논문 99-24-12B-19 한국통신학회논문지 '99-12 Vol.24 No.12B

광 암호화를 이용한 안전한 지문 인식 시스템

정회원 한 종 욱*, 김 춘 수*, 박 광 호*, 김 은 수**

Secure Fingerprint Identification System based on Optical Encryption

Jong-Wook Han*, Choon-Soo Kim*, Kwang-Ho Park*, Eun-Soo Kim** ***Regular Members***

요 약

본 논문에서는 지문 인식을 이용한 보안 시스템에서 지문 정보를 안전하게 보호할 수 있는 방법으로 암호화 방법을 도입한 새로운 안전한 보안시스템을 제안하였다. 광학적 구현을 위하여 LCD 소자를 이용, 랜덤한 이진 키 수열과 지문 영상 데이터를 2차원 광 정보로 표현하였으며, LCD의 편광 특성을 이용하여 암호화 과정인 광 XOR 연산을 실현하였다. 광학적으로 암호화된 영상은 다시 CCD 카메라에 의하여 검출되고, 그 결과는 다시 이전에 암호화하여 저장하였던 데이터 베이스용 지문들과 비교함으로써 입력된 지문 영상의 유효 여부를 판별하게 된다. 본 논문에서는 제안한 시스템의 성능을 증명하기 위하여 컴퓨터 시뮬레이션을 수행함으로써 원래의 입력 영상이 랜덤한 영상으로 암호화됨을 보이고 암호화 과정의 도입에 따른 시스템 성능을 분석하였다. 본 논문에서 제안한 시스템을 이용하면 암호화 방법을 통해 중요한 영상 정보를 보호할 수 있으며, 영상뿐 아니라 2차원 방법에 의한 고속 암호화 시스템 구현에 그 응용이 가능하겠다.

ABSTRACT

We propose a new optical method which conceals the data of authorized persons by encryption before they are stored or compared in the pattern recognition system for security systems. This proposed security system is made up of two subsystems : a proposed optical encryption system and a pattern recognition system based on the JTC which has been shown to perform well. In this system, each image of authorized persons as a reference image is stored in memory units through the proposed encryption system. And if a fingerprint image is placed in the input plane of this security system for access to a restricted area, the image is encoded by the encryption system then compared with the encrypted reference image. Therefore because the captured input image and the reference data are encrypted, it is difficult to decrypt the image if one does not know the encryption key bit stream. The basic idea is that the input image is encrypted by performing optical XOR operations with the key bit stream that is generated by digital encryption algorithms. The optical XOR operations between the key bit stream and the input image are performed by the polarization encoding method using the polarization characteristics of LCDs. The results of XOR operations which are detected by a CCD camera should be used as an input to the JTC for comparison with a data base. We have verified the idea proposed here with computer simulations and the simulation results were also shown.

* 한국전자통신연구원
** 광운대학교 전자공학과
논문번호 : 99324-0817 접수일자 : 1999년 8월 17일

Ⅰ. 서 론

현대 사회가 개인중심의 정보화 사회로 발전되어 감에 따라 개인에 관련된 정보의 보안이 더욱 절실히 요구 되고 있다. 그러므로 이러한 중요 정보의 유출을 미연에 방지하고 또는 유출이 되어도 제3자에게는 유효한 정보가 되지 못하게 하는 기술에 대해서 많은 연구가 최근에 전세계적으로 이루어지고 있다. 일반적으로 회사나 주요 국가 기관 등에서는 제한된 구역의 출입을 제어하여 주는 보안 시스템을 사용하여 소유한 정보의 유지 및 유출 방지하고 있으며 심지어 일반 가정에서도 불법적인 침입 방지를 위하여 보안 시스템을 사용하는 경우가 늘어가고 있다. 이러한 보안 시스템은 미리 출입이 허가된 사람을 인식하기 위하여 음성이나 화상, 지문, 패스워드와 같은 데이터를 사용하고 있으며, 이중 음성이나 화상, 지문과 같은 각 개인의 신체의 독특한 특징을 이용한 보안 시스템이 안전성면에서 장점을 갖고 있어 많이 연구가 되고 있다.[1-4] 통신 시스템의 발달로 인하여 보안 시스템은 네트워크로 구성되어 중앙 제어식으로 운영되는 경우가 늘어나고 있는데 이러한 경우 통신망을 통하여 전송되는 데이터 정보도 간단하게 도청될 수가 있다. 또한 독립적인 보안 시스템의 경우도 데이터 베이스용 정보의 저장을 의하여 메모리 유니트를 갖고 있으므로 이에 대한 불법적인 접근이나 탈취가 이루어진다면 안전성에 큰 문제가 발생할 수가 있게 된다. 그러므로 보안 시스템과 같이 보안이 필요로 되는 곳에서 사용되는 패턴 인식 시스템은 사용 정보에 대한 안전성을 유지할 수 있는 방안을 확보하는 것이 반드시 필요하다고 할 수 있다.

