Journal of Digital Contents Society Vol. 14 No. 2 Jun. 2013(pp. 199-206)
http://dx.doi.org/10.9728/dcs.2013.14.2.199

재압축 기술을 이용한 오디오 파일에서의 가역 정보은닉

황호영*, 김형중**

요 약

데이터를 한정된 양의 저장 공간 및 한정된 속도의 전송매체에서 다루기 위하여 여러 가지 데이터 압축 방식이 개발되었다. 그 중 가장 최근에 개발된 기술인 재압축 기술은 대부분의 다른 압축방식과는 달리 데이터의 정보 엔트로피와는 무관하게 추가적인 정보 삽입이 가능하다. 재압축 기술은 원래의 멀티미디어 데이터를 블럭 단위로 나누어 각 블록의 반전 여부에 따라 0 또는 1을 삽입하는 기술이다. 본 논문에서는 제안한 재압축 기술을 오디오 파일에 적용시켰고, 이를 통하여 가역 정보은닉 방식을 구현하였다.

키워드 : 재압축, 가역 정보은닉, 오디오

Reversible Watermarking for Audio Using Recompression Method

Ho Young Whang*, Hyoung Joong Kim**

Abstract

Various methods of data compression have been developed to handle data within limited storage capacity and limited transmission speed. Recompression technology, a technology most recent among them, is a technology that can embed data regardless of the information entropy of a data. Recompression technology separates original multimedia data in to blocks and embeds 0 or 1 according to whether each block is flipped or not. In this paper, this technology has been applied on audio files. And was able to implement reversible watermarking for audio files.

Keywords : Recompression, Reversible Watermarking, Audio

1. 서론

Shannon의 정보 이론에 따르면 파일을 압축하는 데에 있어서 그 한계는 데이터의 정보 엔트로피의 최대치라고 알려져 있다. 하지만 고려대학교 김형중 교수가 데이터의 의미 정보를 이용하여 데이터를 재압축 하는 기술을 최근에 개발해냈다[1].

이 기술은 어떠한 파일이라도 손실 없이 압축하는 기술이다. 이 기술은 데이터의 정보 엔트로피 값과는 별개로 정보를 삽입할 수 있으므로 정보 은닉에도 활용할 수 있다. 이 기술을 이용한 문서와 영상파일에의 가역 정보은닉은 이미 연구가 진행되고 있으며, 음성파일에도 본 논문을 기점으로 구현을 시작하였다[2-6].

재압축 기술을 사용함으로써 기존의 오디오 파일에서의 가역 정보은닉 연구와 연계하여 정보은닉 기법을 더욱 발전시킬 수 있다[7-10]. 가산 보간법과 에러확장을 이용한 가역 정보은닉 또는 선형 예측과 에러 확장을 이용한 가역 정보은닉 등의 오디오 파일의 가역 정보은닉에서 선행 연구가 이루어진 분야와 상호 충돌하지 않고 오히려 추가적인 응용이 가능하다. 재압축 기

※ 교신저자(Corresponding Author): Hyoung Joong Kim
접수일:2013년 05월 20일, 수정일:2013년 06월 10일
완료일:2013년 06월 19일
* 고려대학교 정보보호대학원
Tel: +82-2-3290-4251 , Fax: +82-2-3290-4256
email: jblitz@nate.com
** 고려대학교 정보보호대학원
Tel: +82-2-3290-4895 , Fax: +82-2-928-9109
email: khj-@korea.ac.kr
▣ 이 논문은 2012년도 대한민국 정부(교육과학기술부)의 재원으로 시행하는 한국연구재단 국제협력사업의 지원으로 수행 된 연구결과임.
(과제번호: 2009-00678)

술을 이용하면 기존의 연구 결과에 추가적인 정보 삽입이 가능하기 때문에 재압축 기술로 가역 정보은닉을 구현할 수도 있고 이중 암호화나 암호화 후 압축 등의 다양한 방향으로 사용될 수 있다. 활용도가 높은 연구 분야로서 기존의 연구들을 보완, 발전시켜 나아갈 수 있을 거라고 보인다.

