JTC 구조와 지문을 이용한 영상 암호화

서 동 환, 이 상 수*, 신 창 목, 박 세 준, 김 종 윤**, 김 수 중
경북대학교 전자전기공학부, *전자통신연구소, **경동대학교
전화: 053-940-8611 / 핸드폰: 011-548-1191

Image encryption using JTC architecture and fingerprint key

Dong-Hoan Seo, Sang-Su Lee*, Chang-Mok Shin, Se-Joon Park,
Jong-Yun Kim**, Soo-Joong Kim
Kyungpook Nat'l University, *ETRI, **Kyungdong University
E-mail : dhseo@palgong.knu.ac.kr

Abstract

In this paper, we proposed a personal identification method using binay image encryption technique and decryption system in JTC structure. Logo which represents the group symbol was encrypted with personal fingerprint and JTC structure decrypts this logo. The logo can not decrypted by other unused fingerprint even if the encrypted image was lost or stolen. So this method can give more safe personal identification.

I. 서론

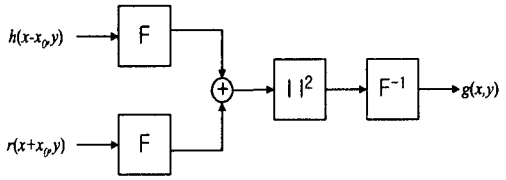
현대 정보화 사회로 접어들면서 인터넷의 급격한 확산과 함께 개인, 기업 및 사회전반에 걸쳐 정보나 보안 등에 대한 관심이 지극히 높아지고 있다. 인터넷 기술의 발달로 인한 전자상거래나 금융권에 있어 거래의 내역이나 개인 정보의 누출 등에 대한 우려가 커지고 있다. 그리고 개개인을 통제할 수 없는 인터넷의 사용 환경 또한 이러한 우려들이 지속되게 하는 요인으로 작용하고 있다. 이런 분위기 속에서 개인의 독특한 신체적 특성이나 행동양식을 이용하여 개개인의 신원을 확인하는 생체인식기술에 대한 관심이 고조되어 왔다. 생체인식을 이용한 기술은 기존의 ID나 패스워드에 비해서 사용상의 장점이 여러 가지가 있으며 특히 자신의 신체일부를 활용하는 것이므로 실존(實存)에 의한 인증이라는 것이 기존의 인증 방법에 비하여 가장 큰 장점이라 할 수 있다. 즉 해당자가 실제 있어야만 본인인지 확인이 가능하므로 분실이나 대여로 인한 오용을 방지할 수 있게 된다. 한편 광을 이용한 시스템은 실시간 처리가 가능하고 공간 광 변조기나 홀로그램을 이용하여 복소값을 동시에 다룰 수 있어 이를 이용한 광보안 및 광정보보호시스템에 대해 많이 연구되어 왔다.

본 논문에서는 JTC(Joint Transform Correlator)를 이용한 이진 영상 암호화 및 복호화 과정 중 개인서명(Signature) 혹은 단체의 로고(Logo)영상에 대한 암호키 및 복호키를 개인의 지문으로 사용하여 신원의 적합성을 확인할 수 있는 방법을 제안하였다. 제안한 방법은 개인 복호키를 사용함으로써 암호화된 카드가 분실 및 위조 되더라로 카드 소유자의 지문이 없는 한 개인 인증을 할 수 없는 장점을 제공한다. 간단한 입력을 사용한 컴퓨터 모의실험을 통해 제안한 방법의 타당성을 확인하였다.

II. JTC 구조를 이용한 광학적 영상 암호화 방법

2.1 전통적인 JTC

JTC 시스템은 Vader Lugt 광 상관기의 광축정렬문제를 해결하기 위하여 입력평면에 기준영상과 입력영상을 함께 두어 제곱법칙 검출기(square-law detector)에서 획득한 이들의 푸리에 변환 영상으로부터 입력평면에 존재하는 데 주로 사용되며 시스템의 블록도는 그림 1과 같다.



