通信情報保護學會誌
第5卷 第3號, 1995. 9

패턴인식 기법을 이용한 보안 시스템

Security Systems Using Pattern Recognition Techniques

김 구 영*, 원 치 선*

요 약

본 고에서는 정교한 칼라 복사기와 디지탈 영상처리 기법의 발달과 함께 보안성에 대한 요구가 증대되고 있는 크레딧카드, 은행카드, 운전면허, Membership 카드 등에 적용될 수 있는 패턴인식 기법에 대해 알아본다. 개인 ID의 확인을 위해 사용될 수 있는 패턴들은 지문, 얼굴모양, 홍채패턴, 서체, 손가락 구조, 음성패턴, 타이핑 리듬 등이다. 이들 특성들로부터 개인의 ID를 확인할 수 있는 방법들을 기존의 제안들을 중심으로 살펴본다.

1. 서 론

최근에 정교한 칼라 복사기의 출현과 함께 수표뿐만이 아니라 현금까지도 복사해서 불법 유통시키는 신종 범죄가 발생하여 국내의 여론에 지목을 받은 적이 있다. 그 뿐만 아니라 스캐너와 컴퓨터를 통한 디지털 영상처리 기법의 발달과 함께 현금과 수표 등에 포함되어 있는 복잡한 패턴을 재생하는 것도 가능해졌다. 1993년에 전 세계적으로 크레딧카드 사건에 의한 손해가 10억 달러(미국 달러)에 달한다는 보고도 있다[1].

본 고에서는 날이 갈수록 그 사용 빈도가 높아지고, 따라서 사용상의 보안성에 대한 요구가 증대되고 있는 크레딧카드, 은행카드, 운전면허증, Membership카드 등에 적용되어 온 패턴인식 기법을 조사하고 앞으로의 기술을 전망해 본다.

개인 ID 시스템은 패턴인식 및 분류과정과 ID확인 과정으로 나누어 질 수 있는데 패턴의 인식 및 분류 과정은 입력된 패턴과 데이타베이스에 저장된 패턴 중 가장 가까운 패턴을 찾는 과정이다. 이와 같이 찾은 패턴은 ID 확인 과정에서 정당한 입력으로 받아들일 것인지 아니면 거절할 것인지의 이진 결정을 내린다. 개인의 ID 인식을 위해 많이 사용되어 오고 있는 특징 요소는 지문, 얼굴모양, 홍채(Iris)패턴, 서체, 손가락의 구조, 음성패턴, 타이핑 리듬[2] 등의 생체적 특징들이 있고, 그 밖에 비밀 번호나 로고(logo)도 분류를 위한 인식의 패턴이 될 수 있다. 이들 생체적 특징들은 인식의 복잡도, 정확도 및 패턴입력 과정의 용이성에 따라 장단점을 가지고 있다. 따라서 응용 분야의 요구 사양에 적합한 생체적

* 동국대학교 전자공학과

특징을 선택하여 사용해야 하며 경우에 따라 복합(Hybrid) 특징도 사용할 수 있다.

현금이나 수표 또는 크레딧카드나 여권 등에 복사기로 복사될 수 없는 특수 패턴 혹은 로고를 홀로그램으로 저장하는 기법이 사용되고 있다. 광학적 복사기는 보통 빛의 세기에 따라 반응하고 그것의 위상 성분은 복사될 수 없다는 특성을 이용한 기술이다. 그러나 최근에 스캐너와 컴퓨터에 의한 디지탈 영상 처리 기법의 발달로 CCD(Charge-Coupled-Device) 카메라로 홀로그램 영상을 다각도로 촬영하고 컴퓨터로 분석하여 상용화되어 있는 광학 기기로 재생할 수 있는 기술이 가능해 졌다[3]. 이와 같은 홀로그램 불법 복제를 방지할 수 있는 방법으로 복사도 스캐닝도 되지 않는 위상마스크(Phase Mask)로 패턴을 보호하는 기법[3]과 얼굴 등의 특징 영상을 압축하여 IC카드의 마그네틱(Magnetic) 필름에 저장하여 센터에 저장되어 있는 원 영상과 비교하는 방법[1] 등이 제안되고 있다.