현재 사용되고 있는 보안 시스템중은 허가된 사람의 인증 수단으로서 인위적으로 구성한 개인 정보를 이용하는 경우가 대부분을 차지하고 있으나 이 방법은 정확도는 높일 수 있지만 훼손, 도난, 위조 등으로 관리가 어려운 단점을 갖고 있다. 그러므로 이러한 단점을 해결하기 위한 방법으로 개인간에 명백한 영상 차이가 존재하는 선천적인 신체 정보인 지문을 이용하는 방법이 제시되어 연구되고 있다. 지문을 이용한 개인 식별은 선천적으로 주어지는 유일성과 불변성으로 인해 가장 효율적인 개인 인증 수단으로 사용될 수 있으므로 개인 식별을 위한 연구가 매우 활발히 진행이 되고 있다.[2-4] 지문을 이용한 개인 식별은 입력된 지문 영상과 데이터 베이스로 저장되어 있는 기준 영상과의 일치성을 구별하여 인식하는 패턴 정합으로 수행된다. 하지만 입력 영상과의 비교를 위한 기준 영상들의 방대함으로 인하여 디지털 방식에 의한 구현은 시스템이 지나치게 복잡하게 되거나 처리 시간이 과도하게 되어 실질적인 응용에 제한이 되고 있다. 그러므로 지난 몇 년동안 지문 인식을 위한 광 패턴 인식을 포함한 다양한 구조의 시스템들이 제안되었으며, 특히 광 상관기에 의한 지문 인식 시스템은 실질적인 응용이 가능한 결과들을 내놓고 있다. 따라서 본 논문에서는 JTC(Joint Transform Correlator)에 근거한 광 지문 인식 시스템에 적용할 수 있는 광 암호화 방식을 제안하여 안전한 보안 시스템 모델을 제시하였다.

본 논문에서 제안한 시스템은 기준이 되는 지문 영상들을 암호화하여 저장하고 입력되는 지문 영상도 암호화하여 처리하는 안전한 2차원 패턴 인식 시스템에 근거한 보안 시스템으로 데이터 베이스용 지문뿐만 아니라 시스템 내부에서의 지문 데이터 처리도 암호화된 상태로 처리되므로 매우 안전한 시스템이 되겠다.

본 논문에서는 입력 영상 및 암호화용 키 수열 데이터의 2차원적인 표현 및 광 정보로의 변환을 위하여 현재 광정보처리 분야에서 가장 많이 사용이 되어 오고 있는 공간 광 변조기인 LCD(Liquid Crystal Device)[5]를 이용하였다. 제안한 시스템은 입력 지문 영상과 암호화 알고리즘에서 출력되는 키 수열 데이터의 표현을 위하여 LCD 2개로 구성이 되는 암호화 부분과 암호화 부분에서 출력된 암호화 영상과 미리 저장된 데이타를 비교하는 LCD 1개로 이루어진 JTC부분으로 구성이 된다. 암호화 과정은 암호화 키 수열과 2차원 지문 영상을 XOR (Exclusive OR) 연산을 통하여 이루어지며, LCD의 편광 특성을 이용하여 암호화 키 수열과 입력 영상간에 광 암호화 과정이 실시간적으로 수행될 수 있도록 하였다. 본 논문에서는 컴퓨터 시뮬레이션 결과를 통하여 입력된 2차원 지문 영상이 랜덤한 영상으로 암호화됨을 보임으로 제안된 방법을 증명하였으며, JTC의 상관 출력 결과를 비교함으로써 제안된 시스템의 성능을 분석하였다.

Ⅱ. JTC에 의한 지문 인식 시스템

지문은 그 유일성과 불변성으로 가장 효율적인 개인 인증 수단으로 인식이 되고 있으나 좁은 영역

에 많은 정보들이 집중이 되어 있어 방대한 2차원 정보의 실시간 처리가 요구된다. 그러므로 디지탈적인 실현을 위해서는 엄청난 메모리 용량과 고속처리 알고리즘 및 시스템 등이 요구되므로 실제적인 제약성을 가지고 있다. 따라서 병렬성 및 고속성의 특징을 지닌 광을 이용한 지문 인식 기술이 새롭게 대두되어 반도체 레이저의 발달과 공간 광 변조기의 개발 및 고속 CCD (Charge Coupled Device) 카메라와 같은 광 검출기의 개발로 광정보처리 기술을 이용한 지문 인식 시스템이 각광을 받고 있다.

효과적인 지문 인식을 위해서는 각 개인에 따른 다양한 지문에서 어떤 공통의 특징을 추출하여 이를 기준으로 대표적인 몇 가지 범주로 나누어서 입력된 지문이 어느 부류에 속하는 가를 판단하고 그 입력된 지문이 등록 지문과 일치하는 가를 구별하는 과정을 거치게 된다. 이와 같이 지문 인식을 통한 개인 식별을 위해서는 결국 지문의 조합을 행해야 하는데 등록 지문의 방대함으로 효율적인 지문 인식을 위하여 최종 인식에 앞서 먼저 입력 지문을 특정 범주로 분류하고 정합에 사용될 지문의 개수를 최소화하여 이용하는 것이 일반적이다.

지문 영상을 살펴보면 수많은 융선이 주로 곡선의 형태를 이루며 융선폭은 매우 좁은 상태와 매우 깊은 굴곡을 이루고 있다. 이로 인하여 지문 영상은 평균치 방법이나 메디안 방법에 의하여 이진화시키기가 매우 용이함을 알 수가 있다. 이진화된 영상은 급격한 명도차로 고주파 신호를 발생시키게 되며 이는 진폭 신호를 발생시키는 면적보다 위상 신호를 발생시키는 선의 정보로 이루어지게 된다. 한편 서로 다른 지문 영상은 진폭에서는 유사하나 위상에서 급격한 차이를 보이므로 입력 영상의 주파수 위상을 데이터 베이스에 수록된 지문 영상의 주파수 위상과 주파수 영역에서 위상 정합시키면 두 지문간에 유사성을 판단할 수 있다.

