論文2003-40SD-8-1

BPEJTC를 이용한 광 비쥬얼 크립토그래피

(Optical Visual Cryptography based on Binary Phase Extraction JTC)

李 相 二 *, 李 丞 玄 **

(Sang-Yi Yi and Seung-Hyun Lee)

요 약

비쥬얼 크립토그래피는 암호법에서 중요한 정보를 암호화하여 복수 회원에게 분산시킨 후 회원의 합의에 의하여 해독이 가능하게 하는 thresholding scheme을 디지털 시스템인 아닌 인간의 시각 시스템으로 해독이 가능하게 하였다. 그러나 표현의 한계로 인하여 몇 가지 문제점을 지니고 있었다. 이후 인간의 시각을 대신하여 레이저를 사용하는 광 비쥬얼 크립토그래피가 제안되어 광학 시스템에 암호법을 적용할 수 있게 되었다. 그러나 이 시스템은 기존의 비쥬얼 크립토그래피의 문제점을 완전히 극복하지 못함으로 인하여 또 다른 문제를 발생하였다. 이 것은 데이터 처리 시스템을 시각에서 광학으로 전환하는 과정에서 발생하였으므로 문제의 분석과 해결 역시 광학적으로 접근하는 것이 타당하다. 본 논문에서는 joint transform correlator를 이용하여 광 비쥬얼 크립토그래피에서 발생하는 잡음의 정도와 안정성을 주파수 관점에서 분석하였다.

Abstract

Visual cryptography made it possible to decrypt thresholding scheme with not digital system but human vision system. This method, however, has some limit in it. Optical visual cryptography was proposed which used laser instead of human eyesight. As a result, it was possible to adapt cryptography to optical system. However, it also had some difficulties because it did not overcome the existing problem of visual cryptography completely. These problems occurred in the process of transferring data processing system from visual to optics. Therefore, it is appropriate to approach these problems in terms of optics. This paper analyzes the level of noise and the security characteristics foroptical visual cryptography in terms of frequency based on joint transform correlator

Keyword : Joint Transform Correlator, Binary Phase Extraction JTC, Visual Cryptography, Secret Sharing Schemes

* 正會員, 國家保安技術研究所
(National Security Research Institute)
** 正會員, 光云大學校 電子工學部
(Dept. of Electronics Engineering, Kwangwoon Univ.)
※ 본 논문은 2002년도 광운대학교 교내학술연구비 지원에 의해 연구되었음
接受日字:2002年11月5日, 수정완료일:2003年7月31日

Ⅰ. 서 론

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 비

밀 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 암호법에서 매우 중요한 부분을 차지하고 있다. 이 이후 thresholding scheme의 한 가지 응용형태인 visual cryptography(VC)를 제안하였다[2].

VC는 매우 독특한 구조로 구성되어 있다. RSA와 같이 수학적 알고리즘을 사용하는 것도 아니고 DES와 같이 하나의 키를 이용하여 큰 데이터를 암호화하는 방식도 아니다. Stream ciper 와 같은 랜덤 변수 발생기로 랜덤 변수를 발생시키고 이에 따라 데이터를 한 가지 상태 또는 다른 상태로 구성하는 것이다. 해독을 위한 별도의 키는 존재하지 않으며 키의 길이도 데이터 크기 만큼 크다. 키가 길다는 것은 암호학적으로 좋지 않다. 그럼에도 불구하고 높은 안전성과 해독의 편리성으로 관심이 높다.

VC는 키의 길이와 같은 안전성 측면외에 이진 영상 사용, 복호 후 해상도 감소라는 입출력 데이터에 대한 단점도 있다. 그레이 영상 사용에 대한 연구는 상당히 발전하고 있으나 이것으로 인한 단점도 동시에 증가하고 있다. 해상도 향상에 대한 한계는 이미 수학적으로 증명되어 있다. 즉 입력과 출력은 유사하는 동일하지 않다. 다만 인간의 시각적으로 문제 미미할 뿐이다[3].

광학 시스템에서는 양자의 성질을 이용하는 quantum cryptography를 제외하고 암호 시스템이라고 명명할만한 것은 없는 상태이다. 다만 최근에 VC를 광학적으로 적용하려는 시도가 있었다. 새로이 제안된optical visual cryptography(OVC)는 광정보처리 특히 이진 컴퓨터 형성 홀로그램(BCGH)에 적용하여 유용한 결과를 얻었다[4, 5]. Decryption은 완전히 광학적으로 이루어졌으며 암복호 데이터로 그레이 레벨 영상을 사용할 수 있었다. 특히 VC에서는 근본적으로 해결이 불가능한 해상도 문제도 해결하였다. 그러나 복호된 영상이 암호 입력과 완전히 동일하지는 않은 상태이다.

