2020년도 한국통신학회 하계종합학술발표회

MNIST 이미지와 오토인코더를 활용한 보안 통신 기법

이인성[1], 김완진[2], 김덕경[1*]
인하대학교[1], 국방과학연구소[2]

insung237@naver.com[1], kimwj@add.re.kr[2], kdk@inha.ac.kr[1*]

Secure Communication Technique using MNIST image data and Auto-Encoder

In Sung Lee[1], Wan Jin Kim[2], Duk Kyung Kim[1*]
Inha University[1], Agency for Defense Development[2]

요 약

본 논문은 오토인코더를 이용한 보안 통신 기법을 제안한다. 기존의 보안 통신 방법은 신호의 스펙트로그램을 조작하는 방식으로 이루어져 주파수 상의 불연속 점이나 왜곡 점이 발생한다는 단점이 존재 하였다. 하지만 본 논문에서는 오토인코더를 이용하여 원 데이터의 차원을 줄인 특성 데이터를 이용함으로써 위에서 언급한 주파수 상의 문제를 발생시키지 않았다. 또한 오토인코더의 장점인 denoising 효과를 이용하였다. 시뮬레이션 결과에서는 랜덤 잡음 만을 고려 하였으며 다양한 SNR 값에 대해 좋은 성능을 보였다.

Ⅰ. 서론

보안 통신 또는 은밀 통신 기술이란 정보를 빠르고 정확하게 전달해야 한다는 일반적인 통신 목적과 함께 은밀하게 정보를 전송해야 하는 목적을 가진 통신 기술이다. 은밀 통신의 조건은 채널 상에 신호의 존재 자체를 알 수 없도록 하거나 설령 신호가 가로채기 당하더라도 그 신호를 복구하기 어렵게 만드는 것을 의미 한다.

은밀 통신 기술은 현대 사회에서 시간이 지나면 지날수록 점점 중요하지는 통신 기술 중의 하나로 자리 잡고 있다. 과거에는 주로 군사 목적으로 은밀 통신 기술이 많이 연구되었으나 현대에는 기업과 기업 사이의 통신, 개인과 개인 사이의 통신에서도 관련된 연구의 필요성이 언급되고 있다. 기존 은밀 통신 기법들의 몇 가지 예를 들자면 변형 LSB기반의 은밀 통신 기법과[1] 돌고래의 휘슬 음의 컨투어를 따서 흉내 내는 방식의 수중 은밀 통신 기법들이 있다[2]. 위 두 가지 방법들은 모두 소리의 스펙트로그램을 이용하여 Chirp Spread Spectrum (CSS) 기반의 은밀 통신 기법을 소개하고 있다. 하지만 이때 필연적으로 주파수의 불연속점이 생기거나 왜곡이 발생한다는 단점이 존재한다.

하지만 본 논문이 제시하는 방법은 머신 러닝의 구조체 중 하나인 Auto Encoder (AE) 를 이용하여 송수신 데이터의 차원을 변형시키는 방법을 이용함으로써 위의 두 논문들과 같은 주파수 상의 불연속점이나 왜곡 점이 발생하지 않는다. 오토인코더는 encoder, hidden layer, decoder로 이루어져 있는 머신 러닝 구조체 중 하나이다. Encoder는 입력 받은 데이터를 압축 시키는 역할을 하고 hidden layer에 이렇게 압축된 feature data가 저장된다. 마지막의 decoder는 feature data를 다시 원래 형태의 입력 데이터 형태로 복구하는 역할을 한다. 위 과정에서 생성 된 특성 데이터는 생성 과정에서 어느 정도의 필연적인 정보의 손실은 존재 하지만 original data의 고유한 특성들을 잘 보존한다는 특징을 지니고 있는데 이 점을 이용하여 feature 기반 은밀 통신을 구현 하였다.

은밀 통신을 구현 할 때 MNIST data를 입력으로 넣은 오토인코더의 특성 데이터를 이용하여 구현 하였다. MNIST data란 28*28크기의 숫자 손 글씨 이미지들 이다. 각각의 픽셀은 0~255사이의 정수로 이루어져 있으며 label 0~9총 10가지의 label로 구성되어 있다. MNIST data는 매우 잘 정돈된 데이터 셋으로 접근성이 용이하다는 장점이 있어 사용 하였다. 꼭 MNIST가 아닌 스펙트로그램과 같은 다른 이미지 데이터를 사용 하여도 무방하다. 또한 기존의 오토인코더를 활용하여 무선 통신에서 채널을 통과하며 발생하는 여러 가지 데이터의 손실을 보상해주는 End-to-End기법을 참고하여 denoising 효과를 추가하였다[3].

