논문 20-45-06-18 The Journal of Korean Institute of Communications and Information Sciences '20-06 Vol.45 No.06
https://doi.org/10.7840/kics.2020.45.6.1083

디지털 워터마킹에서 데이터 보호를 위한 극부호의 효율성 연구

이 승 호•, 신 수 용°

Efficiency of Polar Codes in Providing Error Protection in Digital Watermarking

Seung Ho Lee•, Soo Young Shin°

요 약

디지털 워터마킹은 저작권 보호를 위해 주로 사용된다. 원본 데이터에 데이터를 삽입하는 방식으로 그 대표적인 방법으로 스테가노그래피가 있다. 이 기술은 사람이 인지하기 어려울 정도로만 원본 데이터를 변형하여 추가 데이터를 삽입하는 방식이다. 이 기술은 워터마킹 데이터의 은닉이 핵심이다. 하지만 데이터는 압축이나 노이즈에 쉽게 훼손 될 수 있으며, 다른 사람에게 발견되어 추출되는 경우도 발생 할 수 있다. 본 논문에서는 이를 대비해 오류 정정 코드를 사용하여 데이터를 강화하고, 암호화 기법으로 보안성을 가지게 된다. 다양한 오류 정정 코드 중 극부호가 오류 정정 외에도 추가적인 보안성을 가질 수 있음을 확인하고 암호화와 같은 부호화 과정을 줄이기 위한 노력을 하였다. 극부호에서 사용되는 고정 비트는 송신자와 수신자가 사전에 약속이 되어있어야 하는 비트로 잘못된 값을 사용 할 경우 정보 비트에도 영향을 줄 수 있다. 128개의 비트로 된 정보 비트를 1/2의 코드율로 극부호를 사용한 부호화를 하여 각각의 고정 비트를 잘 못 입력하였을 때, 정보 비트의 오류율을 실험으로 확인하였다. 최소 12.5%의 오류를 보였으며, 최대 53.125%까지 오류율을 보였다. 이는 극부호를 사용 할 경우, 추가적인 암호화 과정을 대신 할 수 있다는 것을 보여준다.

Key Words : Digital watermarking, Steganography, Polar codes, Frozen bits

ABSTRACT

Digital watermarking is mainly used for copyright protection. Steganography is the representative method of embedding data into the original data. This technique is a way of embedding additional data by modifying the original data only to the extent that it is difficult for a person to perceive. This technique is the key to hiding watermarking data. However, data can be easily damaged by compression or noise, and can be extracted by others. For this, data is strengthened by using error correction codes, and secured with encryption technique. In this paper, it is confirmed that the polar codes has additional security as well as error correction. And we made efforts to reduce the encoding process such as encryption. The frozen bits used in the polar codes are bits that the sender and the receiver have to make an appointment in advance and can affect the information bits. To test the information bits error rate, 128 information bits are coded at a code rate 1/2 using a polar codes. And each frozen bits make a situation where an error occurred. The error rate of the information bit is at least 12.5% and up to 53.125%. This shows it can replace the encryption process when the polar codes are used.

※ "이 논문은 2020년도 정부(교육과학기술부)의 재원으로 한국연구재단의 대학중점연구소 지원사업으로 수행된 연구임" (2018R1A6A1A03024003)

• First Author : Kumoh National Institute of Technology IT Convergence Engineering, orangetreeo@kumoh.ac.kr, 학생(석사) 학생회원
° Corresponding Author : Kumoh National Institute of Technology Electronic Engineering professor, wdragon@kumoh.ac.kr, 부교수, 종신회원

논문번호 : 201909-205-C-RN, Received September 24, 2019; Revised November 2, 2019; Accepted November 2, 2019

Ⅰ. 서 론

최근 멀티미디어 기술의 발달로 디지털 자료가 점점 더 늘어나면서 자료의 생산 및 유통에 대한 수요 또한 증가하고 있다. 이에 사람들은 개인의 지식 재산이 미래 산업의 중요한 요소임을 느끼고 디지털 자료를 보호하는데 많은 관심을 보이고 있다. 최근 설문에서 불법 복제물 사용을 피하게 되는 요인으로 저작권 보호의식이 높아짐과 동시에 경로가 힘들어지거나 소송의 문제가 발생 할 수 있기 때문이라고 나타났다. 이는 저작권 보호에 대한 지속적인 연구가 미래 아이디어 자원을 지키는데 큰 역할을 하고 있다는 것이다.

