

광시각 암호화에 위상과 진폭이 미치는 영향

Effect of the Phase and Amplitude for Optical Visual Encryption

이석기

프롬투정보통신(주) 전무이사

류충상

전파연구소 선임연구원

구향옥

충북대학교 컴퓨터공학과 석사과정

오창석

충북대학교 전기전자및컴퓨터공학부

Seog-Ki Lee

Director, From2 Information & Communications Co. Ltd.

Chung-Sang Ryu

Senior Researcher, Ministry of Information and Communication

Hyang-Ohk Koo

M.S. student, Dept. of Computer Eng., Chungbuk National Univ.

Chang-Suk Oh

Professor School of Electrical & Computer Engineering

중심어 : 정보보호, 시각 암호, Computer Generated Hologram

요약

시각암호는 정보보호 분야에서 중요한 정보를 암호화하여 복수 회원에게 분산시킨 후 회원의 합의에 의하여 해독이 가능하게 하는 thresholding scheme을 디지털 시스템인 아닌 인간의 시각 시스템으로 복호가 가능하게 하였다. 그러나 이러한 방법은 표현의 한계로 인하여 몇 가지 문제점을 안고 있었다. 이후 인간의 시각을 대신하여 레이저를 사용하는 광시각암호가 제안되어 광학 시스템에 암호 기법을 적용할 수 있게 되었다. 그러나 이 시스템은 기존의 시각 암호의 문제점을 완전히 극복하지 못함으로 인하여 또 다른 문제를 발생하였다. 이것은 데이터 처리 시스템을 시각에서 광학으로 전환하는 과정에서 발생하기 때문에 문제의 분석과 해결 역시 광학적으로 접근하는 것이 타당하다. 본 논문에서는 상관기를 이용하여 광시각 암호의 처리에서 발생하는 잡음의 정도와 암호 특성을 주파수 관점에서 분석한다.

Abstract

Visual cryptography made it possible to decrypt the information encrypted by thresholding scheme not with digital system but with human vision system. This method, however, has some limit in it because of the lack of resolution in both the spatial and amplitude domain. Optical visual cryptography, which used laser system instead of human eyesight, was proposed by conjunction of the optical theory with the cryptography. However, it also had some difficulties because it did not overcome the existing problem of visual cryptography completely. The 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. In this paper, we analysis, in the aspect of frequency, the security characteristics and the noise level occurred in the process of optical visual encryption.

1. 서론

정보화 사회로 급속하게 진행하는데 있어서 가치가 있는 정보를 불법으로 획득하려는 이들과 이를 보호하려는 관계가 정책기반의 통합보안관리 체계를 발달시키고 있다[1]. 이에 따라 단일 시스템에서 보호하여야 할 정보량은 증가하였고 고속처리의 필요성이 발생하고 있다. 또한 컴퓨터 및 통신 기술의 발달에 따라 공격기술은 보다 빠르고 정확해 졌고, 이를 방어하기 위한 암호 알고리즘 또한 복잡해지고 고속처리를 요구하게 되었다. 따라서 암호 알고리즘을 ASIC화된 칩을 이

용하여 구현하는 것이 일반적인 추세이다[2]. 고속 처리라는 관점에서 광학은 여러 가지 강점을 지니고 있으며 최근 관심이 집중되고 있다[3].

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 scheme을 제안하였다[4]. 이것은 여러 사람이 암호화된 데이

터를 나누어 가지고 있다가 권리를 행사하기 위하여 제한된 수 이상의 소유자가 모여 서로의 데이터를 합쳐 키 또는 평문을 찾아내는 방식으로서 암호 분야에서 매우 중요한 부분을 차지하고 있다. 이 이후 thresholding scheme의 한가지 응용 형태인 시각 암호가 제안되었다[5].

시각 암호는 매우 독특한 구조로 구성되어 있다. RSA와 같이 수학적 알고리즘을 사용하는 것도 아니고 DES와 같이 하나의 키를 이용하여 큰 데이터를 암호화하는 방식도 아니다. 암호문의 크기와 평문의 크기가 다르며, 사용 목적에 따라 평문 데이터가 한 가지 이상의 암호문 상태로 구성된다. 특히 thresholding scheme의 특성에 따라 복호를 위한 별도의 키는 존재하지 않는다.

시각 암호는 키의 길이와 같은 비도 측면 외에 이진 영상 사용, 복호 후 해상도 감소라는 입출력 데이터에 대한 단점도 있다. 그레이 영상 사용에 대한 연구[5]는 상당히 발전하고 있으나 이로 인한 단점도 동시에 증가하고 있다. 해상도 향상에 대한 한계는 이미 수학적으로 증명되어 있다.