본 논문에서 소개하는 오토 인코더 기반의 은밀 통신 기법의 장점 및 기여도는 다음과 같다.

- 원 데이터를 송신자가 지정한 크기로 압축한 특성 데이터를 이용하기 때문에, 지정된 특성 데이터의 크기를 모르는 사람들은 데이터의 구조 및 형태를 절대로 알 수가 없으므로 더욱 견고한 은밀 성을 가진다.
- 오토인코더를 이용하여 줄어든 차원의 특성 데이터를 이용하고 이에 따른 denoising 효과를 은밀 통신 기법 연구에 새롭게 시도해 보았다.

Ⅱ. 본론

1) 제안하는 방식의 송수신 과정

송수신 과정에는 2 가지의 AE 가 이용된다. 첫 번째로는 원본 이미지 데이터를 입력으로 받아 원본 이미지 데이터를 출력하는 Original Auto Encoder (OAE) 와 두 번째로는 noisy image data 를 입력으로 받아 denoised 이미지 데이터를 출력하는 Denoising Auto Encoder (DAE) 이다. 송수신 과정을 순서대로 설명하자면 처음에 송신 할 원본 특성 데이터를 선택한 후 이 특성 데이터를 OAE 의 decoder 를 이용하여 이미지 데이터로 복원 시킨다. 이 복원된 이미지에 random noise 를 추가 한 후 DAE 의 encoder 로 입력된다. 이때 DAE 의 encoder 는 noisy 이미지 데이터에서 랜덤 잡음의 영향을 줄여주는 역할을 하여 비교적 랜덤 잡음의 영향이 작아진 denoised 특성 데이터를 출력한다. 마지막으로 출력된 denoised 특성 데이터와 처음 송신하였던 원본 특성 데이터의 ED 를 비교하여 송수신의 성공 여부를 결정한다.

2) 특성 데이터들의 특징

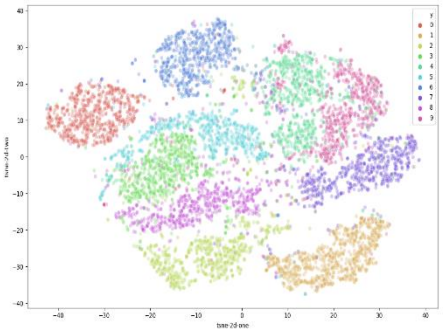

그림 1. 특성 데이터들의 t-SNE 분류 결과

그림 1 은 시뮬레이션에서 사용한 32 차원의 MNST 특성 데이터들 7000 개를 t-SNE 기법을 통해 분류 한 결과 이다. 위에서 분류한 특성 데이터들은 784 차원 크기의 MNIST 데이터를 OAE 의 Encoder 의 출력된 결과이다. 위 서론에서 언급 한 것과 같이 각각의 0~9, 총 10 개의 label 로 잘 분류 하며 기존의 MNIST 데이터들의 특징들을 잘 보존하였음을 알 수 있다.

1) 제안하는 통신 기법의 원리

제안하는 기법의 기본적인 원리는 기존의 QPSK 와 같이 신호 공간에서의 Euclidean Distance (ED)를 비교하여 송수신 성공 여부를 판단하는 원리 이다. 그러므로 수많은 특성 데이터들 중 통신에 이용할 특성 데이터들을 선별해야 한다. 이때 이 과정은 매우 중요한데 선별 조건은 M 개의 특성 데이터를 선택 하였을 때 서로서로 최대한 ED 가 떨어져 있어야 한다는 점이다.