또한, 재압축 기술은 무손실 압축 방식이기 때문에, 어떠한 파일 형식에도 적용할 수 있다는 장점이 있다. mp3나 wma와 같은 손실 압축 방식에도 원본 파일의 정보 손실 없이 재압축을 할 수 있고, flac이나 ogg와 같은 무손실 압축 방식에도 또한 원본 파일의 정보 손실 없이 재압축이 가능하다. 이와 같이 강력한 잠재력을 가지고 있는 재압축 기술을 오디오에 적용하는 연구의 초석으로 본 논문에서는 재압축 기술을 이용한 오디오 파일에서의 가역 정보은닉을 구현하였다.

2. 재압축 기술

2.1 작동 원리

재압축 기술의 압축 방식은 다음과 같다. 파일을 일정 크기의 블럭들로 나눈 후, 각 블럭마다 1비트의 데이터를 숨기는 것이다. 0을 숨길 경우에는 원본 그대로 저장하고, 1을 숨길 경우에는 블럭 안의 모든 비트를 뒤집어서 저장하는 것이다.

재압축 기술의 복원 방식은 다음과 같다. 압축되어있는 데이터를 복원하면서 복원시의 정보가 유의미한 정보일 경우 원본을 그대로 저장하고 0을 추출해내며, 무의미한 정보일 경우 블럭 안의 모든 비트를 뒤집어서 저장하고 1을 추출해내는 것이다.

2.2 암복호화 방식

<표 1> ‘mammal’이란 단어를 암호화한 후 다시 복호화하는 과정을 확인해보자. 우선, ‘mammal’이란 단어를 구성하는 알파벳들을 모두 나열하여 각 알파벳의 빈도가 큰 순서로 정렬한다. 그 후 각 알파벳을 허프만 부호화하여 원문을 비트열로 표현한다.

<표 1> 원문 메세지의 허프만 부호화

Original Message	mammal		
Alphabet	m	a	l
Frequency of Occurrence	3	2	1
Huffman Code	0	10	11
Bitstream	010001011		

<Table 1> Huffman Code of Original Message

<표 2>에서 원문의 비트열과 워터마크를 XOR 연산을 하여 암호문 비트열을 생성한다. 예제에서는 워터마크를 1로 정하고 블럭은 전체 비트열을 한 블럭으로 설정하였다.

<표 2> 원문 비트열에 워터마크 삽입

Original Bitstream	010001011
Watermark	1
Encrypted Bitstream	101110100

<Table 2> Embedding Watermark in Original Bitstream

이제 암호문에서 원문과 워터마크를 복호화하는 과정을 확인해보자. 주어진 암호문의 비트열을 주어진 블럭 사이즈에 따라 나누고, 각 블럭의 비트열들을 주어진 허프만 부호록의 부호 워드에 따라 변환한다. <표 3>에서는 블럭 사이즈가 전체 비트열의 길이이므로 전체 비트열을 허프만 부호 워드를 이용하여 변환한다. 허프만 부호 워드로 전체 비트열이 완벽히 변환되지 않는 경우 사전을 검색할 필요도 없이 반전되었다고 볼 수 있다. 변환한 문자열을 사전에서 검색하여 사전에 존재하는 단어인지를 확인한 후, 찾으면 정확히

복호화 되었다고 보고 워터마크는 0으로 추출할 수 있다. 만약 문자열이 사전에 존재하지 않는다면, 블럭 안의 비트열을 1과 XOR 연산을 하여 반전시킨 후 다시 허프만 부호 워드를 이용하여 변환한 문자열로 사전에서 검색한다. 이번에는 사전에서 문자열이 검색될 것이며, 정확히 복호화 되었다고 보고 워터마크는 1로 추출할 수 있다.

<표 3> 암호문 비트열의 복호화

Watermark	0	1
Bitstream	101110100	010001011
Convertion to Alphabet	alaam	mammal
Meaning (Dictionary)	meaningless	meaningful

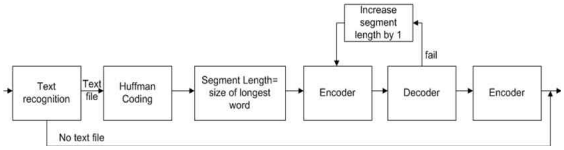
<Table 3> Decrytion of Encrypted Bitstream

2.3 적용 분야

현재 재압축 기술을 이용하여 연구가 진행중인 분야에는 문서와 영상 분야가 있다. 데이터의 의미 정보를 이용해서 재압축을 구현하기 때문에 데이터의 유의미성을 손쉽게 파악하기 쉬운 텍스트와 이미지 분야에서 먼저 진행되었다.

