IoT 환경에서의 스테가노그래피 기술에 대한 연구 사례 조사

김현지[1], 임세진[2], 김덕영[2], 윤세영[2], 서화정[3]
[1]한성대학교 정보컴퓨터공학과 박사과정
[2]한성대학교 융합보안학과 석사과정
[3]한성대학교 융합보안학과 교수
khj1594012@gmail.com, dlatpwls834@gmail.com, dudejrdl123@gmail.com,
sebbang99@gmail.com, hwajeong84@gmail.com

Research cases of steganography technology in the IoT environment

Hyun-Ji Kim[1], Se-Jin Lim[2], Duk-Young Kim[2], Se-Young Yoon[2], Hwa-Jeong Seo[3]
[1]Dept. of Computer Information Engineering, Han-Sung University
[2]Dept. of Convergence Security, Han-Sung University
[3]Dept. of Convergence Security, Han-Sung University

요 약

최근 사물인터넷 및 통신 기술 및 통신 기술이 발달하면서 사물인터넷 상에서의 데이터 보호에 대한 관심이 지속되고 있다. 이에 따라 데이터 보호를 위한 기술적 요구들이 커지고 있으며, 데이터를 송수신하는 과정에서 비밀 데이터가 숨겨져 있다는 사실을 자체를 숨기는 스테가노그래피 기술이 활용되고 있다. 본 논문에서는 IoT 환경에서의 스테가노그래피 기술이 만족해야하는 조건과 연구 사례에 대해 살펴본다.

1. 서론

최근 사물인터넷 (Ineternet of Things, IoT) 및 통신 기술의 발달로 인해 디지털 데이터의 양이 급격히 증가하고 있다. 이에 따라 중요한 정보를 보호하기 위한 기술적 요구가 커지고 있으며, 데이터 암호화와 더불어 데이터의 존재 자체를 숨기는 스테가노그래피 기술이 활용되고 있다. 본 논문에서는 IoT 환경에서의 스테가노그래피 기술의 조건과 연구 사례를 살펴본다.

2. 스테가노그래피

스테가노그래피[1]는 중요한 비밀 데이터를 은닉하기 위해 텍스트, 이미지 등의 파일 (커버 데이터)에 데이터를 삽입하는 기술이다. 이때 사용되는 스테가노그래피 (임베딩) 알고리즘은 비밀 데이터가 삽입되었음을 육안으로 식별할 수 없도록 해야 하며, 스테가노그래피를 통해 생성되는 스테고 오브젝트는 원본 파일과 매우 유사한 모습을 가진다.

스테가노그래피는 크게 데이터 암호화와 데이터 임베딩 과정으로 구성된다. 데이터 암호화는 임베딩 할 비밀 데이터에 비밀키 및 공개키 암호화를 수행하는 과정이다. 물론 암호화를 수행하지 않을 수도 있다, 그러나 암호화를 수행하지 않을 경우, 보안성이 임베딩 알고리즘의 성능에만 의존하게 되므로 보안성 측면에서 한계점이 존재한다. 비밀키 및 공개키 암호화를 수행할 경우, 데이터에 대한 보안성은 향상되지만 데이터의 크기가 증가하고, 커버 데이터의 용량이 한정되어 있으므로 임베딩 가능한 데이터의 크기가 줄어들 수 있게 된다.

암호화 된 비밀 데이터는 스테가노그래피 알고리즘을 통해 커버 데이터에 삽입된다. 이때, 고려해야할 점은 커버 데이터의 왜곡과 손상이 최소화하여 비밀 데이터가 숨겨져 있다는 사실이 드러나지 않도록 해야한다. 이를 위해 LSB (Least Significant Bit)[2], Pixel Value Differencing (PVD)[3], Wavelet Obtained Weights (WOW)[4] 등의 알고리즘이 존재한다. 위와 같은 데이터 암호화 및 임베딩 과정을 거치면 데이터의 존재 자체와 값을 보호하게 되므로 데이터 통신에서의 보안성을 확보할 수 있다.

