論文
5-9-25

광 비쥬얼 크립토그래피를 이용한 지문인식
Fingerprintidentificationbasedonopticalvisual cryptography

이승현(Seng-Hyun Lee)[1]

요약

본 논문에서는 광 시각 암호기술에 근거한 개인 정보보호 방식을 제안하였다. 실험에 사용된 지문 데이터는 광 시각 암호 기술과 개방형 네트워크를 통해 전달된 공유 데이터의 일부를 고려한 secret sharing 방법에 의해 처리되었다. 필요에 따라 한 개인은 자신의 지문을 다른 공유 정보에 제공하는 방식으로 본인의 것을 확인할 수 있다. 다양한 환경 조건에서도 어려움 없이 효과적으로 지문을 인식 할 수 있음을 실험을 통해 검증하였다.

ABSTRACT

We propose an individual authentication method based on optical visual cryptography in that a fingerprint data is processed by secret sharing method taking into account the optical visual cryptography and a part of shared data transmitted through an open network. Whenever it is necessary, submitting his fingerprint with the other shared information can authenticate the owner of the fingerprint. The system efficiently identifies fingerprints through optical correlation, regardless of difficulties of acquisition of exact fingerprint image in the various environments.

Keywords: Joint Transform Correlator, Visual Cryptography, Secret Sharing Schemes, Fingerprint Identification

논문접수 : 2004. 12. 01.
심사완료 : 2004. 12. 24.

1) 정회원 : 광운대학교

* 본 연구는 정보통신부 대학IT연구센터 육성지원사업의 연구결과 및2003년도 광운대학교 교내 연구비에 의해 연구되었습니다.

1. INTRODUCTION

사회 구조가 복잡해짐에 따라 중요한 정보를 보호하기 위하여 복수 회원에게 정보를 분산시킨 후 회원의 합의에 의하여 접근이 허가되는 비밀 관리의 구조가 발달하고 있다. 1979년 A. Shamir는 접근 권한이 동등한 회원으로 구성된 그룹에 적용하기 위한 평등한 비밀 분산법인 thresholding scheme 제안하였다[1]. 이것은 여러 사람이 암호화된 데이터를 나누어 가지고 있다가 권리를 행사하기 위하여 제한된 수 이상의 소유자가 모여 서로의 데이터를 합쳐 키 또는 plane text를 찾아내는 방식으로 크립토그래피에서 매우 중요한 부분을 차지하고 있다. 이이후 thresholding scheme의 한가지 응용 형태인 비쥬얼 크립토그래피가 제안되었다.[2] 인간의 시각 시스템과 같이 영상을 처리하기에 적합한 구조로서 2차원 광학 시스템을 고려할 수 있다. 광학 시스템 구현에 적용할 수 있는 광 정보처리 기술[3-5]은 실시간 처리가 요구되는 분야에서 가장 중요한 기술 중의 하나이다. 특히 2차원으로 확장된 광 정보처리 기술에서는 디지털 알고리즘에서 사용되는 화소 대 화소의 1차원 처리 개념을 영상 대 영상의 2차원 처리 개념으로 확장할 수 있다. 2차원으로 병렬 처리하는 방법은 입력 영상의 크기에 무관한 처리 속도를 제공한다. 최근에 시각 암호를 광학적 특성에 적용하기 위한 연구가 시도되고 있다[6,7]. 이것은 광 시각 암호에 있어서 복호가 완전히 광학적으로 이루어지며, 암복호 데이터로서 계조도를 갖는 영상을 사용한다. 특히 시각 암호에서는 근본적으로 해결이 불가능한 해상도 문제도 개선될 수 있다. 그러나 광 시각 암호에 대한 연구는 아직까지는 초기 단계로서, 그 원리와 응용 가능성만이 제시되어 있는 수준으로 구체적인 구현 방법과 응용 범위는 연구 대상으로 남아 있다. 광 시각암호의 비도는 시각 암호의 비도에 준하고 있으므로 광 시각 암호에 대한 평가는 입력 평문에 대한 복호문의 해상도 평가를 중심으로 수행한다.