주파수 관점에서 지문 영상을 살펴보면 모든 지문 영상은 고유 주파수를 지니고 있으므로 기본적으로 주어지는 기준 영상의 주파수를 고유 주파수로 이용하여 주파수 영역에서 패턴 정합을 시도하면 효과적인 결과를 얻을 수 있다. 지문 영상은 2차원적으로 존재하므로 주파수도 2차원으로 발생시키는 것이 적당하다. 2차원 주파수 발생은 퓨리에 변환 렌즈를 이용하여 광학적으로 발생시킬 수 있으며 2차원 주파수 평면에서 입력 영상의 밝기 정보는 진폭 신호로 나타나고 영상의 명도 차이는 주파수 평면에서 위상 신호를 발생시킨다.

지난 몇 년동안 지문 인식을 위하여 광 패턴 인식의 사용을 포함한 다양한 구조의 시스템들이 제안되었다. 초기에 광학 시스템을 이용하여 주파수 영역에서 지문 인식을 위한 알고리듬으로는 Vander Lugt의 공간 정합 필터를 사용한 인식 방법이 시도되어 많은 연구가 계속되었으나 공간 정합 필터의 제작 과정이 복잡하고 모든 지문 영상에 대해서 필터를 제작하여야 하는 단점으로 실제 응용상에 단점을 가지고 있다. 그러므로 최근들어 레이저 기술의 발달과 공간 광변조기 및 CCD 카메라의 해상도 증가로 인하여 광 상관 시스템 구성이 가능하게 됨으로써 실시간 병렬 처리의 장점을 갖고 있는 광 JTC를 이용한 실시간 지문 인식 시스템이 각광을 받고 있다.[2-4] 광 JTC 시스템은 광 퓨리에 변환을 이용하여 주파수 평면을 구성하고, 기준 지문 영상의 주파수와 입력 지문 영상의 주파수를 2차원 정합시켜 동일한 지문 및 부분 입력 지문을 판별하게 되는 것이다. 또한 퓨리에 변환의 특성상 입력되는 지문 영상의 위치에 무관한 이동 불변 특성을 얻을 수 있다.

그림 1은 지문 인식을 위한 광 JTC 구성도를 나타낸 것이다.

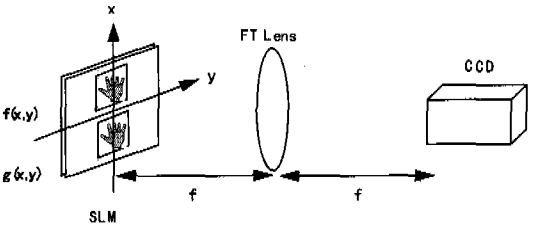


그림 1. 광 JTC 시스템

광 JTC는 입력 및 기준 영상을 하나의 입력 평면에 구성하고 동시에 퓨리에 변환을 하여 광 간섭 세기를 검출한 후, 다시 역 퓨리에 변환을 함으로서 광학적으로 상관 결과를 얻을 수가 있게 된다. JTC는 퓨리에 입출력 모두가 실수 형태로 구성이 되므로 LCD와 같은 공간 광 변조기를 이용하여 입력 평면을 구성할 수가 있고, CCD와 같은 에너지 검출기를 이용하여 출력 시스템을 구성함으로써 상관 결과를 위한 신호를 얻을 수가 있다. 한개의 LCD를 두개의 평면으로 분리하여 위에는 입력 지문이, 아래에는 데이타 베이스용 지문을 표현하고, 이 두 지문 영상을 동시에 FT Lens로 퓨리에 변환을 수행하면 출력 CCD에는 JTPS(Joint Transform

Power Spectrum)가 검출이 된다. 그런 후 이 결과를 다시 역 퓨리에 변환하게 되면 두 지문간의 상관 값을 얻게 됨으로서 입력 지문의 유효 여부를 알 수가 있게 되는 것이다.

Ⅲ. 광 XOR 연산

지문 영상은 수많은 융선이 주로 곡선의 형태를 이루며 융선폭은 매우 좁은 상태와 매우 깊은 굴곡을 이루고 있다. 이로 인하여 지문 영상은 이진화시키기에 매우 용이함을 알 수가 있다. 그러므로 지문 인식 시스템에서는 지문 영상을 사용하기 전에 우선 이진화 과정을 거치게 하고 있으므로 본 논문에서 암호화 방법으로 사용하고자 하는 XOR 연산을 이진화된 지문 영상에 적용할 수가 있겠다.