연속되는 장에서 다루어질 주제는 다음과 같다. 제2장에서는 기존의 패턴인식 기법을 각 생체적 부위별로 기술하고 이들의 장단점을 논하였고, 제3장에서는 밝기의 세기에 비례해서 복사되는 기존의 광학적 복사기로는 복사할 수 없는 패턴의 보안 기법에 대해 홀로그램을 이용한 방법, 위상마스크 이용 방법, 그리고 영상압축 기법의 응용 사례로 살펴본다. 제4장에서는 제2장과 3장에서 논의된 패턴인식 기법들의 실제 구현 방법을 광학적 기구와 신경망(Neural Network)을 통해 알아본다. 마지막으로 제5장에서는 본 고의 결론을 맺는다.

2. 생체 패턴인식 기법

2.1 손구조 인식 (Hand Recognition)[5]

3차원(입체) 구조를 갖는 사람의 손은 인식 소자로서의 몇 가지 장점들을 가지고 있다. 손을 스캐닝하고 그 결과를 산출하는데 불과 1.2초로 매우 빠르며, 손의 구조에 대한 내용은 신용카드에 쉽게 저장할 수 있는 약 9-byte의 적은 데이타로 압축이 가능하다. 따라서 사용자의 측면에서는 매우 편리하게 특징 패턴을 입력시킬 수 있다. 예를 들어 사용자는 자신의 확인 코드를 누르고 일련의 안내핀이 있는 금속 평면위의 지정된 위치에 손바닥을 올려놓는다. CCD디지탈 카메라로 금속 평면 양옆에 있는 거울로 손의 옆모양과 윗등을 동시에 조사한다. 손 모양으로부터 ID 특징을 알아내기 위해 내장된 마이크로프로세서를 동작시켜 이진 디지탈 영상을 분석한다. 소프트웨어는 사용자가 시스템에 등록한 (손)특징과 입력된 손을 비교한다. 이때, 카메라의 배율을 알고 있고 기하학적 비교와 측정에 근거하여 실 거리에서 거리당 픽셀수를 계산하면 손가락 길이, 넓이, 부피와 같은 손 부분들의 특징 요소가 결정된다. 이와 같이 얻은 손의 특징 요소는 손의 각부분들 사이에 존재하는 밀접한 상호관계를 이용하여 더욱 함축된 패턴으로 표현될 수 있다. 예를 들면 약지 손가락의 길이가 길다면 집게 손가락 역시 대부분이 길 것이므로 이러한 상호관계를 이용하여 손구조를 나타낼 수 있는 9-byte의 식별벡타(Identity feature vector)를 찾는다. 신원 확인시 9-byte의 벡타가 시스템에 저장되어 있는 9-byte의 식별벡타와 비교되어 두 벡타사이의 차이 값이 계산된다. 이 차이 값에 따라 입력된 손의 수용 여부의 이진 결정을 단행한다.

이러한 손구조 식별 방법은 사용자들에게 편리하며, 최소의 컴퓨터 메모리를 필요로하므로 시스템을 쉽게 구현할 수 있다. 256개의 손구조를 인식할 수 있는 시스템이 $2150로 비교적 저렴하지만 장치의 크기에 있어서 키패드(Keypad)나 문손잡이에 장치할 수 없는 문

제점을 가지고 있다. 또한 ID number을 알고 있고 인조 손을 사용한다면 이 시스템을 속일 수 있다. 하지만 패스 카드나 키 또는 코드와 같은 보안장치보다는 훨씬 유용하다.