저작권 보호를 위한 다양한 기술 연구 중에는 디지털 워터마크 기술이 있다. 이는 디지털 오디오, 이미지 및 비디오와 같은 멀티미디어에 다른 추가 정보를 삽입하는 기술이다. 추가 정보의 삽입은 데이터 전송을 더 효율적으로 해줄 뿐만 아니라 제작자의 정보를 삽입하여 멀티미디어 자료에 저작권이 생기게 한다.

디지털 워터마크 기술은 데이터를 더 견고하게 만들거나 사람들이 쉽게 알기 어렵게 만드는 것과 같이 다양한 방향으로 연구되고 있다. 그 대표적인 방향으로 스테가노그래피(steganography)가 있다[1-3].

스테가노그래피(steganography)는 데이터를 숨기는 방식이다. 정보를 은닉하여 다른 형태로 위장시켜 다른 사람이 워터마킹 데이터의 존재조차 알기 힘들게 만든다. 이는 중요한 암호나 비밀문서를 주고받을 때 효과적이다.

멀티미디어 데이터에 데이터를 은닉하는 방식은 기본적으로 공간 도메인(Spatial Domain)과 주파수 도메인(Transform Domain)으로 나뉜다. 공간 도메인은 RGB와 같이 색공간에서 데이터를 수정하여 은닉한다. 주파수 도메인의 경우 다양한 변환 기술을 사용하여 다른 영역에서 데이터를 숨기게 된다.

공간 도메인의 대표적인 방법은 LSB(Least Significant Bit)를 변형하는 것이다. 이는 데이터의 최소 비트 값을 변형시켜 데이터를 삽입하게 된다. 하지만 이 방법은 간단한 신호 처리 기법에도 워터마킹 데이터가 손상될 수 있기 때문에 효율적이지 않다. 특히 압축이나 간단한 변환에도 약하기 때문에 주파수 도메인 방식과 함께 사용되는 것이 일반적이다.

주파수 도메인 방식의 경우 원본 데이터를 변환하여 다른 영역에서 워터마킹 데이터를 삽입하는 방식이다. 흔히 Fourier Transform을 활용하고, Discrete Cosine Transform(DCT)나 Wavelet Transform과 같이 다양한 방식이 있다. 영상이나 이미지의 압축의 경우 위와 같은 방식을 기본적으로 사용하기 때문에 공간 도메인보다 간단한 신호 처리에서 더 강한 모습을 보인다.

다양한 방법으로 데이터를 은닉 할 수 있지만, 여전히 신호 처리 기법과 노이즈 환경에서 취약하다. 따라서 오류 정정 코드로 부호화 하는 방식이 함께 연구되어왔다. 부호화를 통해 오류가 발생하더라도 복구가 가능해지며, 워터마킹 데이터는 더 강하게 된다[4].

이러한 방식은 데이터를 강화하는 방법이지만 만약 은닉에 실패하고 데이터의 존재가 드러나면 숨겨진 메시지는 다른 사람들에게 공개된다. 이를 방지하기 위해 오류 정정 부호와 함께 암호화가 사용된다. 워터마킹 데이터의 존재를 알고 추출한다 하더라도 대칭키를 가지고 있지 않을 경우 비밀 메시지의 내용을 알 수 없게 하는 것이다[5].

하지만 데이터를 오류 정정 코드와 암호화로 하는 것은 스테가노그래피 사용에 복잡도를 커지게 만든다. 수신자는 워터마킹 추출 방법과 오류 정정 코드와 암호화의 복호화 방법을 알고 있어야한다. 수신자 측 복잡도는 스테가노그래피의 효율성을 떨어뜨리게 된다.