3. IoT 환경에서의 스테가노그래피를 위한 조건

2.2 IoT 기술 개요와 스테가노그래피

IoT는 사물인터넷을 의미하며, 인터넷에 연결된 여러 디바이스들이 서로 통신하며 데이터를 주고 받는 기술이다. 주로 실시간 정보 수집, 센싱 등에 사용되고, 스마트 홈, 스마트 시티 등의 분야에 적용되고 있으며 그 범위가 확장되고 있다. 그러나 IoT 기술은 물리적 공격, 인증, 데이터 유출과 같은 보안 문제점이 존재한다. 특히, IoT 네트워크에 연결된 수많은 디바이스에서 오고 가는 개인 정보들이 유출될 경우, 개인 및 사회적인 측면에서 큰 문제를 야기할 수 있다. 따라서 이러한 문제를 예방하기 위해 데이터 암호화, 데이터 은닉, 접근 제어 등의 보안 기술이 연구되었다. 이러한 기술의 예시로 경량 암호화와 앞서 설명한 스테가노그래피 기술이 있다. 그러나 IoT 디바이스에서는 메모리 및 계산 능력이 제한되어 있고, 대체적으로 데이터 전송 속도가 느리며 통신 대역폭이 작다. 또한, 주로 실시간 데이터 수집 등에 사용되므로 데이터 처리에 필요한 시간 및 자원을 최소화 할 수 있는 스테가노그래피 알고리즘이 필요하다. 즉,보안성을 위한 기술뿐만 아니라 메모리 및 계산 효율성을 만족하는 기술들이 요구된다. 그러므로 스테가노그래피를 IoT 환경에 적용할 경우, 경량 알고리즘 (암호화 및 통신 프로토콜) 사용, 최적화, 보안성 등을 고려해야한다.

4. IoT 환경에서의 스테가노그래피 기술 연구 사례

[5]에서는 IoT 상에서의 통신 기술인 Zigbee 프로토콜에 스테가노그래피를 적용하여 통신 당사자 간에 주고 받는 데이터에 대한 보안성을 확보하였다. 전체적인 과정은 다음과 같다. 데이터를 전송할 때 프레임의 지정된 필드 메시지에 비밀 정보를 임베딩한다. 이때, 데이터에 대한 공개키 암호화를 수행한 후, 암호문을 지정 위치에 은닉한다. 비밀 데이터를 삽입할 수 있는 위치는 데이터 프레임과 비콘 프레임, MAC 명령어 프레임의 프레임 제어 필드 및 주소 정보 필드의 소스 주소 영역이다. 해당 영역들은 프레임의 특정 위치에 해당하며, 임베딩 가능한 용량은 각각 다르다. 먼저, 데이터 프레임의 프레임 제어 필드는 7~9번째 비트 (3비트)와 12~13번째 비트 (1비트)에 해당하는 부분에 임베딩이 가능하고, 소스 주소 필드에는 16비트와 64비트 메시지를 임베딩 할 수 있다. 두 번째로 비콘 프레임의 프레임 제어 필드와 소스 주소 정보 필드는 데이터 프레임과 유사하다. 그러나, 소스 주소 필드는 최대 10 바이트까지 임베딩이 가능하다. 다음으로 응답 프레임의 프레임 제어 필드에는 2바이트의 비밀 데이터를 임베딩할 수 있으며, MAC 명령어 프레임의 프레임 제어 필드 및 주소 정보 필드에는 2바이트 및 4~20 바이트까지의 데이터를 숨길 수 있다. 이후, 데이터 수신자는 수신한 데이터 프레임에서 비밀 데이터를 얻은 후 개인키로 복호화하여 데이터 원본을 추출할 수 있게 된다. 이처럼 프레임의 정해진 영역에 비밀 데이터를 은닉함으로써 Zigbee 통신에서의 보안성을 향상시킬 수 있도록 하였다.