VC에서 해상도 평가는 매우 간단하고 단순하다. 하나의 화소를 몇 개의 부 화소로 분리하는가가 관건이며 대체로 1/subpixel 개수만이 유효 데이터이다. 이것은 해상도가 매우 낮아 출력을 시각적으로 확인하는 것만으로도 해상도를 판단할 수 있다는 것을 의미한다. OVC의 출력은 보다 높은 해상도를 유지하므로 시각적으로는 판단이 어렵다. 특히 주파수 평면에서 처리하고 있으므로 잡음이 화소 보다는 평면 전체에 분포되어 있다. 따라서 단순히 영상처리 방법을 적용하는 것만으로는 유사도 판단이 어렵다. 그리고 화소 단위로 처리하는 것은 적당하지 않다.

평면 전체에 대한 유사도 판정은 공간정합필터를 사용하면 적당하다. 그러나 처리하려는 데이터량이 많고 빠른 시간에 데이터 간에 교체를 시도해야 하므로 공간정합필터보다는 joint transform correlator(JTC)가 적당하다. JTC는 실수 평면에서 사용할 수 있는 장점으로 인하여 구현이 쉽고 응용분야도 넓다. 최근에는 그 동안 문제점으로 지적되고 있던 자기상관문제도 해결되었고 위상 성분만으로 joint transform power spectrum(JTPS)도 구현이 가능하게 되었다.

본 논문에서 정합하고자 하는 대상이 작은 표적의 형태가 아니라 전체 면적대 면적 비교를 하는 것이므로 진폭에 의하여 sidelobe가 발생하는 정합기를 사용하는 것보다는 위상 비교를 하는 것이 효과적이다. 여기에 적당한 JTC가 BPEJTC이다[6]. 이것은 위상 특성이 강할뿐만 아니라 JTPS를 이진화하여 BPEJTC로 구성하면 실시간 광상관기로도 구현할 수 있는 매우 유용한 도구이다. 본 논문에서는 먼저 VC를 간단히 정리하고 OVC를 구성하는 방법을 기술한다. 그리고 암호화 입력에 대한 decryption 출력의 잡음의 정도와 안전성 특성을 주파수 관점에서 분석하기 위하여 단일 입력 영상에 대하여 다양한 암호 seed를 적용하여 서로 다른 암호 출력을 얻은 이후 PEJTC로 결과를 평가한다. 평가를 위해 안정성은 암호화된 평면에 적용되며 유사도 판정은 최종 출력에 대하여 평가된다. 이 모든 과정은 컴퓨터를 이용한 시뮬레이션으로 이루어졌으나 광학적으로 구현하기 위한 모델도 함께 제안하였다.

Ⅱ. 비쥬얼 크립토그래피

Thresholding scheme에 기초하고 있는 VC는 암호적인 투표 기법, 키 위탁 및 키 복구, 그룹 서명, 전자 화폐등에 응용하려는 목적으로 연구가 진행되고 있다. VC의 강점은 구현의 편리성이다. 암호화는 몇 장의 투명한 용지에 원 영상을 분산하여 구성하는 것으로 간단히 구현할 수 있다. 여러장으로 분산된 투명한 용지 중 임의의 한 장 또는 몇 장을 암호 영상으로 선택하면 나머지 용지는 키 영상이 된다. 그러나 나머지 용지 모두가 키 영상이 되는 것은 아니다. 여기까지는 출력

데이터를 투명한 용지에 그렸다는 것을 제외하면 thresholding scheme과 별다른 차이점이없다. 그러나 복호는 상당한 차이가 있다. 우선 복호가 너무 간단하다. 암호 영상 위에 키 영상을 순서에 관계없이 겹쳐서 중첩시키면 원 영상이 나타난다. 이와 같이 시각 암호화는 별도의 복호 알고리즘을 수행하지 않고 단순히 인간의 시각으로 복호할 수 있다.

