결합변환상관기 구조를 이용한 위상 암호화 영상의 인식 및 복호화

신창목*, 김수중*
경북대학교 전자전기컴퓨터학부*

Identification and Decryption of Fully phase-encrypted image Using Joint Transform Correlator Structure

Chang-Mok Shin*, Soo-Joong Kim*
School of Electrical Engineering & Computer Science, Kyungpook Nat'l University*

요 약

본 논문에서는 결합변환상관기(joint transform correlator)와 위상 암호화된 영상들을 이용하여 영상의 인식 및 복호화가 가능한 광 암호화 시스템을 제안하였다. 그레이 값을 가지는 원 영상은 동일한 그레이 값을 가지는 이진 영상으로 나누어 표현할 있다. 이러한 이진 영상들을 각각의 다른 이진 무작위 영상과 위상 부호화한 XOR 연산을 이용해 암호화할 수 있으며, 암호화한 영상들을 결합한 후 위상 부호화 과정을 거쳐 최종 암호화 영상를 구한다. 키 영상은 암호화에 사용된 각각의 이진 무작위 영상들을 최종 암호와 영상를 얻을때의 과정처럼 결합하여 역시 하나의 영상으로 구할 수 있다.
최종 암호화 영상과 키 영상을 제안한 결합변환상관기의 입력으로 사용하여 구한 상관치는 높고 폭이 좁은 특성을 가지고 있으므로 분별성능이 좋은 인식 시스템을 구현할 수 있을 뿐만 아니라 복호화 영상도 구할 수 있다. 컴퓨터 모의 실험으로 제안한 방법을 확인해보았다.

1. 서론

최근 몇 년 동안, 정보 보호는 복사기술의 발전과 원 정보의 인증의 필요성에 의해 그 중요성이 점점 대두되고 있다. 일정한 보호수준을 유지시키기 위해서, 정보보호 시스템은 원 정보에 대한 높은 분별성과 함께 무분별한 복사에도 강한 특성은 지녀야 한다. 위상 부호화된 정보는 기본적으로 눈으로 보이지 않는 특성을 지니고 있기 때문에 세기 검출기로 쉽게 복사할 수 없다. 이러한 위상 부호화된 정보를 기반으로 한 광 정보 보호 기술들은 광범위하게 연구되고, 다양한 이론들이 제안되어져왔다.

이러한 광 보호 기술들[1-3] 중 이진 위상 XOR 연산 방법이 있다[2]. 이 방법은 기본적으로 두 위상 영상간의 간섭현상을 이용한 암호화 방법으로써, 간단한 구현이 가능하다는 장점이 있으나, 이진 정보의 암호화에만 적용된다는 단점을 가지고 있다.

본 논문에서는 위상 암호화된 영상과 결합변환

상관기를 이용한 새로운 광 인증 및 복호화 시스템을 제안하였다. 제안한 방법에 의해 위상 암호화된 영상들 즉 암호화 영상과 키 영상은 [0; 2π]사이의 무작위로 분포한다. 이 영상들은 XOR 연산과 위상부호화 과정으로 암호화되었기 때문에 서로 다른 백색 잡음의 특성을 가지고 있을 뿐만 아니라, 둘 사이의 상관치가 매우 좁고 높은 특성이 있다. 또한, 이 영상들을 사용해 복호화 영상도 바로 추출할수 있기 때문에 인증 뿐만 아니라 복호화도 가능한 시스템을 구현할 수 있다. 본 논문에서는 결합변환상관기(joint transform correlator)를 사용하여 제안한 시스템을 구현하였다.

2. 암호화 과정

n 개의 레벨을 가지는 그레이 원 영상을 $o_n(x,y)$ 라 하면, 첫번째 과정으로 이 영상을 동일한 그레이 레벨을 가지는 이진 영상들로 나눌 수 있으며 이렇게 나누어진 이진 영상들을 위상 부호화 한다. 원 영상을 이진 영상으로 나누면

$$o_n(x,y) = 1\cdot b_1(x,y) + 2\cdot b_2(x,y) + \ldots + n\cdot b_n(x,y) \quad (1)$$

과 같다. 여기서 $b_1, b_2, b_3 \ldots b_n$은 0 또는 1의 값을 가지는 이진 영상들을 나타낸다. 각각의 나누어진 이진 위상들은 서로 다른 이진 영상들의 화소값에는 영향을 받지 않는 독립적인 화소값의 특성을 가진 영상이 된다.

두번째 과정으로, 나누어진 영상을 이진 무작위 위상영상들 $\exp(j\pi r_1)$, $\exp(j\pi r_2)$, $\exp(j\pi r_3)\ldots$ $\exp(j\pi r_n)$과 위상 부호화된 XOR 연산을 이용해 암호화하며, 암호화에 사용되는 위상 부호화 XOR 연산은 다음 표 1과 같이 표현할 수 있다.