현대 암호 시스템중에 하나인 스트림 암호 시스템에서는 암호화용 키 데이터를 알고리즘에 주입하여 발생되는 무한 이진 수열로 암호화하고자 하는 평문을 암호화하는데 이때 이 알고리즘을 키 수열 발생기라고 한다. 스트림 암호 시스템은 키 수열 발생기로 1970년대 초반부터 주로 유럽에서 연구 발전된 선형 쉬프트 레지스터(Linear Feedback Shift Register : LFSR)를 이용한 암호 시스템으로 다른 암호 시스템과 달리 비교적 수학적 분석이 가능하여 주기, 선형 복잡도 등과 같은 여러 가지 중요한 수치에 대한 이론적인 값을 정확히 계산할 수 있다는 장점이 있다. 또한 데이터에 대한 에러 전파 현상이 발생하지 않으므로 통신망상의 암호 시스템에 적용할 수가 있으며 실현이 용이한 장점이 있다.[6, 7] 이와 같은 스트림 암호 시스템에서는 키 수열 발생기에서 생성되는 랜덤 키 수열로 이진 값에 대한 XOR 논리 연산을 이용하여 암호화 및 복호화 과정을 수행한다. 즉, 평문의 이진 비트 열을 암호 알고리즘에 의하여 생성되는 키 수열 비트와 XOR 연산함으로써 원 평문 신호 자체의 모든 고유 성분을 제거한 암호문을 생성하게 되며 복호화는 암호문 생성시 사용되었던 동일한 키 수열 비트와 암호문을 XOR 연산함으로써 이루어진다.

본 논문에서는 키 수열 데이터와 입력 지문 영상간의 암호화 과정인 XOR 연산을 광학적으로 수행하는 시스템을 제안하였다. 본 논문에서는 광정보처리 분야에서 많이 사용되고 있는 공간 광 변조기로서 LCD 소자를 입력 지문 영상과 키 수열 데이터를 2차원 광 신호로 표현하기 위하여 사용하였으며, 또한 여러 연구에서 증명 및 사용되었던 LCD 소자의 편광 특성을 이용하여 XOR 연산을 광학적으로 수행할 수 있도록 하였다.

최근 광정보처리 분야에서 급속하게 발전되고 사용이 되고 있는 실시간 공간 광 변조기인 SLM중 하나인 LCD는 액정 셀의 특성에 의하여 입사되는 광의 편광 성분을 인가 전압에 따라 회전시키는 특징을 지니고 있으므로, 이러한 편광 현상을 이용하여 SLM으로 광 정보 처리 분야에서 가장 많이 사용되고 있다. 본 논문에서 사용한 액정 소자인 LCD는 Twisted Nematic Cell 구조를 가지고 있으며 두개의 편광기인 Polarizer와 Analyzer가 LCD 양쪽에 위치하여 인가 및 통과되는 광 신호를 제어하여 주게 되어 있다. 즉, 이 두개의 편광기는 0°에서 360°까지 회전이 되어 수직 및 수평 성분의 투과량을 조절하여 주게 된다. 앞면의 편광기는 LCD에 입력되는 광 신호의 편광 성분을 제어하여 LCD로 입력되는 편광 성분을 결정하여 주게 되며, 뒷면의 편광기는 LCD를 통과한 편광 성분의 투과를 제어, 결정하여 준다. 액정 분자들은 두 투명 전극층 사이에 위치하여 전계의 인가 정도로 입력 편광 성분의 회전 정도를 결정함으로써 입력 광의 수평, 수직 성분의 투과를 조절하여 준다. 양단의 전극에 전압이 인가되지 않으면 액정 분자들은 두 전극 사이에서 90° 회전이 일어나게 되어 입력 편광 성분은 90° 회전이 되며, 최대 전압 V가 인가되면 전극에 수직하게 배열이 되어 입력 편광 성분이 그대로 통과하게 된다. 이러한 원리로 LCD, LCTV등의 액정 소자들이 동작을 하며 광정보처리 분야등에서 액정 소자가 갖는 편광 성분을 이용하여 여러가지 응용에 많이 사용되고 있다.[8-12]

그림 2는 LCD의 편광 특성을 이용하여 논리 상태를 정의한 것이다.

(a) (b)

그림 2. LCD 편광 특성을 이용한 논리 상태 정의 (a) 논리 "1" 상태 (V>0) (b) 논리 "0" 상태 (V=0)

논리 0 상태는 입력 편광 성분을 회전없이 그대로 통과시키고, 논리 1 상태는 입력 편광 성분을 90° 회전시키게 하여 수직 성분은 수평 성분으로 수평 성분은 수직 성분으로 되게 한다. 입력 편광

성분의 회전 여부를 결정하는 두 전극간 전압은 LCD에 표현하여 주는 Gray 레벨 값으로 조절하여 주며 이 Gray 레벨 값은 0 부터 255까지 차례로 LCD상에 표현하면서 각 편광 값을 측정하여 구할 수 있다. 실제로 Gray 레벨과 입력 편광 성분간의 회전 정도를 특정하여 보면 선형적인 관계가 아니고 일정 값이 되면 포화 상태에 이르므로 이진수 표현이외의 여러 단계를 표현하고자 할 때는 반드시 Gray 레벨과 편광 성분의 회전 정도를 측정해 보아야 한다. 이후로 본 논문에서는 입력 편광 성분을 90° 회전시키는 LCD상의 Gray 레벨을 논리 1 상태로, 입력 편광 성분을 회전 없이 통과시키는 경우를 논리 0 상태로 정의하여 사용한다. 전압에 따른 입력 편광 성분의 회전이 위에서 설명하였던 경우와 반대인 경우의 LCD 소자들도 사용이 되고 있다. 반대 경우의 소자를 사용하는 경우 편광기 배열 등에만 차이가 발생할 뿐 시스템 구성은 똑같게 된다.

그림 3은 위에서 정의한 기본 논리 상태를 이용하여 LCD 소자로 XOR 연산을 구성하여 본 것으로 $A \otimes B \otimes C$ 연산을 나타내고 있다.

