Journal of Korea Multimedia Society Vol. 15, No. 4, April 2012(pp. 526-539)

비밀데이터의 패턴정보에 기반한 새로운 정보은닉 기법

김기종†, 신상호††, 유기영†††

요 약

현재까지 연구된 대부분의 정보은닉 기법관련 알고리듬들은 커버영상(cover image)의 변경 또는 조작을 통해 비밀데이터를 삽입(embedding)하여 스테고영상(stego image)을 생성하고, 생성된 스테고영상으로부터 비밀데이터를 추출(extraction)하였다. 이러한 알고리듬은 PSNR의 수치가 높고, 비밀데이터의 수용량(capacity)이 많을수록 좋은 것으로 간주한다. 본 논문에서는 비밀데이터의 패턴(pattern)을 분석하여 숨기는 비밀데이터의 양이 많고, PSNR의 값이 우수한 효율적인 정보은닉 알고리듬을 제안한다. 제안하는 정보은닉 알고리듬은 비밀데이터를 분석하여 비밀데이터 내의 빈도수가 높은 값들을 찾고, 이들의 좌표 값과 인덱스(index)정보를 이용해 커버영상에 삽입한다. 이를 통해 커버영상과 스테고영상 간의 차이는 줄이면서 기존의 제안되었던 알고리듬에 비해 높은 수용량을 보여줌을 실험을 통해 비교한다. 실험결과에서는 5 종류의 비밀데이터와 8 가지 이하의 패턴을 이용해 커버영상에 삽입하여 생성된 스테고영상과의 차이를 측정한 PSNR과 숨겨진 비밀데이터의 양의 결과를 통해 기존에 제안되었던 알고리듬들 비해 제안하는 정보은닉 알고리듬이 우수함을 보여준다.

A New Information Data Hiding Scheme based on Pattern Information of Secret Data

Ki-Jong Kim†, Sang-Ho Shin††, Kee-Young Yoo†††

ABSTRACT

This paper proposes a high capacity data hiding method using high frequence secret data indexing algorithm. Many novel data hiding methods based on LSB and PVD methods were presented to enlarge hiding capacity and provide an imperceptible quality. In this paper, first, calculating data iteration frequency of the secret message and make up the high frequency data index matrix (HFDT) using high frequence data's location information. Next, HFDT uses to that data hiding process on the cover image and recovering process on the stego image. The experimental results demonstrate the efficiency of the proposed high frequency secret data indexing method. For the data hiding method, experiments are conducted for four cases: 2 pattern secret data (2PD), 4 pattern secret data (4PD), 8 pattern secret data (8PD) and higher pattern secret data (HPD). When comparing the proposed method with other data hiding methods, for the HPD case, the results show that the proposed method has a good PSNR and more capacity, and for the other case, the results show that the proposed method has a higher PSNR and larger capacity.

Key words: Steganography(스테가노그래피), Pattern data(패턴 데이터), LSB(최하위비트 은닉방법), PSNR

※ 교신저자(Corresponding Author) : 유기영, 주소 : 대구광역시 북구 대학로 80 경북대학교 IT대학 컴퓨터학부(702-701), 전화 : 053)950-5553, FAX : 053)957-4846, E-mail : yook@knu.ac.kr
접수일 : 2011년 10월 18일, 수정일 : 2011년 12월 19일
완료일 : 2012년 2월 1일

† 정회원, 영진전문대학 컴퓨터정보계열
(E-mail : kjkim@yjc.ac.kr)
†† 정회원, 경북대학교 전자전기컴퓨터학부
(E-mail : shshin80@infosec.knu.ac.kr)
††† 정회원, 경북대학교 컴퓨터학부
※ 본 연구는 2010년도 경북대학교 학술연구비 및 2단계 두뇌한국(BK21)사업의 지원에 의하여 연구되었음.

1. 서 론

컴퓨터와 통신기술의 발전 및 활발한 인터넷 활용으로 다양한 형태의 디지털 멀티미디어 콘텐츠들이 여러 응용 분야에 널리 이용되고 있다. 이러한 디지털 멀티미디어 콘텐츠들은 사용자간 미디어 교환 및 전송의 편의성, 미디어 접근 방법 및 사용의 용이성 등 많은 장점을 지니고 있다.

디지털 멀티미디어 콘텐츠 정보를 보호하기 위한 방법에는 크게 암호화(cryptography)와 스테가노그래피(steganography)가 존재한다. 암호화는 메시지(plaintext)의 내용과 관계없이 비밀키(secret key)로 메시지의 내용을 스크램블링(scrambling)한 암호문(ciphertext)을 전송한다. 즉, 암호문(ciphertext)는 랜덤(random)한 형태로 변형 되었으므로 제 3자는 이를 해독하는 것이 어렵다. 그러나 랜덤 형태의 정보가 송신 및 수신되는 과정에서 공격자 혹은 감시자에게 드러나게 되어, 이 정보가 암호문이라는 의심을 가지고 정보를 공격하거나 통신을 차단하게 할 수 있다.

스테가노그라피는 정보의 존재를 숨기는 방법이다. 스테가노그라피의 어원은 그리스어로부터 왔는데 steganos의 “covered“와 graphos의 “writing“ 혹은 “drawing“이 합쳐진 “covered writing“의 의미를 가지고 다른 정보매체를 이용하여 비가시적으로 비밀정보를 숨기는 기법을 의미한다. 이 기법은 문서, 영상, 오디오, 비디오 등과 같이 커버(cover)라 불리는 미디어에 전달하고자 하는 비밀정보를 비가시적으로 은닉하여 스테고(stego)를 생성하고 전송하는 비밀 통신의 한 방법이다[1-7]. 영상을 이용한 스테가노그라피는 비밀정보를 숨기기 위한 대상 커버로써 디지털 영상(digital image)을 사용하는 것이다. 즉, 커버영상(cover image)에 송신자가 비밀정보를 공격자 및 감시자 몰래 비가시적으로 은닉시키고 생성된 스테고영상(stego image)을 수신자에게 전달하면, 이것을 전달 받은 수신자는 스테고영상에서 비밀정보를 추출하여, 그 내용을 확인할 수 있다[8]. 여기서 비밀데이터는 자막, 설명문, 또 다른 영상, 제어신호 또는 비트 스트림 형태로 표현할 수 있는 것들이어야 한다. 비밀정보는 은닉 처리를 하기 전에 압축이나 암호화가 될 수도 있다[8,9].

지난 20년 동안 연구되었던 스테가노그래피는 대체적으로 디지털 영상(커버영상)내에 숨기는 기법들이 제안되었고, 원본영상의 변형과 공간영역(spatial domain)과 주파수영역(frequency domain)의 특징들을 이용해 많은 비밀 정보를 숨기는 기법이 주류였다[10-17,24]. 공간영역을 이용한 기법들로는 LSB, PVD, 히스토그램 시프트(histogram shift) 등이 있고, 주파수영역을 이용한 기법들로는 DCT, DWT 등을 이용하여 제안을 되어져 왔다. 최근에는 이 두 영역을 결합(hybrid)한 기법들도 연구되어지고 있다.

본 논문에서는 은닉하고자 하는 비밀 데이터를 분석하고 분석 결과를 활용하여 고용량의 비밀 데이터를 비가시적으로 커버영상에 은닉할 수 있도록 하는 새로운 스테가노그라피 알고리듬을 제안한다. 제안하는 방법은, 비밀 데이터의 빈도수를 측정하고 고빈도 데이터(high frequency data: HFD)의 위치 정보를 추출하여 인덱스(index)를 매트릭스(matrix) 형태로 구성한 후 구성된 인덱스 매트릭스를 이용하여 커버영상 내에 고용량의 비밀 데이터를 숨긴다. 본 논문의 우수성을 증명하기 위하여 제안하는 기법을 기존의 관련 연구와 함께 여러 가지 실험 데이터를 이용해 실험을 실시하고, 실험 결과와 수치적 계산결과를 비교 및 분석을 할 것이며, 도출된 성능 평가를 통해 본 논문에서 제안하는 스테가노그라피 기법의 우월성을 확인한다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 커버영상의 공간영역 내에 비밀데이터를 삽입하는 LSB 기법과 PVD 기법에 대해 소개한다. 2장에서는 본 논문에서 제안하는 방법에 대해 설명한다. 제안하는 방법에 대한 실험 및 성능 분석은 4장에서 제시하고, 5장에서 결론을 맺는다.