2.2 지문 인식 (Fingerprint Recognition)[6]

경찰이 범죄자를 확인하기 위해 지문 전문가가 지문을 수고스럽게 조사한 이래로 지문 인식은 자동화에 대한 분명한 대상이 되었다. 1971년에 상업성을 갖는 최초의 자동화 시스템이 나타났으며, 그 후 약 12년 동안의 기술적인 개발이 이루어진 후 1983년 Identix사가 상용화된 제품을 생산하기 시작했다.

범죄자들의 지문을 조사하는 자동 신원 확인 알고리듬은 FBI와 National Bureau of Standard, Cornell Aeronautical Laboratory 그리고 Rockwell Internation사와 제휴하여 1950년초에 개발하였다. 10년후 NEC Technologies사 (Tokyo), Printrak사 (Calif), Morpo system (Paris)가 자동화 시스템 분야에 참가했으며, 몇몇 회사는 신경망 기술과의 적합성을 연구하였다.

Identix System은 고해상도의 지문 형상을 얻기 위해 빛, 렌즈, 그리고 CCD 영상센서로 이루어진 단말기를 사용한다. 단말기는 68,000CPU로 IBM PC의 주변장치로 설치될 수 있으며, Network의 일부분이나 독립적인 시스템으로 작동할 수 있다. 사용자는 등록을 위해 개인 ID Number(PID)를 할당받고 한 손가락을 CCD영상 센서가 스캐닝하도록 유리나 플렉시 유리판 위에 놓는다. 250-Kilobyte(손가락) 영상이 디지탈화되고 분석되어지며 지문은 약 1-Kilobyte의 수학적 특성을 갖는다. 이러한 작업은 약 30초의 시간이 걸리며 신원 확인에 소요되는 시간은 1초 미만이다. 지문 식별 장치의 처음의 false-reject는 약 2%이며, false-accept는 0.0001%이었다. 각각의 독립 장치는 48개의 지문 원형(Template)을 저장할 수 있으며 부가적인 메모리를 사용하여 846개의 지문을 저장할 수 있다.

지문인식은 많은 응용에 있어서 유용하며 대부분의 사람들에게 친밀하다. 현재 Identix System은 40여 국가에서 사용하고 있다. Touchprint라 불리는 또 다른 Identix제품이 미국 각주들 간에 범죄자 신원 확인 시스템 입력 소자의 하나로 사용되고 있다. 이 경우에 지문 데이타는 전화선과 지역망을 통해 전송된다.

2.3 홍채 인식(Iris Recognition)[7]

망막(Retina) 패턴인식이 시도되었지만 사람과 인식 장치와의 밀착된 접촉을 필요로 하는 망막 패턴인식 시스템에 대한 심리적인 요소(선천적인 눈에 대한 보호심)에 의해 발전이 지연되어 왔다. 이제는 새로운 생물학적 신원확인 수단으로 홍채인식 방법에 주목하고 있다. 강력한 소프트웨어와 표준 비디오 영상 기술과 결합한 표준 흑백 비디오 또는 사진 기술로 30-40cm의 거리에서 홍채를 인식할 수 있게 되었다. Iriscan사의 Mount Laurel, N. J가 고안한 이 기술은 안과의사인 Leonard Flom과 Aran Satir이 개발하고 특허를 얻은 원리와 John Daugman이 발전시킨 수학적 알고리즘에 근거한다. Flom과 Satir은 모든 Iris가 수 십년 동안은 변화 없이 안정한 매우 섬세하고 독특한 구조를 가지고 있음을 관찰했다. 홍채의 구조는 지문보다도 6배 이상 독특하며, 더욱이 홍채는 시력 손실 없이는 변경되어질 수 없으며 각막에 의해 충격이나 외부적 변화로부터 보호받는다.

