

Walsh code를 이용한 계층적 광 암호화

김남진*, 신창목, 조규보, 조창섭, 서동환**, 김수중

경북대학교 *정보통신학과, 경북대학교 전자공학과, **한국해양대학교 전기전자공학부

lallala@ee.knu.ac.kr

We proposed an hierarchically optical security method based on the walsh code which is an orthogonal characteristic. Computer simulation results are further demonstrated to verify the proposed method

정보산업이 급속히 발전하고 있는 현대 사회에서 단체나 개인의 다양한 정보공유의 필요성이 대두되고 있으며, 이에 따라 정보 보호의 중요성이 함께 중요시 되고 있다. 따라서 개인이나 단체의 정보에 대한 불법적인 접근이나 사용으로부터 보호하려는 수많은 보안 들이 제안되고 구현되어 왔으며, 이 중 계층적 암호화 이론은 허가된 사용자들에게 정보의 수준에 따른 선별적인 접근을 가능케 함으로써 보다 효율적인 정보보호를 할 수 있다.

본 논문에서는 walsh code⁽¹⁾ 영상과 이진 위상 영상을 이용하여 상위 계층의 정보⁽²⁾는 높은 보안 수준의 키 영상으로, 하위 계층의 정보는 낮은 보안 수준의 키 영상으로만 복원 되는 계층적 광 암호화 방법을 제안하였다. 우선 원 영상들에 무작위 위상 영상을 곱하여 푸리에 변환하면,

$$A_i(u, v) = \mathcal{F} \{ I_i(x, y) \exp[j2\pi r(x, y)] \} \quad (1)$$

과 같다. 이 때 $I_i(x, y)$ 는 원 영상들을, $\exp[j2\pi r(x, y)]$ 는 무작위 위상영상, 그리고 $\mathcal{F}\{\cdot\}$ 푸리에 변환 기호를 나타내며, i 는 수준에 따른 영상의 수를 의미한다. 암호화 영상은 $A_i(u, v)$ 을 확장한 후 walsh code 영상과 이진 위상 영상을 곱하여 생성하며,

$$E_i = A_i'(u, v) \cdot W_i \cdot \exp[j\pi R(u, v)] \quad (2)$$

와 같다. $A_i'(u, v)$ 는 $A_i(u, v)$ 를 walsh code 영상에 대응하도록 확장한 영상이다. W_i 는 walsh code 영상, $\exp[j\pi R(u, v)]$ 는 무작위 이진위상 영상이다.

세 개의 영상을 이용한 계층적 암호화의 예는

$$\begin{aligned} L_1 &= E_1 \\ L_2 &= E_1 + E_2 \\ L_3 &= E_1 + E_2 + E_3 \end{aligned} \quad (3)$$

과 같다. L_1 , L_2 , 그리고 L_3 는 하위 계층, 중간 계층, 상위 계층의 암호화 정보들을 각각 나타낸다. 계층에 따른 정보를 복호화하기 위해 시스템 내에 사용하는 키 영상은

$$K = (W_1 + W_2 + W_3) \exp[j\pi R(u, v)] \quad (4)$$

와 같다. 제안한 암호화 방법의 타당성을 컴퓨터 모의 실험을 통해 확인하였다. 그림 1은 계층적 암호화-영상-생성을 위해 사용한 원 영상들이며, 이를 이진 위상 영상과 walsh code 영상의 곱 영상인 그림 2로 확산시켜 식 (2)와 같이 암호화 할 수 있다.

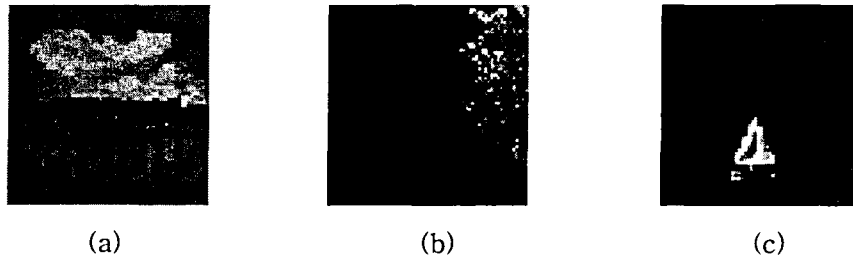


그림 1. 원 영상들

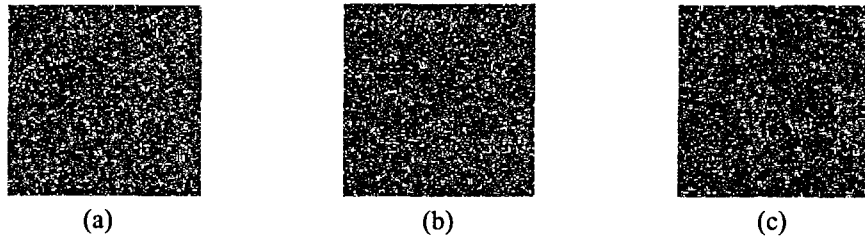


그림 2. 이진 위상 영상과 walsh code 영상의 곱한 영상

암호화한 영상 E_1 , E_2 , E_3 에 식 (3)을 적용하여 최종 계층적 암호화 영상을 그림 3과 같이 얻을 수 있다.

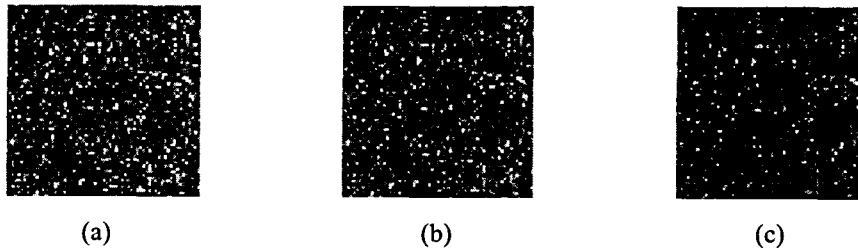


그림 3. 계층적인 암호화 영상 (a) 하위 영상 L_1 , (b) 중간 영상 L_2 , (c) 상위 영상 L_3

따라서 계층적 암호화 영상을 식 (4)의 키 영상과 곱하여 그림 4와 같이 각각 복호화 할 수 있다.

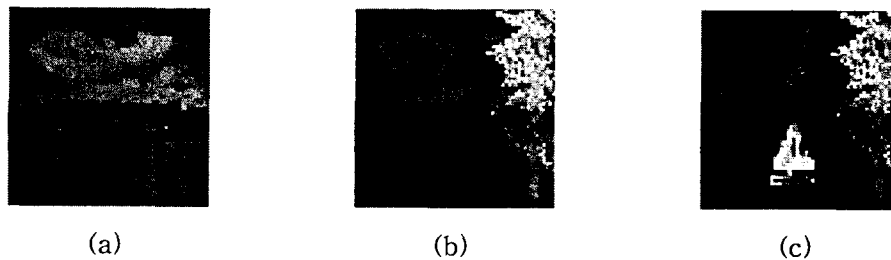


그림 4. (a) 하위 영상 L_1 의 복원 영상, (b) 중간 영상 L_2 의 복원 영상, (c) 상위 영상 L_3 의 복원 영상

[참고문헌]

1. Kyu-Tae Kim, Jang-Hwan Kim, Eun-Soo Kim, "Multiple information hiding technique using random sequence and Hadamard matrix", Optical Engineering, 40, 2489-2494 (2001).
2. Chia H. Yeh, Hsuan T. Chang, Hung C. Chien, and Chung J. Kuo, "Design of cascaded phase keys for a hierarchical security system", Applied Optics 41, 6128-6134 (2002).

F
E