<표 1> 일반적인 XOR 연산과 제안한 위상 부호화 XOR 연산

XOR			Phase encoded XOR		
b_n	e_n	r_n	$\exp(j\pi e_n)$	$\exp(j\pi r_n)$	$\lvert\exp(j\pi e_n)-\exp(j\pi r_n)\rvert \times 0.5 = b_n$
0	0	0	1	1	0
0	1	1	-1	-1	0
1	0	1	1	-1	1
1	1	0	-1	1	1

n번째의 이진 암호화된 영상은

$$\exp(j\pi e_n) = \exp(j\pi b_n)\cdot\exp(j\pi r_n) \quad (2)$$

로 나타낼 수 있으며, 차 연산(subtraction operator)을 이용하면, b_n은

$$b_n(x,y) = \left| [\exp(j\pi e_n) - \exp(j\pi r_n)]/2 \right| \quad (3)$$

으로 표현할 있다.

그러므로 원 영상은 식 (3)과 차 연산을 이용해 표현 가능하며,

$$\begin{aligned} o_n &= \left|\{1\cdot[\exp(j\pi e_1)-\exp(j\pi r_1)] + 2\cdot[\exp(j\pi e_2)-\exp(j\pi r_2)] \right. \\ &\quad \left. \ldots + n\cdot[\exp(j\pi e_n)-\exp(j\pi r_n)\}/2\right| \\ &= \left|\{[1\cdot\exp(j\pi e_1) + 2\cdot\exp(j\pi e_2) + \ldots n\cdot\exp(j\pi e_n)] - \right. \\ &\quad \left. [1\cdot\exp(j\pi r_1) + 2\cdot\exp(j\pi r_2)] + \ldots n\cdot\exp(j\pi r_n)]\}/2\right| \end{aligned} \quad (4)$$

와 같이 구할 수 있다.

식 (4)로부터 암호화된 부분과 암호화에 사용된 무작위 영상부분을 따로 분리하여 두개의 그레이 무작위 영상을 얻을 수 있으며, 이는

$$\begin{aligned} E(x,y) &= [1\cdot\exp(j\pi e_1) + 2\cdot\exp(j\pi e_2) + \ldots + n\cdot\exp(j\pi e_n)]/2 \\ R(x,y) &= [1\cdot\exp(j\pi r_1) + 2\cdot\exp(j\pi r_2) + \ldots + n\cdot\exp(j\pi r_n)]/2. \end{aligned} \quad (5)$$

로 표현된다.

마지막 단계로 $E(x, y)$와 $R(x, y)$를 n으로 나눈후 위상 부호화하여 최종 암호화 영상과 키 영상을 구한다. 암호화 영상과 키 영상은

$$\begin{aligned} \tilde{E}(x,y) &= \exp(j\pi E/n) \\ \tilde{R}(x,y) &= \exp(j\pi R/n) \end{aligned} \quad (6)$$

과 같이 표현 할 수 있다. $\tilde{E}(x,y)$ 는 암호화 영상 $\tilde{R}(x,y)$ 은 키 영상을 나타내며, 원 영상을 인증하고 복호화하기 위해 제안한 시스템의 입력으로 사용된다.

3. 인증과 복호화 과정

3.1 인증과정

그림 1과 같이 인증모드로 하였을 때 $\tilde{E}(x,y)$ 와 $\tilde{R}(x,y)$를 결합변환상관기의 입력으로 사용하여 인증과정을 수행할 수 있다. 푸리에 렌즈를 거친후 출력영상은

$$
\begin{aligned}
&I_{CCD1}(u,v)\\
&=\left| F.T[\tilde{E}(x,y)]\cdot\exp(j2\pi u_0 x)+F.T[\tilde{R}(x,y)]\cdot\exp(-j\pi 2u_0 x)\right|^2 \qquad (7)\\
&=|F.T[\tilde{E}(x,y)]|^2+F.T[\tilde{E}(x,y)]^*F.T[\tilde{R}(x,y)]\exp(-j4\pi u_0 x)+\\
&\quad F.T[\tilde{E}(x,y)]F.T[\tilde{R}(x,y)]^*\exp(j4\pi u_0 x)+|F.T[\tilde{R}(x,y)]|^2
\end{aligned}
$$

과 같다. 여기서 u_0는 결합변환상관기에서의 입력 영상과 기준 위치와의 거리를 의미한다.

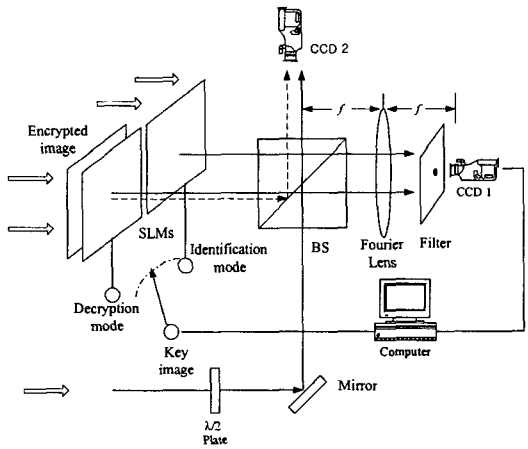

그림 1. 제안한 인증 및 복호 시스템

입력 영상들의 상관치는 위 세기 영상의 역푸리에 변환으로 구하며,

$$
\begin{aligned}
&F.T^{-1}[I_{CCD1}(u,v)]\\
&=\tilde{E}(x,y)\bullet\tilde{E}(x,y)+[\tilde{R}(x,y)\bullet\tilde{E}(x,y)]*\delta(x+2u_0)+ \qquad (8)\\
&\quad[\tilde{E}(x,y)\bullet\tilde{R}(x,y)]*\delta(x-2u_0)+\tilde{R}(x,y)\bullet\tilde{R}(x,y)
\end{aligned}
$$