본 논문에서는 제한된 입력 영상의 사용과 암복호시 해상도 감소라는 기존 시각 암호의 문제를 해결하기 위하여 광학 시스템을 도입한 광 시각 암호의 특징을 평가 분석하여 이에 적합한 실시간 시각 시스템의 구성을 제안하고 응용 가능성을 확인하였다. 공간정합필터를 사용하지 않는 상관기인 JTC는 광 전자 시스템을 사용하여 구현하기에 매우 적합한 방식[8]이지만 직류 성분(DC)과 자기 상관 성분으로 인하여 상관 효율이 매우 낮다. 이를 개선하기 위하여 1990년대 중반 광 간섭 세기분포인 JTPS(Joint Transform Power Spectrum)를 재구성할 수 있는 기술이 개발[9]되어 상관 성능을 높이고 또한 광 시각 암호 시스템의 성능을 실시간으로 확인할 수 있었다. 성능 평가 결과는 암호화 이전의 원 영상과 복호 후 영상의 유사도로 표시할 수 있다. 유사도가 높으면 암복호 성능이 우수한 것이며, 유사도가 낮으면 성능이 좋지 않음을 나타낸다. 하지만 유사도는 반드시 발생해야 하며, 만일 유사도가 발생하지 않으면 암호문이 변조된 것으로 확인된다. 즉 상관 첨두치를 확인하면 암호문의 변조 여부를 알 수 있다. 제안된 시스템의 성능을 평가하기 위하여 시스템 구현에 적용한 소자들을 컴퓨터 시뮬레이션을 위한 데이터로 입력하고 암호 알고리즘의 seed 값에 따른 결과를 확인하였다. 유사도 판정은 암호화 입력에 대한 복호 출력의 잡음 정도와 암호 특성을 주파수 관점에서 분석하기 위하여 위상과 진폭 성분의 가중치를 변경하며 수행하였으며, 분석 결과를 이용하여 응용 분야에 대한 적용 가능성을 확인하고 실시간으로 구성되는 지문 정보보호 시스템의 구성 방법을 제시하였다.

2. Optical visual cryptography

비쥬얼 크립토그래피는 이진화된 입력 영상의 사용, 낮은 해상도 등으로 인한 표현의 한계로 응용범위가 극히 제한되고 있다.이를 해결하기

위하여 다양한 연구가 진행되고있으며 최근에 binary computer generated hologram(BCGH)에 비쥬얼 크립토그래피를 적용하는 광 비쥬얼 크립토그래피가 제안되었다.

일반적인 암호 시스템은 수학적으로 모듈러 연산이나 "XOR"를 이용하고 있다. 이것은 컴퓨터를 이용하여 구현하기에는 효율적이나 광학 시스템으로 구현하기에는 매우 비효율적이다. 이와 달리 시각 암호화는 복호를 위하여 "OR" 연산을 수행하는데, 이것은 광학에서도 간단히 이루어질 수 있으며, 병렬처리가 가능하다.

광 비쥬얼 크립토그래피에서는 "OR" 연산 특성을 지닌 시각 암호 기법을 BCGH에 적용하여 홀로그램 정보를 보호할 수 있는 방법을 제안한다. 이 방법은 BCGH의 각각의 셀을 시각 암호의 화소로 대체하고 시각 암호화를 수행하는 것으로 간단히 이루어진다. 제안된 방법으로 복호 및 복원된 영상은 기존 시각 암호화 방법으로 복호된 영상에 비하여 높은 해상도를 지닌다. 그럼에도 불구하고 시각 암호와 동일한 비도를 유지한다.

기존의 암호 방법은 디지털 처리에는 적당하나 광학에 적용하기는 매우 비효율적이다. 기존의 알고리즘을 적용하기 위해서는 광 데이터를 디지털로 전환하여 보관하고 복호하여 다시 광 데이터로 전환해야 한다. 이것은 적당하지 못한 방법으로 암호 알고리즘을 광시스템에 적용하기 위해서는 광학적으로 복호하는 것이 필수적이다. 즉 CGH에 기록되는 정보는 블록 암호, 스트림 암호, 공개키 암호 등과 같이 기존에 암호학에서 알려진 방법을 직접 적용하기에는 적당하지 않다. 따라서 암호화는 디지털적으로 이루어져도 복호는 광학적으로 수행될 수 있는 알고리즘이 요구된다. 시각 암호화는 강력한 영상 암호 기능을 지니고 있음에도 불구하고 많은 제한점을 갖고 있다. 대상이 되는 영상은 이진화되어 있어야 한다. 일반적으로 이진화된 영상은 백화소 주변의 화소는 백화소일 가능성이 매우 높고 흑화소 주변의 화소는 흑화소일 가능성이 매우 높다. 이것은 안전성를 낮추는 강한 요인이 된다. 또한 암복호 과정에 부화소의 더하기 과정만이 존재하므로 복호된 영상의 백화소 부분에는 각 화소당 하나 이상의 흑 부화소가 존재하여 신호대잡음비가 낮다. BCGH는 이진값으로 구성되어 있어도 회색 준위의 영상을 표현할 수 있다. 특히 패턴인식에 이용되는binary phase-only filter는 백화소 주변의 화소가 백화소일 가능성은 최대 50%를 넘지 못하며, 이것은 흑화소의 경우에도 동일하다. BCGH는 시각 암호화에서 요구하는 입력 조건을 만족하고 있다. 따라서 BCGH에는 시각 암호화 기법을 적용할 수 있으며 보호된 BCGH는 시각 암호의 안전성을 갖는다. 광 비쥬얼 크립토그래피 구성 방법은 그림 2와 같다. 먼저 암호화 하고자 하는 원영상이 주어진다. 이때 영상은 이진화되어 있을 필요는 없다. 이 영상은 직접 이용되는 것이 아니라 광학적 처리를 위하여 BCGH로 제작된다. 여기에 비쥬얼 크립토그래피를 적용한다. BCGH는 여러 개의 share로 나뉘어질 것이며 각각의 share는 서로 다른 사람들이 보관하게 될 것이다. 이때 발생하는 share의 개수는 사용하고자 하는 용도와 알고리즘에 따라 결정된다. 복호화는 요구되는 숫자 만큼의 share가 겹쳐지면 나타날 것이다. 암호화의 결과는 BCGH 이다. 그러나 암호화 이전의 BCGH와 동일하지는 않을 것이다. Original BCGH의 cell이 share 구성을 위하여 subcell로 만들어지는 과정에서 발생한 잡음이 추가되어 있다. 복원된 BCGH를 복원하면 원영상과 차이가 있게되는데 이것은 subcell이 움직이는 면적의 범위에 영향을 받는다. 시각 암호화는 화소를 부화소로 나누어 암호화하므로 원 영상의 해상도를 낮춘다. 즉 복호된 BCGH의 해상도가 낮아진다. BCGH의 해상도가 낮아지면 BCGH내에 기록된 영상은 크게 손상을 입을 것임을 예측할 수 있다. 복호된 BCGH에는 상대적으로 흑화소가 증가해 있으나 백화소의 수는 원 BCGH의 백색 셀의 수와 일치하며 위치변화도 제한적이다. 백화소의 이동은 하나의

