가상위상영상을 이용한 잡음 및 변이에 강한 암호화 시스템

Shift and noise tolerance encryption system using a phase-based virtual image

서동환, 조규보, 신창목, 박상국*, 김성용*, 김수중
경북대학교 전자공학과, *위덕대학교 컴퓨터공학과
dhseo@palgong.knu.ac.kr

We propose an improved image encryption and the shift-tolerance method in the Fourier space using a virtual phase image. The encrypted image is obtained by the Fourier transform of the product of a phase-encoded virtual image, not an original image, and a random phase image. We demonstrate the robustness to noise, to data loss and shift of the encrypted image or the Fourier decryption key in the proposed technique.

최근에는 광학 기술을 이용한 보안 시스템에 관한 연구가 활발히 진행되고 있는데 이는 광의 병렬성과 고속성을 충분히 이용할 뿐만 아니라 위상 정보와 세기 정보를 동시에 광학 매질에 기록할 수 있으므로 사람의 눈이나 세기검출기로는 위상정보를 추출하는 것이 불가능하여 위조나 복제를 근본적으로 차단할 수 있다는 특성에 기인한다. 본 논문에서는 암호화된 영상을 분석함으로써 있을 수 있는 복제 가능성을 배제하기 위해 위상 변조된 가상 영상을 이용하여 암호화 수준을 향상시키고 퓨리에 영역에서 암호화된 영상과 복호화 키 영상의 변이가 발생하더라도 원 영상이 복원됨을 제안하였다. 암호화된 영상은 원 영상의 어떤 정보도 포함하지 않은 위상 변조된 가상 영상과 컴퓨터로 발생시킨 무작위 위상 영상을 곱하여 퓨리에 변환하여 만든다. 따라서 허가되지 않은 사용자가 암호화된 영상을 분석하더라도 가상 영상을 원 영상으로 오인하게 되므로 복호화 키의 정보 없이는 결코 원 영상의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하다는 장점을 가진다. 복호화 과정은 암호화된 영상과 제안한 위상 대응 규칙으로 만들어진 퓨리에 복호화 키를 간섭시킨 후 퓨리에 역변환하여 간단히 원 영상을 재생한다. 컴퓨터 모의 실험을 통하여 제안한 암호화 방법이 잡음이나 암호화된 영상이 절단되거나 변이가 발생하더라도 영상의 복원이 가능함을 검증하였다. 원 영상 $f(x, y)$, 암호화할 가상 영상 $v(x, y)$, 무작위 영상 $r(x, y)$, 복호화키 영상 $d(x, y)$라고 하면 위상 변조된 원 영상 $f_p(x, y)$는 제안한 암호화 방법에서

$$f_p(x,y) = \exp[j\pi f(x,y)] = \exp\{j\pi[v(x,y) + r(x,y) - d(x,y)]\} \quad (1)$$

로 표현된다. 먼저 암호화할 가상 영상 $v(x,y)$와 컴퓨터로 발생시킨 무작위영상 $r(x,y)$을 각각 위상 변조하고 두 위상 변조된 영상을 곱한 영상을 $e(x,y)$라 두면

$$\begin{aligned} e(x,y) &= v_p(x,y)\, r_p(x,y) \\ &= \exp\{j\pi[v(x,y) + r(x,y)]\} \end{aligned} \quad (2)$$

와 같고 원 영상과 무작위 영상의 선형적인 합임을 알 수 있고 이를 퓨리에 변환하여 암호화된 영상

$E(u, v)$로 사용한다. 이때 만약 허가되지 않은 개인이나 그룹이 암호화된 영상을 퓨리에 변환이나 위상 측정 방법 등으로 분석하더라도 가상영상을 원 영상으로 오인하게 되므로 정확한 복호화키 없이는 결코 원 영상의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하다는 장점을 가진다. 본 논문에서 제안한 위상 대응 규칙에 의한 복호키 영상을 만드는 방법은

$$d_p(x, y) = \exp[j\pi d(x, y)] = \exp\{j\pi[v(x, y) + r(x, y) - f(x, y)]\} \tag{3}$$