따라서 본 논문은 오류 정정 코드의 방법 중 하나인 극부호를 사용하여 추가적으로 암호화를 사용하지 않아도 보안성을 가질 수 있는 방법을 연구하였다[6,7].

본 논문은 스테가노그래피 방식의 디지털 워터마킹 기술을 활용한다. 주파수 도메인을 활용하여 워터마킹 데이터를 은닉한다. 사용 된 기법은 2장에서 자세히 설명하며 이어 은닉한 데이터를 강화하기 위해 사용된 극부호에 대해 설명한다. 3장에서는 스테가노그래피 기법의 디지털 워터마킹 기술에 극부호를 활용하여 보안을 늘리는 실험하며 4장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1 스테가노그래피

스테가노그래피는 원본 데이터에서 원하는 데이터를 숨기는 정보 은폐 기법 중 하나이다. 이것은 종종 암호화와 비교된다. 정보 암호화는 암호화키를 사용하여 데이터를 변환한다. 암호화키가 없으면 원래 데이터를 읽을 수 없게 된다. 즉, 제 3자는 암호화 된 정보의 존재를 이미 알고 있다고 가정한다. 이것이 은닉의 목적을 가진 스테가노그래피와 가장 다른 부분이다.

스테가노그래피는 다른 사람들로부터 정보의 "존재"를 숨기는 것이 특징이다. 원본의 손상을 최소화하고 사람들이 알아차리기 힘들게 만든다. 데이터를 숨기는 특징은 영상이나 이미지와 같은 멀티미디어

데이터에 저작권 정보를 담은 워터마킹 데이터를 삽입하여 불법 복제를 막을 수 있게 한다. 또한 원본에 훼손이 적다는 점에서 원본이 필요 이상의 품질을 가지고 있다면 추가적인 데이터 전송도 할 수 있게 만든다. 하지만 이는 다양한 바이러스나 악의적인 코드를 숨기는데도 종종 악용된다.

스테가노그래피에서 데이터를 삽입하는데 많은 주의가 필요하다. 데이터를 섬세하게 숨기는 만큼 외부 자극에도 쉽게 훼손 될 수 있다. 따라서 삽입되는 워터마킹 데이터를 강하게 만드는 것이 필요하다. 특히 압축이나 노이즈와 같은 경우는 데이터의 존재를 모른다 하더라도 충분히 발생 할 수 있는 상황이다. 따라서 데이터에 변형을 하더라도 외부 자극에 충분히 강하게 만들어야 한다. 또한 워터마킹 데이터가 지나치게 커질 경우, 삽입하는 과정에서 원본 데이터에 큰 영향을 미칠 수 있다. 이는 데이터를 숨기는 목적에 맞지 않은 결과로 이어지게 된다. 하지만 워터마킹 데이터를 강화시키려는 노력에 자연스레 데이터의 양이 커질 수 있기 때문에 은닉과 강화를 적절히 염두에 두어야한다.

그림 1은 워터마킹 알고리즘을 나타낸 것이다. 이미지 데이터에 워터마킹 데이터를 삽입하는 방법으로 주파수 도메인을 활용한다. 원본 이미지 데이터를 fast Fourier Transform을 활용하여 주파수 도메인으로 변환하여 크기와 위상 성분을 분리하게 된다. 이때 사용되는 Fourier Transform 식은 다음과 같다.

$$F(u,v) = \frac{1}{WH}\sum_{x=0}^{W-1}\sum_{y=0}^{H-1} f(x,y)e^{-j2\pi(ux/W+vy/H)} \quad (1)$$

수식 (1)에서 x와 y는 원본 이미지의 x축과 y축 값이 되고, u와 v는 각각 주파수 도메인에서 크기와 위상이 된다. W와 H는 원본 이미지의 크기를 나타낸다.

