은닉 기법 개요

가역 데이터 은닉 기법은 최근 군사용 혹은 의료용 이미지 데이터를 포함한 특정한 응용분야에서 각광 받고 있는 연성(Fragile) 데이터 은닉 기법의 한 분야이다. 가역 데이터 은닉 기법은 멀티미디어 콘텐츠에 연성 워터마크나 비밀 데이터를 삽입한 후, 콘텐츠의 인증 및 무결성 검사를 제공하는 것과 같은 다양한 목적에서 활용할 수 있다. 가역 데이터 은닉 기법의 가장 큰 장점은 워터마크나 비밀 데이터의 삽입으로 발생하는 콘텐츠의 변경 정도가 극히 미미하고 인간의 지각능력으로는 전혀 알아볼 수 없을 정도이고, 정보 추출 후 원본 콘텐츠와 거의 비슷한 상태로 복원할 수 있다는 점이다. 최근에 여러 가지 방식의 가역 데이터 은닉 기법들이 제안되었다. 이들 기법들은 비밀 데이터를 삽입하는 방법에 따라 다음과 같이 크게 네 가지로 분류할 수 있다.

- 압축 이용 기법 : 비밀 데이터를 삽입하기 위한 공간을 확보하기 위해 이미지의 특징을 이용한 압축 기법을 이용하여 비트 평면을 압축하고 빈 공간에 비밀 데이터를 삽입하는 기법
- 변환 계수 기법 : 변환 영역에서 이루어지는 형태로서 DCT(Discrete Cosine Transform)나 DWT(Discrete Wavelet Transform) 등의 변환 계수에 비밀 데이터를 삽입하는 기법
- 차이값 확장 기법 : 원본 이미지의 특성을 포함할 수 있는 작은 값을 생성하고 그 값을 확장함으로써 확장된 공간에 비밀 데이터를 삽입하는 기법
- 히스토그램 수정 기법 : 이 기법은 구체적인 알고리즘에 따라서 원 이미지의 픽셀값 히스토그램이나 차분 이미지의 히스토그램을 이용하여 비밀 데이터를 삽입하는 기법

먼저, 압축 이용 기법은 무손실 압축 기법을 이용하여 비트 평면을 압축하고 빈 공간에 메시지를 삽입한다. 하지만, 하위 비트 평면에 노이즈가 많이 발생하여 압축효율이 떨어지기 때문에 상대적으로 노이즈가 적은 상위 비트 평면에 비밀 데이터를 삽입함으로서 콘텐츠 왜곡이 심한 문제가 발생한다. 또한 변환 계수 기법은 변환 영역에서 비밀 데이터를 삽입하기 때문에 계산 복잡도가 높은 문제점이 존재한다. 그리고 차이값 확장 기법은 확장 가능한 모든 차분들의 위치정보 맵을 비밀 데이터와 함께 삽입해야하는 부담이 존재한다. 반면에 히스토그램 수정 기법은 모든 처리과정이 공간 영역에서 수행되기 때문에 변환 영역에서의 방법들에 비해 계산 복잡도가 훨씬 낮은 장점이 존재한다.

본 연구에서는 이러한 다양한 가역 데이터 은닉 기법들 중에서 히스토그램 수정 기법에 초점을 맞추고자 한다.

3. 차분 이미지 히스토그램을 이용한 이중 레벨 블록단위 가역 데이터 은닉 기법

본 장에서는 기존의 가역 워터마킹 기법들에 존재하는 공통적인 문제점을 효율적으로 해결하기 위한 이중 블록단위 차분 이미지 히스토그램을 이용한 가역 데이터 은닉 기법을 제안한다. 기존의 가역 데이터 은닉 기법들은 역 S-순서를 사용하고 데이터 처리를 비트단위로 함으로서 은닉 데이터의 삽입량에 대한 효율성이 떨어지는 문제를 공유하고 있다. 본 논문에서는 이러한 기존 연구의 문제점을 해결하기 위해서 이미지 히스토그램의 역 S-순서를 블록단위로 적용하는 이중 블록단위 가역 데이터 은닉 기법을 제안한다. 본 논문에서 제안한 이중 블록단위 기법은 먼저 픽셀 간 차이 값을 산출하고 이에 대한 절대값을 적용한 후 히스토그램을 생성하여 이 히스토그램의 최대값에 비밀 데이터를 삽입하고 이렇게 생성된 데이터에 한 번의 추가적인 전체과정을 반복하여 하나의 최대값에 나머지 비밀 데이터를 삽입한다. 제안한 이중 블록단위 기법은 관련연구의 기법들보다 더 많은 은닉 데이터를 삽입할 수 있는 장점이 있다. 표 1은 본 논문에서 사용하는 기호들에 대한 정의를 보여준다.