텍스트 재압축은 (그림 1)과 같은 과정으로 진행된다. 우선 텍스트를 인지하는 단계를 거쳐서 텍스트 파일이 아닐 경우 종료한다. 만약 텍스트 파일일 경우 허프만 부호화를 하여 블럭의 길이를 정해주고 암호화를 한다. 암호화된 텍스트가 성공적으로 복호화되지 못하면 블럭의 길이를 증가시켜서 성공할 때까지 이 과정을 반복한다. 성공적으로 복호화가 가능한 블럭의 길이를 찾으면, 그 길이의 블럭으로 암호화한다.

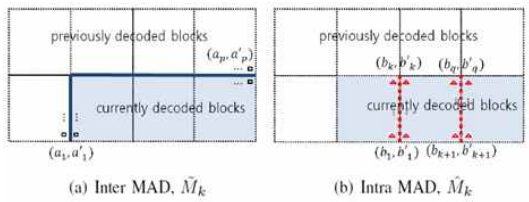
(그림 1) 텍스트 재압축의 흐름도



(Figure 1) Flowchart of Text Recompression

이미지 재압축도 오디오 재압축과 함께 텍스트 재압축 기술과 유사한 과정으로 진행된다. jpeg 형식과 같은 압축된 이미지 파일에 대해서도 암복호화를 구현하는 연구가 진행중에 있다. 이미지 재압축에서는 (그림 2)와 같이 MAD(Mean Absolute Difference)를 이용하여 인접한 블럭이 올바르게 복호화 되었는지의 여부를 판별하는 기법을 이용한다. 이는 서로 인접한 픽셀들 간의 상관관계를 이용하는 방법으로, 블럭과 블럭의 경계에 위치한 픽셀들의 값에는 큰 차이가 있을 가능성이 낮고 비슷한 값일 가능성이 높은 원리를 이용한 방법이다.

(그림 2) 이미지 재압축에서 사용하는 MAD기법



(a) Inter MAD, $\tilde{M}_k$ (b) Intra MAD, $\tilde{M}_k$

(Figure 2) Examples of MAD Computation Used in Image Recompression

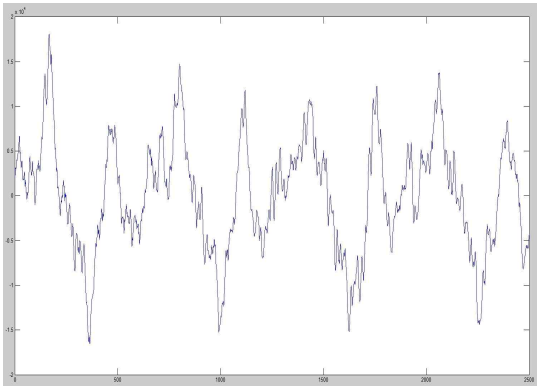
3. 오디오 파일의 특성

본 논문에서 재압축 기술로 오디오 가역 정보은닉을 구현하기 위하여 오디오 파일을 살펴보았다. 오디오 신호는 다음과 같은 분포양상을 보인다. 여러 개의 정현파가 복합된 신호로서, 0을 중심으로 음량이 양수값과 음수값이 교차하며 나타난다.

본 논문에서는 웹사이트[11-12]에서 무료로 제공하는 flac 파일을 wav 파일로 변환하여 실험을 진행하였다. 음원의 이름은 'TV Torso - Clear Lake Strangler' 과 '05-(minus)-everything' 이다.

(그림 3)은 'TV Torso - Clear Lake Strangler'의 left channel의 4500001번째 샘플부터 4502500번째 샘플까지의 파형이다. 전체 오디오의 일부분을 확대하여 그 성질이 조금 더 확실하게 드러남을 알 수 있다.

