JTC 구조를 사용하는 광암호화 시스템의 분석

Analysis of Optical Encryption System using JTC Architecture

주성현, 유재성, 정만호*
청주대학교 대학원 물리광학과, *청주대학교 레이저 광정보공학과
manho@chongju.ac.kr

사회의 정보화가 진전됨에 따라 개인 정보의 보안이 중요한 문제로 대두되고 있고, 이를 위한 보안 시스템들이 활발하게 연구되고 있다. 이 중에서 지문인식이나 얼굴인식과 같은 생체인식을 이용한 시스템들이 차세대 보안시스템으로 채택되는 것은 거스를 수 없는 대세로 받아들여지고 있다. 또한 이러한 보안시스템들이 정상적으로 운영되기 위해서는 외부로 노출되는 반드시 생체패턴을 보호하기 위한 방법이 필요하게된다.

그동안 생체패턴 및 영상정보의 보호를 위하여 랜덤패턴을 기준파로 사용하는 홀로그램의 제작과 같은 방법이 이용되어왔고, 그 중에서 가장 대표적인 방법이 이중 랜덤 위상 암호화(Double Random Phase Encryption) 방법이다. 이 암호화 방법은 암호화된 데이터가 복소값을 가지므로 광학적인 구현시 약간의 문제점이 발생할 수 있고, 특히 해독 알고리즘에 의해 해독될 가능성이 크다는 것이 단점이다. 따라서 이를 보완하기 위해서 Joint Transform Correlator(JTC) 구조를 사용하는 이중 랜덤 암호화 방법이 제안되었다[1-3].

본 논문에서는 생체인증과 같은 실제 보안시스템에 적용하기 위해서 JTC 구조를 사용하는 이중 랜덤 위상 암호화 방법에 대하여 조사하였다. 또한 이 암호화 과정에서 사용되는 이진 암호화 키를 Pixel-Oriented CGH 기법을 이용하여 설계하였고, 구현된 키코드가 실제로 암호화 키로서의 역할을 수행할 수 있는지에 대하여 분석하였다. 그림 1은 본 논문에서 구현된 이진 암호화 키와 그의 재생상을 나타낸다. 그리고 암호화 키의 독립성을 조사해보기 위하여 다음과 같은 연산을 수행하여 표 1에 나타내었다.

$$\begin{aligned} &\mathrm{std}\{\arg[H_i(u,v)H_j^*(u,v)]\} = 0 \quad , \text{if } i = j \\ &\mathrm{std}\{\arg[H_i(u,v)H_j^*(u,v)]\} \neq 0 \quad , \text{if } i \neq j \end{aligned} \tag{1}$$

그림 1(b)에서 이진 암호화 키로부터 재생된 랜덤 위상의 진폭성분이 크게 변조된 것을 확인할 수 있다. 이 진폭변조효과는 암호화 과정에서 암호화된 영상의 진폭을 변화시키게 되며, 결과적으로는 복호화되는 영상의 질을 크게 떨어뜨리는 원인이 된다. 이를 좀더 자세하게 관찰하기 위해서 진폭과 위상에 대한 히스토그램을 조사하였다. 그 결과 위상분포는 서로 상관관계가 존재하지 않고 균일하게 분포되는 것을 확인할 수 있었다.

그림 3, 4는 이진 암호화 키를 사용하여 암호화 및 복호화를 수행한 결과이다.

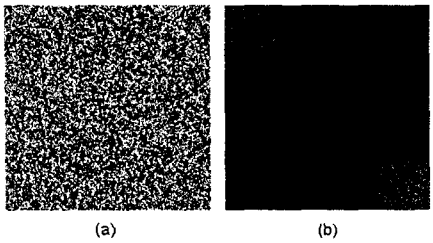

Fig 1. (a) Encryption key, (b) Reconstruction

Table 1. Independence of the encryption key.

	key 1	key 2	key 3	key 4	key 5
key 1	0	1.8098	1.8188	1.8196	1.8127
key 2	1.8098	0	1.8109	1.8123	1.8176
key 3	1.8188	1.8109	0	1.8182	1.8036
key 4	1.8196	1.8123	1.8182	0	1.8143
key 5	1.8127	1.8176	1.8036	1.8143	0

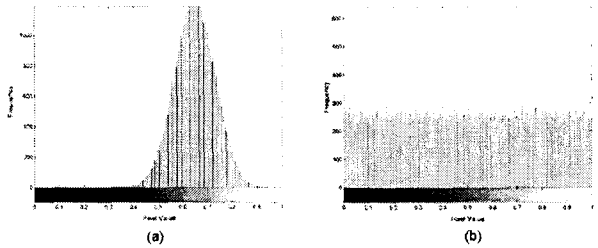

Fig 2. (a) Amplitude and, (b) Phase distribution

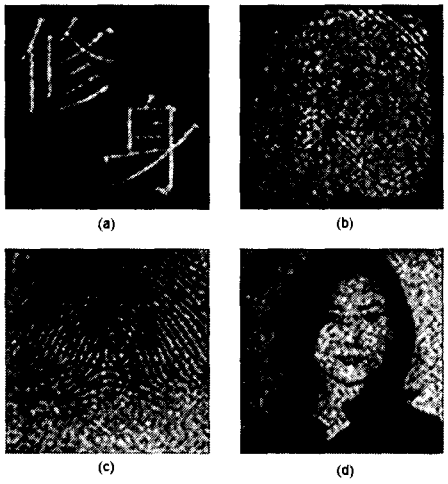

Fig 3. Decryption results

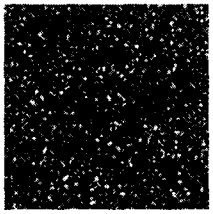

Fig 4. Decryption result using incorre key

참고문헌

1. Takanori Nomura and Bahram Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng., vol. 39, no. 8, pp. 2031-2035, 2000.
2. Takanori Nomura and Bahram Javidi, "Optical encryption system with a binary key code," Appl. Opt., vol. 39, no. 26, pp. 4783-4787, 2000.
3. Takanori Nomura, Shunji Mikan, Yoshiharu Morimoto, and Bahram Javidi, "Optical image Encryption using an optimally designed encryption key," International workshop on optical display and information processing, pp. 34-42, Gyeongju, Korea, May 2002.