구체적으로 구현을 위해서는 영상을 암호적으로 분할하기 위하여 secret sharing problem를 풀어야 한다. 시각 암호화에 의한 secret sharing problem의 가장 간단한 방식은 화상이 흑색과 백색의 2진 화소들의 집합으로 구성되고 독립적으로 조작되는 것을 가정한다. 원 화상은 n 개의 share들로 구성되는 슬라이드에 균등하게 분배된다. 각 share는 m개의 흑/백 부화소의 집합이며, 서로 매우 근접하게 인쇄된다. 구조는 $n\times m$ boolean matix $S=[s_{ij}]$ 로 조작될 수 있으며 이것은 기본 행렬로 불린다. s_{ij} 는 i 번째 슬라이드의 j 번째 부화소가 흑임을 의미한다. r 개의 슬라이드 $i_1,i_2,\cdots,i_r$ 이 함께 포개졌을 때 결합된 share의 회색 준위는 "OR"된 m 벡터 V 의 해밍 가중치 $H(V)$ 에 비례한다. 이 회색 준위는 어떤 고정된 임계치 $1\le d\le m$ 과 상대적인 차 $\alpha<0$ 에 대해 만일 $H(V)\ge d$ 이면 흑으로 $H(V)<d-\alpha\cdot m$ 이면 백으로 시각적으로 보인다.

n 개의 visual secret sharing에서 k 개를 뽑아내는 문제를 위한 해는 $n\times m$ 부울 행렬들의 두 집합 C_0, C_1 으로 구성한다. 백 화소를 분배하기 위하여 제공자는 C_0 에 있는 하나의 행을 임의로 선택하고, 흑 화소를 분배하기 위하여 C_1 에 있는 하나를 임의로 선택한다. 선택된 행렬은 n 슬라이드 각각에 대해 m 개의 부화소의 색을 정의한다. 만일 다음의 3 가지 조건에 부합한다면 해는 유효하다.

1. C_0 에 있는 임의의 S 에 대하여 n 행들 중 임의의 k 에 대한 "OR" V 는 $H(V)\ge d$ 를 만족한다.
2. C_1 에 있는 임의의 S 에 대하여 n 행들 중의 임의의 k 에 대한 "OR" V 는 $H(V)<d-\alpha\cdot m$ 을 만족한다.
3. $q<k$ 인 $\{1,2,\cdots,n\}$ 의 임의의 부분집합 $\{i_1,i_2,\cdots,i_q\}$ 에 대해 C_0 에 있는 각 $n\times m$ 행렬의 행들 $i_1,i_2,\cdots,i_q$ 로 제한함으로써 얻어진 $q\times m$ 행렬들의 $t\in\{0,1\}$ 에 대한 두 집합 D_t 는 동일한 빈도를 가진 동일한 행렬들을 포함하는 의미에서 분간 할 수 없다.

조건 1, 2는 share를 겹쳤을 때 복원되는 화상의 휘도를 나타내며, 조건 3은 강력한 암호 분석기 조차도 k 개의 share보다 더 적은 중첩에 의해서는 분배된 화소가 백인지 흑인지 결정할 때 어떤 정보도 알 수 없다.

이러한 조건을 만족하도록 암호화되고 복호화된 영상은 단지 시각적으로만 의미를 지닐 뿐 원 영상과 차이를 갖는다. 이것은 본래의 영상을 구성하는 화소의 색상에 관계없이 암호화하는 과정에서 하나 이상의 흑 부화소가 할당되고 복호 과정에서 사라지지 않고 나타나기 때문이다. 따라서 복호된 영상의 신호대잡음비가 급격히 나빠져 신호처리와 같은 응용 기술에 적용하기는 제한적이다.

이와 같이 시각 암호화는 2차원 영상에 응용하는 것을 기반으로 하고 있으며 암호에 대한 지식이나 이를 수행하기 위한 장치 없이도 간단히 사용할 수 있는 강점이 있음에도 불구하고 영상처리 분야보다는 기존의 암호학적 응용 분야에 제한되고 있다. 이것은 지금까지 시각 암호가 적용되는 영상이 2진 영상이며 복호 후 해상도가 급격히 나빠지는데 원인이 있다. 이것은 부화소로 구성하는 과정에서 발생하는 명도의 변화와 해상도 감소가 가장 큰 원인이다. 따라서 영상 분야에 적용되기 위해서는 이러한 두 가지 문제를 해결하는 것이 매우 중요하다.

