하이브리드 암호화 방식을 활용한 이미지 보안 알고리즘 설계

김지성 · 장시웅

동의대학교

Design of Image Security Algorithms Using Hybrid Encryption

Ji-Seong Kim · Si-Woong Jang

Dong-Eui University

E-mail : sss4375@naver.com , swjang@deu.ac.kr

요 약

인터넷이 발전하게 되면서 여러 가지 정보들을 메일, 메시지 등을 이용하여 주고받기 시작하였다. 여러 가지 정보들에는 이미지도 포함되는데, 중요한 신상정보나 설계도, 계약서 등의 정보들도 이미지 파일로 주고받는 경우가 생기게 되면서 이 이미지가 실수 또는 해킹 등의 이유로 유출되게 되었을 시 생기는 문제들이 점점 커져가고 있는 상황이다. 이미지를 주고받을 때도 유출을 방지하기 위한 여러 가지 보안방법들이 중요해지고 있다.

본 논문에서는 이미지를 암호화할 수 있게 해주고 암호화를 할 때 사용한 키를 한번 더 암호화 하는 알고리즘을 설계하였다. 기존의 암호화 방식에서 AES 암호화만 이용할 대칭키가 유출될 경우 본래의 데이터도 유출되게 된다. 본 논문에서는 이러한 문제를 방지하기 위해 암호화에 사용된 대칭키를 한번 더 암호화하는 방법을 제안한다. 선택한 원본 이미지 파일의 데이터를 텍스트 데이터로 변환한 후 AES-256암호화를 이용하여 대칭키 암호를 사용자가 설정할 수 있게 하고 그 대칭키 암호를 이용하여 암호화한다. 이때 32바이트 길이의 대칭키를 사용하는데, 대칭키의 유출을 방지하기 위해 RSA 암호화를 이용, 비대칭키를 생성한 후 대칭키를 한번 더 암호화 한다. 암호화된 대칭키는 비대칭키를 이용 복호화할 수 있고, 암호화된 데이터는 대칭키 암호를 이용해서 원래의 데이터로 복호화가 가능하다. 이러한 방법을 사용하여 보안강도를 더 높일 수 있다.

키워드

AES 암호화, RAS암호화, 이미지 보안, 대칭키 암호, 비대칭 키 암호

I. 서 론

인터넷이 발전하게 되면서 계약서나 도면, 개인정보 등의 중요한 정보를 이미지에 담아 메일이나 메시지 등의 인터넷을 이용한 방법으로 주고받게 되면서 이미지의 보안이 중요해 지고 있다.

이러한 중요한 정보들을 이미지 파일형식으로 주고받거나 여러 가지 저장 장치에 저장된 상태로 보관되는데 이 이미지가 해킹 또는 보안사고 등의 문제로 유출되게 된다면 아주 큰 피해를 불러일으킬 수도 있게 되었다. 그러므로 이미지 데이터도 여러 가지 방법으로 보안하는 것에 유의하여야 한다.

데이터 보안에는 여러 가지 방법이 있는데 본 논문에서는 AES 암호화 알고리즘과 RSA 암호화 알고리즘을 사용한다. 이미지 데이터에도 이 두 가지 알고리즘을 적용 가능한데, 이 두 가지 암호화 알고리즘을 모두 사용하여 이미지를 보안하는 방법을 본 논문에서 제안한다.

대칭키 암호화 방식인 AES 암호화로 이미지 데이터를 대칭키를 이용, 암호화 한다. 암호화 할 때 사용한 대칭키가 유출된다면 암호화된 이미지 데이터를 본래의 이미지 데이터로 복호화하는 것도 가능하기 때문에 암호화에 사용 한 대칭키를 RSA 암호화 알고리즘을 통해 한번 더 암호화 한다. 이러한 두 번의 암호화 알고리즘을 사용함으로써 보안수준을 더 높일 수 있다

II. 관련 연구

2.1. AES 암호화 알고리즘

AES 란 <Advanced Encryption Standard> 의 줄임말로 J.Daemen과 V.Rijmen에 의해 제안된 “Rijndael”(레인달) 암호 알고리즘을 미국 표준 기술 연구소에 의해 제정된 국제 표준 대칭키 암호화 알고리즘이다[1]. 대칭키 알고리즘은 암호화 키와 복호화 키가 다른 비대칭 키와는 달리 암호

화 키와 복호화 키가 동일하다. 비대칭키 보다 키 분배가 여렵지만, 암호화 강도가 우수한 편이고, 연산량이 적으며 암호화와 복호화하는 시간이 빠르다는 장점이 있다. 대칭키 암호화 알고리즘에 대한 그림은 그림 1과 같다.