구해진 주파수도메인의 값에서 저주파 성분을 선택하여 그곳에 워터마킹 데이터를 삽입한다. 만일 고주파 성분을 사용하게 될 경우 Blur가 심하게 발생하게 된다. 따라서 비교적 덜 민감한 저주파 영역에 데이터를 삽입하게 된다. 데이터의 삽입은 주파수의 크기 성분에서 이루어진다. 정해진 규칙에 따라 크기 성분에 값을 더하고 빼는 방식을 사용한다. 연산이 끝난 후 위상 성분과 다시 결합한다. 주파수 도메인으로 변형한 방식을 역으로 하여 결과 이미지를 만들게 된다.

워터마킹 데이터는 삽입되기 전 오류 정정 코드를 사용하여 오류에 더 강하게 만든다. 이때 Convolutional 부호나 Turbo 부호나 극부호 등 다양하게 사용 될 수 있다. 그리고 데이터의 존재가 드러나더라도 워터마킹 데이터의 정보를 알 수 없도록 암호화 과정을 거친다.

Algorithm 1 Embedding Algorithm

1: Read the cover image in the original RGB color space.
2: Apply Fast Fourier Transform (FFT) to convert image components to the frequency domain.
3: We separate the magnitude and phase components of the transformed image.
4: Select the Low frequency components only.
5: We perform the embedding in the magnitude components.
6: A decision rule is applied to embed the watermark into the image.
7: The resultant image is then combined with its phase components from STEP 6, so that the image can have its original form.
8: In the next step, we perform IFFT to bring the transformed watermarked image back to RGB.

Algorithm 2 Watermark Preparation Algorithm

1: Read the watermark.
2: Convert the watermark into RAW bits (0s and 1s).
3: Add the error protection e.g. polar coding, convolutional coding etc.
4: The output of the convolutional coder is then encrypted using any encryption standard.

Algorithm 3 Extraction Algorithm

1: Read the watermarked image.
2: Convert the RGB components into frequency domain by applying fast Fourier transform (FFT).
3: The magnitude and phase components are separated and then the magnitude components are used.
4: Using the same decision rule. 0s and 1s are extracted using the decision rule.
5: Inverse of encryption algorithm is applied on the extracted bits and then error correction decoding is applied using the same code rate as the embedding process.

그림 1. 스테가노그래피를 이용한 디지털 워터마킹 알고리즘
Fig. 1. Steganography Digital Watermarking Algorithm

결과 이미지에서 워터마킹 데이터를 추출하는 과정은 삽입의 과정과 같은 방법으로 진행 된다. 주파수 도메인의 크기와 위상 정보를 얻게 되면 정해진 규칙에 따라 워터마킹 데이터를 추출한다. 추출된 데이터는 암호화 기법과 오류 정정 코드를 복호화 하여 워터마킹 데이터를 얻게 된다.

그림 2는 워터마킹 된 이미지를 보여준다. 위에서부터 원본 이미지, 주파수 도메인으로 변환한 이미지, 워터마킹 된 이미지이다. 스테가노그래피의 가장 큰 장점은 원본 이미지와 워터마킹 된 이미지의 차이를 사람이 알아차리기 힘들다는 점이다.