셀을 화소로 해석하고 부화소를 만들기 위해 확장한 해상도 범위내이다. 단지 그 위치가 무작위로 변화하고 있을 뿐이다. 즉 백화소와 백화소간의 평균 간격 비율은 BCGH의 흰색 셀 간격 비율과 일치한다. 따라서 복호된 BCGH를 퓨리에 변환하면 원영상이 복원된다. 무작위 변화는 퓨리에 변환하면 백색잡음으로 변하여 전 대역에 걸쳐 나타난다.

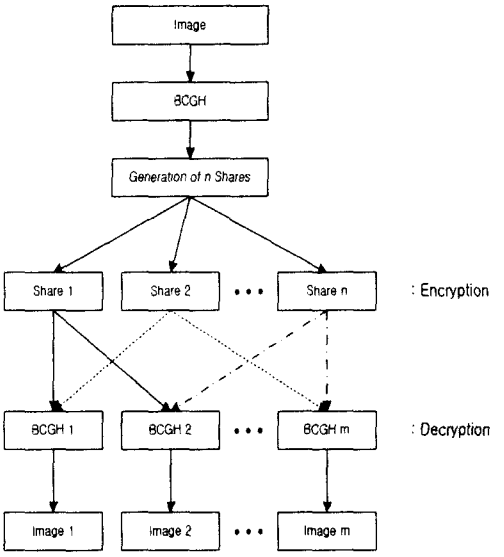


그림 2. 광 비쥬얼 크립토그래피의 구성 절차
Fig. 2 The composing procedureof optical visual cryptography

3.fingerprintidentification

정보화 사회의 발달에 따라 개인 정보 관리에 대한 관심이 급속히 증가하고, 자동화 장치나 보안을 목적으로 하는 많은 분야에서 전기 전자적인 장치를 이용한 개인 인증 시스템의 필요성은 매우 절실하다. 이러한 개인 인증 시스템은 높은 정확성과 함께 인증을 위한 개인 정보의 도난 시 타인이 이용할 수 없어야 하며, 위조가 불가능해야 할 뿐만 아니라 휴대 등으로 인한 훼손에는 즉각 대응할 수 있어야 한다. 개인 인증 시스템에서 개인의 식별에 이용되는 정보는 선천적인 신체 정보, 서명과 같이 습관화되어 재현성의 정확도가 필요한 정보, 그리고 인위적으로 구성한 개별 정보를 들 수 있다. 인위적으로 구성한 개인 정보를 이용하는 경우에는 정확도는 높일 수 있으나 훼손, 도난, 위조 등으로 관리가 어려우며, 범죄를 유발시키는 요인이 되고 있다. 이러한 문제는 선천적인 신체 정보인 지문을 이용함으로써 효과적으로 극복할 수 있으나, 이 정보들이 자연계에 다양한 형태로 존재하기 때문에 데이터베이스 구축 및 판별이 대단히 어렵다. 지문 영상의 특징은 개인 간의 지문 형태가 명백하게 차이가 있는 반면에 좁은 영역에 많은 정보들이 집중되어 있고, 외형적으로는 형태가 매우 복잡하여 지문 간의 육안 판별이 용이하지 않으며 패턴 역시 규격화되어 있지 않다. 하지만 주파수 관점에서 살펴보면, 모든 지문 영상은 고유 주파수를 지니고 있기 때문에 어떤 지문 영상의 고유 주파수를 이용하여 패턴 정합을 시도하면 효과적인 지문 인식 결과를 얻을 수 있다. 즉, 서로 다른 지문 영상의 구분은 입력 지문 영상과 데이터베이스에 수록된 지문 영상에서 주파수 신호를 추출하여 광학적으로 상관시키면, 두 지문 간의 유사성을 쉽게 판단할 수 있다. 따라서 본 논문에서는 개인 인증용 정보로 가장 효과적인 지문 패턴을 대상으로 광 시각 암호 기술을 적용하고, 광 상관기를 통하여 인증 하는 방법을 제안한다. 인증 방법은 외부에서 입력된 영상과 데이터베이스에 저장된 영상을 상관시켜 지문 간의 유사도를 판정한다. 광-디지털 하이브리드 지문 정보보호 시스템은 광학의 2차원 실시간 병렬처리 특성과 디지털 시스템의 알고리즘 유연성 및 정확성을 상호 보완적으로 이용할 수 있게 한다. 제안한 지문 정보보호 시스템은 그림 3과 같은 처리 절차를 가진다.