F: 푸리에 변환 F^{-1} : 푸리에 역변환

그림 1. 전통적인 JTC의 시스템 블록도

그림 1에서 $r(x+x_0,y)$는 중심이 $(-x_0,0)$에 배치되는 기준 영상이고, $h(x-x_0,y)$는 중심이 $(x_0,0)$에 배치되는 입력영상이다. 입력평면의 영상들을 푸리에 변환하면

$$E(u,v)=H(u,v)e^{-j2\pi x_0 u}+R(u,v)e^{j2\pi x_0 u} \tag{1}$$

와 같이 표현되고, 제곱법칙 검출기(square-law) 출력단의 세기 함수는

$$\begin{aligned} I(u,v)&=|E(u,v)|^2=|H(u,v)|^2+|R(u,v)|^2 \\ &+H(u,v)R^*(u,v)e^{-j2\pi x_0 u}+H^*(u,v)R(u,v)e^{j2\pi x_0 u} \end{aligned} \tag{2}$$

와 같이 표현된다. 이 세기 함수를 역변환하면 출력상관평면에서의 광분포 함수는

$$\begin{aligned} g(x,y)=\ & h\bigstar h+r\bigstar r \\ &+\ h\bigstar r*\delta(x-2x_0,y)+r\bigstar s*\delta(x+2x_0,y) \end{aligned} \tag{3}$$

와 같다. 여기서 ★는 상관자(correlation operator)를, *는 상승자(convolution operator)를 뜻한다.

2.2 JTC 구조를 이용한 영상 암호화

암호화에 사용하는 결합변환상관기의 구성도는 그림 2와 같다. L1은 푸리에 렌즈, f는 렌즈초점거리이며

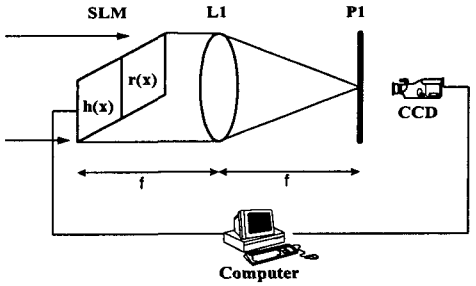


그림 2. 암호화를 위한 JTC 광 구성도

SLM(Spatial Light Modulator)는 결합변환상관기의 입력평면에 놓여진다.

$f(x,y)$를 암호화 할 원 영상, $r(x,y)$를 암호화에 사용하는 키 영상이라고 할 때, $r(x,y)$는 랜덤 위상 마스크 $R(u,v)$를 푸리에 역변환하여 구한다. 암호화된 영상 $h(x,y)$은

$$h(x,y)=f(x,y)\bigstar r(x,y)\Leftrightarrow H(u,v)=F(u,v)^*R(u,v) \tag{4}$$

와 같이 원영상과 키 영상의 상관으로 얻을 수 있다. 복호화 시 암호화된 영상과 키 영상은 거리 $2x_0$만큼 떨어져 그림 2의 SLM에 입력영상으로 올려진 후 푸리에 변환되어

$$e(x,y)=h(x-x_0,y)\ +\ r(x+x_0,y) \tag{5}$$

가 된다. 영상 $e(x,y)$는 L1을 통해 푸리에 변환이 되고, 푸리에 변환된 영상 $E(u,v)$는 L1의 후초점거리에 위치한 평면 P1에 맺힌다. P1에 맺힌 영상을 제곱법칙 검출기인 CCD로 검출하면

$$\begin{aligned} &|E(u,v)|^2 \\ &=|H(u,v)e^{-j2\pi_0(u,v)}+R(u,v)e^{j2\pi_0(u,v)}| \\ &=|H(u,v)|^2+|R(u,v)|^2+H(u,v)R^*(u,v)e^{-4\pi_0(u,v)} \\ &\ +H(u,v)R^*(u,v)e^{4\pi_0(u,v)} \\ &=|H(u,v)|^2+|R(u,v)|^2+F(u,v)e^{-4\pi_0(u,v)} \\ &\ +F(u,v)^*e^{4\pi_0(u,v)} \end{aligned} \tag{6}$$

와 같다. 여기서, $H(u,v)$, $R(u,v)$, $F(u,v)$는 각각 $h(x,y)$, $r(x,y)$, $f(x,y)$의 푸리에 변환 영상이며,

(u, v)는 주파수 영역 변수이다.