광학 시스템에서는 완전 광학 암호 시스템에 대한 연구를 진행하고 있으나 양자의 성질을 이용하는 양자 암호를 제외하고는 암호 시스템이라고 명명할만한 것은 없는 상태이다. 하지만 최근에 시각 암호를 광학적으로 적용하려는 시도가 있었다[3]. 새롭게 제안된 광시각 암호는 광정보처리 특히 BCGH(binary computer generated hologram)에 적용하여 유용한 결과를 얻었다. 복호는 완전히 광학적으로 이루어졌으며 암호 데이터로 그레이 레벨 영상을 사용할 수 있었다. 특히 시각 암호에서는 근본적으로 해결이 불가능한 해상도 문제도 해결하였다. 그러나 복호된 영상은 암호 입력과 완전히 동일하지는 않다.

시각 암호에서 해상도 평가는 매우 간단하고 단순하다. 하나의 화소를 몇 개의 부화소로 분리할 수 있는 것이 관건이며 대체로 부화소 개수만이 유효 데이터가 된다. 이것은 해상도가 매우 낮기 때문에 출력을 시각적으로 확인하는 것만으로도 해상도를 판단할 수 있다는 것을 의미한다. 광시각 암호의 출력은 보다 높은 해상도를 유지하므로 시각적으로는 판단이 어렵다. 특히 주파수 평면에서 처리하고 있으므로 잡음이 화소보다는 평면 전체에 분포되어 있다. 따라서 단순히 영상처리 방법을 적용하는 것으로는 유사도 판단이 어렵고, 또한 화소 단위로 처리하는 것은 적당하지 않다.

따라서 광시각 암호의 타당성은 주파수 관점에서 분석하는 것이 타당하며 주파수는 위상과 진폭의 관점에서 해석되어야 한다. 즉 영상의 변화량과 영상의 명도 관점에서 해석이 되어

야 하는 것이다.

화소대 화소 비교가 아닌 평면 전체에 대한 유사도 판정은 2차원 상관기를 사용하는 것이 적당하다. 그리고 광학적 처리를 고려한다면 실시간으로 2차원 광상관이 가능한 JTC(joint transform correlator)를 이용하면 효율적이다.

본 논문에서는 광상관기를 이용한 광시각 암호의 입출력 상관도 평가를 위하여 먼저 시각 암호에 대하여 간단히 정리하고 광시각 암호를 구성하는 방법을 기술한다. 그리고 암호화 입력에 대한 복호 출력의 잡음 정도와 암호 특성을 주파수 관점에서 분석하기 위하여 JTC의 위상과 진폭 성분의 가중치를 변경하며 성능을 평가한다. 또한 단일 입력 영상에 대하여 다양한 암호 seed를 적용하여 서로 다른 암호 출력을 얻은 이후 결과를 평가한다. 비도는 암호화된 평면에 적용되면 유사도 판정은 최종 출력에 대하여 평가된다. 이 모든 과정은 컴퓨터를 이용한 시뮬레이션으로 이루어졌으나 광학적으로 구현하기 위한 모델도 함께 제안하였다.

II. 시각암호

Thresholding scheme에 기초하고 있는 시각 암호는 암호적인 투표 기법, 키 위탁 및 키 복구, 그룹 서명, 전자 화폐 등에 응용하려는 목적으로 연구가 진행되고 있다. 시각 암호의 강점은 구현의 편리성에 있다. 암호화는 몇 장의 투명한 용지에 원 영상을 분산하여 구성하는 것으로 간단히 구현할 수 있다. 여러 장으로 분산된 투명한 용지중 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 차이점이 없다. 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 복호한다.

구체적으로 구현을 위해서는 영상을 암호적으로 분할하기 위하여 비밀 분산 문제를 해결해야 한다. 시각 암호화에 의한 비밀 분산 문제의 가장 간단한 방식은 화상이 흑색과 백색의 2진 화소들의 집합으로 구성되고 독립적으로 조작되는 것을 가정할 경우이다. 원 화상은 n 개의 share들로 구성되는 슬라이드에 균등하게 분배된다. 각 share는 m 개의 흑백 부화소의 집합이며, 서로 매우 근접하게 인쇄된다. 구조는 $n \times m$