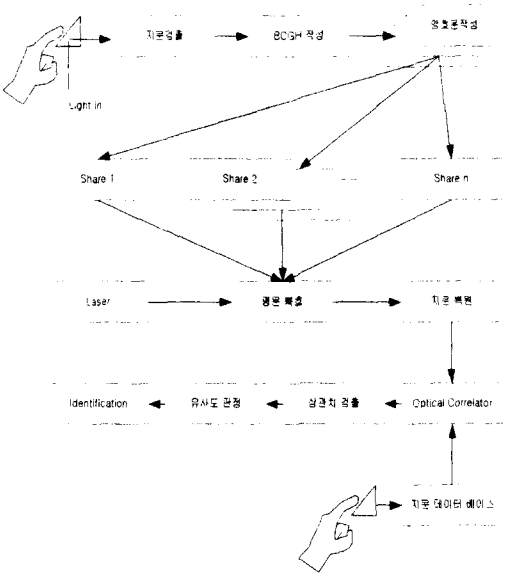


그림 3. 광 시각 암호를 이용한 지문 정보보호 시스템

Figure 3. Fingermark security system by optical visual cryptography

여기에 이용되는 지문 영상은 표준 프리즘을 통하여 입력된다. 시스템 동작을 위하여 암호화 하고자 하는 대상의 지문을 갖는 손가락이 프리즘의 빗면 위에 지문의 융선과 유리가 접하는 곳에서 경계 조건 변화 특성을 이용하여 지문 데이터를 얻는다[10]. 융기된 융선 부분에서 대부분의 광이 흡수되고 지문의 융선과 유리면이 접하지 않는 곳에서는 전반사가 발생한다. 따라서 지문 영상의 융선 만을 얻을 수 있다. 지문 데이터는 데이터 양이 방대하기 때문에 일반적인 지문인식 시스템은 지문 형태에 대한 특징을 추출하여 사용하지만 광 상관기를 이용하는 시각 암호 시스템은 영상 자체를 그대로 사용한다. 광 시각 암호 시스템에 기반하여 구성되는 지문 정보보호 시스템 역시 영상 자체를 그대로 이용한다. 입력된 지문을 BCGH를 사용하여 홀로그램으로 작성하고, 원하는 수만큼 share를 작성한다. 각각의 share는 여러 가지 경로를 통해 다시 모이게 되고 평문으로 복호될 것이다. 복호된 평문을 광학적으로 퓨리에 변환하면 지문 영상이 복원될 것이다. 그리고 이것을 확인하기 위하여 최종 확인자가 자신의 지문을 입력하거나 데이터베이스에서 데이터를 읽어 복원된 지문과 광학적으로 상관을 발생시킨다. 그리고 서로간의 상관도를 판단하여 암호문이 정확한 데이터인가를 확인한다.만일share에 대한 위조가 있는 경우 기본적으로 BCGH가 구성되지 않기 때문에 복호된 평문을 퓨리에 변환하면 어떠한 형태의 지문도 나타나지 않는다. 또한 어떠한 형태의 지문이 입력되는 경우 이 지문이 허위로 작성된 것이라면 상관도 판정을 통과하지 못할 것이다. 광 시각 암호 시스템은 암호화 과정에서 발생하는 백색 잡음으로 인하여 평문을 완벽하게 복구하지는 못한다. 그러나 기본적으로 지문인식 시스템은 데이터를 완전하게 정합시킬 필요가 없으며, 환경이나 지문입력 방법에 따라 정확한 데이터가 입력되지 않으므로 유사도를 통하여 사용자를 효율적으로 식별할 수 있다. 따라서 광 시각 암호 시스템을 지문 정보보호 시스템에 적용하는 것은 매우 타당한 것으로 판단된다.