Iriscan사의 모형 시스템은 비디오 영상 source로 표준 비디오 캠코더와 비디오 프레임 그레버, 그리고 계산에 관한 분석을 위한 Sun

Sparcstation을 이용하고 있다. 분석은 디지탈화된 영상에서 홍채를 확실히 알기 위한 방법으로 2차원의 선형 연산자를 갖는 일련의 미적분을 필요로 한다. 공간 주파수, 방위, 이차원 위치 정보에 대해 최대의 해상도를 제공하는 2차원 Gabor filter함수를 사용하여 홍채 영상에서 구조적 정보를 뽑아 내기 위해 분석이 이루어진다. 기본적인 2-D gabor변환의 계수는 신경망 (Neural Network) 기술로 디지탈화된 영상에서 알 수 있다. 분석의 결과로 256-byte Iriscode가 계산되고 홍채 인식을 위해 filecode로 저장된다. Iriscode을 검색하는데 필요한 시간은 약100ms이다. 다음 단계인 홍채인식은 일반적인 패턴인식에서 사용하는 단순한 통계적 작업을 통해 수행된다. Hamming distance는 실시간 영상에서의 Iriscode와 저장된 file에서의 Iriscode template 두개의 Iriscode의 bit-by-bit 비교에서 생겨나는 에러(Error) 측정이다. Hamming distance는 Iriscan system이 받아들임 또는 거절을 결정할때 사용되는데 실험을 통해 1/131,000의 신뢰성 (false acception rate과 false rejection rate)을 나타냈다.

이 시스템은 아직까지 시장이 조성되지 않았지만 1994년 전반기 동안에 광범위한 분야에 걸친 시험이 행하여 졌다. 주요한 시장으로는 보안 출입, 접근 통제, 크레딧카드, 판매 정보 기록 확인, 컴퓨터와 망(Network) 보안, 여권, 자동 음성 기계, 금융 처리 확인 등의 사용이 예상된다.

2.4 얼굴 인식 (Face Recognition)[8]

자동 식별의 수단으로 얼굴을 사용하는 것은 얼굴이 꾸준히 변화하고 있다는 점에서 매우 복잡한 작업이다. 얼굴 표정, 헤어 스타일, 머리 위치, 카메라 배율 그리고 조명 등의 변화는 필름이나 비디오 테이프에 찍힌 영상과는 다른 영상을 창출한다. 그러나 진보된 영상처리 기술의 응용과 영상분류에 관한 신경망 사용이 이러한 일들을 가능하게 하고 있다. NeuroMetric Vision Systems사의 (Pompano Beach, Fla) 얼굴 인식에 대한 연구는 얼굴을 인식하는데 있어 표정, 헤어 스타일, 머리 위치의 변화에 따라 카메라 배율과 조명효과에 의한 명암을 변경하므로써 가능한 한 제한 조건을 갖지 않는 시스템으로 발전시켰다. 이러한 연구는 얼굴의 중요한 특징, 얼굴의 기하학적 구조의 분석 그리고 얼굴 영상 비교와 같은 기술이 얼굴 인식에 사용되어 질 수 있다는 현실에서 시작되었다. 이러한 접근 방법은 영상 분류 처리를 하기 위해 신경망과 rule-based 논리를 사용하였다.

1992년 최초로 소개된 Neuromeric System은 수치 연산 보조 처리기와 디지탈 신호 처리 카드 그리고 Frame grabber card를 갖는 IBM 386 또는 486 개인용 컴퓨터에서 작동된다. 이 시스템은 실시간에서 비디오 카메라나 비디오 레코더를 사용하여 영상을 얻는다. DSP카드를 작동시키는 소프트웨어는 비디오 프레임에서의 얼굴의 위치를 찾아서 배율과 회전을 행하며 필요하다면 조명 차이를 보상하고 수학적인 변환 (얼굴을 Floating-point feature vector로의 변환)을 수행한다. 이렇게 얻은 특징 벡타 함수는 신경망에 입력되어 1초 이내에 훈련된 영상중 하나와 매치된다. 신경망에 의한 영상처리와 영상분류는 시스템의 DSP card에 의해 행하여지는데 현재의 시스템은 다단 DSP card와 비디오 카메라 다중화로 데이타 뱅크에 5000개의 얼굴들을 유지할 수 있으며 1초에 20명을 확인할 수 있다. 시스템의 Rejection Level은 매칭에 대해 여러 다른 SNR (Signal-to-Noise)을 지정함으로서 조정되어질 수 있다. 예를 들면 매우 높은 SNR을 갖는 시스템은 초기에 시스템에 등록한 얼굴 영상과 정확히 일치하는 사람만을 인식할 수 있다. 즉 높은