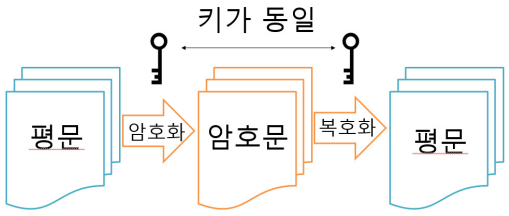

그림 1. 대칭키 암호화 알고리즘 (키가 동일함).

AES는 이론적으로 키의 크기는 제한이 없으나 기본적으로 길이가 128, 192, 256비트인 키를 사용하며 각각 10라운드, 12라운드, 14라운드로 설계되어 있다. 암호화 강도는 키의 크기에 비례하며, AES-128을 초당 256 bits의 연산능력을 가진 장치로 브루트-포스(Brute-Force)공격을 할 경우, 약 149 X 10^{12} 년의 시간이 소요되며, 최고 강도인 AES-256는 약 509 X 10^{50} 년의 시간이 소요된다. 하지만 AES-128에 대한 여러 가지 분석과 연구가 진행되어왔기 때문에, 암호화-복호화 시스템 자체를 공격한 사례도 있다. 그러므로 중요 정보일수록 높은 강도인 AES-128 이나 AES-256을 사용하는 것이 더 좋다[2]. AES 암호화 알고리즘의 종류에 따른 키,블록 길이와 라운드 수는 표 1과 같다.

표 1. AES 강도에 따른 길이와 수

	키 길이 (bits)	블록길이 (bits)	라운드 수
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

2.2. RSA 암호화 알고리즘

RSA는 공개키 암호화 시스템의 하나로 Rivest, Shamir, Adleman의 발명자 이름 첫글자를 따서 RSA가 되었다. 이 암호화 알고리즘은 큰 숫자를 소인수 분해 하는 것이 어렵다는 것에 기반을 두고 있다[3]. RSA 는 두 개의 키를 사용하는데 일반적인 공개키 알고리즘의 공개키(public key) 는 모두에게 알려져 있고 메시지를 암호화하는데 쓰이며, 암호화된 메시지는 개인키(private key)를 가진 자만이 복호화하여 열어볼 수 있다. 하지만 RSA 공개키 알고리즘은 이러한 제약조건 없이, 개인키로 암호화 하고 공개키로 복호화 할 수 있다는 점이 자유롭다. RSA 알고리즘의 암호화, 복호화에 사용되는 공개키 N과 e, 개인키d의 생성 과정은 다음과 같다.

p와 q라는 두 개의 서로 다른 소수를 고른 뒤
1. 두 수를 곱하여 N = p · q를 구한다.
2. Φ(N) = (p-1) · (q-1)을 구한다.
3. 1 < e < Φ(N) 인 정수 e를 찾는다.
   (e와 Φ(N)d은 서로소)
4. d · e를 한뒤 Φ(N)로 나눈 나머지가 1이 되는 d를 구한다. [4]

이렇게 생성된 키로 RSA 암호화, 복호화 연산은 각각 식 (1), 식 (2)와 같이 표현된다.

(1) $C = M^e \bmod N$
(2) $M = C^d \bmod N$

RSA 암호화 알고리즘은 AES와 달리 비대칭키인데 공개키 또는 개인키 둘 다 암호화에 쓰일 수 있고 이 경우 암호화에 쓰이지 않은 개인키 또는 공개키가 복호화 키로 쓰이게 된다. 비대칭키의 암호화 알고리즘은 그림 2와 같다.

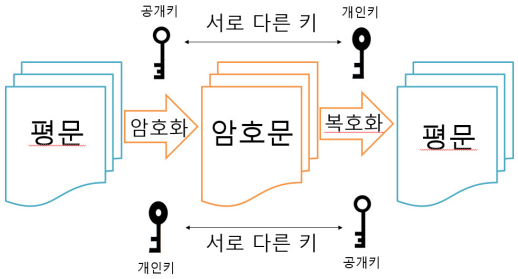

그림 2. 비대칭키 암호화 알고리즘 (키가 동일하지 않음).