(그림 3) 실험 음원의 일부 파형



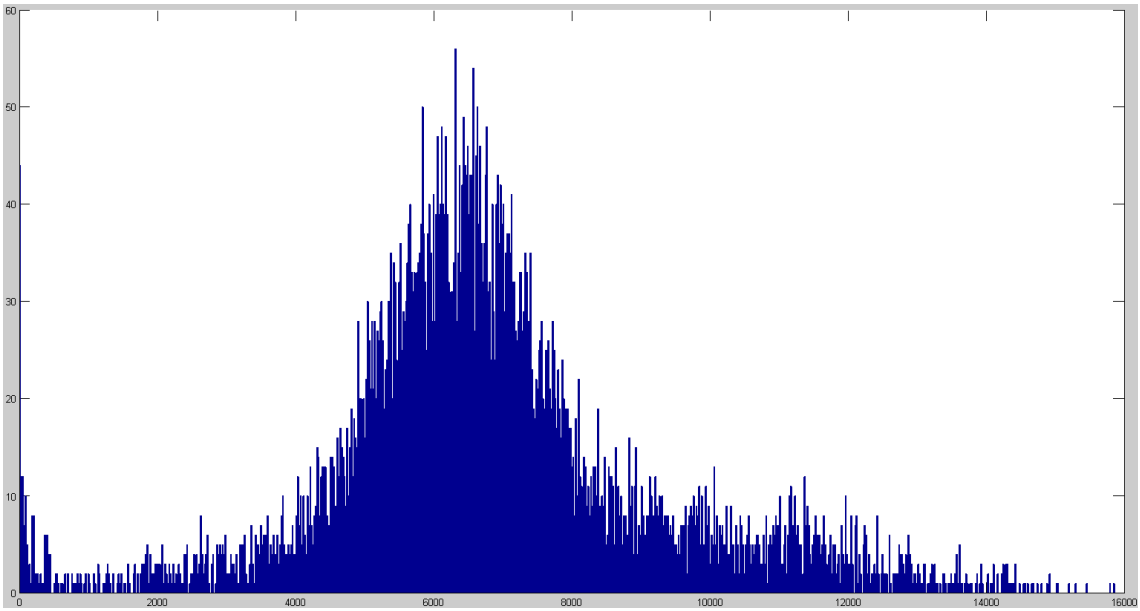
(Figure 3) Partial Waveform of Test Audio

위에서 볼 수 있듯이, 오디오 신호는 정현파들의 복합 신호로서 대부분의 샘플 값들이 0에 근접하게 분포한다는 특징이 있다. 그러므로 일정 블럭 안에서의 원래 음원의 샘플 값들의 평균은 해당 블록의 모든 비트를 반전시켰을 때의 평균보다 작은 성질을 이용하여 재압축 기술을 적용시킬 수 있었다.

다음 (그림 4)와 (그림 5)는 실험 음원을 1100 샘플 당 1블럭으로 나누어 실험한 그림이다.

(그림 4)는 원래 음원이다.