부울 행렬 $S=[s_{ij}]$ 로 조직될 수 있으며 이것은 기저 행렬로 불린다. s_{ij} 는 i 번째 슬라이드의 j 번째 부화소가 흑임을 의미한다. i 개의 슬라이드 j 가 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 $1 \leq d \leq m$ 과 상대적인 $\alpha < 0$ 차에 대해 만일 $H(V) \geq d$ 이면 흑으로 $H(V) < d - \alpha \cdot m$ 이면 백으로 시각적으로 보인다.

k 개의 시각 비밀 분산에서 n 개를 뽑아내는 문제를 위한 해는 $n \times m$ 부울 행렬들의 두 집합 C_0, C_1 구성한다. 백화소를 분배하기 위하여 제공자는 C_0 에 있는 하나의 행을 임의로 선택하고, 흑화소를 분배하기 위하여 C_1 에 있는 하나를 임의로 선택한다. 선택된 행렬은 m 슬라이드 각각에 대해 개의 부화소의 색을 정의한다. 만일 다음의 3가지 조건에 부합한다면 해는 유효하다.

C_0 에 있는 임의의 S 에 대하여 n 행들 중 임의의 k 에 대한 "OR" V 는 $H(V) \geq d$ 를 만족한다.

C_1 에 있는 임의의 S 에 대하여 n 행들 중 임의의 k 에 대한 "OR" V 는 $H(V) < d - \alpha \cdot m$ 를 만족한다.

$q < k \{1, 2, \dots, n\}$ 임의의 부분집합 $\{i_1, i_2, \dots, i_q\}$ 에 대해 C_0 에 있는 각 $n \times m$ 행렬의 행들을 i_1, i_2, \dots, 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 분간할 수 없다.

조건 1, 2는 share를 겹쳤을 때 복원되는 화상의 휘도를 나타내며, 조건 3은 강력한 암호 분석기조차도 k 의 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 원래의 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 2차

원 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.

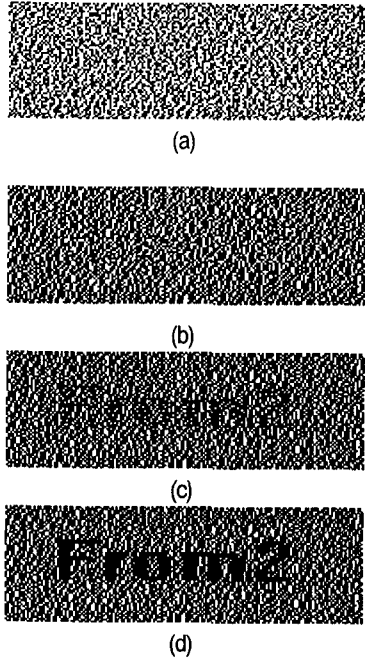
시각 암호의 시험을 위하여 식(1)과 식(2)로 구성되는 기저 행렬 S_0, S_1 을 구성하였다. 흑색을 나타내는 C_0 는 S_0 의 행을 조합하여 얻는 모든 행렬들이고, 백색을 나타내는 C_1 은 S_1 의 행을 조합하여 얻는 모든 행렬들이다. 이것은 4장 중 3장이 합쳐지면 복호가 이루어 3 out of 4 시각 비밀 분산의 한 예이다. 원 영상의 화소가 백색이라면 S_0 에서 share가 선택될 것이고, 흑색이라면 S_1 에서 share가 선택될 것이다. 만일 두 장의 share만을 가지고 있으면 두 장을 겹쳤을 때 1의 개수가 동일하여 원래의 화소가 흑색인지 백색인지 구분할 수가 없다. 3장을 합쳤을 때 비로서 1의 개수 차이가 발생하여 암호화가 이루어진다.

$$S_0 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \quad (1)$$

$$S_1 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (2)$$

그림 1은 흰색 바탕에 검은 색으로 "From 2" 라고 기록된 영상을 식(1)과 식(2)를 이용하여 시험한 결과이다. 그림 1(a), (b), (c)는 총 제작된 총 4장 중 임의의 3장이며 그림 1(c)는 이들을 중첩 시킨 경우로 각각의 share에서는 알아볼 수 없었던 데이터가 나타나기 시작하였으며, 그림 1(d)에서 완전히 복호되었다. 나타난 결과는 인간의 시각을 통해 직관적으로 무엇이 암호화되어 있었는지를 알 수 있으나 해상도가 매우 낮다. 흑색 부분은 정확한 것이나 랜덤한 잡음 형태로 나타난

것은 평문에서 순수한 백색이었다. 이것은 원 영상에서 하나의 화소를 6개의 부화소로 나누는 과정에서 발생한 문제이다.