III. 하이브리드 보안 알고리즘 설계

3.1. 이미지 보안 암호화 개요

이미지의 보안 강도를 높이기 위해 두가지의 알고리즘을 사용하는 것을 제안한다. 한가지 AES 보안 알고리즘만 사용했을 경우 대칭 키 암호가 유출 될 경우 바로 이미지의 보안이 깨지게 된다. 그렇기 때문에 그점을 보안하기 위해 AES 알고리즘으로 암호화 할 때 사용한 대칭키 값을 RSA 알고리즘으로 한번 더 암호화함으로써 보안 강도를 높이는 것이다. 암호화 과정은 그림 3과 같다.

3.2. 이미지 보안 복호화 개요

그림 3과 같이 원본 데이터를 암호화할 때 사용한 대칭키 값을 한번 더 암호화 하여서 대칭키 값도 암호문으로 만들기 때문에 보안 강도가 강해지고 복호화 과정도 어려워진다. 복호화 과정은 암호문으로 되어 있는 대칭키 값을 복호화한 후 그 대칭키 값으로 암호화된 원본 데이터를 원본 데이터로 복호화 하여야 한다. 암호화된 대칭키 값의 복호화는 그림 4와 같다.

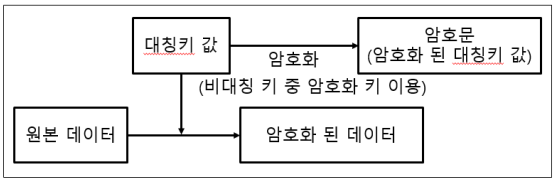

그림 3. 암호화 과정.

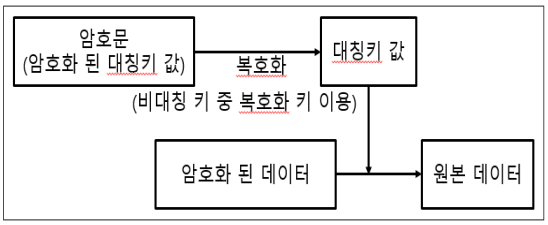

그림 4. 복호화 과정.

IV. 알고리즘 구동 및 테스트

4.1. 이미지 보안 알고리즘 암호화 구동 테스트

실제 이미지 데이터를 AES 암호화 알고리즘으로 암호화한 뒤 사용한 대칭키를 RSA 알고리즘을 이용해 암호화해 보았다. 그림 5는 암호화 과정이다.

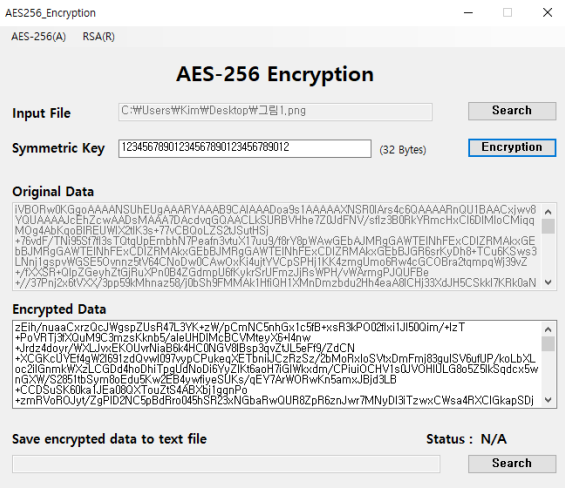

그림 5. AES 이용 이미지 암호화.

여기서 암호화에 사용한 대칭키를 RSA를 이용해 암호화한다. 과정은 그림 6과 같다.

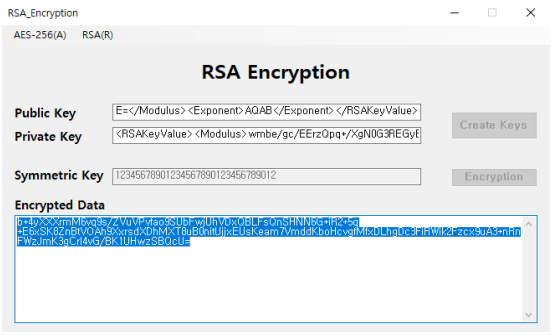

그림 6 대칭키 암호화.