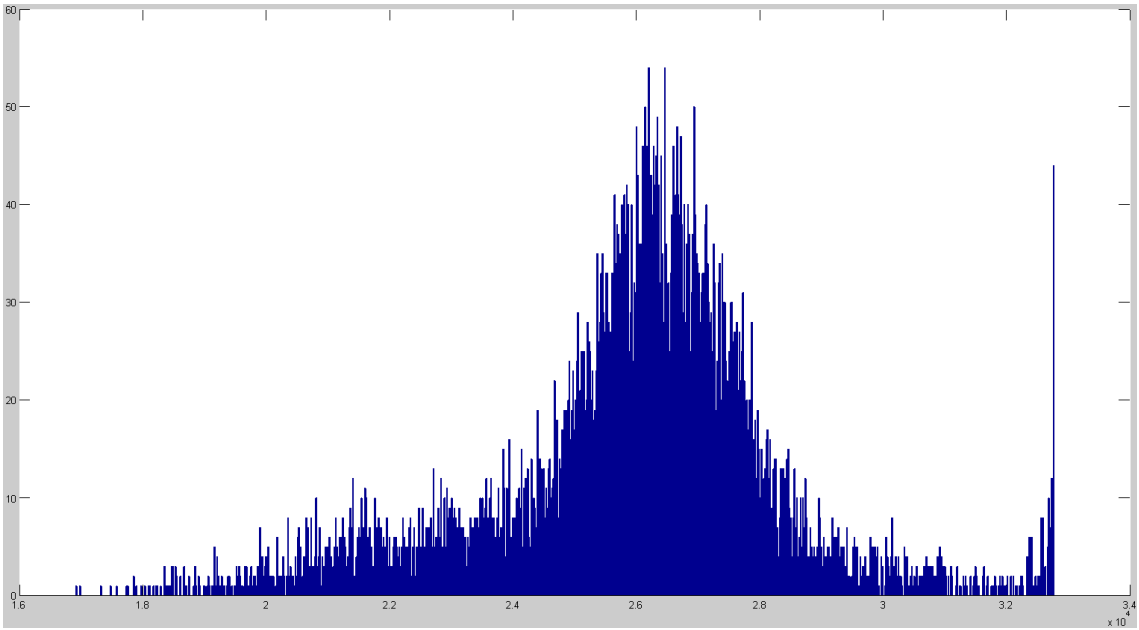
(그림 4) 실험 음원의 블럭 별 평균값



(Figure 4) Mean Values of Blocks of Test Audio

(그림 5)는 비트를 모두 반전시킨 음원이다.

(그림 5) 실험 음원의 반전 후 블럭 별 평균값



(Figure 5) Mean Values of Blocks of Test Audio After Flipping

이와 같이 원래의 음원과 반전 후의 음원의 블럭 별 평균값들이 일정 값을 기준으로 완전히 구분된다. 그러므로 이러한 성질을 이용하여 재압축 기술을 구현할 수 있고, 재압축 기술을 이용한 정보 은닉과 복원이 항상 가능하다.

각 샘플들을 x_k로 놓고, 블럭의 크기를 n이라고 했을 때 블럭 내 샘플들의 평균값은 식 (1)과 같이 구할 수 있다.

$$m = \frac{\sum_{k=1}^{n} x_k}{n} \tag{1}$$

주어진 블럭의 m과 블럭의 비트를 반전시켜 구한 m'을 비교하여 둘 중에 더 작은 값을 취하여 복호화하였다. 이를 바탕으로 다음의 실험을 진행하였다.