SNR은 정확한 매칭을 나타낸다. NeuroMetric 기술이 사용한 신경망은 다층 구조로 입력층은 문제의 입력 변수를 저장하고 출력층은 결과를 나타내며 입력층과 출력층 사이에 있는 히든층은 연결 강도 조정을 한다. NeuroMagnetic시스템에 누군가를 등록시키기 위해서는 얼굴 영상을 찍고 특징 요소를 축출하며 신경망은 이러한 특징들로 부터 훈련(train)된다. 신경망은 일반적으로 다층일 경우 Rumelhart가 제안한 Backpropagation 알고리즘[9]을 - Madaline의 경우는 각 Unit의 양자화가 계단함수 (Hard limiter)을 사용하므로 미분이 불가능하여 사용할 수 없으므로 Adaline의 학습 알고리즘을 확장한 MRⅡ (Madaline ruleⅡ)을 사용한다 - 사용하여 모든 얼굴을 학습(Learn)할 때까지 반복적으로 훈련되며 지속적으로 모든 영상을 확인한다. 시스템은 얼굴 인식 데이타 뱅크로 neural network cluster을 사용한다. 다수의 cluster가 요구될 때 연속적이고도 계층적으로 접근되어질 수 있다. 얼굴이 데이타 베이스에 저장되거나 삭제될 때는 단지 관련 있는 cluster만이 재훈련(retrain)된다. 사람이 똑같은 모습의 쌍둥이를 쉽게 구분할 수 없듯이 NeuroMatric 시스템도 쉽게 구분할 수 없다. 그러나 이 시스템은 쌍둥이 사이에 미세한 차이를 끄집어내거나 비슷한 행동양식을 가지고 있지만 다른 얼굴 특징 요소를 가지고 있는 사람들을 구별하는데 있어 대부분의 사람들보다 매우 객관적이다. 그것은 헤어 스타일 또는 피부 색깔, 안경등의 변화에 덜 영향 받기 때문이다.

NeuroMatrix시스템의 다른 사용은 접근 통제다. 한 사람이 보안 카메라 앞을 지나간다고 생각해 보자. 시스템은 그 사람의 신원을 확인하기 위해 사람 식별 시스템과 연합으로 작동하여 그 사람의 접근을 통제할 수 있다. 또한 NeuroMatric system은 용의자의 얼굴 사진 데이타베이스을 찾는 법 집행 시스템에서 사용된다. 현재까지는 대상이 정지한 채 카메라를 바라보며 서 있어야 하지만 미래에는 움직이는 대상도 입력하여 인식할 수 있도록 해야 할 것이다.

이상에서 살펴본 각 생체적 특징의 장단점을 표1에 요약하였다.

표 1 생체 특징의 장단점 비교

생체 특징	장 점	단 점
손구조	- 사용자로부터 패턴 입력이 용이 - 특징 데이타의 추출이 빠르고 데이타량이 적다.	- 인조 손등을 이용한 위조가 가능하다.
지문	- 신뢰성이 높다.	- 하드웨어가 비싸고 많은 데이타 베이스가 필요하다. - 패턴의 입력이 수월하지 못하다.
홍채(iris)	- 신뢰성이 높다.	- 패턴의 입력이 수월하지 못하다. - 계산량이 많다.
얼굴	- 패턴의 입력이 수월하다.	- 동일인에 대한 입력 패턴의 변화가 있다. - 계산량이 많다.
음성	- 데이타량이 적다.	- 신뢰성이 지문보다 떨어진다. - 동일인에 대한 입력 패턴의 변화가 있다.