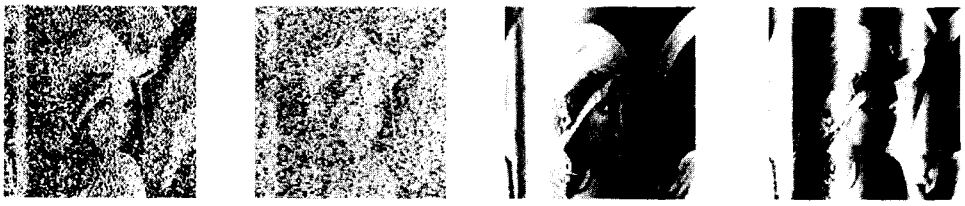
와 같이 표현되며 이를 퓨리에 변환하여 퓨리에 복호화키 $D(u, v)$로 사용한다. 암호화된 영상 $E(u, v)$과 복호화키 $D(u, v)$는 간섭계의 퓨리에 영역에 각각 놓여지며, BS에 의해 합쳐진 영상 $O(u, v)$는

$$O(u, v) = E(u, v) + D(u, v) \tag{4}$$

와 같으며 이 합쳐진 영상은 퓨리에 렌즈 L에 의해 퓨리에 역변환되어 CCD에 나타나는 세기함수는

$$\begin{aligned} |o(x, y)|^2 = & |e(x, y)|^2 + |d_p(x, y)|^2 \\ & + e(x, y)d_p^*(x, y) + e^*(x, y)d_p(x, y) \\ = & 1 + 1 + \exp[j\pi f(x, y)] + \exp[-j\pi f(x, y)] \\ = & 2 + 2\cos[\pi f(x, y)] \end{aligned} \tag{5}$$

와 같으며 여기서 $f(x, y) = v(x, y) + r(x, y) - d(x, y)$ 이다. 식 (5)에서 원 영상이 이진 영상이면 정확히 원 영상의 반전된 영상이 복원되지만 그레이 영상에서는 식 (5)의 여현 함수의 비선형성에 의해 영상의 왜곡이 발생함을 알 수 있으나 이는 컴퓨터의 후처리를 통하여 간단히 복원 가능하다. 그림 1은 제안한 암호화 시스템이 외부 영향에 대한 성능을 평가하기 위해 암호화된 영상을 임의로 절단하여 그에 대응하는 복원 영상과 퓨리에 영역에서 암호화된 영상이 정확한 위치에서 각각 x축을 따라 1과 3 픽셀만큼 변이가 생겼을 경우에 재생된 영상들이다. 여기에서 암호화된 영상의 75%가 절단되더라도 원 영상의 정보를 얻을 수 있음을 알 수 있고 또한 그림 1(c)와 (d)에서 복원 영상의 전 영역에 여현 함수의 위상 성분에 의하여 줄무늬가 발생하고 이 재생된 영상의 줄무늬 개수와 암호화된 영상의 이동된 픽셀 값이 동일함을 알 수 있다. 따라서 재생된 영상을 통하여 암호화된 영상의 변이 정도를 알 수 있음으로 컴퓨터의 후처리를 통하여 보완할 수 있다. 또한 제안한 암호화 방법은 x축 뿐만 아니라 y축과 x-y축에 대한 이동에 대해서도 동일한 특성을 가진다.



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

그림 1. x축을 따라 암호화된 영상이 각각 (a) 25%와 (b) 75% 절단되었을 때 복원된 영상과 x축을 따라 (a) 1과 (b) 3 픽셀만큼 변이가 생겼을 경우에 재생된 영상

참고문헌

[1] B. Wang, C. C. Sun, W. C. Su, and A. E. T. Chiou, "Shift-tolerance property of an optical double-random phase-encoding encryption system," Appl. Opt., vol. 39, pp. 4788-4793, 2000.

[2] N.Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," J. Opt. Soc. Am. A, vol. 16, pp. 1915-1927, 1999.

[3] H. T. Chang, "Image encryption using separable amplitude-based virtual image and iteratively retrieved phase information," Opt. Eng., vol. 40, pp. 2165-2171, 2001.