[표 1] 사용된 기호들에 대한 정의
[Table 1] Definition of used notations

기 호	의 미
P	픽셀 값으로 이루어진 커버이미지 P
i	이미지의 픽셀 순서 번호
j	블록의 픽셀 순서 번호
m	블록 사이즈
n	블록 순서 번호
$P_j^{(n)}$	블록 n 의 픽셀 값
$P_j^{'(n)}$	블록 n 의 차이 값
$P_i^{'}$	전체이미지의 차이 값
$P_i^{''}$	전체이미지의 수정된 차이 값
$P^{'''}$	픽셀 값으로 이루어진 은닉 이미지 $P^{'''}$
PP_k	k^{th}번째 최대값
ZP_k	k^{th}번째 최소값
S_a	a번째 비밀 데이터 비트열
S_b	b번째 비밀 데이터 비트열
sd_t	삽입된 계수 값

3.1 데이터 삽입 과정

이중 블록단위 기법에서 원본이미지에 비밀 데이터를 은닉하기 위한 데이터 삽입 과정은 그림 1과 같다. 이러한 처리를 위해서 데이터 삽입 알고리즘은 $m \times m$ 블록의 원본 이미지 P와 비밀 데이터 S=(S_a, S_b)을 입력으로 은닉 이미지 P'''을 출력하고 전체적인 처리 과정은 다음과 같다. 알고리즘의 수행을 위해 첫 비밀 데이터는 S=S_a로 설정한다.

단계 1 : 원본 이미지 P를 $m \times m$ 블록으로 나눈다.

단계 2 : 각 픽셀 블록의 차분을 계산한다.
블록의 픽셀을 마지막 블록까지 역 S-순서로 스캔하여 인접 픽셀간의 차분을 다음 식으로 계산한다.

$$P_j^{'(n)} = \begin{cases} P_j^{(n)}, & \text{if } j, n = 0 \\ r^{(n)} - P_j^{(n)}, & \text{if } j = 0, n \neq 0 \\ P_{j-1}^{(n)} - P_j^{(n)}, & \text{그외경우} \end{cases}$$

단계 3 : 차분 P'의 절대값을 이용하여 히스토그램을 생성한다.

단계 4 : 생성된 히스토그램 안에서 최대값 PP_k 와 최소값 ZP_k을 찾는다.

단계 5 : 다음 조건에 따라 차분을 수정하고 최대값에 비밀 데이터를 삽입한다. 만약 PP_k와 P_i'이 같다면 비밀 데이터를 원본 이미지에 삽입하고 픽셀 값은 다음 수식을 이용하여 계산한다.

$$P_i'' = \begin{cases} P_i', & \text{if } S = 0 \text{ or } i = 0 \\ P_i' + sd_t, & \text{if } S = 1 \end{cases}$$

만약 PP_k와 P_i'이 같지 않고 $PP_k < P_i' < ZP_k$ 조건을 만족하면 다음과 같이 계산한다.