(a) share 1 (b) 2개의 share 중첩
(c) 3개의 share 중첩 (d) 모든 share 중첩
그림 1. 시각 암호의 예

III. 광시각 암호

시각 암호는 이진화된 입력 영상의 사용, 낮은 해상도 등으로 인한 표현의 한계로 응용범위가 극히 제한된다. 이를 해결하기 위하여 다양한 연구가 진행되고 있으며 최근에 BCGH에 시각 암호를 적용하는 광시각암호가 제안되었다.

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

광시각 암호에서는 "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 지닌

다. 그럼에도 불구하고 시각 암호와 동일한 비도를 유지한다.

3차원 영상을 기록하기에 가장 효과적인 홀로그램은 물체 파와 기준파에 의하여 야기된 간섭패턴을 기록하는 방법으로 구성한다. 컴퓨터를 이용하여 가상의 물체에 대한 간섭 패턴을 수학적으로 합성하고, 매체에 기록하는 방법으로 구성하는 홀로그램을 CGH라 한다. CGH는 물체가 수학적으로 존재하기만 한다면 구성이 가능하다. 최근의 고속 컴퓨터와 DSP(digital signal processing) 기술은 CGH를 이용하여 기존 광학 홀로그램의 대부분을 표현할 수 있게 되었으며, 효율성을 더욱 높여 3차원 동영상까지도 표현이 가능하게 되었다[7].

CGH를 제조하기 위해서는 컴퓨터로 합성한 홀로그래피 데이터를 필름과 같은 물리적 매체에 기록하면 된다. 따라서 데이터를 물질적 매체에 효과적으로 전달하기 위해서 많은 기술들이 연구되었다. 결과적으로 홀로그래피 데이터는 많은 경우에 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. 이러한 원리는 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 가지 이진 코딩 기술은 최근 급격히 발전하고 있는 공간 광변조기 기술과 접목하여 보다 쉽게 응용이 가능하게 되었다.

기존의 암호 방법은 디지털 처리에는 적당하나 광학에 적용하기는 매우 비효율적이다. 기존의 알고리즘을 광학 시스템에 적용하기 위해서는 광 데이터를 디지털로 전환하여 암호화하고, 디지털적으로 복호화한 이후 다시 광 데이터로 전환해야 한다. 이와 같이 광학적 데이터를 디지털로 암호 처리하는 방법은 적절하지 못하다. 암호 알고리즘을 광시스템에 적용하기 위해서는 광학적으로 복호하는 것이 필수적이다. 즉 CGH에 기록되는 정보는 기존의 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 화

소는 흑화소일 가능성이 매우 높다. 이것은 안전성을 저하시키는 요인이 된다. 또한 암·복호 과정에 부화소의 더하기 과정만이 존재하므로 복호된 영상의 백화소 부분에는 각 화소 당 하나 이상의 흑 부화소가 존재하여 신호대잡음비가 낮다.

BCGH는 이진 값으로 구성되어 있어도 회색 준위의 영상을 표현할 수 있다. 특히 패턴인식에 이용되는 POF(binary phase-only filter)는 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 암호화된 BCGH는 시각 암호의 안전성을 갖는다.

광시각암호의 구성 방법은 그림 2와 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 시각 암호를 적용한다. BCGH는 여러 개의 share로 나누어 질 것이며 각각의 share는 서로 다른 사람들이 보관하게 될 것이다. 이때 발생하는 share의 개수는 사용하고자 하는 용도와 알고리즘에 따라 결정된다. 복호는 요구되는 숫자 만큼의 share가 겹쳐지면 나타날 것이다. 복호 결과는 BCGH 이다. 그러나 암호화 이전의 BCGH와 동일하지는 않다. 원래의 BCGH의 셀이 share 구성을 위하여 subcell로 만들어지는 과정에서 발생한 잡음이 추가되어 있다. 만일 앞에서 예시한 3 out of 4 시각 비밀 분산에 적용하기 위하여 1셀을 6개의 subcell로 나누고 암·복호하면 6개의 subcell 범위내에 있는 임의의 한 subcell이 0이 된다. 따라서 복호된 BCGH를 복원하면 원 영상과 차이가 있게 되는데 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 위치 변화는 제한적이다. 백화소의 이동은 하나의 셀을 화소로 해석하고 부화소를 만들기 위해 확장한 해상도 범위내이다. 단지 그 위치가 무작위로 변화하고 있을 뿐이다. 즉 백화소와 백화소 간의 평균 간격 비율은 BCGH의 흰색 셀 간격 비율과 일치한다. 따라서 복호된 BCGH를 푸리에 변환하면 원 영상이 복원된다. 무작위 변화는 푸리에 변환하면 백색잡음으로 변하여

전대역에 걸쳐 나타난다.

