광 상관기와 반복 알고리듬을 이용한 영상 암호화 및 복호화 시스템

Image Encryption and Decryption System using Optical Correlator and Iterative Algorithm

김철수, 조창섭
경주대학교 컴퓨터전자공학부
kimcs@gyeongju.ac.kr

1. 서론

현대 정보화 사회에서는 컴퓨터 시스템 및 통신 시스템의 결합으로 시공간을 초월하여 엄청난 양의 정보교환이 신속히 이루어지고 다양한 형태의 서비스 환경이 창출되어 사회 전반에 걸쳐 빠르게 확산됨에 따라 경제, 사회 등 전 분야에 큰 변화를 일으키고 있다. 이러한 사회는 우리생활을 보다 편리하게 만들어 주고 있지만 때로는 정보의 유출로 인한 막대한 피해를 주기도 하여서 정보보호가 매우 중요한 문제로 대두된다. 특히 정보의 공유와 개방을 목표로 개발된 인터넷으로 인해 통신선로를 통한 정보에의 불법 침입이 새로운 사회적·법적 문제로 대두되고 있다. 또한 정보화 진전에 따라 개인의 정보와 신용이 중요시되고, 인터넷을 통한 상품구매, 의료비 결재를 위한 스마트 카드 보급계획, 여권, 신용카드, 은행카드 등과 같은 개인의 신원을 증명할 수 있는 신분증의 사용이 늘어나고 있다. 그러나 프린터, 스캐너, 복사기, 컴퓨터 관련 장치들과 각종 소프트웨어 기술의 발달로 인해 화폐, 각종 신용카드뿐만 아니라 컴퓨터 칩과 같은 제조품의 위조 및 복제기술의 수준이 높아져 국내외적으로 이로 인한 피해액이 년간 수십 억 달러에 이르고 있는 실정이다. 이에 따라 최첨단 컴퓨터, 디지털 및 광학 기술들을 이용하여 위조 방지 시스템에 관한 연구가 전세계적으로 활발히 이루어지고 있지만 위조 및 복제 기술을 훨씬 능가하는 완벽한 보완시스템은 개발되지 않고 있다. 그러므로 위조나 복제에 대한 방지 기술은 반드시 연구, 개발되어야 한다.

광은 고유의 병렬성과 고속성을 가지므로 많은 양의 정보를 처리할 수 있고, 정보를 표현할 수 있는 방법이 다양하여 기존의 광 세기 검출기를 이용하더라도 복제할 수 없는 특징이 있으므로 개인의 신원을 인증하는 보안시스템 구현에 많이 이용되고 있다.

광을 이용한 기존의 암호화 및 복호화 시스템에는 Refregier 등이 제안한 두 개의 랜덤 위상 마스크를 이용하는 방법[(1)], Mach-Zehnder 간섭계를 이용하는 방법[(2)], 그리고 결합변환 상관기를 이용하는 방법[(3)] 등이 있으며, 최근에는 실제로 구현하여 상용화할 수 있는 방향으로 많은 연구가 진행되고 있는 추세이다.

본 논문에서는 실제 광 보안시스템의 구현을 위해 광 상관기와 반복 알고리듬을 이용하여 이진 및 명암도 영상의 암호화 및 키 영상 정보를 이진값으로 생성하는 방법을 제안하였으며, 컴퓨터 시뮬레이션을 통해 그 타당성을 확인하였다.

2. 제안된 방법

기존의 광학적 암호화 시스템에서의 문제점은 여러 방법을 통해 암호화된 영상과 암호화된 영상을 해독할 때 사용되는 키 영상 정보가 복소값 또는 연속하는 실수값을 가진다는 것과 이를 정확하게 표현할 수 있는 장치의 개발에 어려움이 있다. 본 연구에서는 이진 및 명암도 영상을 암호화하고, 해독에 필요한 키 영상 정보를 랜덤한 이진값으로 표현하여 실제 보안 시스템의 구현이 가능하도록 하기 위해 4-f 광 상관 시스템과 SA(simulated annealing) 알고리듬을 이용하였다.