2. 관련연구

본 논문에서는 스테가노그래피의 공간영역을 활용하는 방법에 기반하여 분석한 비밀데이터를 커버영상에 숨긴다. 이를 위해 공간영역의 활용을 기반으로 널리 사용되는 스테가노그래피 기법들을 본 절에서 소개한다.

2.1 LSB 기법

일반적으로 그레이스케일(grayscale) 커버영상의 각 픽셀은 8-비트로 이루어져 있다. 8-비트의 경우

각 픽셀의 영상을 표현하므로 색의 변화에 따라 256가지의 형태를 취하게 된다. 사람의 시각적인 측면(human visible system: HVS)에서 8-비트 중 최상위 비트(Most Signicant Bit: MSB)가 변경될 경우 일반적으로 사람들은 쉽게 그 사실을 인지할 수 있다. 그러나 최하위 비트(Least Significant Bit: LSB)가 변경될 경우 쉽게 인지할 수 없다. 이러한 사실을 기반으로 LSB 기법이 제안되었고, 8비트 중 LSB 3비트까지 변화시키더라도 HVS는 인지할 수 없다고 실험적으로 증명되었다[18]. 스테가노그래피에서 LSB 기법은 커버 영상의 한 픽셀내에 존재하는 8비트 중 최하위 비트를 비밀 데이터로 변경하여 숨기는 것이다. 만약 커버 영상이 512×512 (픽셀 × 픽셀) 크기로 구성되어 있고, 비밀 데이터를 k-비트를 숨긴다고 가정할 경우 $k\times262{,}144$ 비트만큼의 비밀 데이터를 숨길 수 있다. LSB 과정을 거쳐 비밀 데이터가 삽입(embedding)된 커버영상 즉, 스테고영상(stego image)이 결과물로 나타난다. 이를 수신자가 확인할 수 있도록 인터넷에 공개하면 수신자는 추출(extraction)과정을 통해 커버영상 없이 스테고영상 내에서 비밀데이터를 확인할 수 있다. 이 방법의 주요 결점은 픽셀별로 사용된 LSB의 비트 치환 개수가 4보다 같거나 크게 되면 스테고영상의 품질이 저하되어 사람이 육안으로 영상이 변경된 것을 쉽게 확인할 수 있다는 것이다. 또한, 커버영상을 직접 조작하여 비밀데이터를 은닉하기 때문에 스테고영상의 훼손이나 변형, 왜곡 등의 영상 공격이 발생될 경우 비밀데이터를 확인하기 매우 어렵다. 이러한 문제를 해결하기 위한 방법이 최적화 LBS 치환 방법[18]과, 유전자 알고리즘에 기반한 접근적 최적화 LSB 치환 방법[19]등이 제안되었다.

2.3 PVD기법

픽셀값 차이(pixel-value differencing: PVD)방법은 연속된 두 픽셀의 명암과 부드러움 정도에 따라 숨기는 비밀데이터의 크기를 다르게 하는 것으로 Wu 등이 제안하였다[20]. 그레이스케일의 커버영상에서 중복되지 않는 연속된 두 픽셀을 포함한 블록을 구성하고, 두 개의 연속된 픽셀 p_i와 p_{i+1}로부터 계산된 차이 값이 d_i인 경우, 식은 다음과 같고, $d_i = p_{i+1} - p_i$ d_i,d_i 값은 범위는 [-255, 255] 이다. d_i의 차이 값을 가진 두 픽셀을 포함한 i번째 블록 B_i에 숨길 수 있는 비트 수 n은 다음과 같이 계산되어지고, $n=\log_2(u_i-l_i+1)$, 한편 u_i와 l_i는 정의된 범위 $R_i(i=1,2,...,w)$의 최저와 최고의 범위 값을 각각 의미한다.

비트를 포함한 비밀 데이터의 비트열이 결정되고 새로운 차이 값 d'이 식 (2.1)에 의해 계산되어진다.

$$d' = \begin{cases} l_i + b & \text{for } d \geq 0, \\ -(l_i + b) & \text{for } d < 0 \end{cases} \quad (1)$$

이 때 b는 n값 계산을 위한 부분 비밀 데이터에 대한 정수 값이다. 또한 Wu 등은 커버영상의 부드러운 영역 부분에 LSB 치환 방법을 적용해 향상된 PVD 방법을 제안하였고[20], 이 후 Wang 등은 계수함수(coefficient function)를 적용하여 영상의 품질을 개선한 스테가노그라피 기법을 제안하였다[21].

3. 비밀데이터 분석정보를 이용하는 정보은닉 알고리듬

이 절에서는 본 논문에서 제안한 정보은닉 알고리듬에 대해 설명한다. 제안한 정보은닉 알고리듬에서 고려해야 할 사항들과 본 논문에서 사용되는 용어를 정의하고, 제안한 정보은닉 알고리듬을 설명한다.

3.1 고려사항과 용어 정의

제안하는 정보은닉 알고리듬 내에서 사용되는 비밀데이터의 대상은 영상(image)이다. 이러한 이미지의 픽셀 값에 대한 빈도수를 측정한 다음 인덱스 행렬(index matrix)를 구성하여 커버영상(cover image)에 삽입(embedding)을 한다. 그러므로 비밀데이터는 단순한 형태의 패턴을 가진 영상이나 텍스트 형태의 스캔영상이 적합하다. 본 논문에서 제안하는 정보은닉 알고리듬의 비밀데이터 범주는 다음과 같다. 서명계약서, 여권스캔영상, 워드문서와 같이 일부 색상이 전체의 대다수를 차지하는 것과 8개 이하의 색상으로 표현되는 텍스타일 패턴(pattern), 로고, 설계도면, O/X 답안지, 4지/5지 선다형/택일형의 답안지 등이다.

본 논문에서 제안하는 기법을 기술하고 분석하기 위해 사용되는 용어는 표 1과 같다. 만약 비밀 데이터(secret data: SD)가 $SD=\{S_{00}, S_{01},..., S_{yx}\}$ 일 때, S_{ji}는 j번째 행과 i번째 열의 픽셀 값이고, 각각의 범위가

표 1. 제안하는 정보은닉 알고리듬에서 사용하는 용어의 정의

용 어	정 의	설 명
빈도 데이터 집합	Frequency Data: *FD*	비밀 데이터 내에서 빈도수가 1회 이상인 픽셀 값들의 집합
빈도 데이터	*i*-th *FD*: FD_i	*i*번째 빈도 데이터
고빈도 데이터4	High Frequency Data4: *HFD*4	*FD*중 빈도수 최상위 4개의 픽셀 값들의 집합
고빈도 데이터8	High Frequency Data8: *HFD*8	*FD*중 빈도수 차상위 4개의 픽셀 값들의 집합
저빈도 데이터	Low Frequency Data: *LFD*	*HFD*4와 *HFD*8을 제외한 픽셀 값들의 집합
저빈도 데이터 비트열	Low Frequency Data Sequence: *LFDS*	*LFD*를 비트로 변환한 비트열
비밀데이터 행렬	Secret Data Matrix: *SDM*	비밀 데이터를 커버영상 크기에 맞추어 재배치하기 위한 행렬

$0 \le i \le x,\ 0 \le j \le y$로 구성되어 있다면, 빈도 데이터 집합(*FD*)는

$FD = \{S_{ji}(= FD_0), S_{j(i+1)}(= FD_1), ..., S_{ml}(= FD_{m \times l})\}$ 과 같이 구성되어 있고 픽셀의 빈도수에 따라 내림차순으로 정렬되어 있으며, 다음과 같은 조건이 성립한다.

$$|SD| \ge |FD| \tag{2}$$

고빈도 데이터4(*HFD*4), 고빈도 데이터8(*HFD*8), 저빈도 데이터(*LFD*)의 경우 다음과 같이 구성된다.

$$HFD4 = \{FD_0, ..., FD_3\},\ HFD8 = \{FD_4, ..., FD_7\},\ LFD = \{FD_8, ..., FD_{m \times l}\} \tag{3}$$

이러한 *FD*, *HFD*4, *HFD*8에 대해서 각각의 픽셀 값에 대한 인덱스(index) 정보를 가지고 있는 테이블의 이름을 각각 *FD* 테이블 (*FDT*), *HFD*4 테이블 (*HFDT*4), *HFD*8 테이블 (*HFDT*8)로 정의한다. 한편, 커버영상과 스테고영상의 픽셀 값은 각각 B_{ji}와 B''_{ji}으로 표현한다. B_{ji}와 B''_{ji}은 각각 j번째 행과 i번째 열의 픽셀 값들을 의미하고, 각각의 범위는 $0 \le i \le x,\ 0 \le j \le y$로 구성되어 있다고 가정한다.