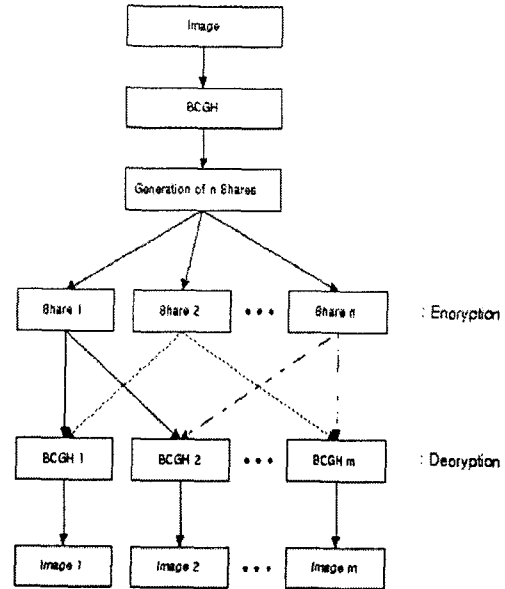
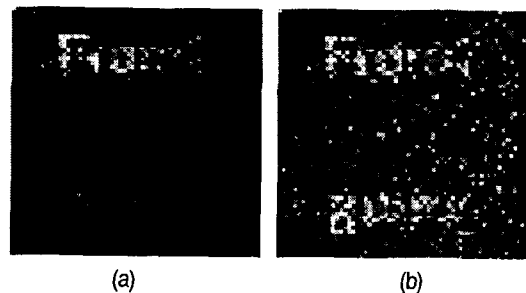


그림 2. 광시각암호 구성 절차

이상의 방법에 따라 얻은 결과를 그림 3에 나타내었다. 그림 3(a)는 BCGH를 변화 없이 사용하여 복원한 것이고, 그림 3(b)는 3 out of 4 시각 비밀 분산으로 BCGH를 암호화하고 복호화한 이후에 복원한 영상이다. 사용한 secret share는 4장을 모두 겹쳐서 사용하였다. 그림 3(a)에 비하여 그림 3(b)가 낮은 신호대잡음비를 나타내고 있으나 이는 단순히 시각 암호화를 적용한 것에 비하여 우수한 결과를 나타내고 있는 것을 직접적으로 확인할 수 있다.



(a) 일반적으로 복원된 영상
(b) 광시각암호를 적용한 후 복원한 영상
그림 3. 상관첨두치 분포 해석

IV. 유사도 판정

광시각암호의 유사도 판정을 하는 시스템은 그림 4와 같다. 시스템은 광 푸리에 변환을 수행하는 3개의 광축으로 구성된다. 두개의 공간광변조기(SLM 1, SLM 2)로 구성되는 가장 위쪽의 푸리에 변환 시스템은 광시각암호를 구현한 것이다. SLM 3을 사용하는 두번째 광축은 JTPS를 얻는 과정이며 마지막 광축은 역푸리에 변환을 통하여 상관도를 얻는다. 시스템 동작은 먼저 키 영상을 SLM 2에 나타내고 평문 영상을 입력 받아 SLM 1에 나타내면 디지털 카메라 1에 복호된 평문 영상이 나타난다. 검출된 영상은 상관기 입력 평면구성에 적당하도록 배치하여 SLM 3에 디스플레이하면 디지털 카메라 2에서 파워스펙트럼을 검출할 수 있다. 파워스펙트럼의 위상과 진폭 성분의 가중치를 재조정하여 SLM 4에 나타내면 디지털 카메라 3에서 상관값이 검출될 것이고 이를 사용하여 결과를 분석한다.

별도의 정합필터 없이 상관이 가능한 JTC는 푸리에 입력 평면(SLM1)을 2단으로 분리하여 한쪽 반평면에 기준 평면 그리고 다른 쪽에 비교 평면을 동시에 위치시키고 상관을 시키게 된다. 본 논문에서는 그림 5와 같이 상하로 2단 분리하여 구성하였다. 상단은 기준 평면으로 BCGH로부터 직접 얻은 값이 위치하고 있으며, 하단은 비교 영상으로 광시각암호의 출력 영상이 위치하고 있다.