$$P_i'' = P_i' + sd_t$$

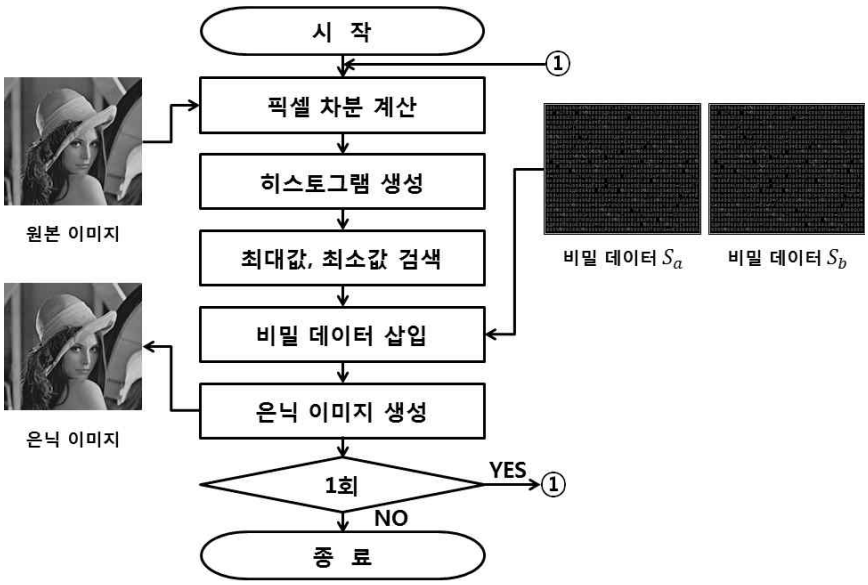
이때, sd_t는 다음 수식을 이용하여 계산한다.

$$sd_t = \begin{cases} 1, & \text{if } p_i' \geq 0 \\ -1, & \text{if } p_i' < 0 \end{cases}$$

단계 6 : 원본 이미지의 P_i와 수정된 차분 P''을 이용하여 P'''_j을 다음과 같이 계산한다.

$$P'''^{(n)}_j = \begin{cases} P''^{(n)}_j, & \text{if } j, n = 0 \\ r^{(n)} - P''^{(n)}_j, & \text{if } j = 0, n \neq 0 \\ P^{(n)}_{j-1} - P''^{(n)}_j, & \text{그외경우} \end{cases}$$

단계 7 : P'''_j을 원본 이미지 P로 치환하여 비밀 데이터 S=S_b를 이용하여 단계 1~6과정을 1번 더 수행한다.



[그림 1] 비밀 데이터 삽입 과정

[Fig. 1] Secret Data Insertion Process

3.2 데이터 추출 과정

이중 블록단위 기법의 은닉 이미지에서 비밀 데이터를 추출하기 위한 데이터 추출 과정은 그림 2와 같다. 이러한 처리를 위한 데이터 추출 알고리즘은 $m \times m$ 블록의 은닉 이미지 P'''을 입력으로 비밀 데이터 (S_a, S_b)와 , 그리고 복원 이미지 P를 출력하며 전체적인 처리 과정은 다음과 같다.

삽입 알고리즘 - 이중 블록단위 가역 데이터 은닉 기법

- 입 력 : $m \times m$ 블록의 원본 이미지 P, 비밀 데이터 S=(S_a, S_b)
- 출 력 : $m \times m$ 블록의 은닉 이미지 P'''
- 처리과정 :

P를 $m \times m$ 블록으로 분할

각 블록의 차분 계산 $P_j^{'(n)} = \begin{cases} P_j^{(n)}, & \text{if } j, n = 0 \\ r^{(n)} - P_j^{(n)}, & \text{if } j = 0, n \neq 0 \\ P_{j-1}^{(n)} - P_j^{(n)}, & \text{그외경우} \end{cases}$

차분 P'의 절대값을 이용하여 히스토그램 생성

생성된 히스토그램에서 최대값 PP_k 와 최소값 ZP_k 검색

if (PP_k== P_i')

{

비밀 데이터 삽입

$$P_i'' = \begin{cases} P_i', & \text{if } S = 0 \text{ or } i = 0 \\ P_i' + sd_t, & \text{if } S = 1 \end{cases}$$

}

else if ($PP_k < P_i' < ZP_k$)

{

$$P_i'' = P_i' + sd_t$$

$$sd_t = \begin{cases} 1, & \text{if } p_i' \geq 0 \\ -1, & \text{if } p_i' < 0 \end{cases}$$

비밀 데이터 삽입

}

P_i와 P'' 을 이용하여 P_j'''을 다음과 같이 계산

$$P_j'''^{(n)} = \begin{cases} P_j''^{(n)}, & \text{if } j, n = 0 \\ r^{(n)} - P_j''^{(n)}, & \text{if } j = 0, n \neq 0 \\ P_{j-1}^{(n)} - P_j''^{(n)}, & \text{그외경우} \end{cases}$$

if 첫 수행, S=S_b, P=P'''로 설정 후 전체과정 1번 더 수행

추출 알고리즘 - 이중 블록단위 가역 데이터 은닉 기법

- 입　　력 : $m \times m$ 블록의 은닉 이미지 P'''
- 출　　력 : $m \times m$ 블록의 복원 이미지 P, 비밀 데이터 (S_a, S_b)
- 처리과정 :