4. Experiment

광 비쥬얼 크립토그래피의 유사도 판정을 하는 시스템은 그림 4와 같다. 시스템은 광 퓨리에 변화을 수행하는 3개의 광축으로 구성된다. 두 개의 공간광변조기(SLM 1, SLM 2)로 구성되는 가장 위쪽의 퓨리에 변환 시스템은 광 비쥬얼 크립토그래피를 구현한 것이다. SLM 3을 사용하는 두번째 광축은 JTPS를 얻는 과정이며 마지막 광축은 역퓨리에 변환을 통하여 상관도를 얻는다. 시스템 동작은 먼저 키 영상을 SLM 2에 나타내고 cipher text image를 입력 받아 SLM 1에 나타내면 디지털 카메라 1에 복호된 plane text image가 나타난다. 검출된 영상은 영상 프로세서에서 PEJTC 입력 평면구성에 적당하도록 재구성하여 SLM

3에 디스플레이하면 디지털 카메라 2에서 파워 스펙트럼을 검출할 수 있다. 이 과정은 스펙트럼 교정기가 PEJTC에 적당하도록 스펙트럼을 재구성할 수 있도록 동작한다. 그리고 이 결과를 SLM 4에 나타내면 디지털 카메라 3에서 상관값이 검출될 것이고 이를 사용하여 결과를 분석한다. 별도의 정합필터를 이용하지 않는 JTC는 퓨리에 입력 평면(SLM1)을 2단으로 분리하여 한쪽 반평면에 기준 평면 그리고 다른 쪽에 비교 평면을 동시에 위치시키고 상관을 시키게 된다. 이 논문에서는그림 5와 같이 상하로 2단 분리하여 구성하였다. 상단은 기준 평면으로 BCGH로부터 직접 얻은 영상이 위치하고 있으며, 하단은 비교 영상으로 광 비쥬얼 크립토그래피의 출력 영상 이 위치하고 있다.

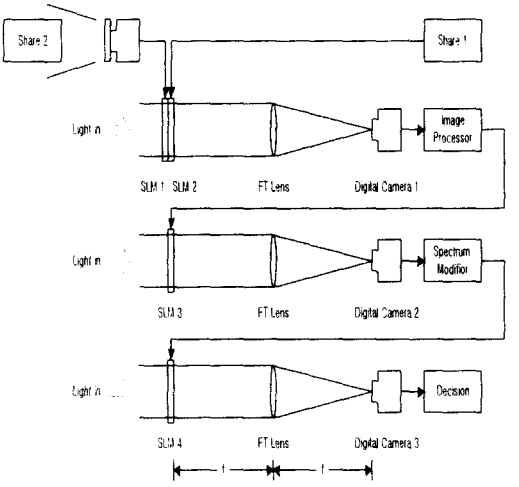


Fig. 4. 유사도 판정 시스템

Fig. 4. The system for discrimination of similarity degree

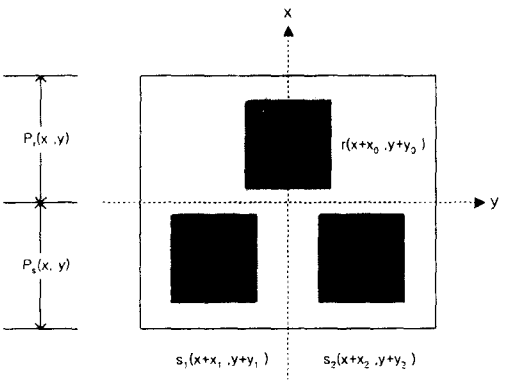


그림 5. JTC 의 입력평면

Fig. 5. Input plane of JTC

이와 같이 하나의 입력 평면을 그림 4의 두번째 광축에 위치시켜 두 평면을 동시에 퓨리에 변환하여 디지털 카메라를 이용하여 검출하면 식(1)과 같은 광간섭세기분포인 JTPS를 얻을 수 있다.

$$E_{JPS}(u,v) = |E_r(u,v) + E_s(u,v)|^2 = |E_r(u,v)|^2 + |E_s(u,v)|^2 + E_r^*(u,v)E_s(u,v) + E_s(u,v)E_r^*(u,v) \quad (1)$$

여기서 $E_r(u,v)$는 상단 평면의 공간 주파수 성분이며, $E_s(u,v)$는 하단 평면의 주파수 성분이다. 그리고 $*$는 복소 공액을 나타낸다. 식(1)은 크게 autocorrelation과 crosscorreltion 2가지 성분으로 나누어 해석할 수 있다. $|E_r(u,v)|^2$, $|E_s(u,v)|^2$이 autocorrelation 성분으로 자기자신간에 발생한 성분이므로 서로 다른 영상간의 상관관계를 측정하려는 목적에 맞지 않는 성분으로 잡음으로 작용한다. 나머지 두성분은 $E_r(u,v)$과 $E_s(u,v)$간의 crosscorreltion 성분으로 필요로하는 신호이다. 이것은 두 영상 상호간에 교대하며 복소수로 이루어진 공간정합필터와 입력으로 작용하며

중첩된 간섭 분포를 이루고 있다. 그러나 그 값은 실수이며 서로간에 원점 대칭을 이루고 나타난다. 만일 두 영상이 동일하다면 처음에 나타난 autocorrelation 값과 동일 할것이다. 따라서 필요한 crosscorreltion 값만을 추출할 필요가 있는데 이것은 식(2)를 구현하는 것으로 가능하다.