3.2 정보 은닉 알고리듬의 비밀데이터 삽입과정

제안하는 정보 은닉 알고리듬은 삽입(embedding) 과정과 추출(extraction)과정으로 나누어진다. 비밀데이터의 삽입과정은 그림 1과 같고, 전체 4단계로 구성되어 있다.

Step 1. 비밀 데이터의 분석과 *SDM* 및 *FD*의 생성

커버영상의 크기가 $H \times W$ (높이×폭)일 경우, 비밀데이터도 커버영상과 동일한 크기로 생성하기 위해

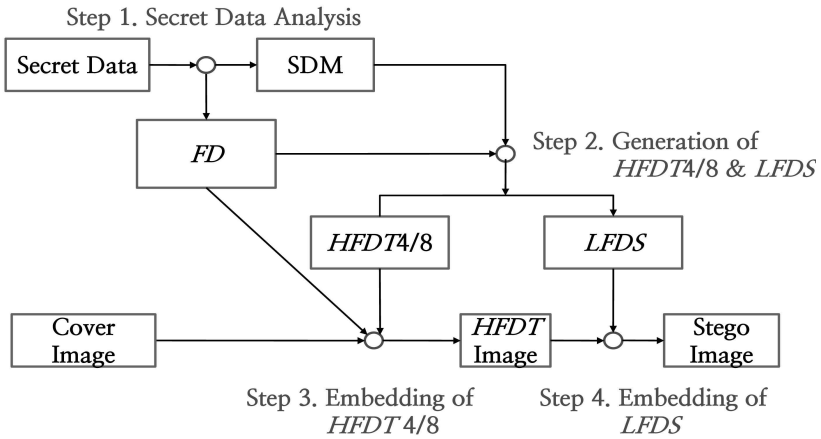


그림 1. 제안하는 정보은닉 알고리듬의 비밀데이터 삽입과정

비밀데이터를 가공을 해야 한다. 비밀데이터가 다음과 같이 비트열(Secret Data-bit Stream: *SDS*)로 구성되었다고 하면 식(4)와 같이 표기한다.

$$SDS = \{s_0, s_1, \ldots, s_{n-1}\} \tag{4}$$

여기서 s_i는 i번째 비트를 의미한다. 이를 8비트 단위($S_{ji} = s_0^{(ji)} s_1^{(ji)} \ldots s_7^{(ji)}$)로 묶은 후 식 (5)와 같이 커버영상과 동일한 크기의 영상(*SDM*)을 생성한다.

$$SDM = \bigcup_{y=0}^{H-1} \bigcup_{x=0}^{W-1} S_{yx} \tag{5}$$

*SDM*을 생성하면서 비밀데이터의 픽셀 값에 대한 빈도수를 체크한 후 *FD*를 생성한다. 다음 단계에서 *FD*를 이용해 *HFD4*, *HFD8*, *LFD*를 각각 구분한다.

Step 2. *HFDT4*, *HFDT8*, *LFDS* 생성

본 단계에서는 *SDM*과 *FD*를 이용해 *HFDT4*, *HFDT8*, *LFDS*를 각각 생성한다. 먼저, *FD*를 이용해 *HFD4*, *HFD8*, *LFD*에 해당하는 픽셀들을 구분짓고, 구분된 집합별로 테이블을 구성한다. 테이블을 구성할 경우 각각의 픽셀 값들에 대한 *SDM*에서의 해당 픽셀의 위치의 좌표 값(y, x)을 각각 기입한다. 예를 들어, 그림 2와 같은 크기가 5×5 *SDM*이 있다고 가정할 때, 짙은 부분(픽셀 값: 46)이 가장 많은 빈도수를 차지하므로, 픽셀 값 46이 FD_0에 해당하고, 이어서 34, 12, 78 순으로 FD_1, FD_2, FD_3에 각각 해당한다. 이렇게 구성된 *HFD4*를 이용해 *HFDT4*를 생성한다.

생성하는 방법은 *SDM* 내에서 지그재그 방식으로 위에서 아래로 검색을 하면서 FD_0 픽셀 값이 위치하고 있는 좌표 값을 각각 *HFDT4* 내의 해당 픽셀 값에 기입한다. 0행 0열에 위치하고 있는 첫 번째 픽셀 12는 FD_2이므로 y값이 0, x값이 0이 된다. 또, 이와 같은 방법으로 *HFDT8*을 생성한다.

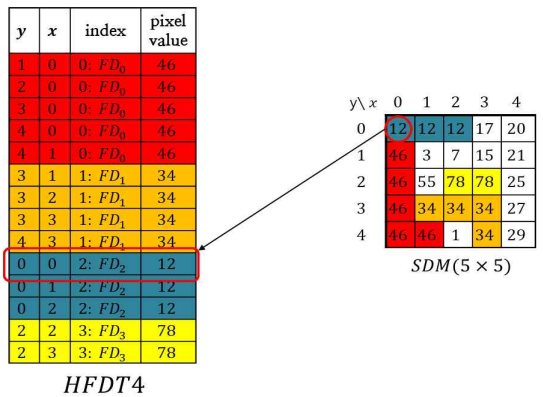


그림 2. *SDM*으로부터 *HFDT4*를 생성하는 예제

한편, *LFD*로 구분된 픽셀 값들의 경우 커버영상에 삽입하기 비트열로 변환되어 *LFDS*를 생성하고, 식 (6)에 의해 수행된다.

$$LFDS = \bigcup_{n=8}^{ml} \{FD_n (= s_0^n s_1^n \ldots s_7^n)\}$$
$$= \{s_0^8 s_1^8 \ldots s_7^8 \| s_0^9 s_1^9 \ldots s_7^9 \| \cdots \| s_0^{ml} s_1^{ml} \ldots s_7^{ml}\} = \{s_0 s_1 \ldots s_{(8\times(ml-8+1))}\} \tag{6}$$

여기서 FD_n은 *LFD*내의 n번째 픽셀 값을 의미하고, 한 픽셀은 8개의 비트들로 구성되어 있으므로 각각의 FD_n은 $b_0^n b_1^n \ldots b_7^n$와 같은 비트열로 변환하여 표현되며, 최종적으로는 0부터 $8\times(ml-8+1)$까지의 인덱스가 부여된 비트열로 표현이 된다.

Step 3. *HFDT4*와 *HFDT8*을 이용한 커버영상 내의 비밀데이터 삽입

제안하는 정보은닉 알고리듬은 고빈도 데이터인 *HFD4*와 *HFD8*을 커버영상에 먼저 삽입한 후 *LFDS*를 커버영상에 삽입하게 된다. 먼저, 고빈도 데이터인 *HFD4*와 *HFD8*를 삽입하는 과정으로 이전 단계에서 생성한 *HFDT4*와 *HFDT8*의 정보를 커버영상 내의 *HFD4*와 *HFD8*에 해당하는 픽셀들에 식 (7)과 같이 삽입한다. 식 (7)은 커버영상 내의 픽셀 값이 *HFD4* 또는 *HFD8*에 해당할 경우 비밀데이터를 삽입하는 방법을 표현한 것이다.

$$B'_{yx} = \begin{cases} LSB_{em1}(B_{yx}, i), \text{ if } y \text{ and } x \in HFDT4, 0 \le i \le 1 \\ LSB_{em2}(B_{yx}, i), \text{ if } y \text{ and } x \in HFDT4, 2 \le i \le 3 \\ LSB_{em3}(B_{yx}, i), \text{ if } y \text{ and } x \in HFDT8, 4 \le i \le 7 \\ B_{yx}, \quad otherwise \end{cases} \tag{7}$$

여기서 i와 y, x는 각각 커버영상으로 생성된 *HFDT4* 또는 *HFDT8*의 좌표 값에 대응하는 FD_i의 인덱스(index) 값과 커버영상의 좌표 값을 의미하고, $LSB_{emk}(B_{yx}, i)$는 i값에 따라 LSB 1비트, 2비트 혹은 3비트에 비밀데이터를 삽입하는 연산을 표현한다.

