사용자 친화형 이미지 보안 시스템의 설계

이서준[1], 장현지[1], 최주언[1], 유동현[2]
[1]전남대학교 인공지능학부 학부생
[2]전남대학교 인공지능융합학과 교수
tjwns1300@jnu.ac.kr, gka1225@jnu.ac.kr, jueon030512@jnu.ac.kr, donghyun.yu@jnu.ac.kr

Design of User-Friendly Image Security System

Seo-Jun Lee[1], Hyeon-Ji Jang[1], Ju-Eon Choi[1], Dong-Hyun Yu[2]
[1]Dept. of Artificial Intelligence, Chonnam National University
[2]Dept. of Artificial Intelligence Convergence, Chonnam National University

요 약

기존 이미지 보안 방식은 낮은 접근 편의성와 키 관리의 불편함으로 인해 활용에 제약이 있다. 본 논문에서는 이러한 한계를 극복하고, 보안성과 실용성을 모두 고려한 이미지 보안 시스템 Encra를 제안한다. 본 시스템은 사용자가 선택한 이미지 영역을 AES로 암호화하고, JPEG 포맷을 그대로 유지하여 암호화 이후에도 이미지 열람이 가능하다. AES 키는 수신자의 이메일 주소 기반으로 IBE 방식으로 보호되며, 별도의 복잡한 키 관리 없이 복호화 권한을 설정할 수 있다.

1. 서론

디지털 환경에서 이미지는 의료, 설계, 행정 등 다양한 영역에서 민감한 정보를 전달하는 수단으로 사용된다. 그러나 기존 이미지 보안 기술은 암호화 과정의 번거로움과 키 관리에 대한 사용자 부담 등으로 인해 실용성에 한계가 있다. 특히 전용 소프트웨어나 복잡한 인증 절차가 요구되어, 일반 사용자나 실무 환경에서는 적용이 제한되는 경우가 많다. 본 논문에서는 이러한 문제를 해결하기 위해, 보안성과 실용성을 모두 고려한 이미지 보안 시스템 Encra를 제안한다. 본 시스템은 사용자가 선택한 민감 정보 영역만을 암호화하고, JPEG 포맷의 호환성을 유지하면서도 이메일 기반의 간편한 키 분배 방식을 통해 실제 사용 환경에서 적용 가능하도록 설계되었다.

2. 이론적 배경 및 관련 연구

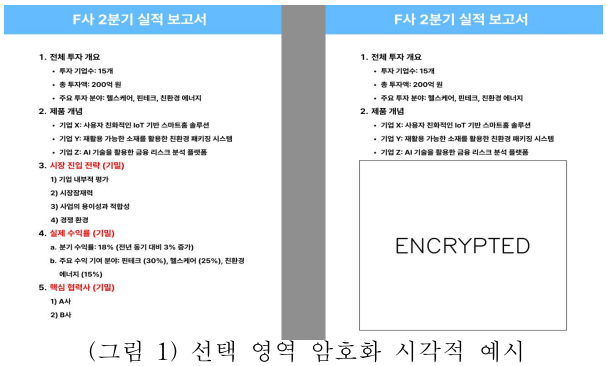
AES(Advanced Encryption Standard)[1]는 128, 192, 256비트 키를 지원하는 대칭키 블록 암호화 알고리즘으로, 빠른 연산 속도와 높은 보안성을 바탕으로 이미지 암호화에도 널리 사용된다. 하지만 암호화된 데이터를 복호화하기 위해 동일한 대칭키를 안전하게 전달해야 한다는 구조적 한계가 존재한다. 이를 보완하기 위해 RSA와 같은 공개키 암호화 방식이 사용되지만, RSA는 키 쌍을 통해 안전한 키 교환이 가능하면서도 인증서 관리 등 복잡한 PKI(Public Key Infrastructure) 구성이 필요해 일반 사용자에게는 진입 장벽이 높다[2].

IBE(Identity-Based Encryption)[3]는 이러한 복잡한 구조를 간소화한 방식으로, 수신자의 이메일 주소와 같은 고유 식별자를 공개키로 활용하여, 별도의 공개키 전달이나 인증서 없이 암호화가 가능하다. 본 시스템은 이미지 데이터를 연산 효율이 뛰어난 AES로 암호화하고, 해당 키는 수신자의 이메일 기반 IBE 방식으로 암호화하는 하이브리드 구조를 채택하였다. 이는 공개키 암호화인 IBE가 이미지 전체와 같은 대용량 데이터를 처리하기에는 연산량이 크고 비효율적이기 때문이며, 상대적으로 가벼운 AES 키만을 암호화함으로써 효율성과 보안성을 모두 충족할 수 있다.

