루빅스 큐브를 이용한 에너지 데이터 암호화 알고리즘

김태혁, 나의균, 이은규
인천대학교 정보통신공학과
e-mail : eklee@inu.ac.kr

Three-Step Encryption Algorithm of Energy Image Data using Rubik's Cube Principle

Taehyuk Kim, Ui-Kyun Na, and Eun-Kyu Lee
*Dept. of Information and Telecommunication Engineering, Incheon National University

요 약

사물인터넷 기술이 에너지 분야에 이미지 데이터가 사용되면서 데이터 보안과 프라이버시에 대한 문제가 점차 커지고 있다. 이미지 데이터는 일반적인 텍스트 데이터와는 달리 가로, 세로 그리고 대각선의 인접한 픽셀 정보들이 강한 연관성과 상관성을 가지기 때문에, 기존에 사용되었던 암호화 알고리즘과는 다른 기술이 사용되어야 한다. 본 논문에서는 이미지의 직관성과 인접 픽셀 간의 강한 연관성을 제거하기 위해 루빅스 큐브 방식을 활용하는 암호화 알고리즘을 제안한다. 제안된 알고리즘을 구현하고, 널리 사용되는 암호화 알고리즘들과의 비교 실험을 통해 제안된 알고리즘이 선택적 평문 공격에 대해 강성을 갖는다는 것을 보인다.

1. 스마트 그리드 개요

스마트 그리드는 기존의 노후화된 전력망에 정보통신 기술을 접목함으로써, 에너지 관련 장비가 상호 통신을 하고, 지능적으로 동작할 수 있도록 한다. 최근에는 사물인터넷 기술이 적용되어 수많은 에너지 기기에 임베디드 시스템이 내장되어 에너지 관련 데이터가 실시간으로 수집된다. 에너지 데이터는 사람이 거주하거나 활동하는 공간으로부터 취합될 수 있는데, 데이터의 방대한 양으로 인해, 간단한 에너지 데이터 분석만으로도 그 공간 거주자의 활동에 대한 내용을 높을 확률로 알아낼 수 있다. 즉, 프라이버시 문제를 발생시킨다. 이러한 에너지 데이터가 이미지 데이터와 연계될 때에는 더욱 심각한 보안 문제를 발생시킨다. 이러한 보안 문제를 줄이기 위한 방법중의 하나로써, 에너지 이미지 데이터를 암호화하는 기술이 사용될 수 있다.

이미지 데이터는 일반적인 텍스트 데이터와 다른 특징을 가지기 때문에, 기존에 사용되었던 암호화 알고리즘과는 다른 기술이 사용되어야 한다. 이미지 데이터는 기존의 텍스트 데이터와 비교하여 직관적으로 가독이 가능한 정보를 가진다. 또한, 데이터 사이즈가 더 크기 때문에 암호화 및 복호화 과정에서 많은 계산 처리가 필요하며 이로 인해 처리시간 길어진다.

이미지 데이터가 갖는 중요한 특징은 이미지 데이터내에서 가로, 세로 그리고 대각선의 인접한 픽셀 정보들이 강한 연관성과 상관성을 가진다는 것이다. 이로 선택적 평문 공격에 취약성을 갖는다. ECB (Electronic Code Book) 모드를 사용하는 대부분의 암호 알고리즘이 이러한 문제를 노출하고 있어 평문 이미지 추측이 가능하다. 이러한 문제를 해결하기 위해 CBC (Cipher Block Chaining) 모드나 CFB (Cipher FeedBack) 모드를 사용할 수 있는데, 블록 단위로 암호화된 정보가 다음 블록 암호화 과정에 참조가 되기 때문에 계산량이 많이 증가하는 단점을 갖는다 [1, 4].

본 논문에서는 이미지의 직관성과 인접 픽셀 간의 강한 연관성으로 인한 선택적 평문 공격에 대해 강성을 갖는 이미지 암호화/복호화 알고리즘을 제안한다. 본 논문에서 제안하는 알고리즘은 기존의 암호화 알고리즘 대신에 루빅스 큐브를 활용한 이미지 암호화 기법을 이용한다. 또한, 선택적 평문 공격에 대해 강성을 갖을 수 있도록 3 단계의 암호화 과정을 거치는 것을 특징으로 한다.