그림 3은 *HFDT4*를 이용하여 커버영상에 비밀데이터를 삽입하는 과정의 예제이다. 커버영상과 스테

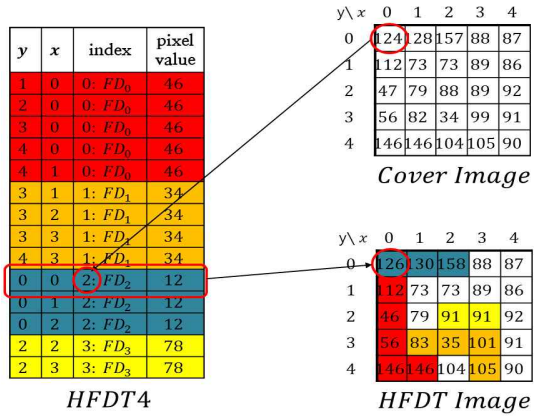


그림 3. HFDT4를 이용한 비밀데이터 삽입 예제

고영상의 크기는 5×5이고, 이전 단계의 예제에서 생성된 *HFDT*4를 이용하여 설명한다. 먼저, 커버영상의 첫 번째 행의 첫 번째 열부터 지그재그방식으로 위에서 아래로 스캔을 실시하며, 커버영상 내의 각각의 좌표 값이 *HFDT*4 내의 좌표 값 정보에 해당하는지를 검색한 후 *HDFT*4 내에 존재한다면 커버영상의 해당 위치에 *HDFT*4의 인덱스 값을 픽셀 값에 삽입한다. 즉, 커버 영상의 첫 번째 행의 첫 번째 열에 해당하는 픽셀 값 124는 $y=0,\ x=0$ 이므로 *HDFT*4 내에서 FD_2의 $y=0, x=0$에 해당한다. 그러므로 FD_2의 인덱스 값인 $i=2$를 커버영상의 픽셀 값 124에 삽입한다. 이런 과정을 반복하여 그림 3의 *HFDT*4가 삽입된 *HFDT* 영상이 생성된다. 만약 *HFDT*4와 *HFDT*8이 모두 존재할 경우 위의 예시와 동일한 방법으로 커버영상을 스캔하면서 커버영상의 픽셀 좌표 값에 해당하는 정보를 *HFDT*4와 *HFDT*8에서 검색하여 해당 픽셀 값에 인덱스 값을 더한다.

Step 4. 압축된 *LFDS* 삽입 단계

압축된 *LFDS* 삽입 단계는 본 논문에서 고려하는 비밀데이터의 범주에서는 필요 없는 부분이지만 일반적인 비밀데이터에 대해서도 사용이 가능하도록 하기 위해 첨가된 것이다. 본 단계는 *HFDT*4와 *HFDT*8에 해당하지 않는 영역에 대해 압축된 *LFDS*의 비트열 중 2비트를 *HFDT*영상의 해당 픽셀의 LSB1영역과 LSB2영역에 각각에 삽입하고, 식 (8)에 의해 수행된다. 또한, 압축 기법은 호프만 부호화 알고리듬[23]을 사용한다.

$$B''_{yx} = LSB_{em2}(B'_{yx}, s_i s_{i+1}) \tag{8}$$

여기서 B'_{yx}은 *HFDT* 영상, $s_i s_{i+1}$은 압축된 *LFDS*내의 i번째와 $i+1$번째 비트 값, $LSB_{em2}(\bullet)$는 LSB2 영역에 $s_i s_{i+1}$를 삽입하는 연산을 표현한 것이다. 예를 들어, 그림 4와 같은 호프만 부호화 알고리듬으로 압축된 *LFDS*와 *HFDT* 영상이 존재한다고 가정하면, *HFDT* 영상 내에서 *HFDT*4 또는 *HFDT*8에 속하지 않는 픽셀들을 검색한다. 0행 3열에 처음으로 속하지 않는 픽셀 값이 88이 나타난다. 이 픽셀에 압축된 *LFDS*의 2비트를 삽입하여 스테고영상의 90처럼 변경된다. 이러한 과정을 반복해 압축된 *LFDS*를 *HFDT*영상에 삽입하여 스테고영상을 생성한다. 생성된 *HDFT*4, *HDFT*8과 압축된 *LFDS*의 비트 길이는 안전한 암호 알고리듬으로 암호화한 후 추출하고자 하는 대상에게 전송을 하여, 비밀데이터 추출과정에서 사용하게 된다.

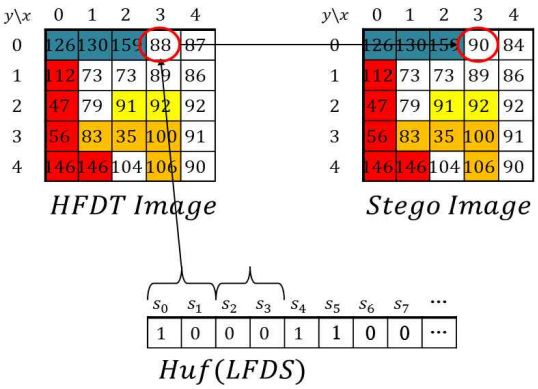


그림 4. 압축된 LFDS의 삽입 예제

3.3 정보은닉 알고리듬의 비밀데이터 추출과정

일반적인 정보은닉 알고리듬은 비밀데이터의 삽입과정과 추출과정이 역순으로 수행된다. 본 논문에서 제안하는 정보은닉 알고리듬의 경우 비밀데이터의 삽입과정과 비밀데이터의 추출과정은 역순으로 유사하게 진행된다.

그림 5는 제안하는 정보은닉 알고리듬의 비밀데이터 추출과정에 대해 보여주고 있다. 추출과정의 경우 삽입과정과 달리 3단계로 간소화하여 수행하고, 각 단계별 세부 내용은 다음과 같다.

Step 1. *LFDS*의 추출 단계

미리 공유된 *HFDT*4와 *HFDT*8 그리고 압축된

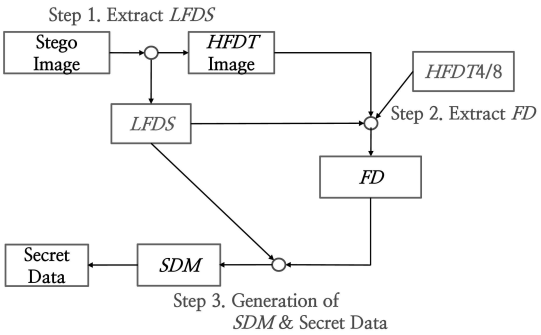


그림 5. 제안하는 정보은닉 알고리듬의 비밀데이터 추출과정

*LFDS*의 길이를 통해 스테고영상으로부터 *LFDS*와 *HFDT*영상을 추출한다. *LFDS*의 추출 방법은 다음과 같다. *HFDT*4와 *HFDT*8에 기입된 픽셀들의 위치를 제외한 나머지 영역의 픽셀들 중 LSB1영역과 LSB2영역에 압축된 *LFDS* 비트들이 2비트 단위로 삽입되었으므로 압축된 *LFDS* 길이만큼 스테고영상에서 압축된 *LFDS*를 추출한다. 이 후 호프만방법을 이용해 압축된 *LFDS*를 풀어서 본래의 *LFDS*를 생성한다. 압축된 *LFDS*를 스테고영상에서 추출하는 방법은 식 (9)와 같다.

$$s_i s_{i+1} = LSB_{ex2}(B''_{yx}) \tag{9}$$

여기서 B''_{yx} 는 스테고영상내의 픽셀값 중 HFDT4와 HFDT8에 포함되지 않은 것을 의미하고, $LSB_{ex2}(\bullet)$는 해당하는 B''_{yx} 의 LSB 2비트를 추출하는 연산을 표현한 것이다.