$$
\begin{aligned}
E_{NEW}(u,v) &= E_{JTC}(u,v) - |E_r(u,v)|^2 - E_s(u,v)|^2 \\
&= E_r^*(u,v)E_s(u,v) + E_r(u,v)E_s^*(u,v) \\
&= |R(u,v)||S(u,v)|\{e^{-i\theta_r}e^{i\theta_s}e^{-i2\pi[u(x_r-x_s)+v(y_r-y_s)]} + e^{i\theta_r}e^{-i\theta_s}e^{-i2\pi[u(x_s-x_r)+v(y_s-y_r)]}\}
\end{aligned}
\tag{2}
$$

식(2)의 구현은 이미 실험적으로 증명이 되었다. 먼저 식(1)에 따라 JTPS를 구하고, 동일한 SLM에 상단면만을 디스플레이하여 디지털 카메라에서 $|E_r(u,v)|^2$ 를 검출한다. 그리고 동일한 SLM 하단면만을 디스플레이하면 $|E_s(u,v)|^2$ 를 구할 수 있다. 그리고 두 값을 JTPS에서 빼면 식(2)가 간단하게 얻어진다.
이상의 상관값에서 위상과 진폭이 모두 고려되어 있다. 따라서 폭넓은 sidelobe가 나타날 수 있다. 기본적으로 중첩을 피하기 위해서는 $r(x+x_r, y+y_r)$ 와 $s(x+x_s, y+y_s)$ 의 간격을 LCD 높이의 1/2 이상 분리하여 사용하여야 sidelobe간에 중첩이 발생하지 않는다. 만일 그 이내에서 사용하려면 진폭을 제거해야 하는데 이미 구해지 값들을 이용하여 식(3)을 구현하면된다.

$$
\begin{aligned}
PH\{E_{NEW}(u,v)\} &= \frac{E_{NEW}(u,v)}{|E_r(u,v)||E_s(u,v)|} \\
&= e^{i\theta_r - i\theta_s}e^{i2\pi[u(x_r-x_s)+v(y_r-y_s)]} + e^{i\theta_s - i\theta_r}e^{-i2\pi[u(x_r-x_s)+v(y_r-y_s)]}
\end{aligned}
\tag{3}
$$

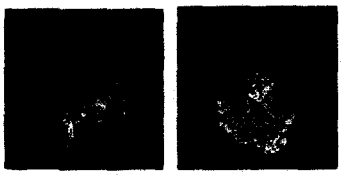
식(3)을 역퓨리에 변환하면 식(4)와 같이 두 개의 공간정합필터를 이용한 상관기 출력이 나타난다.

$$
\begin{aligned}
c_{NEW}(u,v) &= \mathfrak{I}^{-1}\{E_{NEW}(u,v)\} \\
&= Edge\{r(x,y)\} \otimes Edge\{s(x,y)\} * \delta[x+(x_r-x_s), y+(y_r-y_s)] \\
&\quad + Edge\{r(x,y)\} \otimes Edge\{s(x,y)\} * \delta[x-(x_r-x_s), y-(y_r-y_s)]
\end{aligned}
\tag{4}
$$

식(4)의 결과는 DC 성분이 존재하지 않으므로 에너지 효율이 향상되고, 불필요한 상관첨두치가 제거되어었으므로 분리 조건에 자유롭다는 매우 중요한 의미를 지닌다. 특히 영상의 위상 성분을 발생시키는 경계면의 상관 관계를 나타낸다. 즉 면적에 해당하는 진폭 성분이 기여하지 않았으므로 sidelobe가 발생하지 않는다. 그러나 진폭 성분이 제거되었으므로 상관값은 알 수 없고 상과도만을 알 수 있다. 그러나 이것은 본 논문의 목적에 부합한다.

지문 정보보호 시스템의 실험 및 평가를 위하여 세 가지 경우에 대한 가정을 하였다. 첫 번째는 암호문을 복호한 결과가 표적으로 삼고 있는 원래 지문과 동일한 경우이다. 두 번째는 복호한 결과가 표적과 다른 지문으로 복원된 경우로서 신분을 위장하기 위하여 광 시각 암호 제작 알고리즘에 따라 가짜 지문을 이용하여 제작한 암호문이 복호 후에 정상적으로 복원되었을 때이다. 일반적으로 기존의 암호에서는 이러한 가정을 하지 않는데 이것은 서로간의 키가 일치하지 않으면 알고리즘을 알고 있더라고 무의미하기 때문이다. 그러나 별도의 키를 사용하지 않는 시각 암호나 광 시각 암호를 시스템에 적용하기 위해서는 반드시 고려해야 하는 사항이다. 마지막 세 번째는 가장 일반적으로 발생할 수 있는 경우로 누군가가 암호문을 위조 또는 변조한 경우이다. 가짜 지문에 대한 실험을 위하여 그림 6과 같은 지문을 시스템 입력으로 사용하였다. 그림 6(a)는 암호화하여 보호하고자 하는 지문 영상이며, 그림 6(b)는 가짜 지문 영상으로서 원래 지문과 가능한 유사한 지문을 선택하였다. 사용한 가짜 지문은 원래 지문을 약간 오른쪽으로 옮긴 듯한 형태로 무늬의 방향이나 골의 모습이 표적 지문과 유사한 무늬를 가지고 있어서 적지 않은 유사도를 나타낼 것으로 유추할 수 있