영상의 암호화 과정은 다음과 같다. 먼저 영상의 암호화를 위해 먼저 '1'(e^{j0})과 '-1'($e^{j\pi}$)로 구성되는 이진 랜덤 패턴을 공간영역(x,y)과 주파수 영역(u,v)에서 생성하고, 이를 E(x,y) 및 K(u,v)라 한다. E(x,y)를 4-f 상관기의 입력정보, K(u,v)를 필터정보로 생각하고, 두 정보의 상관을 구한다. 이 상관값과 암호화할 원영상과의 평균자승오차를 구하고, 이를 비용함수라 한다. 필터정보 K(u,v)의 각 화소값이 '1'이면 '-1'로 '-1'이면 '1'로 변환환 후 다시 비용함수를 구한 후 비용함수가 변환전의 값에 비해 감소하면 변환을 받아들이고, 증가하더라도 볼쯔만 확률분포에 근거하여 조건부 수용을 하는 SA 알고리듬을 이용한다. 이와 같은 과정을 필터정보의 모든 화소에 대해 반복수행하고, 다시 반복횟수 만큼 수행하면 원영상에 가까운 상관값을 구할 수 있다. 이때 E(x,y)를 원영상의 암호화된 영상, K(u,v)를 암호화된 영상의 해독에 필요한 키 영상으로 한다. 두 영상정보는 랜덤한 이진 값이므로 구현하기 쉬울뿐만 아니라 원영상에 대한 정보가 전혀 포함되어 있지 않다.

영상의 암호화 과정은 반복 알고리듬이 사용되므로 상당한 시간이 소요되지만 암호화된 영상의 복호화 과정은 E(x,y)와 K(u,v)의 상관을 통해 쉽게 구할 수 있고, 처리시간도 광을 이용하면 상당히 짧으므로 실제 구현이 가능하리라 판단된다. 제안된 방법의 검증을 위해 이진 영상인 'KJU'와 Lena 영상의 눈부분을 일부 발췌한 명암도 영상에 대해 컴퓨터 시뮬레이션한 결과 간단한 이진 정보들만의 상관을 통해 복잡한 명암도 영상을 생성할 수 있음을 확인하였다.

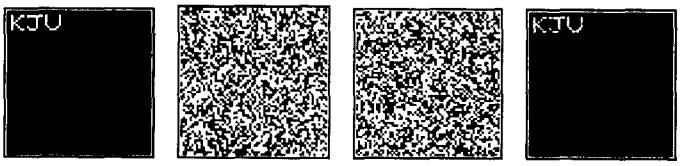

그림 1. 이진 영상
(a) 원영상 (b) 암호화된 영상 (c) 키 영상 (d) 복호화된 영상

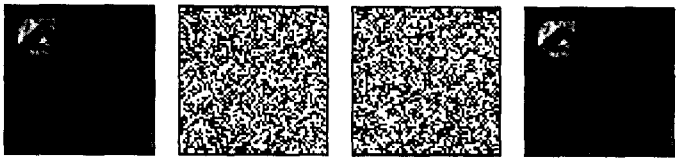

그림 2. 명암도 영상
(a) 원영상 (b) 암호화된 영상 (c) 키 영상 (d) 복호화된 영상

1 P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 32, no. 7, pp. 767- 769, 1995
2 J. Y. Kim, S. J. Park, C. S. Kim, J. G. Bae, and S. J. Kim. "Optical image encryption using interferometry-based phase masks" *Electronic Letters*, vol. 36, no. 10, pp. 874-875, 2000
3. J. Ohtsubo and A. Fujimoto "Practical image encryption and decryption by phase-coding technique for optical security systems" *Applied Optics*, vol. 41, no. 23, pp. 4848-4855, 2002