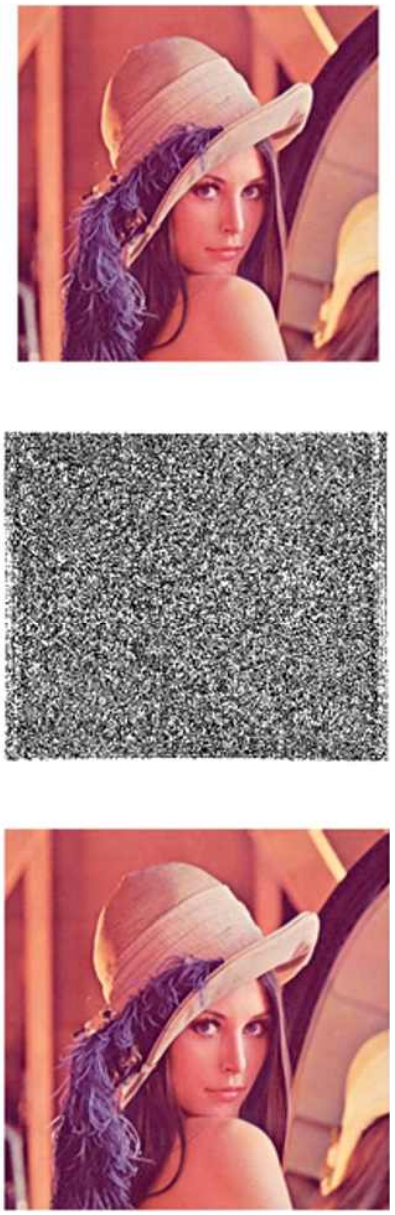

그림 2. 스테가노그래피 알고리즘의 결과. 위에서 부터 원본 이미지, 주파수 도메인으로 변환, 워터마킹 된 이미지
Fig. 2. The result of the steganographic algorithm.. Cover image, Image converted to frequency domain, Watermarked image

2.2 극부호

극부호는 2008년 터키의 Arikan이 제안하였다. 이 부호는 일반적인 채널에서 좋은 성능을 보이면서 낮은 복잡도를 가지고 있다. 극부호는 채널의 결합과 분리로 발생하는 채널 양극화를 이용하여 극도로 좋은 채널과 극도로 나쁜 채널을 생성한다. 이를 통해 좋은 오류 정정 능력을 가지게 된다[8-9].

그림 3은 극부호의 전송 과정을 블록 다이어그램으로 표현하였다. 입력 비트의 수는 왼쪽의 K로 표현된다. 그리고 N-K개의 고정 비트를 추가하여 최종적으로 N개의 비트가 전송된다. N개의 비트는 부호화하여 N개의 채널을 통해 전송된다.

채널의 양극화 과정은 다음과 같다. 전송하고 싶은 정보 비트를 $u_1, u_2, \ldots, u_N$이라고 가정한다. 주어진 채널 W를 N번 생성하여 가상의 채널 W_N을 만든다. W_N은 두 개의 $W_{N/2}$채널의 결합으로 이루어진다.

그림 4는 W_2일 때를 보여준다. 입력 비트 u_1과 u_2가 채널 W_2 통과하면서 출력 비트 y_1과 y_2를 얻을 수 있다. 이 때 천이 확률은 다음과 같이 구할 수 있다.

$$W_2(y_1,y_2|u1,u_2) = W(y_1|u_1 \oplus u_2)\, W(y_2|u_2) \quad (2)$$

이를 확장하여 $W_{N/2}$으로부터 W_N을 구할 수 있게 된다. 이렇게 결합된 채널 W_N을 다시 N개의 이진 입력 채널 $W_N^{(i)}: X \rightarrow Y^N \times X^{i-1}, 1 \le i \le N$으로 분리한다.

$$W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) = \sum_{u_{i+1}^N} \frac{1}{2^{N-1}} W_N(y_1^N|u_1^N) \quad (3)$$

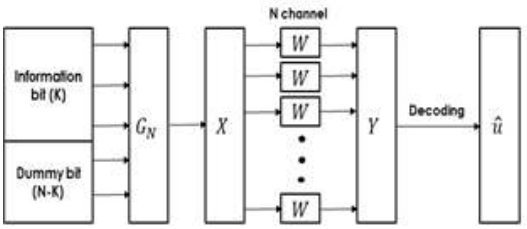

그림 3. 극부호를 사용한 데이터 전송 블록 다이어그램
Fig. 3. Block diagram of data transmission using polar coding

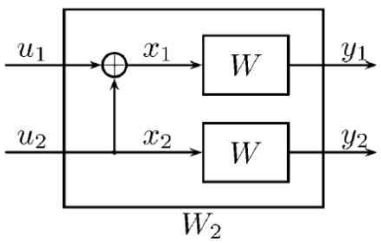

그림 4. W_2 일 때 채널 결합
Fig. 4. Channel combination when W_2

이렇게 분리된 N개의 채널은 N의 값에 따라 채널 용량이 1과 0으로 양극화 되게 된다. 이때 채널 용량이 1에 가까운 채널에 정보 비트를 보내고, 채널 용량이 0인 채널에 고정 비트를 보내게 된다.