[6]에서는 IoT 디바이스와 서버 간의 통신에서 발생하는 정보 노출 문제를 방지하기 위한 스테가노그래피 기술을 제안하였다. 해당 기술은 크게 센서와 홈 서버, 클라우드 서버로 구성된다. 먼저, IoT 디바이스는 주로 센서 디바이스이며, 실시간 정보 수집 및 통신 기능을 수행해야한다. 이를 위해 제안 기법에서는 수집된 데이터에 경량 암호화 (XOR 등)를 수행한 후, 데이터 원본을 MD5를 통해 해시하여 메시지 다이제스트 (Message digest)를 생성한다. 생성된 암호문과 다이제스트는 LSB 스테가노그래피를 통해 임베딩 된다. 이러한 과정을 통해 만들어지는 스테고 오브젝트를 홈 서버로 전송한다. 홈 서버는 IoT 디바이스와 클라우드 서버 사이의 보안성을 확보하기 위해 추가 계산을 수행한다. 즉, 추가 연산을 통해 더욱 안전하게 클라우드 서버로 데이터를 전송해주는 인증 장치라고 볼 수 있다. 홈 서버는 IoT 디바이스로부터 수신한 스테고 오브젝트를 역연산하여 암호문과 다이제스트를 얻고, 복호화를 통해 센서 데이터의 원본을 얻는다. 해당 데이터를 MD5로 해시하여 다이제스트를 계산하고 수신한 다이제스트와 비교한 뒤, 올바른 정보인 경우 다음과 같은 스테가노그래피 과정을 거친다. 홈 서버에서 수행하는 스테가노그래피 또한 IoT 디바이스에서 수행한 것과 유사하다. 그러나 경량 알고리즘을 사용하지 않아도 되므로 AES, DES와 같은 암호 알고리즘을 사용하고, 스테가노그래피 방식으로는 기존의 LSB 방식이 아닌 MSB-LSB 방식을 사용한다. MSB-LSB 방식은 해당 연구에서 제안한 기법으로 MSB와 임베딩할 비밀 메시지의 비트 값에 따라 조건부로 LSB에 임베딩을 수행한다. MSB가 0인 경우, LSB와 비밀 데이터의 첫 번째 비트가 동일하다면 임베딩을 수행하지 않고, 동일하지 않다면 임베딩한다. MSB가 1이고 첫 번째 비트가 0인 경우, MSB는 유지하고 LSB는 1로 설정하며, 메시지 임베딩은 수행하지 않아도 된다. 다음으로, MSB가 1이고 임베딩 메시지의 첫 비트가 1이면서 LSB가 1인 경우, 비밀 데

이터의 두 번째 비트가 0이면 MSB를 유지하고 LSB를 해당 비트로 대체하며, 두 번째 비트도 1이라면 임베딩을 수행하지 않는다. 이처럼 모든 비트에 대해 LSB 임베딩을 수행하는 것이 아니라 MSB와 비밀 데이터의 값을 고려한 LSB 임베딩을 수행하면 데이터 임베딩에 필요한 픽셀의 수가 적으며, 임베딩 후 변경되는 픽셀의 수가 적다. 따라서 적은 픽셀에 동일한 양의 데이터를 임베딩할 수 있으며 데이터의 왜곡이 적어진다는 이점이 있다. 정리하면, 해당 연구에서는 IoT 디바이스에서는 경량 암호화를 사용하고 임베딩 시 연산 복잡도가 낮은 기술을 개발하여 사물인터넷 환경에 적합한 스테가노그래피 기술을 제안하였다.