3. 광학적 복사기로 불법 복제 불가능한 패턴 보호 기법

광학적 복사기는 기본적으로 빛의 세기에 비례하는 양을 복사하므로 위상 정보는 복사할 수 없다. 이와 같은 특성을 이용하여 수표, 현금, 여권 등에 있는 특수 패턴을 보호하기 위해 위상 정보를 사용할 수 있다. 본 장에서는 광학적 복사기로는 불법 복제가 불가능한 패턴 보호 기법으로 홀로그램 방식, 위상마스크 방식, 그리고 영상 압축 방식 등에 대해 알아본다.

3.1 홀로그램에 의한 패턴보호

홀로그램은 3차원 영상을 사진 필름과 같은 평평한 2차원 표면에 기록하는 기술로 기본적인 개념은 물체로부터 산란되는 빛의 크기뿐만이 아니라 위상 정보도 기록하는 것이다. 그러나 광학적 기술 시스템이 모두 빛의 세기에만 반응하므로 위상 정보를 크기의 세기의 변위로 변환시킬 필요가 있다. 즉, 물체로부터 나오는 빛과 동일한 각도로 동일 크기의 기준빔(Beam)을 사진판에 조명하여 기록하므로써 기록된 영상의 재생(인식)에도 똑같은 각도로부터 기준빔을 받아야 볼 수 있도록 하였다.

크레딧카드나 여권 등에 부착된 홀로그램 패턴도 더 이상 안전한 패턴 보호 방법은 아니다. 즉 기록된 홀로그램 패턴을 여러 각도의 기준 빔에 의해 CCD 카메라로 촬영한 후 컴퓨터 등을 이용하여 분석하면 홀로그램의 기록 체계를 이해할 수 있고, 기존의 광학적 기구에 의해 복제 패턴이 합성될 수도 있다[3]. 이와 같은 문제점을 보안하기 위해 다음절에 설명되는 두 가지 방법이 최근에 제안되었다.

3.2 위상마스크를 이용한 패턴보호

홀로그램을 이용한 패턴(로고 등)의 보호는 CCD 카메라와 디지탈 영상 처리 기법의 발달로 보안성이 떨어지고 있다. 특히 홀로그램은 비록 광학적 복사기로는 복사될 수 없지만 사람의 육안으로는 인식될 수 있으므로 비교적 쉽게 재생/복제할 수 있다.

최근에 Jabidi등 [1][3]은 육안으로 식별될 수도 없고 빛의 크기 값에 반응하는 복사기로도 복사할 수 없는 새로운 패턴 보호 기법을 개발하였다. 위상마스크를 이용한 이 방법의 기본 개념은 지문이나 얼굴사진 또는 사인 등의 보호가 필요한 패턴 위에 복소수 신호의 크기와 위상을 갖는 위상 마스크를 영구적으로 붙이는 것이다 [그림1 참조]. 이 마스크는 카드를 파괴시키지 않는 한 제거될 수 없도록 단단히 부착되어 있다. 위상마스크는 수학적으로 $\exp[jM(x, y)]$로 나타낼 수 있다. 여기서 $M(x, y)$는 $\pm\pi$ 값으로 정규화된 실수 함수로 수 mm의 크기에 수백만 개의 픽셀로 이루어진 광학 필름이나 재질 위에 부조 세공(embossing technique)이나 표백 기술을 적용하여 만든다. 만약 보호 대상 패턴의 2차원 신호를 $g(x, y)$로 나타내면 위상 마스크가 부착된 후의 영상은 $i(x, y) = g(x, y) \exp[jM(x, y)]$로 나타낼 수 있다. 따라서 카드를 읽어서 보호된 패턴을 인식하고 인식된 패턴의 유효성 여부를 가리는 카드 단말기는 $i(x, y)$로부터 위상 마스크 $\exp[jM(x, y)]$를 제거하며 입력된 다른 ID로부터 센터에 저장된 $g'(x, y)$를 위상마스크가 제거된 $g(x, y)$와 상관관계(correlation)를 계산하여 유효성 여부를 판정하는 기능을 수행해야 한다. 예를 들어, 그림 2에서와 같이 입력된 카드 상의 보호된 패턴 $i(x, y)$에 빛을 가하고 이를 렌즈를 통과시킴으로써 퓨리에 변환된 신호를 $a-b$ 축 상의 평면에서 기준 위상 마스크와 매치된 공간 필터를 통과시킴으로써 원 패턴 $g(x, y)$를 CCD 카메라로 받은 후 센터에 저장된 $g'(x, y)$와 상관성을 조사하여 상관성의 유무에 따라 입력된 카드의 유효여부를 판단하다. 또 한가지 방법은 그림 3에서와 같이 기준 위상 마스크 $\exp[jM(x, y)]$와 보호된 패턴 $i(x, y)$의 조인트 파워 스펙트럼을 광학