P'''를 $m \times m$ 블럭으로 분할

P'''으로부터 최대값과 최소값을 사용하여 $P_j^{(n)}$을 다음식과 같이 복원

$$P_j^{(n)} = \begin{cases} P_j'''^{(n)}, & \text{if } j, n = 0 \\ P_j'''^{(n)} + sd_t, & \text{if } PP_k > P_{j-1}^{(n)} - P_{j-1}'''^{(n)} \geq ZP_k \\ P_{j-1}^{(n)} - P_j^{(n)}, & \text{그외경우} \end{cases}$$

복원된 블럭 $P_j^{(n)}$을 이용하여 $P_j''^{(n)}$을 다음과 같이 계산

$$P_j''^{(n)} = \begin{cases} P_j'''^{(n)}, & \text{if } j, n = 0 \\ r^{(n)} - P_j'''^{(n)}, & \text{if } j = 0, n \neq 0 \\ P_{j-1}^{(n)} - P_j'''^{(n)}, & \text{그외경우} \end{cases}$$

비밀 데이터를 추출하기 위해서 다음 수식을 계산

$$S = \begin{cases} 0, \text{if } P_j''^{(n)} = PP_k \\ 1, \text{if } P_j''^{(n)} = PP_k + sd_t \end{cases}$$

if 첫 수행, S_a=S, P'''=P''로 설정 후 전체과정 1번 더 수행

else S_b=S, P=P''로 설정 후 처리과정 종료

단계 1 : 은닉 이미지 P'''를 $m \times m$ 블럭으로 나눈다.

단계 2 : 은닉 이미지의 한 블록을 복원하고 수정된 차분의 한 블럭을 다음과 같이 계산한다.

P'''으로부터 최대값과 최소값을 사용하여 $P_j^{(n)}$을 다음식과 같이 복원한다.

$$P_j^{(n)} = \begin{cases} P_j'''^{(n)}, & \text{if } j, n = 0 \\ P_j'''^{(n)} + sd_t, & \text{if } PP_k > P_{j-1}^{(n)} - P_{j-1}'''^{(n)} \geq ZP_k \\ P_{j-1}^{(n)} - P_j^{(n)}, & \text{그외경우} \end{cases}$$

복원된 블럭 $P_j^{(n)}$을 이용하여 $P_j''^{(n)}$을 다음과 같이 계산한다.

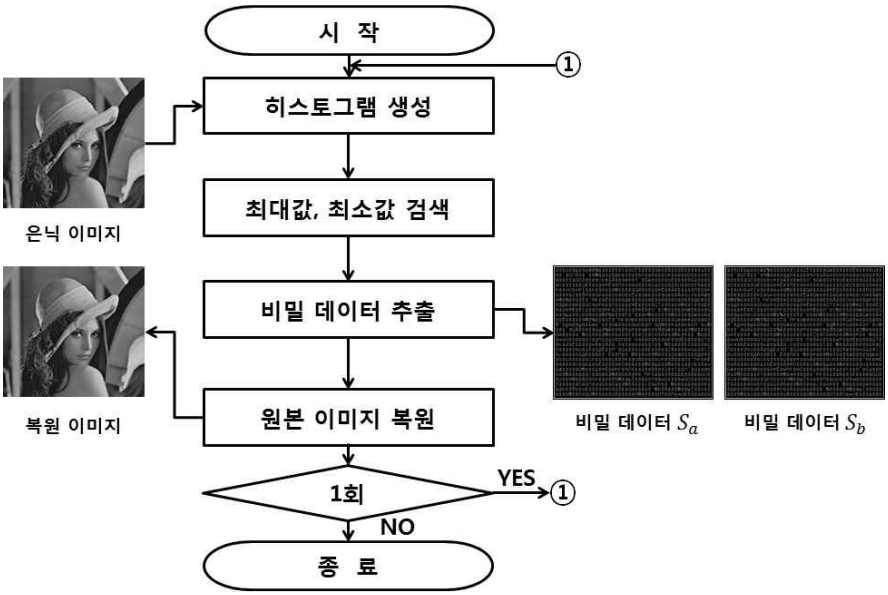
$$P_j^{''(n)} = \begin{cases} P_j^{'''(n)}, & \text{if } j, n = 0 \\ r^{(n)} - P_j^{'''(n)}, & \text{if } j = 0, n \neq 0 \\ P_{j-1}^{(n)} - P_j^{'''(n)}, & \text{그외경우} \end{cases}$$