Step 2. *FD* 추출 단계

이전 단계에서 추출한 *LFDS*와 미리 공유되었던 *HFDT*4와 *HFDT*8 및 *HFDT* 영상을 이용해 원래의 *FD*를 구성하고, *SDM*를 추출한다. 먼저, *LFDS*를 8비트 단위($B_{ji} = b_k b_{k+1} ... b_{k+7}$)로 묶어 픽셀 값으로 변경한 후 *HFDT*4와 *HFDT*8을 이용해 *FD*를 추출한다. 추출된 *FD*는 다음단계에서 추출하는 *SDM*의 구성정보에 참고한다.

Step 3. *SDM*과 비밀데이터 추출단계

추출한 *FD* 및 *HFDT*4와 *HFDT*8을 참고하여 *SDM*의 크기와 각각 좌표에 해당하는 픽셀 값을 삽입한다. 먼저, *HFDT*4를 이용해 *SDM*의 각 좌표에 해당하는 픽셀 값을 삽입한다. 동일한 과정으로 *HFDT*8도 *SDM*에 픽셀 값을 삽입한다. 이 후 비어있는 픽셀에 대해서는 *FD*를 통해 차례대로 삽입을 실시한다. *SDM*를 추출한 후 필요에 따라 비밀데이터로 복원하여 내용을 확인한다.

4. 실험 및 성능평가

4.1 실험에 사용한 커버영상과 성능평가 대상 알고리듬 및 PSNR

본 논문에서 제안한 정보은닉 알고리듬의 성능평가를 위해 LSB, PVD, PVD+LSB 방법들과 PSNR, 수용량(capacity)에 대해 실험하여 비교하였다. 실험에 사용된 커버영상은 스테가노그래피의 실험에서 일반적으로 사용하는 그레이스케일(gray-scale)의 영상 8개를 사용하였고, 영상의 크기는 512×512로 고정하였다. 그림 6은 실험에서 사용한 커버영상 8개를 나타내고 있다.

실험에서 사용한 LSB방법은 최하위 3개의 비트를 이용하여 비밀데이터를 은닉하는 LSB3방식을 채택하였고, PVD방법은 Wu와 Tsai가 제안한 알고리듬[20]을 사용하였으며,

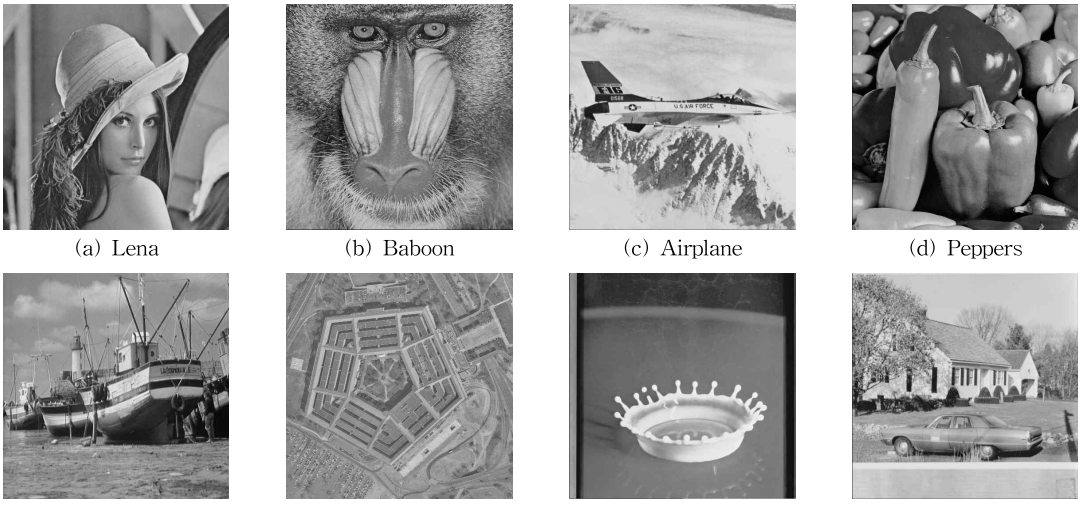
PVD+LSB방법은 Wu 등이 제안한 알고리듬[22]을 사용했다. 또한, 두 픽셀의 차가 16이상일 경우에는 PVD 방법을 적용하였으며 두 픽셀의 차가 15이하인 부드러운 영역에는 각 픽셀당 3비트의 LSB영역에 LSB방법으로 비밀 데이터를 은닉하였다.

PSNR은 비밀데이터가 은닉된 스테고영상 품질을 측정하기 위한 객관적인 평가 기준으로 많이 사용되고 있으며, 커버영상과 스테고영상의 차이를 수치화 하여 나타낸다. 일반적으로 스테고영상의 PSNR 값이 30dB 이상이 되면 비교하는 두 영상의 차이를 눈으로 구분할 수 없는 상태인 것으로 판단하며, 수치가 높을수록 영상의 품질이 높은 것이다. 즉, 두 영상의 차이가 없음을 나타낸다. PSNR 값은 식 (10)과 같이 구한다.

$$PSNR = 10 \times \log_{10} 255^2 / MSE,$$

$$MSE = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (p(x,y) - p'(x,y))^2 / M \times N \tag{10}$$

커버영상의 LSB1 영역만을 랜덤한 비트들로 치환하여 PSNR 값을 측정하게 되면, 평균적으로 49~51dB이 측정되고, LSB1, LSB2 영역을 랜덤하게 치



(a) Lena (b) Baboon (c) Airplane (d) Peppers

(e) Boat (f) Pentagon (g) Splash (h) House

그림 6. 실험에서 사용한 8개의 커버영상

환하면 43~45dB이 된다. 또한 LSB1, LSB2, LSB3 영역을 랜덤한 비트로 치환하게 되면 36~38dB이 측정된다. 그리므로 커버 영상의 LSB1, LSB2, LSB3 영역을 이용하여 비밀 데이터를 숨기게 된다면 생성된 스테고 영상의 품질은 눈으로 차이를 인지할 수 없는 영상이 되는 것이다.

4.2 실험에 사용한 비밀데이터의 종류

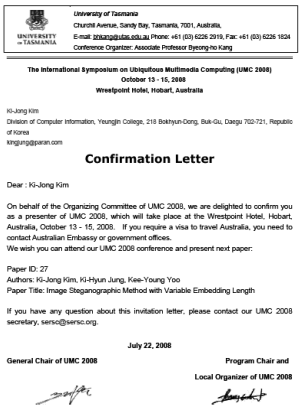
본 실험에서는 문서내용을 캡쳐 한 영상 또는 스캔영상 등 영상 형태의 데이터와 8개 이하 패턴을 가지고 있는 Pattern 형태의 데이터를 구분하여 실험하였다. 그림 7은 본 논문의 실험에서 사용된 5종류의 비밀 데이터 영상을 보여주고 있다. ConfirmLetter는 서명이 포함된 문서를 스캔한 영상이고, Letter의 경우는 손글씨로 작성한 편지를 스캔한 영상이다. 또한 Passport는 일반적으로 사용되고 있는 여권을 스캔한 것이고, Subway는 동경의 지하철 노선도를 캡쳐한 컬러 영상이다. 마지막으로 Paper는 흑과 백 2가지 색상만으로 구성된 문서 영상을 사용하였다. 5종류 비밀 데이터 영상의 데이터 분석결과는 표 2와 같다. 또한 본 실험에서는 2PSD(pattern secret data), 4PSD, 8PSD 형태의 데이터를 사용 하였으며, 그림 8에서는 본 실험에서 사용된 6종류의 비밀 데이터를 보여주고 있다. 2PD(pattern data)는 O,X 형태 문항의 답안 데이터를 의미하며, 4PD의 경우는 사지 선다형(혹은 사지 택일형) 문항의 답안 데이터를 의미한다. 또한 8PD는 8종류 기호로 표시된 등급평가 결과 데이터를 의미하고, 이들의 크기는 모두 512×512이다.