[7]에서는 이미지 스테가노그래피를 활용하여 IIoT (Industrial IoT)상에서의 데이터 보안을 위한 스테가노그래피 기술을 제안하였다. 해당 연구에서는 왜곡이 적은 스테고 오브젝트를 생성하기 위해 최적의 픽셀을 선택하도록 하였다. 최적 픽셀을 선택하는 과정은 다음과 같다. 우선, 어떠한 픽셀에 비밀 데이터를 삽입했을 때 변경되는 값을 최소화해야한다. 변경되는 값은 이미지의 시각적 품질을 향상시키기 위해 사용되는 OPAP (Optimal Pixel Adjustment Process)에 의해 최소화된다. 즉, 스테고 오브젝트와 커버 오브젝트 간의 유사성을 측정하는 함수에 따라 스테가노그래피를 위한 최적 픽셀을 선택하는 것이다. 저자들은 해당 기술이 임베딩 용량과 계산 소요 시간에서 효율적임을 보였으며, 이는 실시간 데이터 처리를 주로 수행하는 IIoT 환경에서 매우 중요한 요소이다. 따라서 해당 연구를 통해 경량 알고리즘을 사용하면서 보안성을 높일 수 있는 스테가노그래피 기술이 제시되었다. 이외에도 IoT 기반 헬스케어 시스템에서의 안전한 의료 데이터 전송을 위한 스테가노그래피[8] 등과 같이 스테가노그래피가 적용된 어플리케이션 사례들이 존재한다.

5. 결론

본 논문에서는 IoT 상에서의 스테가노그래피 기술의 연구 사례에 대해 살펴보았다. 여러 연구들이 IoT 환경에서 효율적인 스테가노그래피를 위해 경량화 알고리즘과 계산 복잡도 및 소요 시간이 적은 기술을 사용하는 추세이다. 그러나 경량 암호화 및 알고리즘을 사용함으로써 보안성이 감소할 수 있다는 문제점이 존재하며, 이를 극복하기 위한 방법들도 연구되고 있음을 확인하였다. 또한, 최근에는 IoT 상에서의 딥러닝 기술들이 개발되고 있고, 딥러닝 기반의 스테가노그래피 기술들도 활발히 연구되고 있다. 그러나 해당 기술들은 고전 알고리즘들에 비해 계산 복잡도가 높을 수밖에 없으므로, 향후에는 딥러닝 기반의 스테가노그래피 기술들에 대한 경량화도 함께 이루어져야 할 것으로 생각된다.

6. Acknowledgements

This work was partly supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services, 50%) and this work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2022-0-00627, Development of Lightweight BIoT technology for Highly Constrained Devices, 50%).

참고문헌

[1] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." ISSA. Vol. 1. No. 2. 2005.

[2] Laskar, Shamim Ahmed, and Kattamanchi Hemachandran. "High Capacity data hiding using LSB Steganography and Encryption." International Journal of Database Management Systems 4.6: 57, 2012.

[3] Wu, Da-Chun, and Wen-Hsiang Tsai. "A steganographic method for images by pixel-value differencing." Pattern recognition letters 24.9-10: pp. 1613-1626, 2003.

[4] V. Holub and J. Fridrich. Designing steganographic distortion using directional filters. In 2012 IEEE International Workshop on Information Forensics and Security(WIFS), pp. 234 - 239, 2012.

[5] Hussain, I., Negi, M. C., & Pandey, N. "Security in ZIGBEE using steganography for IoT communications," System Performance and Management Analytics, pp. 217-227, 2019.

[6] Das, Ria, and Indrajit Das. "Secure data transfer in IoT environment: Adopting both

cryptography and steganography techniques." 2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN). IEEE, 2016.

[7] Hassaballah, M., Hameed, M. A., Awad, A. I., & Muhammad, K. “D,” IEEE Transactions on Industrial Informatics, 17(11), pp. 7743-7751, 2021.

[8] Elhoseny, Mohamed, et al. "Secure medical data transmission model for IoT-based healthcare systems." Ieee Access 6: pp. 20596-20608, 2018.