과 같다. 여기서 기호 •과 *는 각각 상관연산자(correlation operator)와 콘볼류션연산자(convolution operator)를 의미한다. 상관치는 XOR로 암호화된 상관특성에 의해 좁고 높을 뿐만 아니라, 자기상관성분과 떨어져 나타나므로, 공간필터를 써서 자기상관성분을 제거할 경우, $2u_0$ 와 $-2u_0$ 의 위치에서 상관 결과를 쉽게 확인할 수 있다.

3.2 복호화 과정

제안한 시스템을 그림 1과 같이 복호화 모드로 놓고 키 영상 $\tilde{R}(x,y)$를 암호화 영상 $\tilde{E}(x,y)$과 직렬연결 상태로 하여 광을 투영시키면 간섭에 의해 복호화 영상을 구할 수 있으며,

$$
\begin{aligned}
&O_{CCD2}(x,y)\\
&=\left| R(x,y)\exp(j\pi)+R(x,y)\tilde{E}(x,y)\tilde{K}(x,y)\right|^2\\
&=\left| R(x,y)\exp(j\pi)\right|^2\left|1+\exp(-j\pi)\tilde{E}(x,y)\tilde{K}(x,y)\right|^2 \qquad (9)\\
&=\left| R(x,y)\right|^2\left|1-\exp[j\pi E(x,y)]\exp[j\pi K(x,y)]\right|^2\\
&=\left| R(x,y)\right|^2\left|2-2\cos\{\pi[E(x,y)+K(x,y)]\}\right|
\end{aligned}
$$

와 같이 표현할 수 있다. 이 때 기준파 $R(x,y)$ 는 $E\exp(j\theta)$ 이다.

4. 컴퓨터 모의 실험

그림 2는 222값을 최대 그레이 값으로 가지는 128×128 화소의 레나(Lena) 원 영상이다. 그림 3과 그림 4는 암호화 과정에 의한 무작위 영상들이다. 그림 5는 복호화 모드일 때 CCD2에 의해 검출되는 복호화 영상을 나타내며, 상관 모드일 경우 공간필터에 의해 필터링된 상관치는 그림 6과 같이 CCD1에 의해 나타난다. 거짓 암호화된 영상을 입력으로 하였을 때 그림 7와 같이 상관치가 없는 인증이 나타남을 확인할 수 있다.

그림 2. 원 영상

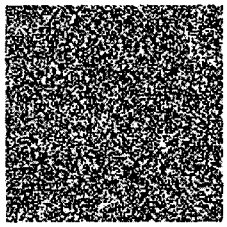

그림 3. 암호화 영상

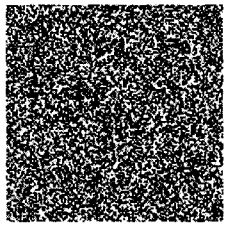

그림 4. 키 영상

그림 5. 복호화 영상

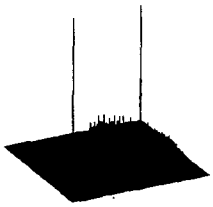

그림 6. 인증 상관결과

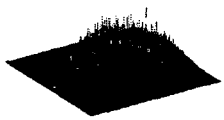

그림 7. 거짓 인증상관결과

5. 결론

본 논문에서는 XOR연산과 결합변환기 구조를 이용하여 인증과 복호화가 가능한 광 보호 시스템을 제안하였다. 제안한 시스템은 인증시 높고 좁은 상관치를 출력평면에 나타낼 뿐만 아니라 복호화 결과도 보여 줄 수 있기 때문에 원 영상에 대해 높은 정보 특성을 가진다.

참 고 문 헌

[1] B. Javidi and A. Sergent, "Fully Phase encoded key and biometrics for security verification", *Optical Engineering*, vol. 36, No. 3, pp. 935-941, March 1997.

[2] J.-Y. Kim, S.-J. Park, C.-S. Kim, J.-G. Bae, and S.-J. Kim, "Optical image encryption using interferometry-based phase mask," *Electronic Letters*, vol. 36, No 10, pp.874-875, May 2000.

[3] P. C. Mogensen, and J. Gluckstad, "Phase-only optical encryption", *Optics Letters*, vol. 25, No. 8, pp. 566-568, April 2000.