CCD로 검출된 영상은 컴퓨터를 거쳐 다시 입력영상으로 들어간 후 L1에 의해 역푸리에 변환되며, 최종출력영상은

$$h(x,y)\bigstar h(x,y)+r(x,y)\bigstar r(x,y) \\ +f(x,y)*\delta(x+2x_0,y)+f(x,y)^{*}*\delta(x-2x_0,y) \tag{7}$$

이 된다. 식 (7)에서 자기상관된(auto correlation) 두 개의 입력영상은 가운데 부분에서, 원 영상 $f(x,y)$은 각각 $2x_0$만큼 떨어져 나타남을 알 수 있다.

그러나, 그림 2에 의한 복호화 방법은 자기상관된 영상의 세기가 너무 커서 원 영상을 그대로 볼 수 없으므로, 자기상관된 영상을 제거하거나 영향을 받지 않도록 하는 작업이 필요하다.

2.3 이진영상과 위상 부호화를 이용한 암호화

$f(x,y)$와 $r(x,y)$ 영상을 각각 '1'과 '0'의 값만 가지도록 이진화한다. 이진화된 영상을 'π'와 '0'의 위상값과 균일한 세기값을 가지는 이진 위상 영상으로 부호화한다. 이렇게 부호화한 랜덤 위상 잡음 영상 $p_r = e^{i\pi r(x,y)}$와 이진 위상 영상 $p_f = e^{i\pi f(x,y)}$ 을 곱하여 얻어진 암호화 영상은

$$h(x,y)=p_f(x,y)p_r(x,y) \tag{8}$$

이며, 위상으로 부호화한 영상들은 균일한 세기값을 가진다.

$$|h(x,y)|^2=|p_f(x,y)|^2=|p_r(x,y)|^2=1 \tag{9}$$

푸리에 변환하여 나타낸 암호화 영상과 키 영상은

$$H(u,v)=P_f(u,v)*P_r(u,v) \tag{10}$$

이며, 이 때 암호화한 영상 $H(u,v)$와 키 영상 $P_r(u,v)$는 모두 복소값을 가진다. 복소값을 가진 암호화 데이터는 크기와 위상 성분으로 이루어지는데, 세기값은 필름을 이용하여, 위상 성분은 광 석판술(optical lithography)을 이용하여 각각 기록할 수 있다.

2.4 JTC 구조를 이용한 복호화

암호화된 이진영상을 복호화하는 구조는 전통적인 결합변환상관기(그림 2)와 같다.

결합변환상관기의 입력으로 푸리에 변환된 암호화 영상 $H(u,v)$과 키 영상 $P_r(u,v)$이 각각 $2u_0$만큼 떨어진 채 SLM에 실린다. 결합변환상관기의 입력평면은

$$E(u,v)=H(u-u_0,v)+P_r(u+u_0,v) \tag{11}$$

와 같다.

SLM의 입력영상은 L1에 의해 푸리에 변환되어 나타나며

$$e(x,y)=h(x,y)e^{j2\pi(u_0x,y)}+p_2(x,y)e^{-j2\pi(u_0x,y)} \tag{12}$$

로 표현된다. $e^{j2\pi u_0}$은 식 (11)의 주파수 이동에 의한 위상 이동 성분이다.

P1에 맺힌 영상을 CCD로 검출하여 위상부분을 '0'으로 할 경우

$$|e(x,y)^2|=\begin{cases} 4, & f(x,y)=0 \\ 0, & f(x,y)=1 \end{cases} \tag{13}$$

이 된다. 이는 원 영상의 반전 영상이 CCD로 검출됨을 의미하며, 식 (7)과는 달리 자기상관된 영상이 원 영상 재생을 방해하기보다는 도움이 된다.

Ⅲ. 지문을 이용한 광 암호화 시스템

지문은 개개인이 가진 고유의 식별자이므로, 랜덤한 암호키로써 사용할 수 있다. 만약, 지문을 승인이 필요한 특별한 마크나 로고와 함께 암호키로 사용할 수 있

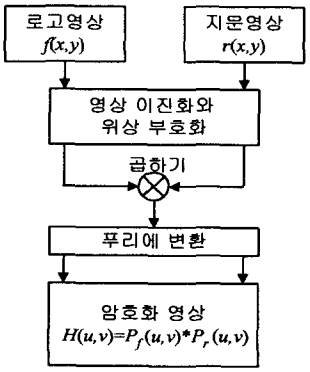


그림 3. 암호화 과정 블록도

다면, 신원의 적합성을 바로 확인할 수 있을 뿐만 아니라, 암호키를 분실하여도 본인이 아니면 복호화 할 수 없기 때문에 매우 높은 보안성을 보장한다.