본 논문에서는 제안된 알고리즘을 구현하고, 제안된 알고리즘이 선택적 평문 공격에 대해 강성을 갖는다는 것을 보이기 위해 실험을 수행한다. 실험에서는 비교군으로 기존에 널리 사용되는 DES (Data Encryption Standard), AES (Advanced Encryption Standard)를 사용하며, 4 가지 형태의 이미지 데이터를 사용한다. 세가지 알고리즘을 사용하여 이미지 데이터가 암호화 되었을 때 데이터의 픽셀변화율을 조사함으로써 강성의 정도를 비교하고 검증한다.

2. 루빅스 큐브

루빅스 큐브(Rubik's Cube)는 퍼즐의 일종으로, 보통 작은 여러 개의 정육면체가 모여 만들어진 하나의 큰 정육면체 형태이며, 각 방향으로 돌아가게끔 만들어져서 흩어진 각 면의 색깔을 같은 색깔로 맞추는 퍼즐이다. 이 큐브를 한 번 흐트려 놓으면 특별한 공

식을 알기 전에는 인간의 감각으로는 다시 맞추기는 매우 어렵다. 간단해 보이는 큐브는 실제로 만들 수 있는 모양이 무려 43252003274489856000 가지나 있다. 가장 일반적인 3×3×3 형태의 큐브부터 피라미드 모양의 피라밍크스 등으로 다양하게 진화하고 있다. 루빅스 큐브는 암호화 알고리즘에 사용되고 있다 [2, 3]. 기존의 연구는 큐브를 회전시키는 알고리즘에 집중하거나, 비트 값을 XOR 하는 방법에 대해 논의한다. 이에 반해 본 논문에서는 키큐브를 사용하는 방법과 XOR 비트 연산을 포함한 3 단계의 과정 새롭게 제안한다. 페이지 제한으로 인해 자세한 성능 비교는 향후에 발표할 기술 문서에 넣을 예정이다.

3. 3 단계 루빅스 큐브기반 암호화 알고리즘

본 논문에서는 제안 암호화 알고리즘은 5×5×5 루빅스 큐브를 사용하며, 다음과 같은 3 단계로 나누어 수행된다. 알고리즘의 설명을 위해 그림 1 과 같은 Lenna 이미지를 사용한다.

(A) 키(Key) 큐브 : 사용자로부터 키 값을 입력받아 XOR 큐브를 만들고 회전 방식을 결정하는데 사용된다.
(B) 1 차 큐브 암호화 : 원본 이미지의 모든 픽셀을 하나의 5×5×5 큐브에 넣어 섞어준다.
(C) 2 차 큐브 암호화 : 1 차 큐브 암호화된 이미지의 모든 픽셀을 여러 개의 5×5×5 큐브에 넣어 섞어 준다.
(D) XOR 큐브 암호화 : 2 차 큐브 암호화된 이미지의 픽셀 값을 변경해 준다.

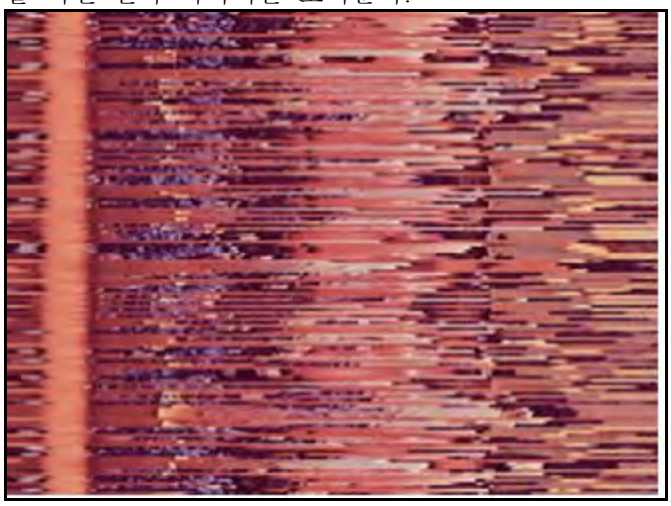
(그림 1) Lenna 이미지.

키(Key) 큐브

첫 번째 과정은 사용자가 키 값을 입력하였을 때 수행하는 키 큐브이다. 키 큐브는 회전 방식을 결정하며 XOR 큐브를 만들 때 사용한다. 사용자가 키 값을 입력하면 한 개의 작은 면에 두 개씩 값이 입력된다. 키 값이 큐브의 150 개의 작은 면을 채우지 못하면 같은 키 값이 반복적으로 작은 면에 입력된다.

