얼굴 사진 보호를 위한 이중 암호화에 관한 연구

이영재, 권혁민*, 이구연**, 김화종***

강원대학교, *강원대학교, **강원대학교, ***강원대학교

A Study on the Double Encryption for the Face Image Protection

Young Jae Lee, Hyuk Min Kwon*, Goo Yeon Lee**, Hwa Jong Kim***

Kangwon Univ., *Kangwon Univ., **Kangwon Univ., ***Kangwon Univ.

dudwo8528@gmail.com, *hykwon8952@gmail.com, **leegyeon@kangwon.ac.kr, ***hjkim3@gmail.com

요 약

오늘날 개인정보 보호는 컴퓨터 네트워크보안에 있어 중요한 이슈이다. 국내 대부분의 상용 메신저들이 개인의 사적인 통신을 안전하게 활용할 수 있도록 돕고 있다. 메신저를 통해 단순한 텍스트 메시지뿐만 아니라 사용자 자신의 사진을 서로 주고받는 것은 일상적인 일이 되었다. 그러나 이미지 데이터는 특성상 인근 픽셀은 유사한 값을 가지게 되며 중복성이 높아 단순한 텍스트 데이터에 비해 상대적으로 공격에 취약하다. 이에 본 연구에서는 Face Detection이 가능한 사진에서 주요 부위인 눈, 코, 입 등 특정 부분을 추출해 비대칭형 암호화 알고리즘(Asymmetric Algorithm)인 RSA 암호화 기법을 이용해 1차 암호화 후 이미지 파일 전체를 AES(Advanced Encryption Standard) 암호화 기법 즉, 대칭형 암호화 알고리즘(Symmetric Algorithm)을 적용해 이중 암호화를 반복 적용한다. 이러한 방법을 통해 이미지 데이터 암호화 문제점을 해결하고자 한다.

Ⅰ. 서 론

개인정보 보호에 관한 관심이 높아짐에 따라 국내 대부분의 상용 메신저들은 종단 간 암호화를 통해 안전하게 개인의 사적인 통신을 활용할 수 있도록 돕고 있다. 일반적으로 128bit 이상의 AES(Advanced Encryption Standard) 알고리즘을 사용하여 메시지를 암호화 하기 때문에 공격자가 중간자 공격을 하더라도 원본 메시지를 알아내기는 힘들다. 최근엔 메신저를 통해 메시지 뿐만 아니라 사용자들이 자신의 사진을 찍고 서로의 사진을 주고 받는 것은 일상적인 일이며 이에 따라 단순한 텍스트 암호화 뿐만이 아니라 사용자 사진의 암호화 통신의 필요성이 대두되게 된다. 그러나 사진과 같은 이미지 데이터는 인근 픽셀은 비슷한 값을 가지는 특성을 가지기 때문에 중복성이 높아 텍스트 데이터에 비해 상대적으로 공격자가 킷값(key value)을 알아내기 쉽다는 취약점을 가진다.[1] 이러한 방식으로 공격자는 이미지 복호화에 성공하고 사진을 도용하는 등의 범죄에 악용할 수 있다. 따라서 본 연구에서는 기존의 단순한 암호화 기법이 아닌 눈, 코, 입 등의 얼굴의 주요 정보를 추가로 암호화 하여 공격자가 AES방식으로 암호화된 이미지를 복호화 하는데 성공하더라도 얼굴의 주요정보는 알아낼 수 없도록 하는 이중 암호화 방식을 제안한다.

Ⅱ. 암호화 기법과 얼굴인식

현대의 암호화 기법은 암호화 알고리즘과 암호키로 구현되고 있다. 암호화 알고리즘은 표준화되어 사용되기 때문에, 암호키를 유지 및 보관하는 것이 암호화의 핵심이라고 할 수 있다. 여러 가지 암호화 알고리즘은 크게 대칭형 암호화 알고리즘과 비대칭형 암호화 알고리즘이 있다. 대칭형/비대칭형 암호화 알고리즘 방법의 예로는 다음과 같다.