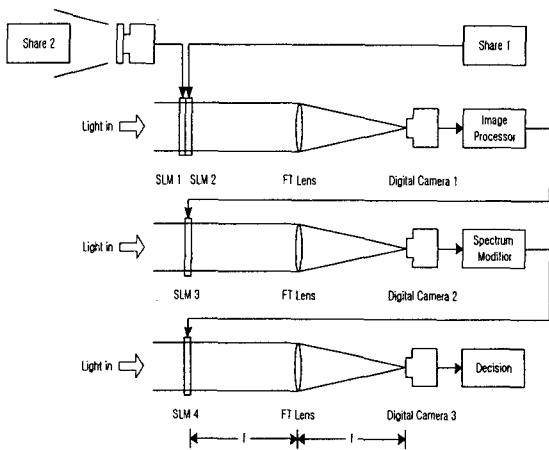


그림 4. 유사도 판정 시스템

이와 같이 하나의 입력 평면을 그림 4의 두번째 광축에 위치시켜 두 평면을 동시에 푸리에 변환하여 디지털 카메라를

이용하여 검출하면 식(3)과 같은 공간합성기분포인 JTPS(joint transform power spectrum)를 얻을 수 있다.

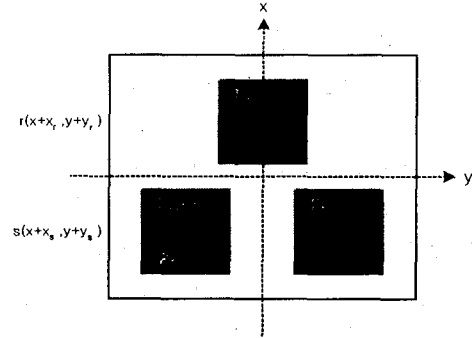


그림 5. JTC 입력 평면

$$\begin{aligned}
 E_{JTC}(u, v) &= E_r(u, v) + E_s(u, v) \\
 &= E_r(u, v) + E_r(u, v) \\
 &\quad + E_r^*(u, v)E_s(u, v) + E_r(u, v)E_r^*(u, v) \quad (3)
 \end{aligned}$$

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 자기 상관과 상호 상관 등 두 가지 성분으로 나누어 해석할 수 있다. 이 자기 상관 성분으로 자기 자신간에 발생한 성분으므로 서로 다른 영상간의 상관관계를 측정하려는 목적에 맞지 않는 성분으로 잡음으로 작용한다. 나머지 두 성분은 $r(x+x_r, y+y_r)$ 과 $s(x+x_s, y+y_s)$ 간의 상호상관 성분으로 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 자기 상관 값과 동일 할 것이다. 따라서 필요한 자기 상관 값을 추출할 필요가 있는데 이것은 식(4)를 구현하는 것으로 가능하다.

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

식(4)의 구현은 이미 실험적으로 증명이 되었다. 먼저 식(3)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(4)가 간단하게 얻어진다.

이상의 상관값에서 위상과 진폭이 모두 고려되어 있기 때문에 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 sidelobe 간에 중첩이 발생하지 않는다. 만일 그 이내에서 사용하려면 진폭을 제거해야 하는데 이미 구해진 값들을 이용하여 식(5)를 구현하면 된다.

$$E_{PHA_AMP}(u, v) = \frac{E_{NEW}(u, v)}{|E_r(u, v)|^\alpha |E_s(u, v)|^\beta} \quad (5)$$

재구성된 JTPS에서 위상과 진폭 량을 조절하는 식(5)에서 $0 \leq \alpha \leq 2$ 와 $0 \leq \beta \leq 1$ 의 값을 적절히 조절하면 여러가지 효과를 얻을 수 있다. $\alpha = 1, \beta = 0$ 인 경우는 POF와 같은 결과를 얻을 것이고 $\alpha = \beta = 1$ 인 경우는 POC(phase only correlator)와 같은 결과를 얻는다.

식(4)를 역푸리에 변환하면 식(6)과 같은 값을 얻을 수 있다.

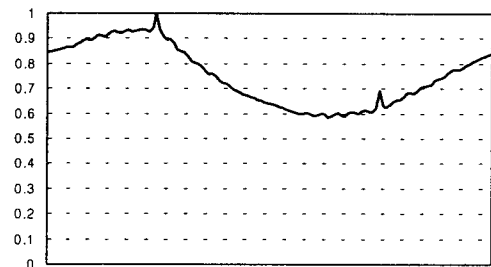
$$\begin{aligned} c(x, y) &= r(x, y) \otimes s(x, y) \\ &\quad * \delta\{x + (x_r - x_s), y + (y_r - y_s)\} \\ &\quad + r(x, y) \otimes s(x, y) \\ &\quad * \delta\{x - (x_r - x_s), y - (y_r - y_s)\} \end{aligned} \quad (6)$$

식(6)의 결과는 DC 성분이 존재하지 않으므로 에너지 효율이 향상되고, 불필요한 상관점두치가 제거되었으므로 분리 조건에 자유롭게 된다.