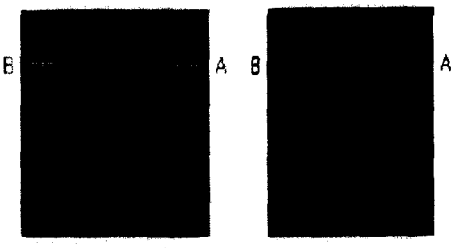
다. 암호문 변조 실험은 기준 영상인 그림 6(a)를 대상으로 제작한 암호문 중에서 임의로 한 장 이상을 선택하여 일정량의 화소 값을 변경하여 실험에 사용하였다. 화소 값 변경은 임의의 한 화소를 선택하여 흑화소를 백화소로 또는 백화소를 흑화소로 바꾸는 방법을 사용하였다.



(a) 암호를 위한 지문 (b) 가짜 지문

그림 6. 지문 정보보호 시스템의 입력 영상
Fig. 6. Input images of the fingerprint encryption system

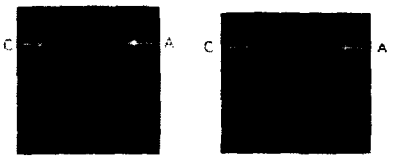
다양한 지문 데이터를 실험에 사용하였고, 다양한 범위의 암호문 변조 및 위조를 시도하였다. 실험 결과 중 그림 6(b)의 가짜 지문을 사용한 결과는 그림 7과 같으며, 임의의 암호문 한 장에 대하여 30% 변조를 발생시킨 경우의 실험 결과는 그림 8과 같이 나타난다. 시각적으로 원래의 지문과 명백히 다른 가짜 지문이 입력된 경우에는 그림 6(b)의 지문을 사용했을 때보다 더 낮은 상관도를 나타내었다. 또한 여러 장의 암호문을 약간 씩 변경한 경우에도 이들이 모두 합쳐진 이후 CGH가 복원되므로 한 장만을 대상으로 한 실험한 결과와 유사하였다. 그림 7은 가짜 지문에 대한 실험 결과로서, 그림 6(b)의 가짜 지문이 지문 정보보호 시스템을 통과한 후 얻은 최종 상관 결과이다. 그림 7(a)는 알파=베타=0 을 사용한 결과이며, 그림 7(b)는 알파=1, 베타=0 을 사용한 결과이다. 상관 평면에서 'A'로 표시한 상관 첨두치는 원래 영상의 복호 후 결과이며, 'B'로 나타낸 부분은 다른 지문에 의한 상관 첨두치이다. 상관기 결과는 알파와 베타에 관계없이 복호된 표적 지문 영상의 상관 첨두치가 가짜 지문 영상에 비하여 분명한 상관 첨두치를 발생시키고 있다. 광 시각 암호 시스템이 정확하게 암복호 동작을 수행한다면 이것은 당연한 결과이다. 그러나 지문 영상은 매번 입력될 때 마다 약간씩 다르게 변화하므로 유사도 판정을 낮은 값으로 설정해야 한다. 이때는 지문의 유사도에 따라 판정 오류가 발생할 수 있으므로 실제로 시스템을 구성하는 경우에는 이를 고려하여야 한다. 이것은 일반적으로 지문 인식 시스템이 갖고 있는 특징[43]으로 이에 대한 판별력이 지문 인식 시스템의 성능이라 할 수 있다.



(a)알파=베타=0 (b) 알파=1. 베타=0

그림 7. 상관 평면(가짜 지문이 입력된 경우)
Fig. 7. Correlation plane(Case of a nontarget input)

그림 8은 암호문이 변조된 경우를 가정하여 시험한 결과이다. 'A'는 그림 7과 같이 표적 영상이 발생시킨 상관 첨두치이며, 'C'는 암호문이 위조된 영상이 발생시킨 상관 첨두치이다. 상관 결과 변조된 암호문에 의한 결과는 상관 첨두치를 전혀 발생시키지 못하였다. 이는 변조된 암호문이 BCGH를 정확히 복호하지 못하데 기인하는 것으로 상관에 참여한 지문 영상은 실제로는 잡음과 같은 형태로서 지문의 형태를 갖추지 못한 결과이다.