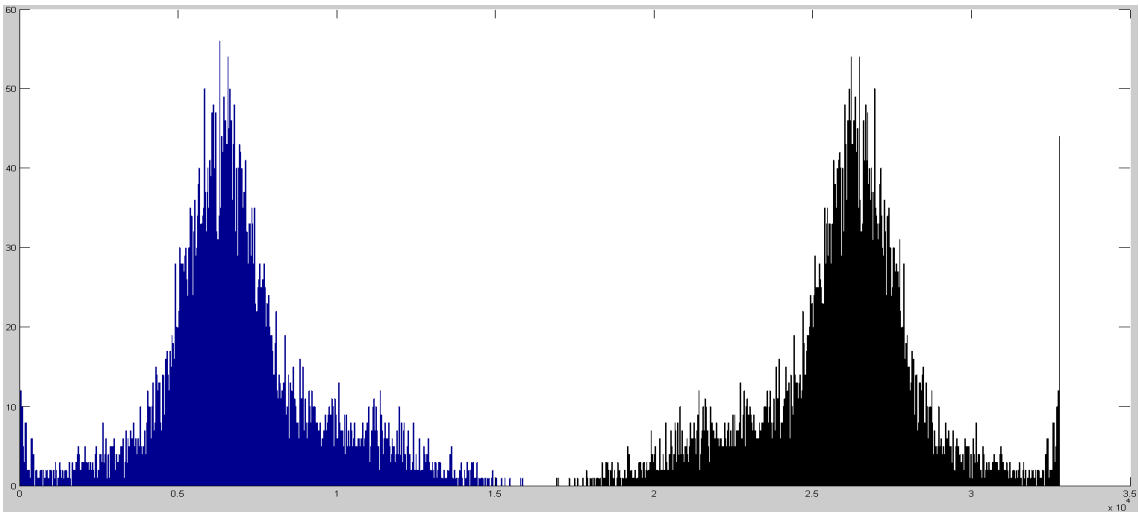
4. 실 험

다음의 그림에서 보이는 분포도는 'TV Torso - Clear Lake Strangler'의 원래 음원의 블럭 별 평균값과 반전 음원의 블록 별 평균값의 분포도와, '05-(minus)-everything'의 원래 음원의 블럭 별 평균값과 반전 음원의 블록 별 평균값의 분포도이다. (그림 6)에서는 'TV Torso - Clear Lake Strangler'의 원래 음원의 블럭 별 평균값과 반전 음원의 블록 별 평균값의 분포도를 같이 그려보았다. (그림 7)에서는 '05-(minus)-everything'의 원래 음원의 블럭 별 평균값과 반전 음원의 블록 별 평균값의 분포도를 같이 그려보았다. 각 음악에 대해서 서로 다른 최소 블록 당 샘플 수를 구할 수 있었으며, 블록 당 샘플 수를 결정한 방식은 매우 큰 크기의 블럭에서부터 분포도가 서로 겹치지 않는 최소 크기까지 점차 줄여나가는 방식으로 구하였다. 블록의 크기는 음악의 진폭에 따라 결정되는 것으로 보인다. 구체적으로, 음악의 진폭과 블록 당 샘플 수는 서로 반비례의 관계를 보인다. 즉, 본 논문에서 사용한 암복호화 방식으로는 재압축 기술을 사용할 때에, 시끄러운 음악일수록 숨길 수 있는 정보의 양이 적어지고, 조

용한 음악일수록 숨길 수 있는 정보의 양이 커지는 현상을 보였다.

(그림 6)에서 사용된 음원의 블록 당 샘플 수는 1100samples/block이다.

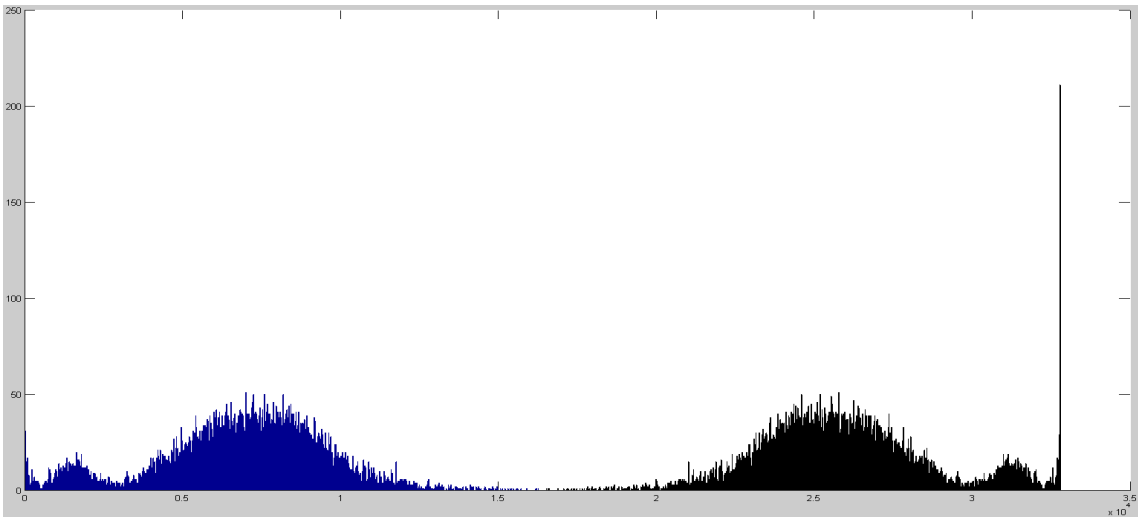
(그림 6) 'TV Torso - Clear Lake Strangler'의 원래 음원과 반전 음원의 평균값 분포도



(Figure 6) Histogram of Mean Values of Blocks in Original Audio and Flipped Audio of 'TV Torso - Clear Lake Strangler'

(그림 7)에서 사용된 음원의 블록 당 샘플 수는 800samples/block이다.