VC의 시험을 위하여 식 (1)과 식 (2)로 구성되는 basis matrix S_0, S_1 을 구성하였다. 흑색을 나타내는 C_0 는 S_0 의 행을 조합하여 얻는 모든 행렬들이고, 백색을 나타내는 C_1 은 S_1 의 행을 조합하여 얻는 모든 행렬들이다. 이것은 4장 중 3장이 합쳐지면 복호화가 이루어지는 3 out of 4 visual secret sharing의 한 예이다. 원 영상의 화소가 백색이 하면 S_0 에서 share가 선택될 것이고, 흑색이라면 S_1 에서 share가 선택될 것이다. 만일 두 장의 share만을 가지고 있으면 두 장을 겹쳤을 때 1의 개수가 동일하여 원래의 화소가 흑색인지 백색인지 구분할 수가 없다. 3장을 합쳤을 때 비로서 1의 개수 차이가 발생하여 복호화가 이루어진다.

$$S_0=\begin{bmatrix}000111\\001011\\001001\\001010\end{bmatrix} \tag{1}$$

$$S_1 = \begin{bmatrix} 1\,1\,1000 \\ 1\,1\,0100 \\ 1\,1\,0010 \\ 1\,1\,0001 \end{bmatrix} \quad (2)$$

<그림 1>에는 식 (1)과 식 (2)를 이용하여 시험한 결과이다. <그림 1(a), (b), (c)>총 제작된 4장 중 임의의 3장이며 <그림 1(d)>는 이들을 중첩 시킨 경우로 각각의 share에서는 알아볼 수 없었던 데이터가 나타났다. 나타난 결과는 인간의 시각을 통해 직관적으로 무엇이 암호화 되어 있었는지를 알 수 있으나 해상도가 매우 낮다. 흑색 부분은 정확한 것이나 랜덤한 잡음 형태로 나타난 것은 plane text에서 순수한 백색이었다. 이것은 원영상의 하나의 화소를 6개의 부 화소로 나누는 과정에서 발생한 문제이다.

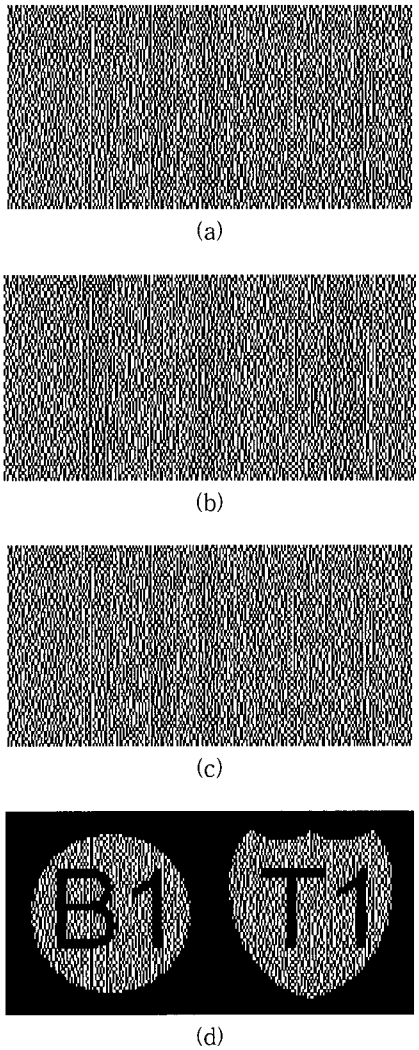


그림 1. 비쥬얼 크립토그래피의 예 (a) share 1 (b) share 2 (c) share 3 (d) share 1 + share 2 + share 3

Fig. 1. Example of visual cryptography (a) share 1 (b) share 2 (c) share 3 (d) share 1 + share 2 + share 3.

Ⅲ. 광 비쥬얼 크립토그래피

VC는 이진화된 입력 영상의 사용, 낮은 해상도 등으로 인한 표현의 한계로 응용범위가 극히 제한되고 있다. 이를 해결하기 위하여 다양한 연구가 진행되고있으며 최근에 이진 컴퓨터 형성 홀로그램(BCGH)에 VC를 적용하는 OVC가 제안되었다.

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

OVC에서는 "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.

3차원 영상을 기록하기에 가장 효과적인 홀로그램은 물체파와 기준파에 의하여 야기된 간섭패턴을 기록하는 방법으로 구성한다. 컴퓨터를 이용하여 가상의 물체에 대한 간섭패턴을 수학적으로 합성하고, 매체에 기록하는 방법으로 구성하는 홀로그램을 CGH라 한다. CGH는 물체가 수학적으로 존재하기만 한다면 구성이 가능하다. 최근의 고속 컴퓨터와 DSP 기술은 CGH를 이용하여 기존 광학 홀로그램의 대부분을 표현할 수 있게 하였으며, 효용성을 더욱 높여 3차원 동영상까지도 표현이 가능하게 하였다[5].