지문 영상을 키 영상으로, 로고 영상을 원 영상으로 하여 암호화하는 과정은 그림 3과 같다. 이진화된 로고 영상과 지문 영상은 위상 부호화한 후 이들의 곱은 푸리에 변환하여 암호화 영상을 얻는다. 그림 4와 같은 로고 영상과 그림 5와 같은 개인 지문 영상을 키 영상을 제한한 방법에 따라 암호화한 영상은 그림 6과 같다. 암호화된 영상은 복소값을 가지므로 일반적인 세기검출기로는 위상값의 측정이 불가능하다.

그림 4. 로고영상

그림 5. 지문영상

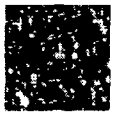


그림 6. 암호화된 영상

암호화된 영상을 복호화할 경우, 그림 7에서와 같이 암호화할 때 사용한 지문영상과 암호화된 영상을 결합변환상관기의 입력으로 나란히 놓고 사용하여 복호화하면 된다. 그림 6의 암호화된 영상을 제안한 방법으로 복호화한 복원 영상은 그림 8과 같다.

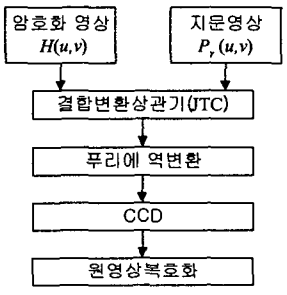


그림 7. 복호화 과정 블록도

그림 8. 복호화된 영상

제안된 방법으로 암호화된 영상을 단체에서 배포하는 ID카드에 부착하여 해당 소속원에게 분배한다. 이후 부착된 암호화된 영상과 CCD와 같은 장비를 통해 얻어진 개인의 지문을 이진위상의 영상으로 전환하여 이의 퓨리어 변환된 영상을 SLM상에 JTC구조로 실어주게 된다. 그리고 구성된 JTC구조에 가간섭성의 레이져 광을 조사하여 퓨리어 변환하게 되면 결과 평면에서는 원래의 로고영상을 다시 얻어낼 수 있게 된다. 이 때 ID카드 소지자의 지문으로만 ID카드에 부착된 암호화된 로고영상을 얻을 수가 있게 된다.

Ⅳ. 결론

본 논문에서는 원 영상과 키 영상의 이진화화 위상 부호화을 이용한 암호화와 방법과 결합변환상관기(Joint Transform Correlator) 구조를 통한 복호화방법을 이용하여 개인서명(Signature) 혹은 단체의 로고(Logo)영상을 개인의 지문으로 암호화하고 다시 당사자의 지문을 통해 암호화된 영상을 복호함으로써 신원의 적합성을 확인하고 보안성을 높일 수 있는 방법을 제안하였다. 제안한 암호화 방법에 사용된 결합변환상관기는 광축을 고려할 필요가 없으므로 광 시스템 구현이 간단하다. 또한, 암호화 데이터는 복소값을 가지므로 공간 광변조기나 LCD로도 표현할 수 있으며, 세기와 위상값을 모두 사용하여 영상을 암호화 하므로 단순한 세기 검출기로만으로는 암호화 영상을 복사 할 수가 없는 장점도 제공한다.

참고문헌

[1] J. W. Goodman, *Introduction to Fourier Optics*, McGraw-Hill, New York, 2nd Ed., 1996.

[2] S. Park, E. Lee, J. Kim, C. Kim, J. Bae, and S. Kim, "Binary image encryption techniques and decrpytion system using JTC," *Proceeding of SPIE*, vol. 4386B, 2001.

[3] 박세준, 서동환, 이승대, 김종윤, 김정우, 이하운, 김수중, "JTC 구조를 이용한 광학적 영상 암호화 시스템," 하계종합학술대회 논문집, 2001.(발표 예정)