단계 3 : 비밀 데이터를 추출하기 위해서 다음 수식을 계산한다.

$$S = \begin{cases} 0, \text{if } P_j^{''(n)} = PP_k \\ 1, \text{if } P_j^{''(n)} = PP_k + sd_t \end{cases}$$

최대값과 최소값은 원본 이미지가 완전히 복원될 때까지 사용한다.

단계 4 : 알고리즘이 첫 수행일 경우 S_a=S, $P^{'''}$=$P^{''}$로 설정 후 단계 1~3과정을 1번 더 수행한다. 만일, 첫 수행이 아닐 경우 S_b=S, P=$P^{''}$로 설정 후 처리과정을 종료한다.



[그림 2] 비밀 데이터 추출 과정

[Fig. 2] Secret Data Extraction Process

4. 실험 및 분석

본 장에서는 본 논문에서 제안한 가역 데이터 은닉 기법에 대한 실험 결과 및 분석을 기존의 연구기법 중 대표적인 기법인 Li등의 기법[17]에 대한 비교 분석을 토대로 제시한다.

4.1 실험 환경

본 논문에서 제안한 기법의 성능 평가를 위한 실험을 위해 Intel Core i5-2500 3.30GHz, RAM Memory 6GB 성능의 컴퓨터 환경을 이용하였다. 크기의 이미지 “Lena”, “Airport”, “Avion”, “Baboon”, “Boat”, “Man”, “Man and woman”, “Peppers”, “Village”의 9개 이미지들을 이용하여 실험을 하였으며, 비밀 정보는 난수(random number) 생성기를 통해 만들었다. 그림 3은 본 논문에서 제안한 블록단위 데이터 은닉 기법들에 대한 실험 이미지들을 보여준다.

본 논문의 기법에 대한 성능에 대한 분석을 위해 실험 결과에 대한 비밀 데이터 삽입량과 이미지의 왜곡 정도를 나타내는 PSNR(Peak Signal-to-noise ratio)을 고려한다. PSNR은 다음 식으로 정의된다.

$$PSNR = \left\{ 10 \bullet \log_{10} \left(\frac{255^2}{MSE} \right) \right\}$$

여기서, MSE(Mean squared error)는 원본 이미지와 비밀 정보가 삽입된 은닉 이미지 간의 평균 제곱오차를 뜻하며, 다음 식으로 구할 수 있다.

$$MSE = \left\{ \frac{1}{MN} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left(I_{(i,j)} - I'_{(i,j)} \right)^2 \right\}$$

여기서, $I_{(i,j)}$와 $I'^{(i,j)}$는 크기의 원본 이미지와 비밀 정보가 삽입된 은닉 이미지이며, PSNR 값이 클수록 좋은 이미지 품질을 갖는다.

[표 2] 가역 데이터 은닉 기법들 간의 속성 비교

[Table 2] Property comparison between reversible data hiding schemes

Scheme / Image	Li 등의 기법[17] 최대값 2개		제안한 기법(16×16)	
	삽입량	PSNR	삽입량	PSNR
Lena	47,201	48.54	84,205	46.37
Airport	30,631	48.39	68,362	45.57
Avion	57,137	48.63	92,164	46.50
Baboon	18,533	48.29	60,930	45.56
Boat	29,210	48.38	68,478	45.57
Man	40,748	48.56	79,915	45.80
Man and Woman	37,602	48.57	78,778	45.58
Peppers	35,155	48.44	72,116	45.57
Village	35,868	48.44	72,661	45.56
Average	38,918	48.49	77,266	45.86