(그림 7) '05-(minus)-everything'의 원래 음원과 반전 음원의 평균값 분포도



(Figure 7) Histogram of Mean Values of Blocks in Original Audio and Flipped Audio of '05-(minus)-everything'

5. 결 론

본 논문에서 이용한 재압축 기술은 컨텐츠의 의미 정보를 이용한 추가적인 정보 삽입이 가능하다. 본 논문에서는 이 기법을 오디오에 적용시켜 기존 오디오에 정보은닉을 구현하였다. 재압축 기술이 오디오 파일에서 정보은닉을 구현하는 데에 쓰일 수 있음을 보였고, 그것을 증명하였다.

향후 과제로 flac, mp3등 다양한 포맷의 오디오 파일에 관한 연구를 진행하고자 한다.

References

[1] S. Kang, H. Kim, and X. Qu, “Compressing JPEG Compressed Image Using Reversible Data Hiding Technique,” IEEE Transactions on Image Processing, vol. 11, no. 4, December 2013

[2] Si-Hwan Jang, Yong Soo Choi, Hyoung Joong Kim, “Improved Visual Cryptography Using Cover Images,” Journal of Korea Digital Contents Society, vol. 13, no. 4, pp. 531-538, Dec. 2012

[3] M. Naor and A. Shamir, "Visual cryptography," Lecture Notes in Computer Science, vol. 950, pp. 1-12, 1995.

[4] Mi-Ra Kim, Ji-Hwan Park, Sang-Woo Park, and Kwang-Jo Kim, "Secret Sharing Scheme Using Visual Cryptography", Journal of The Korea Institute of Information Security & Cryptology, vol. 7, no. 4, pp. 37-50, December 1997

[5] Cheonshik Kim, Eun-Jun Yoon, You-Sik Hong, and Hyoung Joong Kim, "Secret Sharing Scheme using Gray Code based on Steganography", The Institute of Electronics Engineers of Korea - Computer and Information, vol. 46, no. 1, pp. 96-102, January 2009

[6] Hye-Joo Lee and Ji-Hwan Park, "An Extension of Visual Cryptography and Its Application into Digital Watermark", Journal of Korea Multimedia Society, vol. 1, no. 1, pp. 80-89, 1998

[7] J.J. Garcia-Hernandez and L. Delgado-Guillen, “Using Additive Interpolation-Error Expansion for Reversible Digital Watermarking in Audio Signals,” IEEE 55th International Midwest Symposium on Circuits and Systems, no. 6292182, pp. 964-967, August 2012

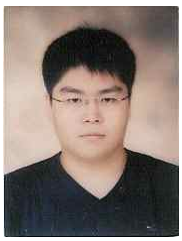
[8] A. Nishimura, “Controlling Quality and Payload in Reversible Data Hiding Based on Modified Error Expansion for Segmental Audio Waveforms,” 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, no. 6274571, pp. 110-113, July 2012

[9] M. Unoki and R. Miyauchi, "Reversible Watermarking for Digital Audio Based on Cochlear Delay Characteristics," 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, no. 6079591, pp. 314-317, October 2011.

[10] A. Nishimura, “Reversible Audio Data Hiding Using Linear Prediction and Error Expansion,” 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, no.6079592, pp. 318-321, October 2011

[11] “TV Torso,” http://tvtorso.bandcamp.com/track/clear-lake-strangler

[12] “LossLess DDL”, http://losslessddl.com/minus-structure-of-simplicity-cd-flac-2001-forsaken/



황 호 영

2007년 : 고려대학교 전기전자전파공학부 (공학학사)

2011년~현 재 : 고려대학교 정보보호대학원 (석사과정)

관심분야 : 정보보호, 디지털 신호처리 등

김 형 중

1978년 : 서울대학교
전기공학과 (공학사)
1986년 : 서울대학교
제어계측공학과 (공학석사)
1989년 : 서울대학교
제어계측공학과 (공학박사)

1990년～2006년: 강원대학교 교수
1992년～1993년: USC Univ. 방문교수
2007년～현 재: 고려대학교 정보보호대학원 교수
관심분야 : Watermarking, Parallel Computing, Image Hashing, Data Compression, Steganography