여기서 사용되는 고정 비트는 송신자와 수신자가 서로 약속으로 정해둔 비트를 말한다. 전송 전 서로는 사용 되는 고정 비트의 값을 알고 있게 된다. 이 경우 채널 용량이 낮은 채널로 전송하게 되더라도 고정 비트 값을 정확히 알 수 있게 된다. 수신단에서는 고정 비트 값을 이용하여 정보 비트의 값을 알 수 있게 된다.

그림 4의 경우를 볼 때, u_2는 u_1와 비교하였을 때 좋은 조건에서 전송되는 것을 볼 수 있다. 이때, u_1은 고정 비트가 되며 수신단은 u_1의 값을 정확히 알고 있게 된다. u_1값의 정보를 활용하여 u_2는 더 좋은 조건에서 전송이 된다.

고정 비트의 핵심은 상호간의 약속이 되어있는 것이다. 이진 대칭 채널의 경우 0과 1의 천이 확률이 같다. 따라서 이 경우에 수신단에서 고정 비트 값만 알고 있다면 그 값이 0 혹은 1 어떤 값이 되어도 영향이 없게 된다. 이를 활용하여 극부호는 오류 정정과 동시에 보안성도 가지게 된다. 수신단에서 고정 비트의 값을 알고 있다면 정보 비트 전송에 큰 도움이 되지만, 값을 정확히 알고 있지 않다면 오히려 오류가 발생하게 된다.

2.3 극부호를 활용한 스테가노그래피

본 논문에서는 워터마킹 데이터를 은닉하여 숨기는 스테가노그래피 기법에 극부호를 활용하여 더 효율적 알고리즘을 보인다. 고정 비트를 활용하여 보안에 더 효과적이면서 다른 오류 정정 코드와 비교하였을 때 성능 또한 우수함을 보인다.

그림 5는 스테가노그래피 환경에서 극부호의 성능을 다른 오류 정정 코드와 비교한 것이다. 32비트의 정보 데이터를 1/3의 코드율로 비교하였다. Message error rate는 반복 실험에서 정보 비트에 오류가 난 경우를 나타내며 사용된 노이즈 환경은 Speckle 노이즈이다. 극부호의 경우 다른 오류 정정 코드에 비해 노이즈에 대한 오류 정정 성능이 우수함을 보여주었다.

극부호는 워터마킹 데이터가 원본 이미지의 주파수 도메인 크기 성분에 삽입되기 전 부호화 과정을 거친다. 부호화 된 워터마킹 데이터는 원본 데이터에 삽입되며 은닉에 실패하여 워터마킹 데이터의 존재가 드러나더라도 고정 비트의 값을 알지 못하는 경우 다른

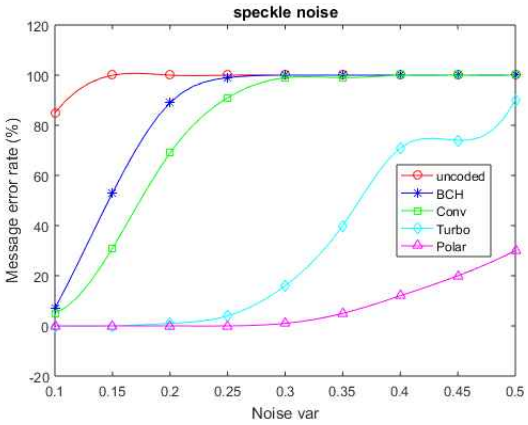

그림 5. 스테가노그래피 기법을 사용한 디지털 워터마크에 Speckle 노이즈를 사용했을 때, 오류 정정 코드 비교
Fig. 5. Comparison of error correction codes according to noise conditions.

암호화 알고리즘을 사용하지 않아도 보안성을 유지하는 것을 확인한다.

