시각 암호화와 가상 위상영상을 이용한 광 암호화 시스템

Optical Encrytion System using Visual Cryptography and Virtual Phase Images

김인식, 조규보, 서동환, 조웅호*, 김수중
경북대학교 전자공학과, *대구공업대학 전산과
insik01@hanmail.net

We propose the encrytion method using visual cryptography and virtual phase images. The decryption is able to be performed when anyone got all of the keys. Original information is extracted by using Mach-Zehnder interferometer.

현대 사회가 정보화 사회로 발전해 감에 따라 각종 정보 공유의 필요성이 커져가고 있으며 이를 위한 여러 가지 수단이 연구되어 온 반면 한편에서는 허가 되지 않은 개인이나 그룹의 불법적인 접근이나 사용으로부터 특정 정보를 보호하기 위한 많은 연구들이 행해지고 있다.

본 논문에서는 가상 진폭영상(virtual amplitude image)과 가상 위상영상(virtual phase image)을 사용하여 암호화를수행하였다. 가상 진폭영상들과 가상 위상영상과 랜덤영상의 곱을 퓨리에 변환하여 카드로 사용하였고 이렇게 함으로서 정당한사용자가 아닌 사람이 이 카드를 훔치더라도 그카드에는 원정보를 전혀 가지지 않는 진폭영상과 가상 위상영상과 랜덤영상만 있기 때문에 정보를 손실할 염려가 사라지게 된다. 복호화에는 Mach-Zehnder 간섭계를 사용하였다.

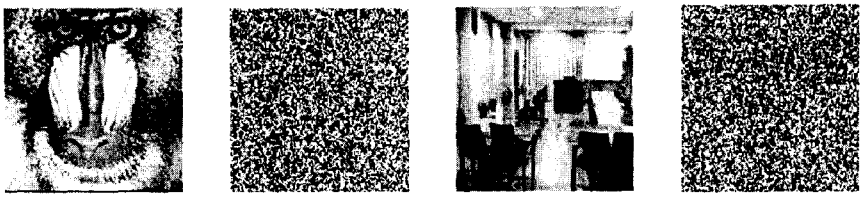
먼저 암호화 하고자하는 영상을 가상영상과 랜덤영상을 사용하여 그 차를 갖는 영상을 키영상이 되는 영상들로 구성한후 이 영상들은 위상변조를 수행하고 가상 진폭영상들은 합이 특정값을 갖도록 영상들을 구성하여서 각각의 진폭영상에 위상변조된 가상영상과 위상변조된 랜덤영상을 곱한 영상을 겹쳐놓아 암호화 하게된다. 이렇게 되면 위상 변조된 영상들이 여러개의 가상 진폭영상에 숨겨지는 효과를 가지게 되며 이 영상을 퓨리에 변환하여 허락된 사용자들에게 나누어 주는 카드들로 사용한다. 복호화 키로는 위상변조된 영상을 사용한다.

복호화는 위의 퓨리에 변환된 카드들을 Mach-Zender 간섭계를 이용하여 영상들이 합을 수행하고 이 영상을 퓨리에 렌즈를 이용하여 역퓨리에 변환을 수행한후 구해진 영상과 위상변조된 키의 곱을 수행하고 그 결과의 영상과 참조파를 선형 중첩시켜 원하는 정보를 얻게된다.

모의 실험에서 사용한 영상들의 크기는 128×128이다. 그림1은 가상 진폭영상들 이다. 그림2는 원영상과 이를 숨기기 위한 가상영상과 랜덤영상과 키의 영상이다. 그림3은 위상변조된 영상과 진폭영상의 곱이 퓨리에 변환된 영상으로 나누어 갖는 카드들이다. 그림4는 Mach-Zehnder 간섭계를 이용하여 재생된 영상이다. 재생된 영상은 반전된 영상이며 여현함수의 비선형성으로 인해 원영상과는 차이는 있으나 거의 무시할수 있을 정도여서 인간의 시각으로는 구분하기가 힘들다.

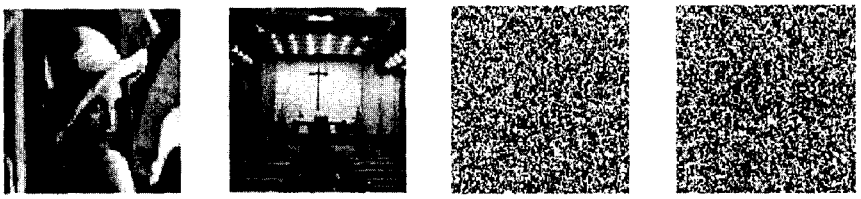
본 논문에서 제안한 시스템은 진폭영상에 정보를 복호하는데 사용되는 가상 위상영상을 숨겨서 퓨리에 변환하여서 암호화 수준을 높였으며 또한 카드를 도난 당하더라도 그 카드는 원정보를 전혀 갖지 않

기 때문에 정보 손실의 염려가 사라지게 되며 각 카드를 가진 소유자들이 다 모여야지 영상을 복호화 할 수있어 높은 정보보호가 가능하다고 여겨진다.



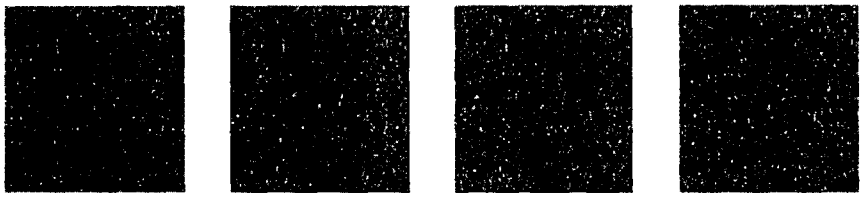
(a) (b) (c) (d)

그림 1. 가상 진폭영상들



(a) (b) (c) (d)

그림 2. 위상변조에 사용된 영상들:(a) 원영상, (b) 가상영상, (c) 랜덤영상, (d) 키영상



(a) (b) (c) (d)

그림 3. 그림1에 위상변조된 영상이 곱해진후 퓨리에 변환된 영상들

(a) (b)

그림 4. Mach-Zehnder 간섭계를 이용하여 재생된 영상: (a) 재생된 영상, (b) 반전시킨 영상

참고문헌

[1] 이상수, "암호화된 위상마스크를이용한 광학적 시각 암호화 방법", 경북대학교 석사학위 논문, pp. 1-8, 2000.

[2] A. Shamir, "How to share a seret," Communications of ACM, vol. 22, pp. 612-613, 1979.