RSA 알고리즘에서 생성한 공개키와 개인키 중 공개키를 이용하여 암호화하였다. 이로써 원본 데이터와 암호화에 쓰인 대칭키 모두 암호화가 되었다.

4.2. 이미지 보안 알고리즘 복호화 구동 테스트

앞서 암호화한 원본 데이터와 대칭키를 다시 평문으로 복호화해 보겠다. 먼저 공개키를 이용해서 암호화하였기 때문에 개인키를 이용해서 대칭키를 먼저 복호화한다. 과정은 그림 7과 같다.

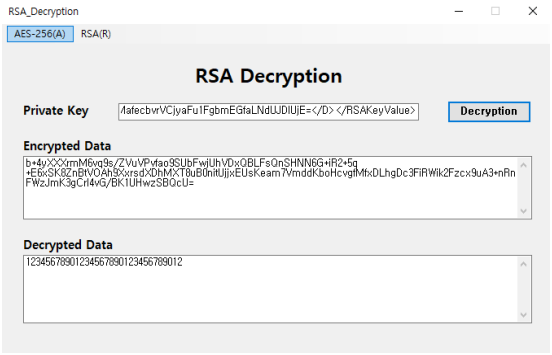

그림 7. 개인키를 이용한 대칭키 복호화.

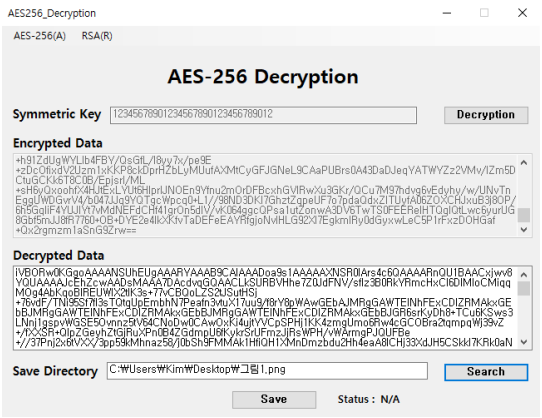

그림 8. 대칭키를 이용한 이미지 데이터 복호화.

이미지 데이터 암호화에 쓰인 대칭 키가 다시 평문으로 복호화된 것을 볼 수 있다. 다음은 복호

화된 대칭 키를 이용해서 암호화되어있는 이미지 데이터를 다시 평문으로 복호화 한다. 과정은 그림 8과 같다.

대칭 키를 이용하여 암호화되어 있던 이미지 데이터를 평문으로 복호화 한 것을 볼 수 있다.

V. 결 론

본 논문에서는 이미지 데이터를 AES와 RSA 두가지 암호화 알고리즘을 이용하여 암호화 하는 암호화 알고리즘을 설계하였다. 이미지 데이터를 AES 암호화 알고리즘을 이용해 한번 이때 사용한 대칭키를 RSA 알고리즘을 통해 한번 총 두 번의 암호화를 통해 한 가지 보안 알고리즘으로 보안하는 것보다 강한 보안강도를 가진 암호화 방법을 가지게 되었다.

ACKNOWLEDGEMENT

이 논문은 과학기술정보통신부 및 정보통신산업진흥원의 재원으로 ICT융합 Industry4.0s(조선해양) 사업의 지원을 받아 수행된 연구임(No. ITAS060618011146000100040020O)

참고문헌

[1] 박중오, 오기욱, “멀티프로세서 기반의 병렬 AES 암호 알고리즘에 관한 연구,” 한국컴퓨터정보학회, Vol.17, No.1, p.171~181, 2012.1

[2] 성동욱, 유재수, 김동주, 박준호, “무선 센서 네트워크에서의 에너지 효율적인 차등 AES 암호화 기법,” 한국정보과학회, Vol.27, No.3, p.115~130, 2011.11

[3] 허석원, 김문경, 이용석, “내장형 시스템을 위한 최적화된 RSA 암호화 프로세서 설계, ”한국통신학회, Vol.29, No.4A, p.447~457, 2004.4

[4] 조욱래, 신경욱, “CIOS 몽고메리 모듈러 곱셈 알고리즘 기반 Scalable RSA 공개키 암호 프로세서,” 한국정보통신학회논문지, Vol.22, No.1, p.100~108, 2017. 12