CGH를 제조하기 위해서는 컴퓨터로 합성한 홀로그래픽 데이터를 필름과 같은 물리적 매개체에 기록하면 된다. 따라서 데이터를 물질적 매개체에 효과적으로 전달하기 위해서 많은 기술들이 연구되었다. 결과적으로

홀로그래픽 데이터는 많은 경우에서 디지털 코드화되어 실제 홀로그램을 만들어낼 수 있음이 밝혀졌다. 특히 컴퓨터로 계산된 복소 파두면을 이진 패턴으로 인코딩하는 홀로그램이 BCGH이다. BCGH의 패턴 기록 방법은 다양하게 알려져 있으나 기본적인 원리는 같다. 불투명한 배경에 많은 투명한 점을 구성하는 것이다. 광투과가 '0'혹은 '1'에 지나지 않을지라도 기록되고 복원되는 영상은 그레이 준위를 지닌 홀로그램과 유사한 성능을 지닌다. 몇 가지의 이진 코딩기술은 최근 급격히 발전하고 있는 공간광변조기 기술과 접목하여 보다 쉽게 응용이 가능하게 되었다. 현재 CGH는 광정보처리, 광패턴인식, 3 차원 영상 복원, 광인터커넥션등 다양한 분야에 응용되고 있다. 이러한 중요성에도 불구하고 이들 정보를 보호하고자 하는 노력은 미비한 상태이다.

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 백 화소 주변의 화소는 백 화소일 가능성이 매우 높고 흑 화소 주변의 화소는 흑 화소일 가능성이 매우 높다. 이것은 안전성를 낮추는 강한 요인이 된다. 또한 암복호 과정에 부화소의 더하기 과정만이 존재하므로 복호된 영상의 백 화소 부분에는 각 화소당 하나 이상의 흑 부화소가 존재하여 신호대잡음비가 낮다.

BCGH는 이진값으로 구성되어 있어도 회색 준위의 영상을 표현할 수 있다. 특히 패턴인식에 이용되는 이진 위상 필터는 백 화소 주변의 화소가 백 화소일 가능성은 최대 50%를 넘지 못하며, 이것은 흑 화소의 경우에도 동일하다. BCGH는 시각 암호화에서 요구하는 입력 조건을 만족하고 있다. 따라서 BCGH에는 시각 암호화 기법을 적용할 수 있으며 보호된 BCGH는 시각 암호의 안전성을 갖는다.

OVC 구성 방법은 <그림 2>와 같다. 먼저 암호화하고자 하는 원 영상이 주어진다. 이때 영상은 이진화되어 있을 필요는 없다. 이 영상은 직접 이용되는 것이 아니라 광학적 처리를 위하여 BCGH로 제작된다. 여기에 VC를 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. 해독은 요구되는 숫자 만큼의share가 겹쳐지면 나타날 것이다. 해독 결과는 BCGH 이다. 그러나 암호화 이전의 BCGH와 동일하지는 않을 것이다. 본래 BCGH의 cell이 share 구성을 위하여 subcell로 만들어지는 과정에서 발생한 잡음이 추가되어 있다. 만일 앞에서 예를든 3 out of 4 visual secret sharing 적용하기 위하여 1셀을 3×2 subcell로 나누면 0의 값을 갖는 위치가 3×2 위치중 어느 한 위치가 된다. 따라서 해독된 BCGH를 복원하면 원영상과 차이가 있게 되는데 이것은 subcell이 움직이는 면적의 범위에 영향을 받는다.

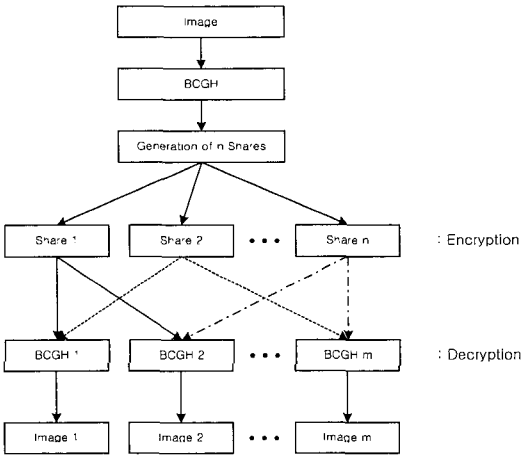


그림 2. 광 비쥬얼 크립토그래피의 구성 절차
Fig. 2. The composing procedure of optical visual cryptography.

시각 암호화는 화소를 부 화소로 나누어 암호화하므로 원 영상의 해상도를 낮춘다. 즉 복호된 BCGH의 해상도가 낮아진다. BCGH의 해상도가 낮아지면 BCGH 내에 기록된 영상은 크게 손상을 입을 것임을 예측할 수 있다.