4.3 실험 결과 및 분석

본 절에서는 실험에 사용된 비밀 데이터를 유형별로 분류하여 각 비밀 데이터 별 실험결과를 제시한다. 실험 결과의 제시방법은 먼저 비밀 데이터의

표 2. 비밀데이터 영상에 대한 HFD4 분석 결과

구 분	FD_0 (빈도율(%))	FD_1 (빈도율(%))	FD_2 (빈도율(%))	FD_3 (빈도율(%))	ETC (빈도율(%))
ConfirmLetter	255 (88.31)	0 (2.14)	120 (0.93)	39 (0.89)	101, 230, ... (7.73)
Letter	161 (23.73)	183 (15.57)	140 (13.13)	160 (9.96)	120, 139, ... (37.61)
Passport	15 (42.18)	14 (12.28)	13 (12.17)	12 (8.04)	11, 10, ... (25.33)
Subway	0 (62.86)	8 (6.60)	9 (2.61)	252 (1.28)	10, 11, ... (26.65)
Paper	255 (67.7)	0 (32.3)	NA	NA	NA


University of Tasmania
Churchill Avenue, Sandy Bay, Tasmania, 7001, Australia.
E-mail: jinkang@utas.edu.au Phone: +61 (03) 6226 2919, Fax: +61 (03) 6226 1824
Conference Organizer: Associate Professor Byeong-ho Kang

The International Symposium on Ubiquitous Multimedia Computing (UMC 2008)
October 13 - 15, 2008
Wrestpoint Hotel, Hobart, Australia

Ki-Jong Kim
Division of Computer Information, Yeungjin College, 218 Bokhyun-Dong, Buk-Gu, Daegu 702-721, Republic of Korea
kingung@paran.com

Confirmation Letter

Dear : Ki-Jong Kim

On behalf of the Organizing Committee of UMC 2008, we are delighted to confirm you as a presenter of UMC 2008, which will take place at the Wrestpoint Hotel, Hobart, Australia, October 13 - 15, 2008. If you require a visa to travel Australia, you need to contact Australian Embassy or government offices.
We wish you can attend our UMC 2008 conference and present next paper:

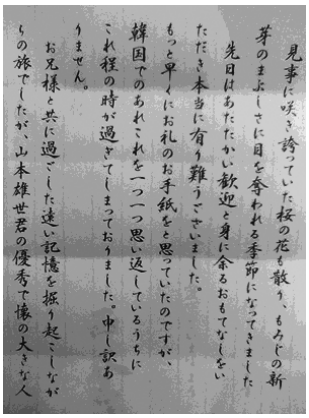
Paper ID: 27
Authors: Ki-Jong Kim, Ki-Hyun Jung, Kee-Young Yoo
Paper Title: Image Steganographic Method with Variable Embedding Length

If you have any question about this invitation letter, please contact our UMC 2008 secretary, sersc@sersc.org.

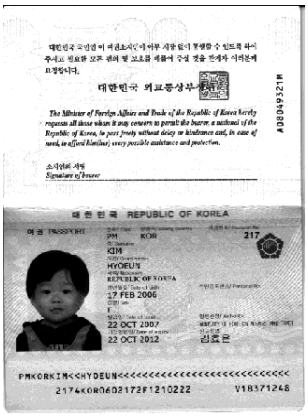
July 22, 2008

General Chair of UMC 2008 — Program Chair and Local Organizer of UMC 2008

(a) ConfirmLetter

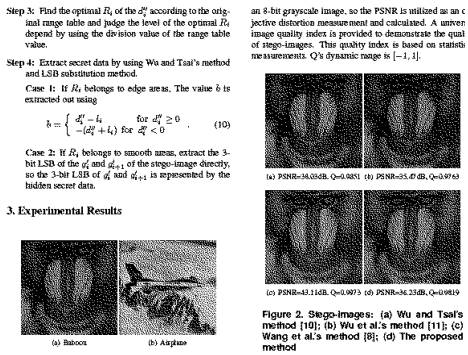

見事に咲き誇っていた桜の花も散り、もみじの新
芽のまぶしさに目を奪われる季節になってきました
先日はあたたかい歓迎と身に余るおもてなしを
ただき本当に有り難うございました。
もっと早くにお礼のお手紙を思っていたのですが、
韓国でのあれこれを一つ一つ思い返しているうちに
これ程の時が過ぎてしまっておりました。申し訳あ
りません。
お兄様と共に過ごした遠い記憶を振り起こしなが
らの旅でしたが、山本雄世君の優秀で優の大きな人

(b) Letter


REPUBLIC OF KOREA
PASSPORT
KOR
KIM
HYOEUN
REPUBLIC OF KOREA
17 FEB 2006
22 OCT 2007
22 OCT 2012
PMKORKIM<<HYOEUN<<<<<<<<<<<<<<<<<<<<<<<<<<<<
2174KOR860217F1210222 V18371248

(c) Passport

(d) Subway


Step 3: Find the optimal R_i of the d_i'' according to the original range table and judge the level of the optimal R_i depend by using the division value of the range table value.

Step 4: Extract secret data by using Wu and Tsai's method and LSB substitution method.

Case 1: If R_i belongs to edge areas, The value b is extracted out using

$$b = \begin{cases} d_i' - l_i & \text{for } d_i'' \geq 0 \\ -(d_i'' + l_i) & \text{for } d_i'' < 0 \end{cases} \quad (10)$$

Case 2: If R_i belongs to smooth areas, extract the 3-bit LSB of the d_i' and d_{i+1}' of the stego-image directly, so the 3-bit LSB of d_i' and d_{i+1}' is represented by the hidden secret data.

3. Experimental Results

(a) Baboon (b) Airplane

an 8-bit grayscale image, so the PSNR is utilized as an o
jective distortion measurement and calculated. A univer
image quality index is provided to demonstrate the qual
of stego-images. This quality index is based on statisti
measurements. Q's dynamic range is $[-1, 1]$.

(a) PSNR=36.036dB, Q=0.9851 (b) PSNR=35.47dB, Q=0.9763
(c) PSNR=43.116dB, Q=0.9973 (d) PSNR=36.23dB, Q=0.9819

Figure 2. Stego-images: (a) Wu and Tsai's method [10]; (b) Wu et al.'s method [11]; (c) Wang et al.'s method [8]; (d) The proposed method

(e) Paper

그림 7. 실험에 사용한 비밀 데이터 영상


XXOOXXXOXXOXOOOO
OXXOOXXOOOOXXOXO
OOXXOOOXXOOOOXXO
OOXOOXXXXOOXXOXXO
XXXXOXXXOXXXOOOOX
XOOOXOOOXOXXXOOO
XXOX

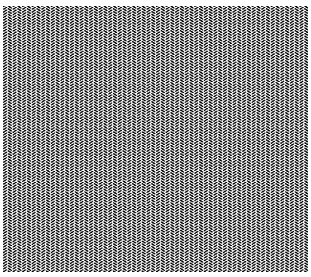
(a) 2PD


CACBBABBCCACBDADA
ACDADDAAABABCDDCD
CDAABACDAABBDDDBC
BDCDBDBBBBBADADDC
ADABCCBCADADBCBBD
CCCCDDBADACCDAABA
CCB

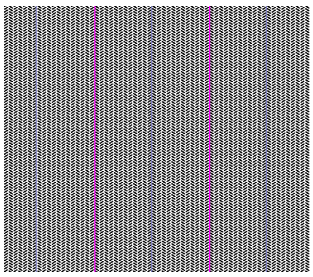
(b) 4PD


BSSSNBFNCNPFCDFDD
PNADBABNAPBCCAABP
BFAPFBCAFBCFSPDACP
NDCPADCBANNSBBCAS
PPANNBCBSDADNFCFB
FSCSSNPPCCCFPADBA
BNS

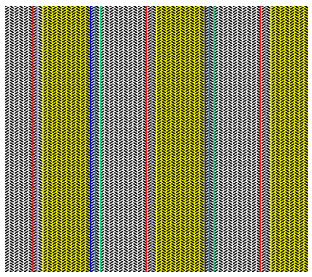
(c) 8PD



(d) 2CT



(e) 4CT



(f) 8CT

그림 8. 실험에 사용한 패턴 비밀 데이터

HFD4 분석결과 표를 이용하여 분석 결과를 제시하며, 임의의 커버 영상에 비밀 데이터 정보를 숨긴 결과로 생성된 스테고 영상을 원본 영상과 함께 제시한다. 그리고 LSB3 방법 및 PVD 방법, PVD+LSB 방법으로 측정한 실험결과와 제안한 정보은닉 알고리듬 방법의 수용량(capacity) 및 PSNR 측정값을 제시한 후 실험결과에 대한 분석을 기술한다.