모든 LCD에 부착된 원래의 편광기 Polarizer와 Analyzer를 분리한 후 양쪽 끝의 LCD 좌우에만 재배열하여 사용하였고, 입사되는 편광 성분은 수직 성분만을 갖는 편광기에 의해서 수직 편광되게 하였다. LCD에 표현하고자 하는 논리 상태는 Gray 레벨의 값을 이용하여 표현하였으며, Gray 레벨 값에 따라서 입력 수직 편광 성분이 90° 회전하여 통과되어 수평 성분이 되거나 수직 성분 그대로 통과하게 된다.

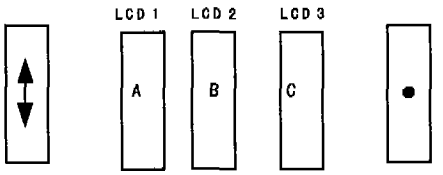


그림 3. A⊗B⊗C 연산을 위한 배열

그림 3에서 보면 그림 2에서 사용하였던 기본 논리 정의를 사용하여 XOR 연산이 가능함을 알 수가 있다. 즉, 만약에 A= 0, B=1, C=0면 LCD 1과 2 사이에서의 편광 상태는 수직 성분 상태이고 LCD 2와 3 사이에서는 수평성분 상태가 된다. 그리고 LCD 3와 뒤의 수평 편광기 사이에선 수평 성분이 되므로 최종 출력은 수평 편광기를 통하여 수평 성분이 나오게 되는 것이다. 따라서 최종 출력 단에 검출기인 Photo-Detector를 배치하면 빛의 세기를 검출할 수 있으므로 논리 1 상태가 결정되게 되므로 $A \otimes B \otimes C$ 연산이 수행이 된다.

이상과 같이 본 논문에서는 편광 특성을 갖는 LCD 소자를 이용하여 지문 영상과 키 수열 데이터 간의 XOR 연산을 수행할 수 있게 하였다. N×N 형태의 지문 영상을 암호화하기 위하여 우선 N×N 2차원 형태로 배열된 키 수열 데이터를 하나의 LCD 소자에 표현하고 지문 영상은 다른 LCD 소자에 표현한 함으로써 두 LCD 소자에 표현된 영상 간의 XOR 연산을 수행하게 하였다. N×N 형태로 구성이 되는 키 수열 데이터와 지문 영상은 동일한 위치에 존재하는 값간에 XOR 연산이 이루어지며 결과 값도 N×N 형태로 표현이 된다.

Ⅳ. 제안된 시스템 및 실험 결과

본 논문에서는 광 JTC를 사용한 지문 인식용 보안 시스템에 암호화 장치를 추가함으로써 중요 정보를 보호할 수 있는 새로운 보안 시스템 모델을 제안하였다. 즉, 광 JTC 전단에 입력 지문 영상을 암호화하는 장치를 구성하여 암호화 기능을 부여하는 것이다.

그림 4는 본 논문에서 제안한 새로운 보안 시스템의 블록 구성도이다.

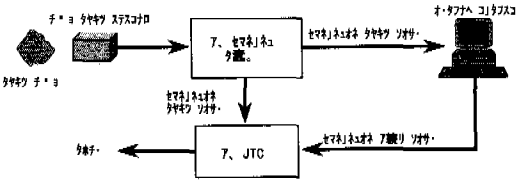


그림 4. 제안한 시스템의 블록 구성도

그림 4와 같이 제안된 보안 시스템은 크게 광 암호화 장치와 광 JTC등 두 개의 주요 장치로 구성이 된다. 우선 입력 지문은 레이저, 프리즘, CCD 카메라 등으로 구성된 지문 입력 시스템을 통하여 광 암호화 장치로 입력된 후 앞장에서 설명하였던 2차원 광 XOR 연산에 의하여 키 수열 데이터와 암호화됨으로써 암호화된 랜덤한 영상으로 변하게 된다. 암호화된 영상은 우선 데이터 베이스용 영상인 경우에는 데이터 베이스용 메모리 유니트에 저

장이 되고, 만약 출입 허가를 위하여 입력된 지문 영상이면 광 JTC로 입력이 된다. 광 JTC로 입력된 영상은 미리 암호화되어 데이터 베이스로 저장되어 있던 각 영상과 상관 정도를 측정함으로써 유효성 여부을 측정하게 된다. 이때 동일한 영상이 발견이 되면 출입을 허가하여 주고 동일한 영상이 존재하지 않는다면 출입을 하지 못하게 함으로써 보안 시스템의 역할을 수행하는 것이다.

광 JTC에서 상관 값을 측정하여 그 크기에 따라 결정을 내려 주는 부분, 데이터 베이스 영상을 저장하기 위한 부분, 광 암호화 장치에서 디지털 암호화 알고리즘에 의하여 키 수열 데이터를 생성하는 부분, 사용되는 모든 LCD 소자에 2차원 데이터를 표현하여 주는 부분등은 디지털 시스템에 의하여 동작이 되지만 그 밖에 암호화 과정과 상관도 측정을 위한 상관 과정 등 모든 주요 부분은 광학적으로 처리가 된다. 또한 디지털 알고리즘에 의한 키 수열 생성 방법을 광학적으로 구현할 수 있는 연구가 발표된 예가 있으므로 이 부분은 광학적 구현이 가능할 것이다.

