광암호화 시스템에서 암호화된 영상의 왜곡 및 오차분석
Analysis of Distortion and Error Tolerance of Encrypted image in Optical Encryption Systems

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

영상 정보 및 생체 패턴의 보호를 위해서 랜덤 위상 패턴을 기준파로 하는 홀로그램의 제작과 같은 암호와 방법이 사용되어 왔는데, 이런 방법들 중 가장 대표적인 것으로 이중 랜덤 위상 암호화(Double Random Phase Encryption)기법이 있다[1].

이중 랜덤 위상 암호화 방법은 진폭 기반의 방법과 위상 기반의 방법으로 구분한다. 암호화와 복호화의 과정은 그림 (1)에서 복호화 과정은 그림 (2)에서 보여주고 있다.

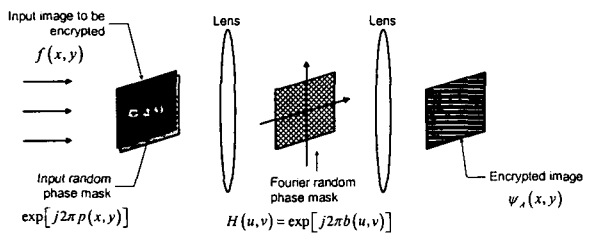

Fig 1. Encryption process

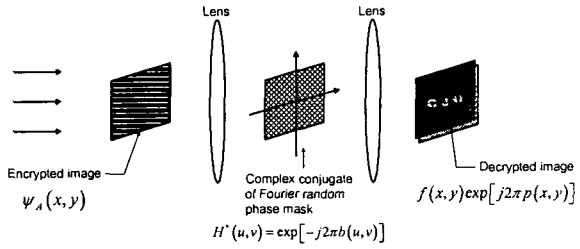

Fig 2. Decryption process

본 논문에서는 암호화할 입력영상으로 일반적인 생체인식에서 사용되는 영상을 사용하였고, 복호화된 영상과 원래 영상을 비교하기 위해 평균 제곱 오차(Mean Squared Error, MSE)와 신호대 잡음비(Signal to Noise Ratio. SNR)을 사용했다. 또한, 처리되는 데이터의 형태에 따라서 진폭형과 위상형 방법으로 나누어 암호화 및 복호화를 수행하였다. 진폭형 및 위상형 암호화 방법에서 올바른 키를 사용했을 경우 모두 MSE는 0에 가까운 값을 갖고 SNR은 무한대의 값을 갖았으나, 위상형이 좀더 우수한 성능을 나타내었다. 그림 3은 4가지의 서로 다른 입력영상에 대하여 진폭형 방법과 위상형 방법을 비교한 것이다. 다음으로 암호화된 영상에서 발생될 수 있는 영상왜곡을 고려하여 두 암호화 방법을 비교하였다. 영상왜곡으로는 잡음의 부가와 영상정보의 손실에 대하여 고려하였다. 영상에 부가되는 잡음의 형태로 Additive Gaussian White Noise를 고려하여 잡음의 표준편차를 증가시키면서 MSE와 SNR을 비교하였다[2]. 이 결과를 그림 4에 나타내었다. 그 결과 암호화 방법이 진폭형 방법보다 부가잡음에 대한 영향을 훨씬 덜 받는다는 것을 쉽게 확인할 수 있었다. 즉, 진폭형 방법에서 잡음에 대한 허용오차는 약 0.5였으나 위상형 방법에서는 약 2.0으로 4배 이상 차이가 발생하였다. 다음으로 암호화된 영상의 정보유실을 고려하였다. 먼저, 암호화된 영상의 한 쪽에서부터 정보가 손실되는 경우를 고려하였고 그 다음으로 사방으로부터 정보가 손실되는 경우로 암호화된 영상의 외부에서 내부로 정보 손실량을 증가시키면서 복호화를 시도하였다. 이 결과를 그림 5에 나타내었다. 그 결과 진폭형 방법보다는 위상형 방법을 사용한 경우 정보 손실에 대한 영향을 덜 받는 것으로 나타났다. 정보 손실량을 기준으로 진폭형 방법에서

선택할 수 있는 최대 오류허용오차는 한쪽 방향으로 정보가 손실될 경우와 사방으로 손실된 경우와 관계없이 약 70%이하인데 반해 위상형 방법에서는 약 90%이하로 택할 수 있다. 한 쪽 방향으로 정보가 손실된 경우와 사방으로 손실된 경우 비교했을 때 암호화된 영상에서 원 영상을 복원시킬 수 있는 정보들이 어느 한 곳에 집중되지 않고 모든 영역으로 분산되어 분포하고 있다는 것을 알 수 있었다.