시뮬레이션을 진행 할 때 다음과 같은 방법을 이용 하였다. 첫 번째로 원하는 각 특성 데이터들 사이의 최소 ED 와 통신에 이용할 특성 데이터 개수 M 을 설정 한다. 두 번째로 모든 특성 데이터들의 평균 특성 데이터를 구한 후 이 평균 특성 데이터와 ED 가 가장 가까운 중심 특성 데이터를 선정한다. 세 번째로, 선정한 중심 특성 데이터와 설정한 최소 ED 보다 멀리 위치하는 모든 특성 데이터들을 선별한다. 선별된 특성 데이터들 중에서 중심 특성 데이터와 가장 ED 가 작은 특성 데이터를 새로운 중심 특성 데이터로 선정한다. 마지막으로 새로 선정한 중심 특성 데이터와 이전에 선별해 놓았던 모든 특성 데이터들의 ED 를 계산 한 후 초기에 설정해 놓았던 최소 ED 보다 작은 ED 를 가지는 특성 데이터들을 모두 제외시키고 이 과정들을 M 개의 특성 데이터들을 선별할 때까지 반복한다. 아래 table 1 은 M 개의 특성 데이터를 선택 하였을 때 설정 한 최소 ED 값을 보여준다.

Table 1 Minimum ED per number of features M

Number of features M	Minimum ED
2	55
4	36
8	20
16	9
32	4

이때 위 표의 결과는 label 4 의 data 982 개 만을 이용한 결과 이다.

2) 시뮬레이션 결과

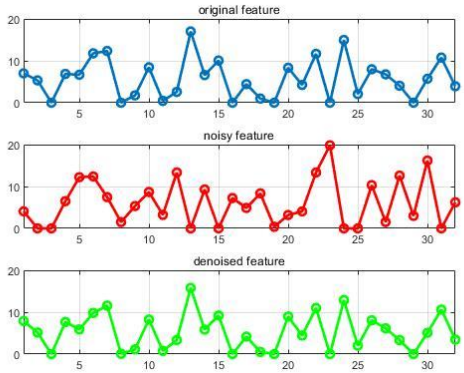

그림 2. 시뮬레이션의 feature 들의 결과

위 그림 2 는 본 시뮬레이션의 결과 중 일부를 보여준다. 상단의 파란색 그래프는 원본 특성 데이터, 즉 송신 특성 데이터를 의미하고 중앙에 위치하는 빨간색 그래프는 noise 가 첨가된 이미지의 특성 데이터를 의미하며 마지막 하단의 초록색 그래프는 denoised 된 수신 특성 데이터를 보여준다. 위 그림 2 에서 송신 특성 데이터와 수신 특성 데이터의 ED 차이는 4.77 로 table 1 을 참고하면 16 개의 특성 데이터를 통신에 사용 가능 하다고 할 수 있다. 잡음이 없는 상황, SNR 이 0dB, 그리고 6dB 인 총 3 가지 상황을 가정하고 시뮬레이션을 진행 하였다. 랜덤 잡음이 없는 환경에서도 송수신 ED 가 4 가 넘는 경우가 존재하였기 때문에 실제로 통신에 사용 가능한 특성 데이터의 개수 M 은 16 이라는 결론을 내렸다.

0dB 의 SNR 환경과 6dB 의 SNR 환경에서는 16 개의 특성 데이터를 이용하여 각각의 특성 데이터들이 gray coding 이 되었다고 가정 하고 송수신 시뮬레이션을 진행 하였다. 각 특성 데이터들 마다 10 번씩 총 160 번의 송신을 진행 하였을 때 0dB 에서는 약 $2.03 * 10^{-4}$의 BER 성능을 보였고 6dB 에서는 약 $3.12 * 10^{-5}$의 BER 성능을 보였다.

Ⅲ. 결론

MNIST 이미지와 오토인코더를 이용한 보안 통신 기법의 여러 가지 시뮬레이션 결과들을 따르면, 최대 16 개의 특성 데이터들을 통신에 이용 할 수 있다는 결론을 내릴 수 있었고 denoising AE 를 이용 함으로써 랜덤 잡음에 대해 좋은 성능을 보임을 알 수 있었다.

ACKNOWLEDGMENT

본 연구는 국방과학연구소의 지원으로 수행되었음 (UD200001DD)

참 고 문 헌

[1] 이용욱, 이상국, 김덕경, “변형 LSB 기반 생체모방 수중 은밀 통신 기법”, 한국통신학회논문지 제 45 권 제 3 호, November, 2019

[2] Jongmin Ahn, Hojun Lee, Yongcheol Kim, Sangkug Lee,and Jaehak Chung, “Mimicking dolphin whistles with continuously varying carrier frequency modulation for covert underwater acoustic communication”, Japanese Journal of Applied Physics, February, 2019

[3] Sebastian Cammerer, Sebastian Dörner, Adriano Pastore, “Machine Learning for Communications Emerging Technologies Initiative”, IEEE ComSoc, 2019