그림 5는 본 논문에서 제안한 안전한 광 보안 시스템을 나타낸 것이다.

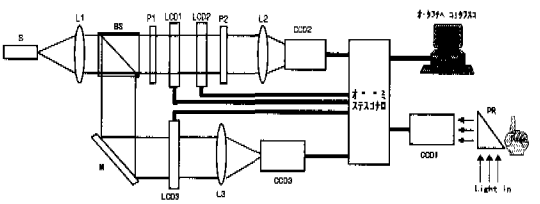


그림 5. 제안된 광 암호화 시스템

그림 5에서 여기서 S는 광원인 레이저을 의미하며, L1과 L2는 렌즈로서 각각 평행광과 효율적인 영상 검출을 위하여 사용을 한다. P1과 P2는 각각 광학적인 XOR 연산을 위한 수직, 수평 성분으로 편광된 편광기이며, LCD1과 LCD2는 각각 입력 지문 영상과 암호화 알고리즘에 의한 이진 키 수열 데이터를 2차원 광신호로 표현하기 위한 LCD 소자이다. LCD3는 광 JTC를 위한 LCD 소자로서 JTC 시스템에서 입력 평면 및 주파수 평면이 된다. L3는 퓨리에 변환 렌즈로서 입력 평면에 위치된 암호화된 지문 영상과 기준 영상의 JTPS을 표현하게 하여 주며 다시 JTPS를 역퓨리에 변환하여 상관 값을 발생하게 한다. BS와 M은 하나의 레이저에서 생성되는 광 신호를 암호화 부분과 광 JTC 부분에서 분할하여 사용할 수 있게 하는 빔 분할기와 거울이다. 그림 5에서 광 암호화 부분은 P1, LCD1, LCD2, P2, L2, CCD2로 구성이 되고, 광 JTC 부분은 LCD3, L3, CCD3로 구성이 된다.

입력 지문 영상은 프리즘 PR에 입사되는 광원에 의하여 손가락이 놓인 경계 조건이 바뀌므로 지문의 융선 부분이 반사되어 CCD1로 검출된다. CCD1에 의하여 검출된 지문 영상은 디지털 시스템에 의하여 이진화된 후 LCD1에 표현된다. 입력 지문 영상을 LCD 1에 N×N 형태로 표현한 후 디지털 암호화 알고리즘에 의하여 생성된 키 수열 데이터도 마찬가지로 N×N의 2차원 배열로 LCD 2에 표현하여 XOR 연산을 수행, 암호화 과정이 이루어지게 된다. LCD 1과 LCD 2를 통하여 암호화된 영상은 CCD 2에 의하여 검출되어 데이터 베이스에 기준 영상으로 저장이 되거나 광 JTC를 구성하는 LCD 3의 입력 영상이 된다. LCD3로 입력된 암호화된 영상은 데이터 베이스로부터 출력된 기준 영상과 상하로 대칭적으로 동일한 N×N 형태로 표현이 되고 퓨리어 렌즈 L3를 통하여 JTPS으로 검출되게 된다. CCD3에 의하여 검출된 JTPS는 다시 LCD3로 입력이 되어 L3에 의하여 역퓨리에 변환이 됨으로써 최종적으로 두 암호화된 지문 영상간의 상관 값이 CCD3로 검출되게 된다. 그러므로 CCD3로 검출된 상관 첨두치 값의 크기로 두 영상간의 유사성을 판별하게 되며 상관도가 없거나 낮게 되면 데이터 베이스로부터 다른 기준 영상을 입력 받아 LCD3의 기준 영상으로 사용함으로써 다시 상관도를 측정하게 된다. 이와같은 과정을 반복하여 동일한 지문 영상을 찾게 되면 입력된 지문 영상에 대한 유효성을 승인하게 되며 모든 기준 영상들에 대해서 동일한 영상을 찾을 수가 없으면 입력된 영상에 대해서 승인 거부를 하게 된다.

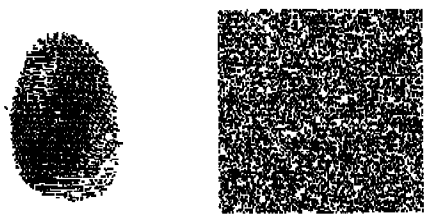
그림 5의 디지털 시스템은 LCD 동작 회로, CCD 검출 관련 회로, 데이터 베이스 관련 회로, 지문 영상에 대한 이진화 기능 등이 포함된다. 디지털 시스템에 의하여 암호화 과정과 광 JTC에서의 동작이 순차적으로 수행되며 최종적으로 입력된 지문 영상에 대한 승인 결정을 내려 결과에 따른 동작을 수행한다.

이상과 같이 제안된 시스템은 입력된 영상이 일단 암호화 되어 사용이 되며, 또한 기준 영상도 암호화되어 데이터 베이스에 저장이 되므로 불법적인 접근 시도로부터 중요 정보를 보호할 수가 있어 안

전한 보안 시스템이 될 수가 있겠다.

본 논문에서는 그림 5의 제안된 시스템의 성능을 평가하기 위하여 컴퓨터 시뮬레이션을 수행하였다 시뮬레이션을 위한 입력 영상은 256×256으로 구성이 되었으며 지문 영상은 이진화된 영상을 사용하였다.

그림 6은 컴퓨터 시뮬레이션을 위한 입력 영상들을 나타낸 것으로 (a)는 입력 지문 영상이고 (b)는 2차원 형태로 배열이된 암호화용 키 수열 데이터이다.