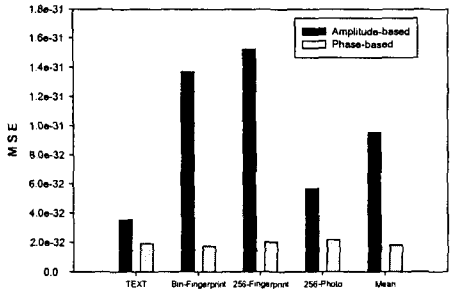

Fig 3. Comparison of amplitude-based and phase-based method

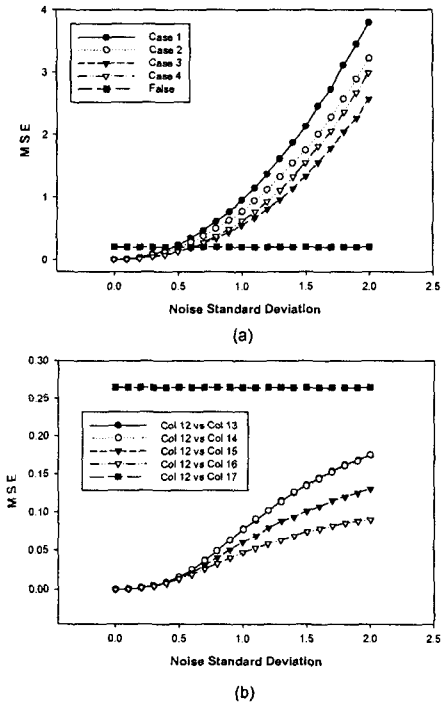

Fig. 4 Noise perturbation.
(a) Amplitude-, (b) Phase-based method

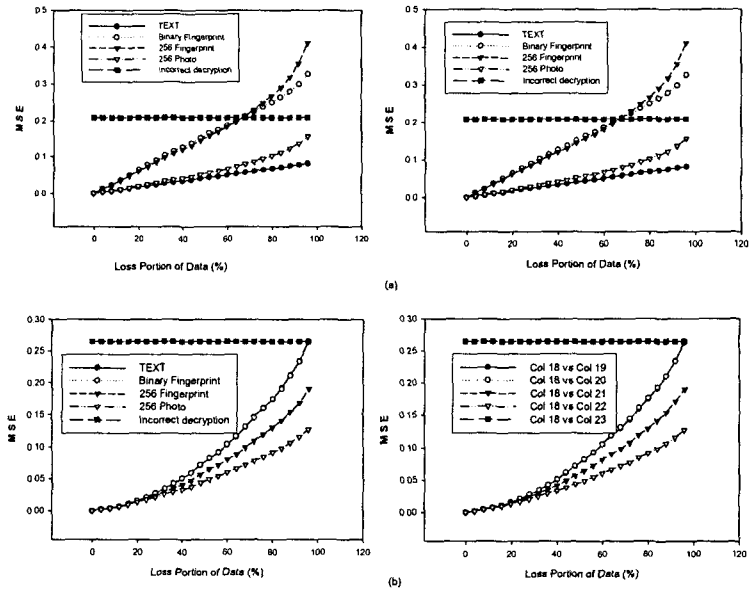

Fig 5. Damage of Information
(a) Amplitude- , (b) Phase-based method

[참고문헌]

1. Philippe Refregier and Bahram Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett., vol. 20, no. 7, pp. 767-769, 1995.
2. Bahram Javidi, Laurent Bernard and Nasser Towghi, "Noise performance of double-phase encryption compared to XOR encryption," Opt. Eng., vol. 38, no. 1, pp. 9-19, 1999.