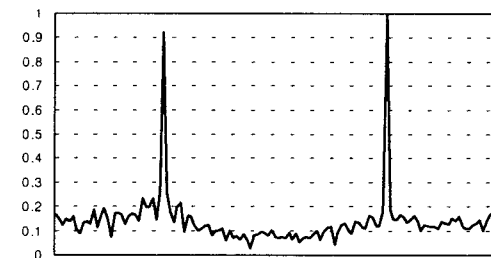
그림 6은 시뮬레이션을 통하여 얻은 광시각 암호 상관 결과이다. 그림 6(a)는 위상과 진폭 성분이 모두 사용되는 $\alpha = \beta = 0$ 인 경우, 그림 6(b)는 정합필터의 위상 성분이 제거되는 $\alpha = 1, \beta = 0$ 인 경우, 그리고 그림 6(c)는 정합필터와 입력 영상 모두에서 위상성분이 제거되는

$\alpha = \beta = 1$ 에 대한 결과이다. 그림 6에서 α 와 β 값에 관계없이 두개의 상관 침두치가 발생하고 있는데 우측의 상관침두치는 암호화되지 않은 영상의 상관결과이며 좌측의 상관침두치는 광시각암호를 적용하여 암호화한 결과이다.

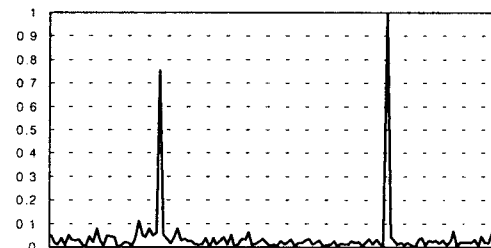
그림 6에서 암호화된 영상이 원 영상과 매우 유사한 결과를 나타내고 있음을 확인할 수 있다. 그러나 만일 secret share가 위조되었다면 BCGH가 복원되지 않을 것이고 상관침두치도 전혀 발생하지 않을 것이다. 그러나 적용하는 상관기에 따라 서로 다른 결과를 나타내고 있는데 이것은 위상과 진폭의 가중치에 따른 것으로 분석된다. 특히 진폭 성분이 강한 경우에는 암호화한 것이 원 영상 보다도 더 유사한 결과를 나타내고 있는데 이것은 구성되는 평면의 밝기에 영향을



(a) $\alpha = \beta = 0$



(b) $\alpha = 1, \beta = 0$



(c) $\alpha = \beta = 1$

그림 6. 유사도 판정 결과

받는 것으로 예측된다. 그러나 영상의 변화량 즉 글자의 형태에 영향을 받는 위상 성분은 암호화된 영상이 원 영상과 차이가 있음을 나타내고 있다. 이상의 결과는 광시각암호는 데이터를 비교적 우수하게 암호화 할 수 있으나 데이터 주변에 잡음이 많이 발생하고 있음을 알 수 있다.

그림 7은 동일한 데이터에 대하여 랜덤변수 발생기의 seed를 바꾸면서 $\alpha = \beta = 1$ 로 설정하고 JTC를 반복 구동하며 측정된 상관첨두치 변화를 기록한 것이다. 일반적으로 랜덤변수 발생기는 특성상 seed의 변화에 따라 완전히 다른 값을 나타내게 되어 있으며 여기서는 32차 LFSR(linear feedback shift register)을 사용하였다. 그러나 그림 7은 seed 값을 50회 바꾸며 유사도를 판정한 것이다. Seed에 관계없이 상관첨두치의 변동폭은 광시각 암호를 적용하지 않은 상관첨두치의 변화량이 매우 적다는 것을 나타내는 것이다.

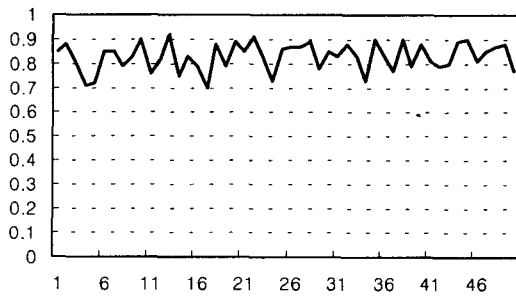


그림 7. 랜덤변수 발생기 seed를 바꾸며 시험한 결과

그림 7의 결과는 BCGH가 암호화되는 과정에서 첨가된 잡음이 심각한 영향을 미치지 않고 있음을 나타내기 때문에 광시각암호의 타당성을 확인할 수 있다.