4.3.1 비밀데이터 영상을 이용한 실험 결과 및 분석

각각의 비밀데이터 영상에 대한 HFD4는 표 3과 같다. 표 3에서 ETC의 경우 HFD4에 속하지 않는 다른 픽셀 값들에 대한 분포를 의미하고 있다. 이를 이용하여 본 논문에서 제안한 정보은닉 알고리듬의 삽입과정을 수행 후 수용량과 PSNR에 대해 실험해 본 결과 각각 표 5와 표 6과 같다. 표 5의 수용량에 대한 실험 결과는 제안한 정보은닉 알고리듬이 다른 알고리듬에 비해 우수함을 보여준다. 특히, paper와 같이 고빈도 데이터의 구성이 0과 1인 경우, 또는 ConfirmLetter와 같이 고빈도 데이터의 비율이 90% 이상인 경우는 많은 양의 비밀데이터를 커버영상에 은닉할 수 있음을 알 수 있었다. 이에 반해 고빈도 데이터의 비율이 가장 낮았던 Letter의 경우 전반적으로 다른 비밀 데이터 영상에 비해 수용량이 낮음을 알 수 있었다. 이를 통해 고빈도의 데이터가 비밀데이터 영상에 많은 경우 제안한 정보은닉 알고리듬이 우수한 성능을 보여줌을 알 수 있었다. 표 6의 PSNR에 대한 실험 결과 역시 제안한 정보은닉 알고리듬이 다른 알고리듬에 비해 우수한 성능을 보여주었다. 일반적으로 PSNR이 35dB 이상일 경우 사람의 눈으로 두 영상간의 차이점을 인지하기 어렵다. 이러한 사실에서 비록 다른 알고리듬에 비해 월등히 우수한 성능을 보여주는 것은 아니지만 비밀데이터 영상의 수용량을 대폭 늘린 것에 반해 PSNR의 수치는 비슷하거나 약간씩 높아졌다. 특히, Paper의 경우 0과 1의 픽셀 값으로 이루어져 있어서 수용량과 PSNR 실험결과 모두에서 우수한 성능을 보여주었다.

4.3.2 패턴데이터 영상을 이용한 실험 결과 및 분석

다음으로 패턴 데이터 영상에 대해 실험한 결과를 분석한다. 표 4는 각각의 PD에 대한 빈도율을 분석한 결과이다. 이를 이용해 커버영상에 대해 패턴데이터 영상을 은닉하는 실험을 통해 수용량과 PSNR의 결과는 각각 표 7 및 표 8과 같다. 표 7의 수용량에 대해선 8PD에 대해서만 실험을 수행하였다. 4PD와 2PD의 경우 제안한 정보은닉 알고리듬에서 100% 은닉하므로 생략을 하였다. 다른 알고리듬과 비교 했을 경우 약 37% 이상의 수용량을 증가시켰음을 알 수 있었다. 이에 반해 PSNR의 경우 다른 알고리듬에 비해 소폭 상승하였다. 특히 2PD, 4PD, 8PD 방법은 각각 LSB1, LSB2, LSB3 방법과 거의 비슷하다. 고로 8PD의 경우 LSB3와 비슷하지만 2PD의 경우 우수한 PSNR 값을 보여준다. 이는 비밀데이터 영상의 Paper와 동일한 형태로 구성되어 있다. 이를 통해 제안한 정보은닉 알고리듬은 2가지 패턴의 데이터에 대해 우수한 수용량과 PSNR을 나타냄을 알 수 있었다.

5. 결 론

본 논문에서는 정보은닉의 대상이 되는 비밀 메시지 분석을 통한 효율적인 자료은닉 방법을 연구 하였고, 고용량의 비밀 데이터를 숨길 수 있는 방법으로 비밀 데이터의 테이터 빈도수를 측정 및 고빈도 데이터의 발생위치 정보를 추출하여 인덱스를 구성한 후 구성된 인덱스 매트릭스를 이용하여 영상데이터에 숨기는 방법을 제안하였다. 소수의 패턴 형태로 구성된 비밀 데이터가 은닉에 사용될 경우에는 기존의 방법들 보다 본 논문에서 제안한 정보은닉 알고리듬이 우월하다는 것을 수치적 분석을 통해 증명하였다.

실험 결과에서는 8개 이하의 색상 또는 패턴을 가진 비밀 데이터의 경우 모든 데이터가 인덱스화 될 수 있으며, 최대 수용량이 커버 영상의 크기와 근접한 크기가 됨을 알 수 있었다. 타 방법과의 비교실험을 한 결과로는 제안 방법이 LSB3와 비교하여 2.6배, PVD와 비교하여 5배, PVD+LSB와 비교하여 2.7배의 수용량을 가짐을 알 수 있었다. 이와 같이 많은 수용량을 가지면서도 PSNR 측정 결과도 타 방법과 비교하여 우수한 결과를 보였다. 또한 FD의 개수가 8을 초과하는 비밀 데이터도 비밀 정보에 포함된 데이터 중 일부 데이터의 비중이 클 경우에 본 논문에서 제안한 알고리듬이 효율적이라는 것을 실험을 통해 확인 할 수 있었다.

향 후 연구로는 본 논문에서 다루지 못한 부분인 다양한 공격에 대한 실험을 수행 후 공간 영역 기반의 알고리듬들도 주파수 영역 기반의 알고리듬들보

표 3. 비밀데이터 영상에 대한 HFD4 분석 결과

구 분	FD_0 (빈도율(%))	FD_1 (빈도율(%))	FD_2 (빈도율(%))	FD_3 (빈도율(%))	ETC (빈도율(%))
ConfirmLetter	255 (88.31)	0 (2.14)	120 (0.93)	39 (0.89)	101, 230, ... (7.73)
Letter	161 (23.73)	183 (15.57)	140 (13.13)	160 (9.96)	120, 139, ... (37.61)
Passport	15 (42.18)	14 (12.28)	13 (12.17)	12 (8.04)	11, 10, ... (25.33)
Subway	0 (62.86)	8 (6.60)	9 (2.61)	252 (1.28)	10, 11, ... (26.65)
Paper	255 (67.7)	0 (32.3)	NA	NA	NA

표 4. 패턴데이터 영상에 대한 빈도율 분석 결과

구분	FD_0 (빈도율)	FD_1 (빈도율)	FD_2 (빈도율)	FD_3 (빈도율)	FD_4 (빈도율)	FD_5 (빈도율)	FD_6 (빈도율)	FD_7 (빈도율)
2PD	88 (50.06)	79 (49.94)	NA	NA	NA	NA	NA	NA
4PD	66 (25.08)	67 (25.02)	65 (24.97)	68 (24.93)	NA	NA	NA	NA
8PD	83 (12.61)	68 (12.61)	65 (12.61)	80 (12.48)	70 (12.46)	78 (12.42)	66 (12.42)	67 (12.39)

표 5. 커버영상 내에 비밀데이터 영상의 은닉 실험 결과(수용량, 단위: bit)

커버영상	비밀데이터 영상	LSB3	PVD	PVD+LSB	제안 알고리듬
Lena	ConfirmLetter	786,432	409,804	765,889	1,671,488
	Letter	786,432	409,807	765,889	967,200
	Passport	786,432	409,807	765,889	1,161,216
	Subway	786,432	409,807	765,889	1,141,200
	Paper	786,432	409,807	765,889	2,052,624
Baboon	ConfirmLetter	786,432	450,777	717,946	1,671,488
	Letter	786,432	457,015	717,946	967,200
	Passport	786,432	456,994	717,946	1,161,216
	Subway	786,432	457,081	717,952	1,141,200
	Paper	786,432	456,988	717,946	2,052,624
Splash	ConfirmLetter	786,432	398,877	782,889	1,671,488
	Letter	786,432	398,877	782,889	967,200
	Passport	786,432	398,877	782,889	1,161,216
	Subway	786,432	398,880	782,889	1,141,200
	Paper	786,432	398,877	782,889	2,052,624
House	ConfirmLetter	786,432	420,611	755,774	1,671,488
	Letter	786,432	420,614	755,774	967,200
	Passport	786,432	420,611	755,774	1,161,216
	Subway	786,432	420,614	755,774	1,141,200
	Paper	786,432	420,614	755,774	2,052,624

표 6. 커버영상 내에 비밀데이터 영상의 은닉 실험 결과(PSNR, 단위: dB)