1 차 큐브 암호화

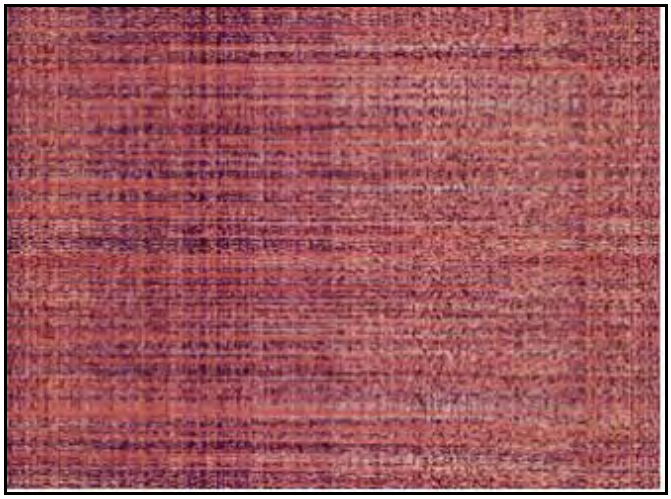
1 차 큐브 암호화는 이미지를 전체적으로 섞어주는 역할을 한다. 1 차 큐브 암호화에서는 하나의 이미지가 150 개로 나누어진다. 나누는 방식은 이미지의 좌측 상단을 시작으로 차례대로 나누어진다. 이렇게 나누어진 이미지는 큐브의 작은 면에 각각 하나씩 입력되어 하나의 큐브가 만들어진다. 이렇게 만들어진 큐브는 키(Key) 큐브에서 결정된 회전 방식대로 회전한다. 그림 2 는 원본 이미지로 1 차 큐브 암호화 과정을 거친 결과 이미지를 보여준다.



(그림 2) 1 차 큐브 암호화된 이미지.

2 차 큐브 암호화

2 차 큐브 암호화는 1 차 큐브에서 섞인 전체적으로 섞인 이미지를 작게 나누어 다시 섞어준다. 1 차 큐브에서 큐브의 작은 면에 여러 개의 픽셀이 입력되었지만 2 차 큐브에서는 작은 면 하나에 하나의 픽셀만이 입력된다. 그러므로 여러 개의 큐브가 생성된다. 이 후에 키(Key) 큐브에서 결정된 회전 방식대로 회전한다. 그림 3 는 2 차 큐브 암호화 과정을 거친 결과 이미지를 보여준다.

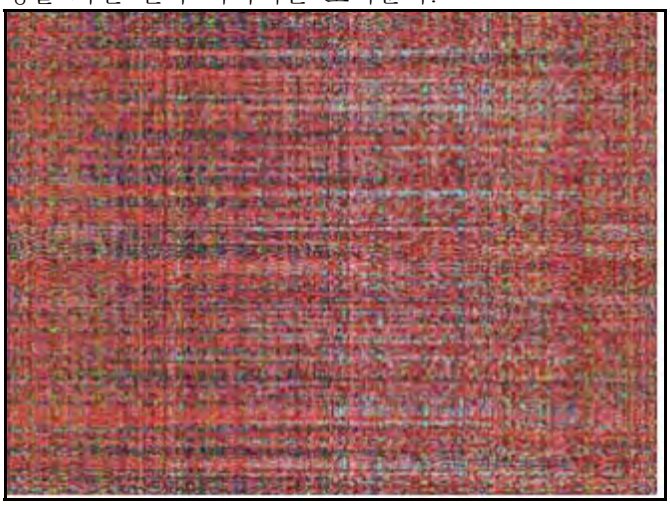


(그림 3) 2 차 큐브 암호화된 이미지.

XOR 큐브 암호화

2 차 큐브 암호화를 거친 이미지는 픽셀의 위치는 바뀌었지만 픽셀의 값은 변하지 않았다. XOR 큐브는

이미지의 픽셀 값을 변경해 준다. XOR 큐브는 키(Key) 큐브로부터 만들어진다. 키(Key) 큐브는 작은 면에 두 개의 값이 입력되어 있는데 두 개의 값은 XOR 연산이 되어 한 개의 작은 면에 한 개의 값만 갖게 된다. 이 후에 키(Key) 큐브에서 결정된 회전 방식대로 XOR 큐브를 회전한다. 2 차 큐브 암호화된 이미지의 픽셀 값과 XOR 큐브는 XOR 연산을 하여 픽셀 값을 변경시킨다. 그림 4 는 XOR 큐브 암호화 과정을 거친 결과 이미지를 보여준다.



(그림 4) XOR 큐브 암호화된 이미지.