3. 제안하는 이미지 보안 시스템

3.1. 사용자 선택 영역 암호화 방식

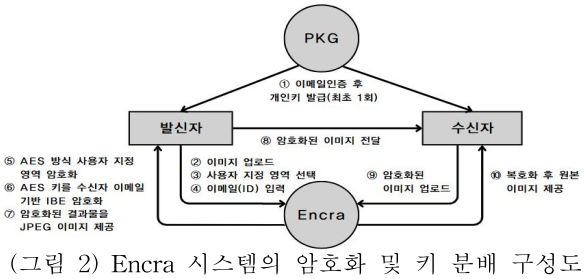
본 시스템은 사용자가 GUI를 통해 이미지 내 특정 영역을 선택하고, 해당 부분만 AES 방식으로 암호화한다. 암호화된 영역은 'ENCRYPTED'와 같은 텍스트 워터마크가 삽입되어, 사용자가 암호화 여부를 명확히 인지할 수 있도록 설계되었다.



(그림 1) 선택 영역 암호화 시각적 예시

암호화된 결과는 JPEG의 APP13(Application Marker 13) 세그먼트에 삽입된다. 이를 통해 전체 이미지는 JPEG 확장자를 유지하면서도, 기존 이미지 뷰어에서 정상적으로 열람할 수 있다.

3.2. Encra의 전체 암호화 과정



(그림 2) Encra 시스템의 암호화 및 키 분배 구성도

(그림 2)는 발신자와 수신자 간의 이미지 암호화와 키 분배 과정을 도식화한 것이다. 사용자는 Encra 플랫폼을 통해 암호화할 이미지를 업로드하고, 수신자의 이메일 주소를 입력한다. 시스템은 AES 방식으로 암호화를 수행한 후, 해당 키를 수신자의 이메일 기반 IBE로 보호한다. 암호화된 이미지는 JPEG 형식으로 저장되어 수신자에게 전달되며, 개인키를 통해 로컬 환경에서 복호화를 수행한다. 이 과정에서 개인키 생성 기관인 PKG(Private Key Generator)는 최초 인증된 사용자에게만 개인키를 발급하며, 암호화된 데이터에는 접근하지 않는다. 전체 구조는 중앙 서버 개입을 최소화하면서도, 실사용 환경에서의 보안성과 편의성을 모두 충족할 수 있도록 설계되어 있다.

3.3. 기존 암호화 방식과 Encra 시스템 비교

<표 1> 기존 암호화 방식과 Encra 시스템의 비교 분석

항목	AES 단독 방식	RSA 단독 방식	AES+RSA 혼합 방식	Encra
포맷 호환성	압축 파일 필요	별도 형식 필요	전용 처리 필요	JPEG 포맷 유지
키 관리 방식	대칭키 수동 전달	공개키 인증 필요	인증서 및 키 분배 절차 요구	이메일 기반 자동 키 관리
실무 적용성	빠르나 사용자 개입 요구	설정 복잡, 진입 장벽 높음	보안 우수, 운용 부담 큼	보안성과 실용성의 균형

<표 1>에서 확인할 수 있듯이, 기존 방식들은 전용 포맷 요구, 키 관리의 복잡함, 제한적인 적용성 등으로 인해 활용에 제약이 있었다. 반면 Encra는 JPEG 호환성 유지, 이메일 기반의 간편한 키 분배, 높은 실무 적용 가능성을 바탕으로, 사용자 친화적인 보안 시스템을 지향한다.

4. 결론

본 논문에서는 JPEG 포맷의 호환성을 유지하면서도 사용자가 지정한 민감 영역만을 선택적으로 AES로 암호화할 수 있는 실용적인 이미지 보안 시스템, Encra를 제안하였다. 전체 암호화 없이 핵심 정보만 보호함으로써, 보안성과 공유 편의성을 동시에 확보하였으며, GUI에서 영역 선택 후 즉시 암호화되는 구조를 통해 사용자는 직관적으로 암호화를 수행할 수 있다. 또한, IBE 기반 키 분배 구조를 도입함으로써 수신자 이메일만으로 개별 복호화 권한을 설정할 수 있으며, 인증서 없이도 간편한 키 관리가 가능하다. 수신자는 한 번 발급받은 개인키만으로 서버 개입 없이 로컬 환경에서 복호화를 수행할 수 있어, 보안성과 사용자 편의성을 동시에 확보할 수 있다.

향후 연구에서는 PDF를 비롯한 다양한 문서 포맷에 대한 호환성을 지원하고, 접근 권한 설정 인터페이스를 보다 직관적이고 정교하게 개선함으로써, 사용자 경험을 중심으로 한 보안 시스템으로의 확장이 가능할 것이다.

Acknowledgement

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 인공지능융합혁신인재양성사업 (IITP-2023-RS-2023-00256629) 및 한국인터넷진흥원(KISA)-정보보안 특성화대학 지원사업의 지원을 받아 수행된 연구임

참고문헌

[1] J. Daemen and V. Rijmen, AES Proposal: Rijndael. *National Institute of Standards and Technology*, 1999.

[2] D. Park, “Social Life of PKI: Sociotechnical Development of Korean Public-Key Infrastructure,” *IEEE Annals of the History of Computing*, vol. 37, no. 2, pp. 59 - 71, 2015.

[3] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” *SIAM J. Comput.*, vol. 32, no. 3, pp. 586 - 615, 2003.