- **RSA 암호화**
  비대칭형 암호화 알고리즘(Asymmetric Algorithm)으로 공개키 암호 방식의 형태의 하나로서 오늘날, 전자서명, 전자 상거래, 암호화 등 광범위하게 사용되고 있다. 이 암호화 방식은 다수가 알고 있는 공개키에 대해 개인 키(key)를 가진 사람만 복호화할 수 있는 알고리즘이다.[2] 따라서 안전하게 암호화할 수 있는 장점을 가지고 있지만, 복잡한 수학적 연산 때문에 구현이 어렵고, 대칭형 암호화 알고리즘에 비해 속도가 매우 느리다.
- **AES 암호화(Advanced Encryption Standard)**
  고급 암호화 표준이라고도 하며 미국 표준 기술 연구소(NIST)에 의해 제정된 대칭형 암호화 알고리즘(Symmetric Algorithm) 형태의 하나이다. 이 암호화 방식은 데이터를 암호/복호화 시 블록 단위로 처리하는 방식의 블록 암호 알고리즘이다. 비대칭형 암호화 알고리즘에 비해 암호화하는 방식이 다양하고 암호/복호화 과정이 빠르지만, 상대방과 키 공유 시 안전하게 키를 공유하기 어려운 단점이 있다.[5]
- **스테가노그래피(Steganography)**
  암호화 알고리즘과는 다른 방식으로 메시지를 숨기고자 하는 방법으로 데이터를 암호화시키지 않고 특정 공간 속에 숨기는 것이다.[3] 4차 산업혁명이 발전한 현대 디지털 시대에서는 디지털 스테가노그래피라고 명명하기도 한다. 즉, 디지털 메시지를 숨기는 기술로서 텍스트 파일, image 파일, 오디오 파일, 동영상 파일 등이 그 대상이 된다. 그 중에서도 주로 image 파일을 대상으로 하기 때문에 image 파일에 메시지를 숨기는 기술로 인식되기도 한다. 그 방법은 다음과 같다.[6]
  - **Spatial domain 기법**
    image 파일의 pixel을 다루는 기법이다.
  - **Transform(or Frequency) domain 기법**
    image 파일의 transform 혹은 frequency에 정보를 숨기는 기법이다.
  - **Distortion 기법**
    image 파일을 변형시켜 정보를 숨기는 기법으로 해독하는 자는 원본 image 파일을 가지고 있어야 한다.
  - **Masking and filtering 기법**

image 파일의 특정 부분의 밝기나 휘도를 변형시켜 정보를 숨기는 기법이다.

- **Face Detection**
  image에서 얼굴이 어디에 위치했는지 알아내는 컴퓨터비전 관련 기술을 말한다.[4]

Ⅲ. 이중 암호화를 통한 이미지 데이터 암호화 설계

본 논문에서 연구된 이중 암호화를 통한 사진 이미지 암호화 처리 과정을 그림으로 나타내면 다음과 같다.

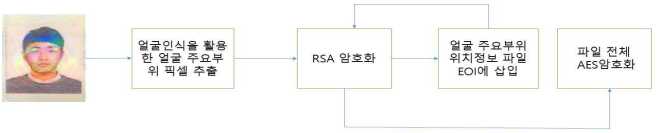

그림 1. 이미지 데이터 이중 암호화 흐름

그림에서 얼굴인식(Face Detection)을 통해 눈, 코, 입과 같은 주요 부위의 픽셀을 추출한 후 이를 RSA 암호화 기법을 사용해 암호화한다. 이 기법은 비대칭형 암호화 기법으로 공개키를 통해 암호화를 하기 때문에 개인 키를 가지고 있을 경우만 복호화가 가능하다. 상대적으로 속도가 느리고 제한된 크기의 데이터에서 사용하는 방식이므로 Face Detection 기법을 이용하여 얼굴의 주요 부위를 추출하고 해당 픽셀만 안전한 비대칭형 암호화 방식으로 암호화한다. 비대칭형 암호화 기법은 주로 타원곡선 암호화 기법을 사용하지만 RSA 암호화 기법과 비교했을 때 암호화에 유리하나 복호화에서의 처리량이 많아 불리하다는 특징을 가지며 본 연구는 서버 통신에서 트래픽량이 많았을 때를 가정하여 암호화된 이미지 파일을 받는 서버 측에서의 처리량을 줄이기 위해 복호화에 유리한 RSA 암호화 방식을 사용하였다.