적 기구를 이용하여 얻은 후 비선형 기구를 통과시켜 $i(x, y)$의 위상 성분과 기준 위상 마스크의 $\exp[jM(x, y)]$가 상쇄되어 $g(x, y)$를 얻을 수 있도록 한다.

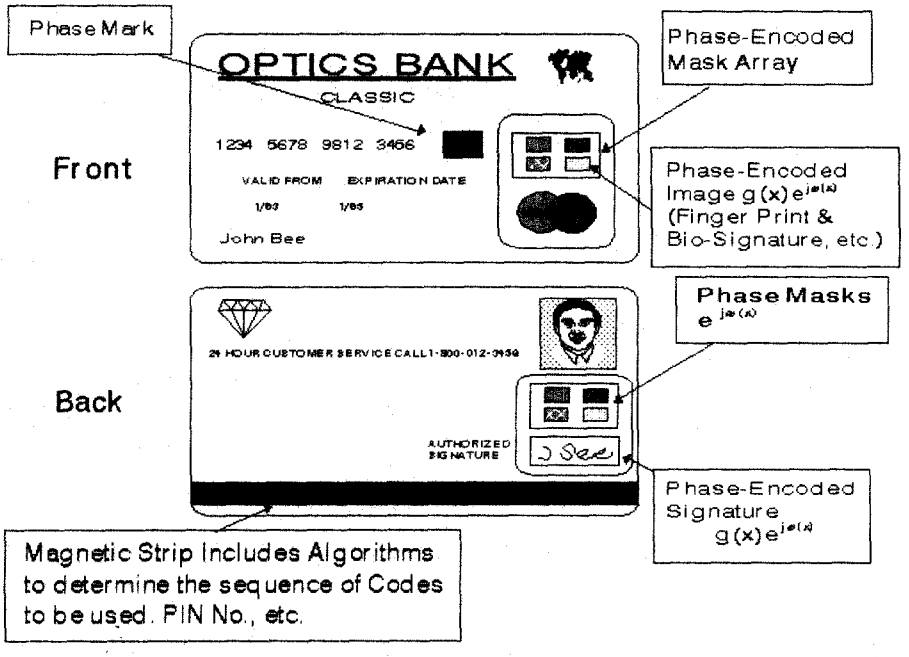


그림1 위상마스크의 ID카드 사용 예 (그림 출처 : 참고문헌[3])