Ⅲ. 실 험

원본 데이터는 512×512 크기의 이미지에서 이루어진다. 이미지는 영상 처리에서 흔히 쓰이는 'Lenna' 이미지로 한다. 스테가노그래피를 활용한 디지털 워터마킹 기법은 2장에서 보인 알고리즘을 이용한다. fast Fourier Transform으로 주파수 도메인의 크기 값을 구해 디지털 워터마킹 데이터를 삽입한다. 이때 디지털 워터마킹 데이터는 128비트의 데이터이다. 이 워터마킹 데이터는 1/2의 부호율을 가지는 극부호로 부호화 한다. 따라서 원본 이미지에 심겨지는 데이터 크기는 256 비트가 된다.

고정 비트의 보안성을 확인하기 위해 수신자는 워터마킹 이미지에서 데이터를 추출한 뒤 부호화에서 사용 된 고정 비트와 다른 값으로 복호화 한다. 128개의 고정 비트 인덱스를 각각 다른 값으로 사용하였을 때, 복호화가 진행 된 후 워터마킹 데이터에 얼마나 오류가 발생하였는지 확인한다. 오류율(Error rate)는 전체 128 워터마킹 데이터 비트 중 오류가 발생한 비트의 비율을 나타냈다.

그림 6는 수신자가 고정 비트를 다르게 알고 있을 경우 전달하는 메시지의 오류율을 나타내었다. 128개의 고정 비트 인덱스를 각각 다르게 하여 전체 메시지에서 오류가 발생한 비트의 비율을 확인하였다. 전체 워터마킹 데이터에 가장 적은 영향을 미친 고정 비트 인덱스는 128개의 데이터 중 16개의 데이터 오류

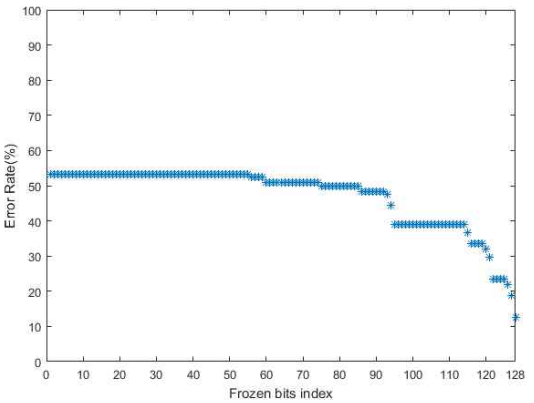

그림 6. 고정 비트 인덱스 별 오류율
Fig. 6. For each fixed bit index, the watermarking data error rate

(12.5%)를 발생시켰다. 그리고 데이터 오류에 가장 많은 영향을 미친 고정 비트 인덱스는 전체 데이터 128개 중 68개의 데이터 오류(53.125%)를 발생시켰다.

데이터를 보호하기 위해서 주로 쓰이는 방법으로 암호화가 있다. 이 방식은 대칭키를 가지며 오류 정정 코드 복호 외에도 추가적인 복호화 과정이 필요하다. 하지만 극부호의 경우 고정 비트를 대칭키로 사용하여 추가적으로 암호를 복호하는 과정이 필요하지 않게 된다. 이는 스테가노그래피의 데이터 추출 속도와 복잡성을 줄이는데 도움을 줄 수 있다.