암호화된 픽셀의 좌표정보는 스테가노그래피 기법을 활용하여 파일에 RSA로 암호화하여 삽입한다. image 파일(jpeg, png, gif 등)에는 파일의 끝을 알리는 EOI(End Of Image) 바이트가 존재하고 이 이후의 데이터는 파일을 읽는 과정에서 무시되므로 해당 바이트에 데이터를 넣어 파일의 용량을 유지한 상태로 암호화된 좌표정보를 삽입할 수 있다.

마지막으로 비대칭형 암호화 기법으로 부분 암호화된 image 파일 전체를 상대적으로 암호화와 복호화 속도가 빠른 대칭형 암호화 알고리즘인 AES기법을 활용해 암호화하여 전송한다.

이러한 과정을 통해 공격자가 중간에 패킷을 탈취하여 image를 복호화하더라도 얼굴의 주요 부위를 복호화하는 것은 거의 불가능 하기 때문에 사용자의 개인정보는 보다 안전하게 보호될 수 있다.

Ⅳ. 결론

본 논문에서는 디지털 통신에서 이슈 중 하나인 이미지 데이터에 대한 암호화하는 방법을 제안하였다. 사진과 같은 이미지 데이터는 특성상 인근 픽셀의 값들이 유사하다. 따라서 본 연구에서는 이를 눈, 코, 입과 같은 주요 부위는 비대칭형 암호화 알고리즘, 주요 부위의 위치는 스테가노그래피 기법을 통해 EOI(End Of Image)에 위치 값을 저장 후 이를 다시 비대칭형 암호화 기법으로 암호화, 이미지 전체 파일은 대칭형 암호화 알고리즘을 통해 구현하도록 설계하였다.

클라이언트의 경우에는 개개인의 이미지 파일을 암호화하므로 그중에서도 크기가 작은 주요 부위(눈, 코, 입)를 비대칭형 암호화 기법을 적용하였다. 그중에서도 서버에서는 많은 양의 데이터를 받아 복호화하기 때문에 복호화에 유리한 RSA 암호화 방식을 사용하였다. 이미지 파일 전체를 전송할 때는 암호/복호화 방식에 유리한 대칭형 암호화 기법 중 AES 기법을 적용해 전송하도록 했다. 이처럼 두 가지 암호화 방식을 반복 적용하여 이중 암호화를 통해 이미지 데이터 암호화를 해결하고자 한다.

본 연구는 이미지 용량이 커지게 되면 Face Detection 과정을 통한 얼굴 주요부위 추출 과정과 주요부위 비대칭형 암호화과정에서 계산량이 많아 비효율적일 가능성이 있다. 또한, 대상 이미지가 사람 사진에만 국한된다는 한계점을 가진다. 향후 연구에서는 속도, 용량 측면에서의 비효율성을 개선하고 본 연구를 응용하여 데이터에서의 주요정보 이중 암호화 방식을 활용하여 다른 도메인으로 확장한다면 이는 현 중요한 이슈인 네트워크에서 이미지 데이터 통신에서의 개인정보 문제를 해결하는데 많은 도움이 될 것이다.

ACKNOWLEDGMENT

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No. 2018-0-00261, IoT 환경에서 일반 개인정보보호 규정에 부합(GDPR Compliant)하는 개인 정보 관리 기술개발)

참 고 문 헌

[1] D.I. G.Amalarethinam, J.S.Geetha, “Image encryption and decryption in public key cryptography based on MR”, International Conference on Computing and Communications Technologies (ICCCT,15), 2015

[2] M. Preetha, M. Nithya, “A STUDY AND PERFORMANCE ANALYSIS OF RSA ALGORITHM”, IJCSMC, Vol. 2, Issue. 6, June, 2013

[3] Channalli S, Jadhav A “Steganography an Art of hiding data”, Int J Comput Sci Eng (IJCSE), 2009

[4] M.S. Roy, M.S. Podder, “Face detection and its applications International Journal of Research in Engineering & Advanced Technology”, 2013

[5] 오주영, 서진형,(2010).AES 암호화 알고리즘의 실험적 분석.한국정보전자통신기술학회 논문지,3(2),58-63.

[6] 황선준, 김중헌,(2018).지도학습 기반 다중 이미지 스테가노그래피.한국통신학회 학술대회논문집,(),1134-1134.