본 논문에서 제시한 기법에 대한 분석을 제시하기 위해서 9개 원본 이미지를 통한 실험 결과를 기반으로 비밀 데이터의 삽입량과 은닉 이미지의 왜곡 정도에 대한 비교를 표 2를 기반으로 제시한다. Lena 이미지에 대한 실험 결과 Li등의 기법에서는 47,201비트의 비밀 데이터를 숨길 수 있었고 은닉 이미지의 PSNR 값은 48.54dB이었으며, 제안한 기법 에서는 84,205비트를 숨길 수 있었고, PSNR 값은 46.37dB 이었다. Lena 이미지에 대한 두 방법을 비교하였을 때, 비밀 데이터의 삽입량

(a) Lena (b) Airport (c) Avion

(d) Baboon (e) Boat (f) Man

(g) Man and woman (h) Peppers (i) Village

[그림 3] 실험 이미지

[Fig. 3] Experimental Images

은 37,004비트만큼 증가하였고, PSNR 값은 2.17dB 만큼 감소함을 알 수 있다. 하지만, PSNR 값이 30dB 이상일 때 사람의 눈으로는 이미지의 왜곡을 확인 할 수 없는 정도이고, 특히 비밀 데이터가 이미지에 숨겨진 것 자체를 모를 정도이기 때문에 이미지의 왜곡이 적다고 할 수 있다.

평균을 고려할 때 비밀 데이터의 삽입량은 본 논문에서 제안한 기법이 77,266비트로 Li 등의 기법보다 38,348비트 향상시킬 수 있음을 확인할 수 있고, PSNR 값은 45.86dB로 2.63dB 만큼 감소하였지만 여전히 45dB 이상으로 이미지의 왜곡이 적음을 확인할 수 있다.

5. 결론

본 논문에서는 기존의 가역 워터마킹 기법들 중 히스토그램 수정 기법들에 존재하는 공통적인 문제점을 효율적으로 해결하기 위한 차분 이미지 히스토그램을 이용한 이중 레벨 블록 단위 가역 데이터 은닉 기법을 제안하였다. 기존의 가역 데이터 은닉 기법들은 역 S-순서를 사용하고 데이터 처리를 비트단위로 함으로서 은닉 데이터의 삽입량에 대한 효율성이 떨어지는 문제를 공유하고 있다. 본 논문에서는 이러한 기존 연구의 문제점을 해결하기 위해서 이미지 히스토그램의 역 S-순서를 블럭단위로 적용하는 이중 블록단위 가역 데이터 은닉 기법을 제안하였다. 실험결과에서 확인한 바와 같이 본 논문에서 제안한 기법은 기존 기법들과 비슷한 PSNR을 보이면서 비밀 데이터 삽입량을 효율적으로 향상시킬 수 있음을 확인하였다.

참고문헌 [Reference]

[1] S-K. Lee, Y-S. Ho, Lossless information hiding based on the histogram of the difference image, The Korean Society of Broadcast Engineers. (2003), Vol. 9, No. 4, pp. 31-34.

[2] S-H. Bae, K-H. Lee, Reversible watermarking using multiple histogram shifting, Journal of Korean Society for Imaging Science & Technology. (2008), Vol. 14, No. 3, pp. 194-200.

[3] J. Fridrich, M. Goljan and R. Du, Invertible authentication, Proc. of the SPIE, Security and Watermarking of Multimedia Contents, San Jose, CA, (2001), vol.4314, pp. 197-208.

[4] B. Yang, M. Schmucker, C.B.W. Funk and S. Sun, Integer DCT-based reversible watermarking for images using compounding technique, Proc. of the SPIE, Security, Steganography, and Watermarking of Multimedia Contents, San Jose, CA, (2004), Vol. 5306, pp. 405-415.

[5] G. Xuan, Q. Yao, C. Yang, J. Gao, P. Chai, Y.Q. Shi and Z. Ni, Lossless data hiding using histogram shifting method based on integer wavelets, International Workshop on Digital Watermarking, Lecture Notes in Computer Science. (2006), Vol. 4283, Springer, Jeju Island, Korea, pp. 323-332.

[6] S. Lee, C.D. Yoo and T. Kalker, Reversible image watermarking based on integer-to-integer wavelet transform, IEEE Trans. on Information Forensics and Security. (2007), Vol. 2, No. 3, pp. 321-330.