이상에서 광시각 암호는 회색 준위를 가진 영상을 암호화할 수 있을 뿐만 아니라 암호가 BCGH에 적용되므로 원 영상의 화소를 부화소로 만들기 때문에 시각 암호에서 발생하는 문제들을 극복하였다는 것을 상관 결과를 통하여 입증하였다. 즉 광시각암호는 암호학을 광학에 적용하기에 타당한 알고리즘이라 할 수 있다.

V. 결론

본 논문에서는 시각 암호가 광학에 접목시키기 타당한 알고리즘이라는 것을 실험적으로 증명하였다. 최종 출력 결과가 화소대 화소 방식으로 비교를 하면 모든 화소가 원 영상과

차이가 있을 지라도 영상대 영상의 유사도로 측정하면 유사도가 매우 높아 실제 응용이 가능한 수준이라는 것을 알 수 있었다. 광시각 암호는 단순히 BCGH를 암호화하는 방법을 제시한 것뿐만 아니라 시각 암호화의 응용분야를 확장함으로써 기존에 수학적으로 응용되는 암호 기술을 광학에 적용할 수 있도록 하는 것이다. 그러나 암호화 과정에서 발생하는 광학적 잡음을 제거하는 문제 등을 해결하기 위하여 지속적인 연구가 수행되어야 한다.

참고 문헌

- [1] 정연서, 장종수, 오창석, "정책기반의 통합보안관리," COMSW2001, pp.342-346, 2001.
- [2] 유형준, 김영국, 이옥연, 정교일, 조현숙, "CryptoModule 2000을 이용한 KASUMI 알고리즘의 구현," 한국정보처리학회 춘계 학술발표논문집, 제8권, 제1호, pp.437-440, 2000.
- [3] 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.
- [4] A. Shamir, "How to share a secret," "Communications of ACM," Vol.22, pp.612-613, 1979.
- [5] M. Naor and A. Shamir, "Visual Cryptography," Advances in Cryptography Eurocrypt94, Vol.950, pp.1-12, 1995.
- [6] C. Blundo, A. De Santis and D. R. Stinson, "On the contrast in visual cryptography schemes," [ftp://theory.lcs.mit.edu/pub/tycryto/96-13.ps](http://theory.lcs.mit.edu/pub/tycryto/96-13.ps), 1996.
- [7] G. Tricoles, "Computer generated holograms: an historical review," Appl. Opt., Vol.26, No.20, pp.4351-4360, 1987.

이석기(Seog-Ki Lee)

중신회원



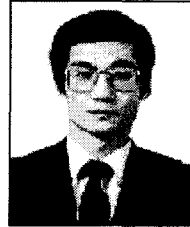
1980년 2월 서강대학교
전자공학과(공학사)
1982년 2월 서강대학교
전자공학과(공학석사)
2002년 2월 충북대학교
컴퓨터공학과(공학박사)

1983년 9월 ~ 1988년 2월 현대전자산업(주)
1988년 3월 ~ 1998년 6월 한국전자통신연구원
1998년 7월 ~ 현재 프롬투정보통신(주) 전무

<관심분야> : 정보보호, VPN, VOIP, Home Gateway

오창석(Chang-Suk Oh)

중신회원



1978년 2월 연세대학교
전자공학과(공학사)
1980년 2월 연세대학교
전자공학과(공학석사)
1988년 8월 연세대학교
전자공학과(공학박사)

1985년 ~ 현재 충북대학교 전기전자및컴퓨터공학부
교수

1982년 ~ 1984년 한국전자통신연구원 연구원
1990년 ~ 1991년 미국 Stanford대학교 객원교수

<관심분야> : 컴퓨터 네트워크, 뉴로 컴퓨터,
차세대 인터넷, 정보 보호

류충상(Chung-Sang Ryu)

정회원



1990년 2월 서울산업대학교
전자공학과(공학사)
1993년 8월 광운대학교
전자공학과(공학석사)
1997년 8월 광운대학교
전자공학과(공학박사)

1984 ~ 1987 우일상운(주)
1998년 5월 ~ 현재 정보통신부 전파연구소
선임연구원

<관심분야> : 영상인식, 보안

구향옥(Hyang-Ohk Koo)

준회원



1999년 8월 한밭대학교
컴퓨터공학과(공학사)
2001년 현재 충북대학교
컴퓨터공학과 석사과정

<관심분야> : 컴퓨터 네트워크, 뉴로 컴퓨터,
차세대 인터넷, 정보 보호