(a)알파=베타=0 (b) 알파=1, 베타=0

그림 8. 상관 평면(암호문이 변조된 경우)
Fig. 8. Correlation plane (Case of a counterfeit input)

이상의 실험 결과는 암호문의 변조는 다른 영상에 의한 결과 보다 검출하기 쉽다는 것을 알 수 있다. 이는변조된 암호문이 BCGH를 손상시키고 이로 인하여 지문이 복원되지 못하기 때문이다. 그러나 CGH 특성상 CGH의 일부만이 남아 있더라도 반복 수행에 의하여 지문을 복원해 낼 수 있다. 따라서 암호문이 변조가 아니라 손상이라면 복원해 낼 수 있다. 그러나 광 시각 암호 시스템의 비도는 시각 암호 시스템의 암호 강도와 같으므로 이러한 홀로그램의 데이터 복원 특성을 이용하여 암호문을 해독하는 것은 시각 암호를 해독하는 것과 유사한 난이도를 갖는다. 광 시각 암호 시스템 구성은 크게 두 부분으로 구성되며, 영상을 복호하는 전처리 단과 유사도를 판단하는 후처리 단으로 구성하였다. 즉, 전처리 단에서는 암호문을 복호하여 BCGH를 만들고 이를 퓨리에 변환하여 기록된 영상을 복원하면 후처리 단에서 암호문의 변조 여부를 확인하였다. 전처리 단에서 영상을 기록하고 암호화에 사용된 BCGH는 사용목적에 따라 다양하게 사용될 수 있다. 본 논문에서는 성능 평가를 위하여 필터 구성에 적합한 수준으로 BCGH 방법을 사용하였으며 보다 고품질의 영상을 얻기 위해서는 복잡한 다른 알고리즘을 사용해야 한다. 그러나 이러한 수준을 만족하기 위해서는 보다 화소수가 많은 LCD를 사용해야 한다. 일반적으로 사용되고 있는 LCD는 1024 x 768 화소를 넘지 않고 있으므로 고품질의 영상을 사용하기 위해서는 보다 화소수가 많은 LCD를 제작해서 사용해야 한다. 그리고 영상 자체를 보는 것을 목적으로 하는 경우에는 후처리 단을 사용할 필요가 없으며, 레인보우 홀로그램이나 프라넬 홀로그램을 사용한다면 전처리 단의 구성도 이에 적합하게 변형하여야 한다. 그러나 광 시각 암호 시스템 구현 원리는 그대로 유지되며, 홀로그램 복원 방법만 바뀔 것이다. 그리고 영상 기록 장치 외에 정합필터 자체를 보호하거나 Dammann grating과 같은 필터를 입력 데이터로도 사용할 수 있다. 만일 저해상도 LCD를 사용한다면 암호 키 데이터를 전송하는 방법으로도 사용이 가능하다.

5.conclusion

본 논문에서는 하이브리드 광전자 시스템을 구성하여 실시간 시각 암호 시스템을 구현하는 방법을 제시하고 시뮬레이션을 통하여 구현상의 문제점 및 타당성을 도출하였다. 새롭게 제안된 광 시각 암호는 광 상관기 기반의 광 정보처리에 적용하여 유용한 결과를 얻었으며, 기존 시각 암호에서 근본적으로 해결이 불가능하였던 해상도 문제를 개선할 수 있었다. 또한 광 시각 암호 기술을 이용한 지문 정보보호 시스템을 구성하여 광 시각 암호의 응용 가능성을 확인하였다. 실험 결과의 분석을 통하여 디지털 및 사람의 시각에 의존하고 있던 임계치 방식 암호를 광학 분야로 적용 가능함을 확인하였으며, 시스템으로도 구현이 가능함을 알 수 있었다.

References

[1] A. Shamir, "How to Share Secret", CACM, Vol.22, pp.612-613, 1979.

[2] M. Naor and A. Shamir, "Visual Cryptography", Proc. of Eurocrypt'94, pp.1-12, 1994.

[3] R. Hughes et al, "Quantum Cryptography," Contemporary Physics, Vol.36, No.149, 1995.

[4] F. T. S. Yu, Optical Information Processing, John Wiley & Sons, 1983.

[5] D. Flannery and J. Horner, "Fourier Optical Signal Processors", Proc. of IEEE, Vol.77, No.10, pp.1511-1527, 1989.

[6] Sang-Yi Yi, Chung-Sang Ryu, Seung-Hyun Lee, and Eun-Soo Kim"Encryption of Cell-Oriented Computer Generated Hologram by using Visual Cryptography", CLEO/Pacific Rim'99, 1999.

[7] B. Brown and A. Lohmann, "Computer Generated Binary Holograms", IBM J. Res. Develop., Vol.13, pp.160, 1969.

[8] B. Javidi, "Comparison of Binary Joint Transform Correlators and Phase-Only Matched Filter Correlators", Opt. Eng., Vol.28, No.3, 1989.

[9] K. Macukow and C. Gorecki, "Optoelectronic Implementation of the Quasi-Phase Correlator", Opt. Comm., Vol.93, No.1,2, pp.11-18, 1992.

[10] D. Vernon, "Automatic Detection of Secondary Creases in Finger-print", Opt. Eng., Vol.32, No.10, pp.2616-2623, 1993.