[7] J. Tian, Reversible data embedding using a difference expansion, IEEE Trans. on Circuits and Systems for Video Technology, (2003), Vol. 13, No. 8, pp. 890-896.

[8] A. M. Alattar, Reversible watermark using the difference expansion of a generalized integer transform, IEEE Trans. on Image Processing, (2004), Vol. 13, No. 8, pp. 1147-1156.

[9] L. Kamstra and H. J. A. M. Heijmans, Reversible data embedding into images using wavelet techniques and sorting, IEEE Trans. on Image Processing, (2005), Vol. 14, No. 12, pp. 2082-2090.

[10] D. M. Thodi and J. J. Rodriguez, Expansion embedding techniques for reversible watermarking, IEEE Trans. on Image Processing, (2007), Vol. 16, No. 3, pp. 721-730.

[11] Z. Ni, Y.-Q. Shi, N. Ansari and W. Su, Reversible data hiding, IEEE Trans. on Circuits and Systems for Video Technology, (2006), Vol. 16, No. 3, pp. 354-362.

[12] E. Varsaki, V. Fotopoulos and A. N. Skodras, A reversible data hiding technique embedding in the image histogram, Technical Report HOU-CSTR-2006-08-GR, Hellenic Open University, (2006)

[13] J. H. Hwang, J. W. Kim and J. U. Choi, A reversible watermarking based on histogram shifting, International Workshop on Digital Watermarking, Lecture Notes in Computer Science, (2006), Vol. 4283, Springer-Verlag, Jeju Island, Korea, pp. 348-361.

[14] W.-C. Kuo, D.-J. Jiang and Y.-C. Huang, Reversible data hiding based on histogram, International Conference on Intelligent Computing, Lecture Notes in Artificial Intelligence, (2007), Vol. 4682, Springer-Verlag, Qing Dao, China, pp. 1152-1161.

[15] C.-C. Lin, W.-L. Tai and C.-C. Chang, Multilevel reversible data hiding based on histogram modification of difference images, Pattern Recognition, (2008), Vol. 41, No. 12, pp. 3582-3591.

[16] P. Tsai, Y.-C. Hu and H.-L. Yeh, Reversible image hiding scheme using predictive coding and histogram shifting, Signal Processing, (2009), Vol. 89, No. 6, pp. 1129-1143.

[17] Y. C. Li, C. M. Yeh., and C. C. Chang., Data hiding based on the similarity between neighboring pixels with reversibility, Digital Signal Processing, (2010), Vol. 20, pp. 1116-1128, 2010

[18] S.-K. Lee, H.-M. Yoo, Y.-H. Suh and J.-W. Suh, Improved Reversible Data Hiding Based on Histogram Modification of Difference Images, International Conference on Consumer Electronics, (2010), pp. 181-182.

[19] K.-S. Kim, M.-J. Lee, H.-Y. Lee and H.-K. Lee, Reversible data hiding exploiting spatial correlation between sub-sampled images, Pattern Recognition, (2009), Vol. 42, No. 11, pp. 3083-3096.

저자 소개

조성환 (SungHwan Cho)

2011년 2월 : 경일대학교 컴퓨터공학부 공학사
2011년 3월~현재 : 경북대학교 대학원 전자전기컴퓨터학부 석사과정
관심분야 : 정보보호, 스테가노그라피

윤은준 (Eun-Jun Yoon)

2008년 2월 : 경북대학교 컴퓨터공학과 공학박사
2007년~2008년 : 수성대학교 컴퓨터정보계열 교수
2009년~2011년 : 경북대학교 전자전기컴퓨터공학부 계약교수
2011년 9월~현재 : 경일대학교 사이버보안학과 교수
2012년 3월~현재 : 경일대학교 사이버보안학과 학과장
관심분야 : 암호학, 인증 기술, 스마트카드 보안, 네트워크 보안, 무선 통신 보안, 스테가노그라피

유기영 (Kee-Young Yoo)

1976년 2월 : 경북대학교 수학교육과 이학사
1978년 2월 : 한국과학기술원 전산학과 공학석사
1992년 3월 : 미국 Rensselaer Polytechnic Institute 전산학과 공학박사
1978년 3월~현재 : 경북대학교 IT대학 컴퓨터학부 교수
관심분야: 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