4. 실험 및 결과

본 논문에서 제안하는 알고리즘이 선택적 평문 공격에 강성을 갖는다는 보이기 위해 제안 알고리즘을 구현하였으며, DES, AES 와의 비교 실험을 진행한다. 실험에는 윈도우 7 로 동작하는 Intel Core i7 2.30GHz 시스템을 사용하며, 알고리즘은 Visual C++로 구현되었다. 성능 비교를 위해 <사람>, <강>, <도시>, <도면>과 같은 4 종류의 서로 다른 이미지 데이터를 사용한다. 이들은 BMP 형태이며 픽셀 사이즈는 400 x 300 으로 모두 동일하다.

선택적 평문 공격은 평문을 선택하고 작은 부분을 변화를 주어 암호화된 이미지를 분석한다. 분석된 데이터를 통하여 평문과 암호화된 이미지와 의미 있는 연관성을 분석하는 공격법이다. 선택적 평문 공격에 대한 강성을 측정하기 위해서는 평문과 암호화된 이미지 데이터의 픽셀 차이점을 분석하는 NPCR (Number of Pixel Change Rate) 분석법을 사용한다. NPCR 은 평문과 암호화된 이미지 사이에 같은 위치에 픽셀이 다른 정도를 측정하여 퍼센트로 표현한다.

<표 1> <사람> 이미지 데이터를 사용할 때의 실험 결과

구분	NPCR 값
제안 기법	99.99833333
DES_CBC	99.63862100
DES_ECB	99.60681332
AES_CBC	99.60995998

표 1 에서는 <사람> 이미지 데이터를 대상으로 제안 기법 암호화, DES 그리고 AES 에 대하여 NPCR 을 비교한 것이다. 이 표에서 확인할 수 있는 것은 본 논문에서 제안한 기법이 암호화 강성이 입증된 DES, AES 와 비교하여 더 높은 강성을 보이는 것을 확인할 수 있다. 제안 기법은 99.99833333 의 수치를 보였는데 이는 가로 400, 세로 300 인 이미지에서 120000 개의 픽셀 중 200 개의 픽셀만이 변화하지 않는다는 것을 의미한다. AES_CBC 는 99.60995998 의 수치를 보였는데 이는 가로 400, 세로 300 인 이미지에서 120000 개의 픽셀 중 470 개의 픽셀이 변화하지 않는 것을 의미한다. 제안 기법으로 DES, AES 보다 선택적 평문 공격에 강성을 가질 수 있음을 보인다.

4 종류의 이미지 데이터를 제안 기법으로 암호화한 이미지 데이터의 NPCR 값은 다음과 같다. NPCR 은 최소 99.83583333 의 수치를 나타냈다. <도면> 이미지가 나머지 이미지보다 비교적 낮은 수치를 보인다. 그 이유는 도면 이미지에서 다양한 색상이 사용되지 않기 때문이다. 모든 이미지의 NPCR 은 보장 강성 수치(99.6)이상을 보여주었다.

5. 결론

본 논문에서는 에너지 IT 분야에서 사용되는 이미지 데이터를 3 단계 큐브를 이용하여 암호화하는 알고리즘을 제안하였다. 구현을 통하여 3 단계 암호화 과정이 가능함을 보였다. 그리고 실험결과를 통해 기존에 강성이 입증된 DES, AES 보다 선택적 평문 공격에 대한 강성이 향상됨을 보였다. 본 논문에서는 이미지 암호화를 하는데 걸리는 시간에 대한 고려를 하지 않았다. 제안 기법의 선택적 평문 공격에 대한 강성을 유지하며 보다 경량화 되고 빠른 이미지 암호화 기법에 대해 향후 연구하고자 한다.

Acknowledgement

본 연구는 2016 년도 산업통상자원부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구과제입니다. (20162010103900) 교신저자는 이은규.

참고문헌

[1] Guan, Z. H., Huang, F., & Guan, W. (2005). Chaos-based image encryption algorithm. Physics Letters A, 346(1), 153-157.

[2] Shen, J., Jin, X., & Zhou, C. (2005). A color image encryption algorithm based on magic cube transformation and modular arithmetic operation. In Advances in Multimedia Information Processing-PCM 2005 (pp. 270-280). Springer Berlin Heidelberg.

[3] Loukhaoukha, K., Chouinard, J. Y., & Berdai, A. (2012). A secure image encryption algorithm based on Rubik's cube principle. journal of electrical and computer engineering, 2012, 7.

[4] 정장영(2015), “클라우드 환경에서 초 고해상도 이미지 기밀성을 위한 2 단계 이미지 암호화 기법”, 동국대학교 박사학위 논문