복호된 BCGH에는 상대적으로 흑 화소가 증가해 있으나 백 화소의 수는 원 BCGH의 백색 셀의 수와 일치

하며 위치 변화도 제한적이다. 백 화소의 이동은 하나의 셀을 화소로 해석하고 부 화소를 만들기 위해 확장한 해상도 범위내이다. 단지 그 위치가 무작위로 변화하고 있을 뿐이다. 즉 백 화소와 백 화소간의 평균 간격 비율은 BCGH의 흰색 셀 간격 비율과 일치한다. 따라서 복호된 BCGH를 퓨리에 변환하면 원영상이 복원된다. 무작위 변화는 퓨리에 변환하면 백색잡음으로 변하여 전대역에 걸쳐 나타난다.

이상의 방법에 따라 얻은 결과를 <그림 3>에 나타내었다. <그림 3(a)>은 암호화에 사용한 plane text image이다. 이 영상은 OVC의 강점을 살펴볼수 있도록 회색 준위를 갖도록 하였다. <그림 3(b)>는 BCGH를 변화 없이 사용하여 복원한 것이고 <그림 3(b)>는 3 out of 4 visual secret sharing으로 BCGH를 암화화하고 복호화한 이후 복원한 영상이다. <그림 1>에 비하여 <그림 2>의 해상도나 낮아진 것은 홀로그램을 제작하는 과정에서 나타난 것으로 암호화와는 무관하다. <그림 3(b)>에 비하여 <그림 3(a)>가 낮은 신호대잡음비를 나타내고 있으나 이는 단순히 시각 암호화를 적용한 것에 비하여 우수한 결과를 나타내고 있는 것을 직적으로 살펴볼 수 있다. 자세한 평가는 다음 장에서 PEJTC를 통하여 살펴본다.

(a) (b)

(c)

그림 3. 상관첨두치 분포 해석 (a) JTC 입력 평면 (b) JTC 출력 평면

Fig. 3. The distribution analysis of correlation peak (a) JTC input plane (b) and (c) JTC output plane.

Ⅳ. 유사도 판정

OVC의 유사도 판정을 하는 시스템은 <그림 4>와 같다. 시스템은 광학적인 퓨리에 변화를 수행하는 3개의 광축으로 구성된다. 두개의 공간광변조기(SLM 1, SLM 2)로 구성되는 가장 위쪽의 퓨리에 변환 시스 템은 OVC를 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 영상처리기에서 PEJTC 입력 평면구성에 적당하도록 재구성하여 SLM 3에 디스플레이하면 디지털 카메라 2에서 파워스펙트럼을 검출할 수 있다. 이 과정은 PEJTC에 적당하도록 되어있는 스펙트럼 수정기가 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 논문에서는 <그림 5>와 같이 상하로 2단 분리하여 구성하였다. 상단은 기준 평면으로 BCGH로부터 직접 얻은 값 $r(x+x_r, y+y_r)$이 위치하고 있으며, 하단은 비교 영상으로 OVC의 출력 영상 $s(x+x_s, y+y_s)$이 위치하고 있다.

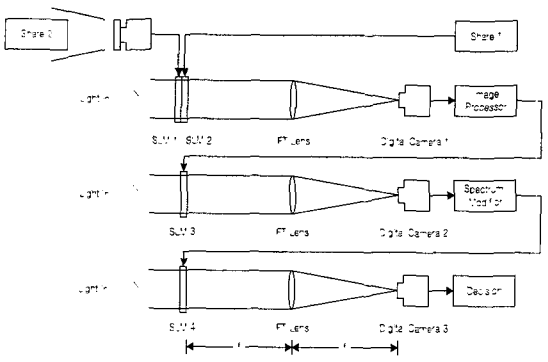


그림 4. 유사도 판정 시스템

Fig. 4. The system for discrimination of similarity degre.

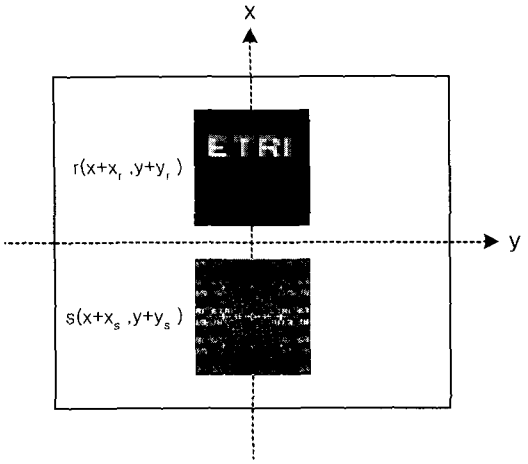


그림 5. PEJTC의 입력 평면
Fig. 5. Input plane of PEJTC.