(a) (b)

그림 6 시뮬레이션을 위한 입력 영상 (a) 입력 지문 영상 (b) 랜덤 키 수열 데이터

그림 6의 (b)는 디지털 암호 알고리즘에서 구한 랜덤 키 수열 데이터로서 입력 지문 영상과 마찬가지로 256×256 크기를 갖으며 완전한 랜덤한 특성을 갖고 있음을 알 수가 있다. 그림 6의 (a) 지문 영상을 (b)의 키 수열 데이터로 암호화하기 위하여 XOR 연산을 수행함으로써 그림 7의 (a)와 같은 완전히 랜덤한 특성을 갖는 암호화 영상을 얻게 되었다.

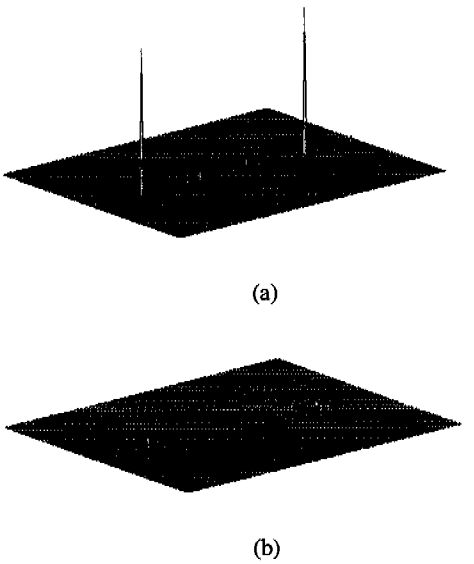
그림 7은 컴퓨터 시뮬레이션 결과로서 (a)는 암호화된 영상 (b)는 그림 6의 (b) 키 수열 데이터로 복호화한 영상이다.

그림 7의 (a)에서 암호화된 영상은 랜덤한 이진값으로 구성이 되어있고 그 랜덤한 값이 전체 영상에 걸쳐서 균일하게 분포가 되므로 암호화 과정에서 사용하였던 동일한 키 수열 데이터를 갖고 있지 않은 한 원래 입력 영상을 알아내는 것은 매우 어렵다고 할 수 있다. 복호화 과정은 암호화 과정과 동일한 시스템에서 수행이 되며, 그림 5의 LCD1에 지문 영상대신에 암호화된 영상이 표현된다는 점만 다르게 된다.

그림 8은 보안 시스템에서 입력된 지문 영상과 기준 영상들간의 상관도를 측정하기 위해 사용되는 JTC 시스템의 성능 분석을 위하여 컴퓨터 시뮬레이션한 결과이다 본 논문에서는 BPEJTC(Binary Phase Extraction JTC)를 사용하여 시뮬레이션을 수

(a) (b)

그림 7. 시뮬레이션 결과
(a) 암호화된 지문 영상 (b) 복호화된 지문 영상



(a)

(b)

그림 8 암호화된 두 지문 영상간의 상관 첨두치 결과 (a) 동일한 지문 영상 (b) 다른 지문 영상

행하였다. 그림 8의 (a)는 동일한 암호화된 지문 영상을 입력으로 사용하였을 경우의 상관 정도를 나타낸 것이며, (b)는 서로 상이한 두 암호화된 지문 영상간의 상관 정도를 나타낸 것이다.

그림 8의 결과로 볼 때 동일한 지문 영상이 암호화된 경우 두 영상간의 상관 첨두치가 크게 출력됨을 볼 수가 있으며, 서로 다른 상이한 지문 영상을 암호화 한 후 상관 관계를 구하는 경우에는 상관 첨두값이 거의 없음을 알 수가 있다. 그러므로 지문을 인식하기 위한 패턴 인식 시스템에서 영상을 암호화한 후 유사도를 구하여도 지문 식별에는 문제가 없음을 알 수가 있으며, 입력 영상 및 기준 영상들을 암호화하여 사용함으로써 불법적인 접근 시도로부터 보안 시스템을 안전하게 유지할 수가 있겠다. 제안된 보안 시스템의 안전성은 암호화 과정시

사용되는 디지털 암호화 알고리즘의 안전성에 좌우가 되며 현재 사용되고 있는 알고리즘의 안전성을 감안할 경우 암호화 과정에서 사용하였던 키 수열 데이터를 알지 못하면 암호화된 영상으로부터 원 영상을 추출한다는 것은 거의 불가능하다고 보아야 겠다.

본 논문에서는 입력 영상에 대한 인증을 하기 위하여 기준 영상을 1대 1로 비교하였으나 더욱 효율적이고 고속의 수행을 위해서는 LCD 소자의 해상도가 허락하는 범위안에서 동시에 여러 기준 영상을 입력 평면상에 입력 영상과 위치시켜 JTC 시스템을 구성할 수도 있다.

이상과 같이 본 논문에서 제안한 보안 시스템에서 사용된 암호화 기술은 기존의 1차원 신호에 국한되어 사용되어 오던 암호화 방식을 2차원 방식으로 암호화하게 함으로써 점점 고속화되어 가고 대용량화 되어가는 정보 통신 시스템에 적용하여 고속용, 대용량용 암호화 시스템 개발에 그 응용이 가능하리라 생각이 된다.