커버영상	비밀데이터 영상	LSB3	PVD	PVD+LSB	제안 알고리듬
Lena	ConfirmLetter	36.13	37.38	34.66	37.76
	Letter	37.67	41.43	37.44	38.18
	Passport	37.65	40.68	36.66	37.94
	Subway	36.97	41.12	36.11	38.08
	Paper	37.81	38.08	35.01	51.23
Baboon	ConfirmLetter	36.14	32.95	32.04	37.74
	Letter	37.67	37.45	35.52	38.17
	Passport	37.66	36.36	33.88	37.94
	Subway	36.94	37.09	34.97	38.06
	Paper	37.79	33.95	32.91	51.23
Splash	ConfirmLetter	36.20	38.10	35.25	37.86
	Letter	37.75	42.34	37.65	38.28
	Passport	37.75	41.53	36.98	38.03
	Subway	37.05	42.17	35.99	38.19
	Paper	37.86	38.88	35.34	51.23
House	ConfirmLetter	35.96	35.10	33.44	37.86
	Letter	37.67	39.39	36.65	38.19
	Passport	37.57	38.60	35.63	37.97
	Subway	37.07	39.56	35.72	38.15
	Paper	37.72	36.03	34.14	51.22

표 7. 패턴 데이터 8PD 은닉 실험 결과(수용량, 단위: bit)

커버영상	LSB3	PVD	PVD+LSB	제안 알고리듬
Lena	786,432	409,804	765,889	2,093,056
Baboon	786,432	457,048	717,952	2,093,056
Splash	786,432	398,877	782,889	2,093,056
House	786,432	420,614	755,774	2,093,056

표 8. 패턴 데이터들에 대한 은닉 실험 결과(PSNR, 단위: dB)

커버영상	패턴데이터 영상	LSB3	PVD	PVD+LSB	제안 알고리듬
Lena	2PD	36.67	41.12	37.27	51.14
	4PD	36.35	42.52	37.58	44.16
	8PD	36.68	42.36	37.71	37.94
Baboon	2PD	36.68	37.07	35.53	51.14
	4PD	36.34	38.68	36.62	44.16
	8PD	36.67	38.38	36.47	37.93
Splash	2PD	36.74	42.08	37.58	51.15
	4PD	36.41	43.67	37.51	44.16
	8PD	36.73	43.34	37.71	38.03
house	2PD	36.66	39.14	36.56	51.14
	4PD	36.41	40.04	37.18	44.19
	8PD	36.72	40.69	37.22	37.91

단 취약하지만 어느 정도 안전한 알고리듬에 대한 연구를 수행할 것이다.

참 고 문 헌

[1] N.F. Johnson and S. Jajodia, "Exploring Steganography : Seeing the Unseen," *Computer Practices*, Vol.31, No.2, pp. 26-34, 1998.

[2] R.J. Anderson and F.A.P. Petitcolas, "On the Limits of Steganography," *IEEE Journal on Selected Areas in Communications*, Vol.16, No.4, pp. 474-481, 1998.

[3] N. Johnson and S. Jajodia, "Steganalysis of Images Created using Current Steganography Software," *Second Information Hiding Workshop held in Portland, Oregon, USA, LNCS 1525*, pp. 273-289, 1998.

[4] S. Katzenbeisser and F.A.P. Peticolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House Books, London, 2000.

[5] E. Kawaguchi, H. Noda, and M. Niimi, "Image Data Based Steganograpy," *Information Processing Society of Japan(IPSJ MAGAZINE)*, Vol.44, No.3, pp. 236-241, 2003.

[6] J. Zollner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf, "Modeling the Security of Steganographic Systems," *Proceedings of 2nd Workshop on Information Hiding*, pp. 345-355, 1998.

[7] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," *Proceedings of International Symposiumon Circuits and Systems*, Vol.2, pp. 912-915, 2003.

[8] K. Nozaki, M. Maeda, K. Tsuda, and E. Kawaguchi, "A Model of Anonymous Covert Internet Mailing System using Steganograpy," *Proceedings of Pacific Rim Workshop on Digital Steganograpy (STEG 2002)*, pp. 7-10, 2002.

[9] H. Noda, J. Spaulding, M.N. Shirazi, M. Nimi, and E. Kawaguchi, "BPCS Steganograpy Combined with JPEG2000 Compreasion," *Proceedings of Pacific Rim Workshop on Digital Steganograpy (STEG 2002),* pp. 98-107, 2002.

[10] C. Cox, J. Killian, T. Leighton, and T. Shamoon, *Secure Spread Spectrum Communication for Multimedia, Technical Report,* N.E.C. Research Institute, 1995.

[11] M. Swanson, M. Kobayashi, and A. Tewfik, "Multimedia Data Embedding and Watermarking Technologies," *Proceedings of IEEE*, Vol.86, No.6, pp. 1064-1087, 1998.

[12] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," *Proceedings of IEEE*, Vol.86, No.6, pp. 1079-1107, 1998.

[13] G.W. Braudaway, K. A. Magerlein, and F. Mintzer, "Protecting Publicly-available Images with a Visible Image Watermark," *Proceedings of the SPIE International Conference on Electronic Imaging*, Vol.2659, pp. 126-133, 1996.

[14] T. Kalker, *Watermark Estimation Through Detector Observation*, Philips Research Eindhoven, Netherland, preprint, 1998.

[15] J.P.M.G. Linnartz, A.C.C. Kalker, G.F. Depovere, and R. Beuker, "A Reliability Model for Detection of Electronic Watermarks in Digital Images," *Proceedings of Benelux Symposiumon Communication Theory*, pp. 202-208, 1997.

[16] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Images, Audio and Video," *Proceedings of International Conference on Image Processing(ICIP96)*, pp. 243-246, 1996.

[17] B. Macq, "Lossless Multi-Resolution Transform for Image Authenticating Watermarking," *Proceedings of EUSIPCO*, 2000.

[18] C.K. Chan and L.M. Cheng. "Hiding Data in Images by Simple LSB Substitution," *Journal of Pattern Recognition*, Vol.37, No.3, pp.

469-474, 2004.

[19] R.Z. Wang, C.F. Lin, and J.C. Lin. “Image Hiding by Optimal LSB Substitution and Genetic Algorithm,” *Journal of Pattern Recognition*, Vol.34, No.3, pp. 671-683, 2001.

[20] D.C. Wu and W.H. Tsai. “A Steganographic Method for Images by Pixel-Value Differencing,” *Journal of Pattern Recognition Letters*, Vol.24, No.9-10, pp. 1613-1626, 2003.

[21] C.M. Wang, N.I. Wu, C.S. Tsai, and M.S. Hwang. “A High Quality Steganographic Method with Pixel-value Differencing and Modulus Function,” *Journal of Systems and Software*, Vol.81, No.1, pp. 150-158, 2008.

[22] H.C. Wu, N.I. Wu, C.S. Tsai, and M.S. Hwang. “Image Steganographic Scheme based on Pixel-value Differencing and LSB replacement Methods,” *Visual Image Signal Processing*, Vol.152, No.5, pp. 611-615, 2005.

[23] David A. Huffman, “A Method for the Construction of Minimum-Redundancy Codes,” *Proceedings of the I.R.E.*, pp. 1098-1101, 1951.

[24] Y.R Park and J.H Park, “A Study of Steganograhpy Using Cartoon Image,” *Journal of Korea Multimedia Society*, Vol.7, No.7, pp.913-921, 2004.

김 기 종

1994년 2월 경북대학교 전자공학과 공학사
1999년 2월 경북대학교 컴퓨터공학과 공학석사
2010년 2월 경북대학교 컴퓨터공학과 공학박사

1994년 3월～현재 영진전문대학 컴퓨터정보계열 교수
관심분야 : 멀티미디어 시스템, 데이터베이스 시스템, 분산 시스템, 암호학

신 상 호

2006년 8월 금오공과대학교 응용수학/컴퓨터공학 학사
2008년 8월 경북대학교 전자전기컴퓨터학부 공학석사
2009년 3월～현재 경북대학교 전자전기컴퓨터학부 박사과정
관심분야 : 고속암호 알고리듬, 양자암호, 클라우드 컴퓨팅 보안

유 기 영

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, 네트워크 보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