이와 같이 하나의 입력 평면을 <그림 2>의 두번째 광축에 위치시켜 두 평면을 동시에 퓨리에 변환하여 디지털 카메라를 이용하여 검출하면 식 (3)과 같은 광간섭계기분포인 JTPS를 얻을 수 있다.

$$E_{JTC}(u,v) = |E_r(u,v) + E_s(u,v)|^2$$
$$= |E_r(u,v)|^2 + |E_s(u,v)|^2 + E_r^*(u,v)E_s(u,v) + E_r(u,v)E_s^*(u,v) \quad (3)$$

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 (3)은 크게 자기상관과 유사상관 2가지 성분으로 나누어 해석할 수 있다. $|E_r(u,v)|^2$, $|E_s(u,v)|^2$ 이 자기상관 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 유사상관 성분으로 우리가 필요로 하는 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 자기상관 값과 동일 할것이다. 따라서 필요한 유사상관 값 만을 추출할 필요가 있는데 이것은 식 (4)를 구현하는 것으로 가능하다.

$$E_{NEW}(u,v) = E_{JTC}(u,v) - |E_r(u,v)|^2 - E_s(u,v)|^2$$
$$= E_r^*(u,v)E_s(u,v) + E_r(u,v)E_s^*(u,v)$$
$$= |R(u,v)||S(u,v)|\{e^{-j\phi_r}e^{j\phi_s}e^{j2\pi[u(x_r-x_s)+v(y_r-y_s)]} + e^{j\phi_r}e^{-j\phi_s}e^{-j2\pi[u(x_r-x_s)+v(y_r-y_s)]}\} \quad (4)$$

식 (4)의 구현은 이미 실험적으로 증명이 되었다. 먼저 식 (3)에 따라 JTPS를 구하고, 동일한 SLM에 상단 부분만을 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 (4)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 구해진 값들을 이용하여 식 (5)를 구현하면 된다.

$$Ph[E_{NEW}(u,v)] = \frac{E_{NEW}(u,v)}{|E_r(u,v)||E_s(u,v)|}$$
$$= e^{-j(\phi_r-\phi_s)}e^{j2\pi[u(x_r-x_s)+v(y_r-y_s)]} + e^{j(\phi_r-j\phi_s)}e^{-j2\pi[u(x_r-x_s)+v(y_r-y_s)]} \quad (5)$$

식 (5)를 역퓨리에 변환하면 식(6)과 같이 두 개의 공간정합필터를 이용한 상관기 출력이 나타난다.

$$c_{NEW}(u,v) = \Im^{-1}\{E_{NEW}(u,v)\}$$
$$= Edge[r(x,y)] \otimes Edge[s(x,y)] * \delta[x+(x_r-x_s), y+(y_r-y_s)] + Edge[r(x,y)] \otimes Edge[s(x,y)] * \delta[x-(x_r-x_s), y-(y_r-y_s)] \quad (6)$$

식 (6)의 결과는 DC 성분이 존재하지 않으므로 에너지 효율이 향상되고, 불필요한 상관첨두치가 제거되어 있으므로 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 상관도 만을 알 수 있다. 그러나 이것은 본 논문의 목적에 부합한다.

<그림 6>은 시뮬레이션을통하여 얻은 OVC 상관 결과이다. 우측의 상관첨두치는 암복호되지 않은 영상의 상관결과이며 좌측의 상관첨두치는 OVC를 적용하여 암복호한 결과이다. 명백하게 유사도를 확인할 수 있다. 그러나 만일 secret share가 위조되었다면 BCGH가 복원되지 않을 것이고 상관첨두치도 발생하지 않을 것이다.

<그림 7>은 동일한 데이터에 대하여 난수발생기의 seed를 바꾸면서 이 과정을 반복하며 측정한 상관첨두치 변화를 기록한 것이다. 일반적으로 난수발생기는 특성상 seed의 변화에 따라 완전히 다른 값을 나타내게 되어 있으며 여기서 적용한 알고리즘 역시 192 비트 seed를 갖는 강력한 것이다

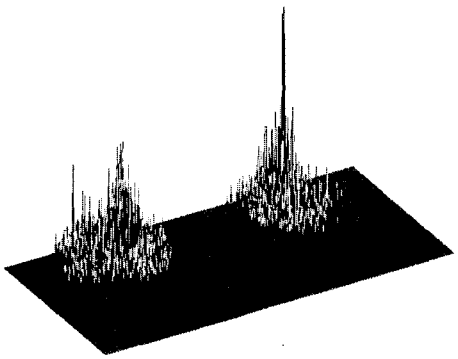


그림 6. 유사도 판정 결과
Fig. 6. The result of discrimination of similarity degre.