Ⅳ. 결 론

멀티미디어 데이터의 활용이 늘어나면서 개인의 아이디어와 같은 지적 재산을 보호하려는 노력이 늘어나고 있다. 저작권 보호를 위해 흔히 사용되는 방법에는 디지털 워터마킹이 있다. 본 논문에서는 스테가노그래피를 활용한 디지털 워터마킹의 환경에서 정보 데이터를 효과적으로 보호하는 방법을 연구하였다. 여러 오류에서부터 워터마킹 데이터를 보호하려는 대표적인 방법으로 오류 정정 코드가 있다. 여러 가지 오류 정정 코드가 디지털 워터마크에서 활용되고 있으면 성능이나 복잡도 등을 고려하여 다양하게 사용되고 있다. 실험에서는 여러 오류 정정 코드 중 극부호가 가질 수 있는 효율성을 확인하였다. 극부호에는 정보 비트의 정확한 전송을 도와주는 고정 비트가 있다. 이 고정 비트는 상호간의 약속으로 이루어져 있기에 수신자는 데이터를 받기 전 이 값들을 알고 있어야한다. 수신자가 고정 비트를 알지 못한 경우 오히려 정보 비트의 훼손을 가져올 수 있다. 본 논문은 이 점을 디지털 워터마킹 데이터의 보안에 활용하였다. 실험에서는 원본 이미지에 128 비트의 정보 비트를 1/2의 코드율을 가지는 극부호로 부호화하여 삽입하였다. 이 때, 고정 비트를 수신자에게 일부러 잘 못 알려주면서 고정 비트가 가질 수 있는 보안성을 확인하였다. 한 개의 고정 비트는 적게는 12.5%의 오류를 발생시켰으며, 53.125%까지 데이터 비트 오류를 발생 시켰다.

스테가노그래피 기술은 사람이 감지 할 수 없는 정도에서 추가적인 데이터 삽입을 할 수 있도록 도와준다. 이 기술의 발전은 불법 복제 방지뿐만 아니라, 데이터 전송에도 크게 기여 할 수 있다. 이 기술을 효과적으로 발전시키는 방법은 오류 정정 코드의 활용 외에도 데이터 삽입 방법과 같은 다양한 분야로 연구 될 수 있다. 특히 주파수 도메인을 활용한 방법에는 현재 Fourier Transform 외에도 다양하게 진행되고 있다. 이 후 데이터 삽입 방식과 데이터 보호 방식의 효과적인 결합을 생각하는 방향으로 연구를 계속 진행 할 것이다.

References

[1] S. V. Kamble and B. G. Warvante, "A review on novel image steganography techniques," *IOSR J. Comput. Eng.*, pp. 1-4, 2013.

[2] R. S. Phadte and R. Dhanaraj, "Enhanced blend of image steganography and cryptography," *ICCMC IEEE*, Erode, India, Jul. 2017.

[3] D. Seo, S. Ko, J. Bae, and H. Park, "Survey on recent steganography," *J. KIISE*, pp. 1614-1616, Busan, Korea, Dec. 2017.

[4] H. Kostadinov and N. L. Manev, "Error correcting codes and their usage in steganography and watermarking," *2015 38th Int. Convention on Info. and Commun. Technol., Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 2015.

[5] C. Lalengmawia, A. Bhattacharya, and A. Datta, "Image steganography using advanced encryption standard for implantation of audio/video data," *IEEE ICRTIT*, Chennai, India, Apr. 2016.

[6] O. O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," *IEEE Trans. Info. Forensics and*

Secur., vol. 7, no. 5, pp. 1472-1483, 2012.

[7] Y.-S. Kim, J.-H. Kim, and S.-H. Kim, "A secure information transmission scheme with a secret key based on polar coding," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 937-940, 2014.

[8] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Info. Theory*, vol. 55, no. 7, pp. 3051-3073, 2009.

[9] K. Niu, et al., "Polar codes: Primary concepts and practical decoding algorithms," *IEEE Commun. Mag.*, vol. 52, no. 7, pp. 192-203, 2014.

이 승 호 (Seung Ho Lee)

2017년 2월 : 금오공과대학교 전자공학부 졸업

2019년 2월 : 금오공과대학교 IT융복합공학과 석사

2020년 3월-현재 : 국립금오공과대학교 IT융복합공학부 박사과정

<관심분야> 부호 이론, 영상처리, 보안

[ORCID:0000-0002-7806-9345]

신 수 용 (Soo Young Shin)

1999년 2월 : 서울대학교 전기공학부 졸업

2001년 2월 : 서울대학교 전기공학부 석사

2006년 2월 : 서울대학교 전기공학부 박사

2010년~현재 : 국립금오공과대학교 전자공학부 교수

<관심분야> 5G/B5G 무선 접속 기술, 드론 응용, 혼합 현실, 블록체인, 머신러닝 및 딥 러닝

[ORCID:0000-0002-2526-2395]