V. 결 론

본 논문에서는 지문 인식을 이용한 보안 시스템에서 지문 정보를 안전하게 보호할 수 있는 방법으로 암호화 방법을 도입한 새로운 안전한 보안시스템을 제안하였다. 보안 시스템에서 사용되는 지문 정보를 보호하기 위하여 암호화 방법을 도입하였으며, 광 지문 인식 시스템에 적용하기 위한 새로운 광학적 암호화 방법을 제안하였다. 제안된 시스템의 구현을 위하여 공간 광 변조기로 LCD 소자를 사용하여 광학적인 암호화 과정을 수행하게 하였다. 광학적으로 암호화된 영상을 CCD 카메라로 검출하여 광 JTC의 입력으로 사용하게 하여 입력된 지문 영상과 기준 영상간의 유사도를 측정, 상관 값의 크기에 따라 지문 영상의 인증을 수행하게 하였다. 컴퓨터 시뮬레이션을 수행을 통하여 입력 지문 영상이 랜덤한 영상으로 암호화됨을 보이고 암호화된 영상간의 상관도 측정 결과가 실제 응용이 문제가 없음을 보임으로 제안된 시스템의 응용 가능성을 보였다. 본 논문에서 제안한 시스템은 기준이 되는 데이터 베이스용 지문뿐만 아니라 시스템 내부에서의 처리되는 입력 지문 데이터도 암호화된 상태로 사용되므로 매우 안전한 시스템이 되겠다. 제안된 암호화 방법을 통해 중요한 영상 정보를 보호할 수 있으며 1차원 데이터에 대한 고속 암호화 처리 및 대용량 암호화 시스템 등에 그 응용이 가능하겠다.

참 고 문 헌

[1] Bahram Javidi and Joseph L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.*, vol.33, no.6, 1752-1756, 1994.

[2] Kenneth H. Fielding, Joseph L. Horner, and Charles K. Makekau, "Optical fingerprint identification by binary joint transform correlation," *Opt. Eng.*, vol.30, no.12, pp.1958-1961, 1991.

[3] Jacques Rodolfo, Henri Rajbenbach, and Jean-Pierre Huignard, "Performance of a photorefractive joint transform correlator for fingerprint identification," *Opt. Eng.*, vol.34, no.4, pp.1166-1171, 1995.

[4] S. H. Lee, H. B. Chae, S. Y. Yi, and E. S. Kim, "Optical fingerprint identification based on binary phase extraction joint transform correlator," *Proc. SPIE,* vol.2752, pp.224-232, 1996.

[5] Alastair D. Mcaulay, *Optical Computer Architectures*, John Wiley & Sons, 1991.

[6] Gustavus Simmons, *Contemporary cryptograph*, IEEE Press, 1992.

[7] Man Young Rhee, *Cryptography and secure communications,* Ch.4, McGraw-Hill, Singapore, 1994.

[8] Altaf H. Khan and Umid R. Nejib, "Optical logic gates employing liquid crystal optical switches," *Appl. Opt.*, vol.26, no.2, pp.270-273, 1987.

[9] Francis T. S. Yu, Suganda Jutamulia, and Don A. Gregory, "Real-time liquid TV XOR- and XNOR-gate binary image subtraction technique," *Appl. Opt.*, vol.26, no.14, pp.2738-2742, 1987.

[10] Jong-Wook Han and Eun-Soo Kim, "Optical threshold generator for stream cipher systems," *Proc. SPIE* vol.3159, pp.172-178, 1997.

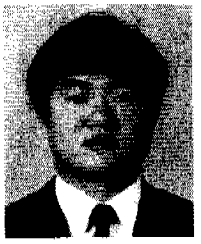
[11] Jong-Wook Han, Seung-Hyun Lee and Eun-Soo Kim, "Optical key bit stream generator," *Opt. Eng.*, vol.38, no.1, pp.33-38, 1999.

[12] Jong-Wook Han, Dae-Hyun Ryu, Choon-Sik Park and Eun-Soo Kim, "Optical image encryption based on XOR operations," *Opt. Eng.*, vol.38, no.1, pp.47-54, 1999.

한 종 욱(Jong-Wook Han) 정회원

1989년 광운대학교 전자공학과 졸업 (학사)
1991년 광운대학교 대학원 전자공학과 졸업 (공학석사)
1996년~현재 광운대학교 대학원 전자공학과 박사과정
1991년~현재 한국전자통신연구원 선임연구원
<주관심 분야> Optical Security, Quantum Cryptography, Optical Computing

김 춘 수(Choon-Soo Kim) 정회원



1987년 숭실대학교 전기공학과 졸업 (학사)
1989년 숭실대학교 대학원 전기공학과 졸업 (공학석사)
1998년 숭실대학교 대학원 전기공학과 졸업 (공학박사)
1990년~현재 한국전자통신연구원 선임연구원

박 광 호(Kwang-Ho Park) 정회원
현재 한국전자통신연구원 책임연구원

김 은 수(Eun-Soo Kim) 정회원
1978년 연세대학교 전자공학과 졸업 (학사)
1980년 연세대학교 대학원 전자공학과 졸업 (공학석사)
1984년 연세대학교 대학원 전자공학과 졸업 (공학박사)
1987년~1988년 미국 CALTECH 전기공학과 객원 교수
1981년~현재 광운대학교 전자공학과 교수
<주관심 분야> Optical Security, Automatic Target Tracking, Optical Memory