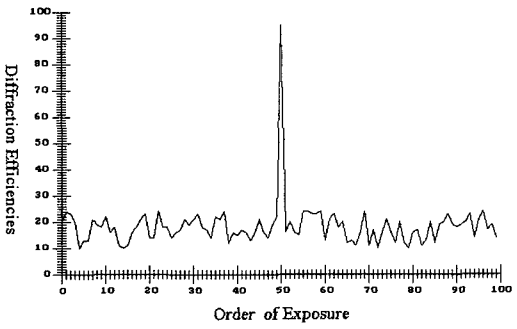


그림 7. 난수 발생기의 seed를 바꾸며 연속하여 시험한 결과
Fig. 7. The testing result of changing seed in random generator.

그러나 <그림 7>은 seed에 관계 없이 상관첨두치의 변화량이 매우 적다는 것을 나타내고 있다. <그림 7>의 결과는 BCGH가 암복호되는 과정에서 첨가된 잡음이 심각한 영향을 미치지 않고 있을 나타내는 것으로 OVC가 타당하다는 것을 나타내는 것이다. 이상에서 OVC는 이진 그레이 레벨을 가진 영상을 암호화할 수 있을 뿐만 아니라 암호화가 BCGH에 적용되므로 원 영상의 화소를 부 화소로 만드므로 인하여 VC에서 발생하는 문제들을 극복하였다는 것을 상관 결과를 통하여 입증하였다. 즉 OVC는 cryptography를 광학에 적용하기에 타당한 알고리즘이다.

V. 결 론

본 논문에서는 VC가 광학에 접목시키기 타당한 알고리즘이라는 것을 실험적으로 증명하였다. 최종 출력 결과가 화소대 화소 방식으로 1:1 비교를 하면 모든 화소가 원 영상과 차이가 있을 지라도 영상대 영상의 유사도로 측정하며 유사도가 매우 높아 실제 응용이 가능한 수준이라는 것을 알 수 있었다. Optical visual cryptgraphy는 단지 BCGH를 암호화하는 방법을 제시한 것만은 아니다. 시각 암호화의 응용분야를 확장함으로써 기존에 수학적으로 응용되는 암호 기술을 광학에는 적용할 수 있도록 하는 것이다. 그러나 아직까지는 LCD들간의 화소를 일치시키는 문제와 같은 어려운 문제들이 남아 있어 추가의 연구를 계속해서 진행할 필요가 있다.

참 고 문 헌

[1] A. Shamir, "How to share a secret," Communications of ACM, vol. 22, pp. 612~613, 1979.

[2] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptography Eurocrypt 94, vol. 950, pp. 1~12, 1995.

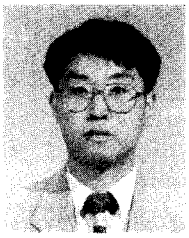
[3] C. Blundo, A. De Santis and D. R. Stinson. "On the contrast in visual cryptography schemes," ftp:// theory.lcs. mit. edu/pub/tcrytol/96-13.ps, 1996.

[4] G. Tricoles, "Computer generated holograms: an historical review," Appl. Opt., vol.26, no.20, pp. 4351~4360, 1987.

[5] S.Y. Yi, C.S.Ryu, S.H.Lee, and E.S.Kim, "Encryption of cell-oriented computer generated hologram by using visual cryptography," CLEO/Pacific Rim'99, pp. 817~818, 1999.

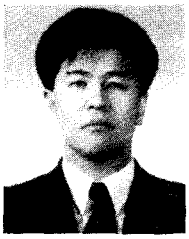
[6] S.H.Lee, S.Y.Yi, and E.S.Kim, "Hardware implementation of multi-target tracking system based on binary phase extraction JTC," Journal of the Korea Institute of Telematics and Electronics, vol. 33-A, no.10, pp. 152~159, 1996.

저 자 소 개



李 相 二(正會員)

1997년 : 광운대학교 전자공학과, 공학박사. 1997년 1월~2000년 12월 : 한국전자통신연구원 선임연구원. 2001년 1월~현재 : 국가보안기술연구소 선임연구원. <주관심분야 : 광정보처리, Holographic Security>



李 丞 玄(正會員)

1993년 : 광운대학교 전자공학과, 공학박사. 현재 : 광운대학교 전자공학부 부교수. 현재 : ISU 한국대표. <주관심분야 : 광정보처리, 3D 디스플레이>