3-D 카오스 맵 기반의 컬러 이미지 암호화†

이상윤*, 조용득*, 박연주*, 최언숙*
*동명대학교 정보통신공학과
e-mail : amayun707@gmail.com

Color Image Encryption Based on 3-D Chaotic Map

Sang-Yun Lee*, Yeon-Ju Park*, Yong-Deuk Cho*, Un-Sook Choi*
Dept of Information & Communications Engineering, Tongmyong Univ.

1. 연구 필요성 및 문제점

네트워크 통신, 멀티미디어와 클라우드 컴퓨팅 기술의 급속한 발달에 따라 이미지는 인터넷 상에서 전송되고, 간행될 뿐만 아니라 아마존 S3와 같은 서드파티에 저장될 수 있다. 이러한 환경에서 불법 복제나 불법 배포로부터 영상을 보호하는 것은 중요한 문제가 되었다. 암호화는 정보를 보호하는 한 기법이다. 그러나 기존에 알려진 AES, DES 등과 같은 고전적인 암호화 기술은 이미지를 암호화하는데 적합하지 못하다[1]. 이는 대용량, 강한 상관관계, 높은 중복도 등 이미지가 가지고 있는 특성 때문이다.

본 논문에서는 셀룰라 오토마타와 3차원 카오스 맵 기반의 영상암호 알고리즘을 제안한다. 또한 몇 가지의 실험을 통해 제안한 영상암호 알고리즘의 안전성을 검증한다.

2. 연구내용과 방법

셀룰라 오토마타(Cellular Automata, 이하 CA)는 역동성과 랜덤성이 뛰어나서 의사 난수열 생성기로 잘 알려져 있다[2]. 특히 가장 긴 주기를 갖는 가역 CA는 복잡하고, 견고한 이미지 암호 시스템을 구축하는 데 적합하다. 암호 시스템의 키공간을 효과적으로 늘이기 위해 5-이웃 최대길이 CA를 사용하여 키이미지를 생성한다. 최대 길이 CA를 이용하여 생성된 키이미지와 원이미지를 XOR연산하여 원이미지의 픽셀 값을 예측할 수 없는 값으로 바꾼다. 다음 단계에서 Chen 등[3]에 의해 제안된 3-D 카오스 캣 맵을 사용하여 이미지의 픽셀 값을 효과적으로 분산시킨다. 이 과정은 컬러 이미지를 적당한 크기의 큐브로 구성한 후 3-D 카오스 캣 맵을 사용하여 픽셀의 위치를 뒤섞은 다음 다시 컬러 이미지의 크기로 변환한다. 그림 1은 제안하는 이미지 암호 시스템의 개념도이다.

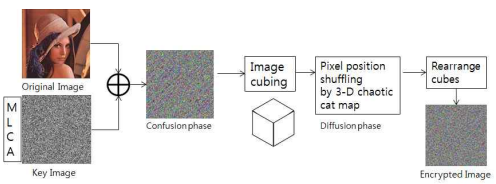

그림 1. 컬러 이미지 암호시스템의 개념도

3. 보안 및 성능 분석

제안된 암호시스템 구현과 안전성 검증을 위한 테스트는 Python 3.7 프로그램으로 작성하였다. 그림 2는 원 이미지와 암호화된 이미지의 히스토그램 분석 및 상관관계 분석을 나타낸다. 그림 2의 (a)와 (b)는 원이미지와 암호화 된 이미지의 히스토그램을 R, G, B 채널에 대하여 나타낸 것이다. 히스토그램 분석 결과 암호화 된 이미지의 픽셀 값은 거의 균등하게 나타나므로 통계적 공격에 안전하다. 그림 2의 (c)와 (d)는 원이미지와 암호화 된 이미지에 대한 R채널에 대하여 수평 방향의 인접한 셀 간의 상관관계를 나타낸다. 상관관계 분석에 의하면 암호화된 이미지는 원래 이미지가 가지고 있는 강한 상관관계가 전혀 나타나지 않음을 볼 수 있다. 따라서 제안된 컬러이미지 암호알고리즘은 안전하다.

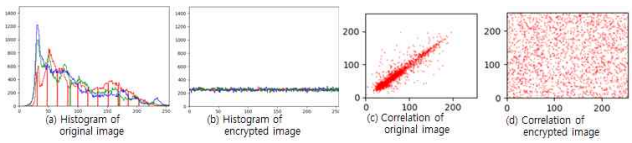

그림 2. 히스토그램 및 상관관계 분석

4. 결론 및 향후 연구

본 논문에서는 5-이웃 최대 길이 CA와 3-D 카오스 캣 맵을 이용한 컬러 이미지 암호알고리즘을 제안하였다. 향후 제안된 방법에 대한 안전성 검증을 위해 다양한 통계적 테스트 및 키공간 분석을 하고자 한다.

† 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음 (No. 1711081052).

참고문헌

[1] X. Wang, L. Teng and X. Qin, “A novel color imge encryption algorithm based on chaos,” Signal Processing, vol. 92, 2012, pp. 1101 - 1108.

[2] S.J. Cho, U.S. Choi, et al., “New synthesis of one-dimensional 90/150 linear hybrid group cellular automata,” IEEE Trans. Comput-Aided Design Integr. Circuits Syst., vol. 26, no. 9, 2007, pp. 1720 - 1724.

[3] G. Chen, Y. Mao and C.K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” Chaos, Solitons and Fractals, vol. 21, no.3, 2004, pp. 749 - 761.