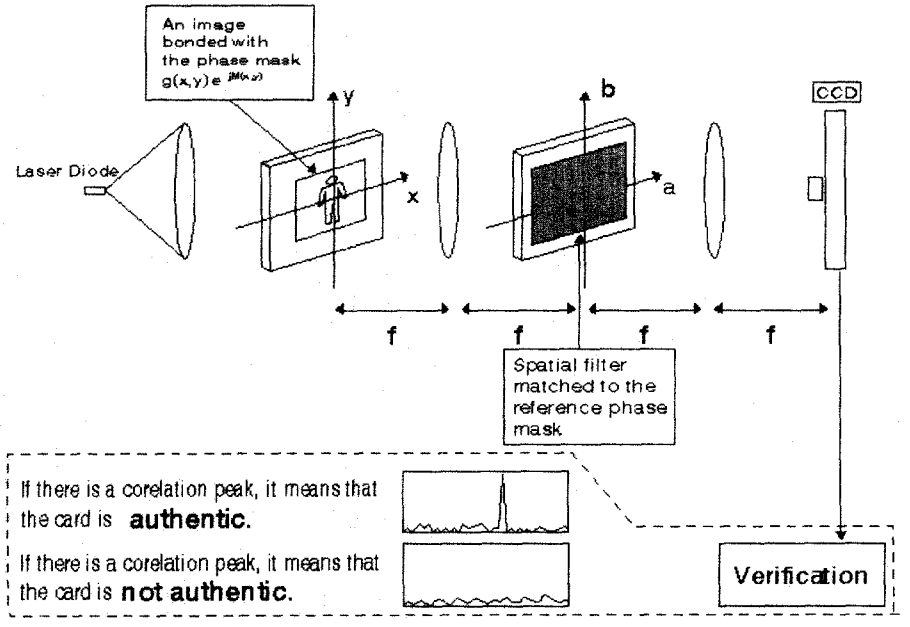


그림2 공간 필터의 광학적 상관 측정기를 사용한 위상마스크 시스템 (그림 출처 : 참고 문헌[3])

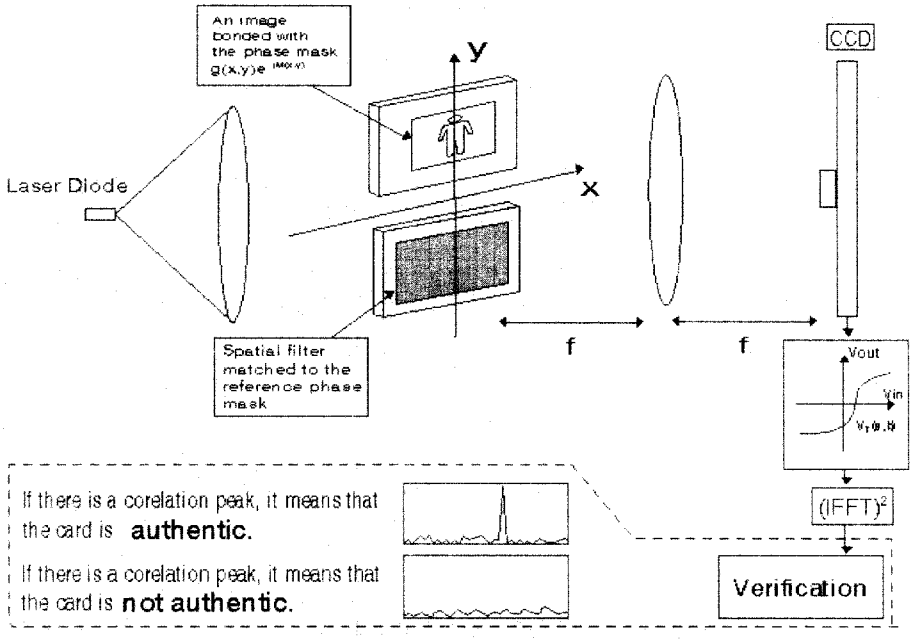


그림3 비선형 조인트 변환 상관 측정기를 이용한 위상마스크 시스템 (그림 출처 : 참고 문헌[3])

3.3 영상압축 기법을 이용한 패턴 보호

최근에 Eastman Kodak사는 9000 Byte 정도의 메모리 용량을 차지하는 여권용 사진의 내용을 영상압축 기법을 사용하여 50 Byte(400 bits)로 압축한 다음 압축된 영상 데이타를 크레딧카드의 마그네틱 테이프 상의 3번째 트랙에 저장하여 각 가맹점에서 크레딧카드를 사용할 때마다 본인 여부를 디스플레이된 영상으로 확인할 수 있는 시스템을 발표하였다[10]. 영상압축 기술을 이용한 이 시스템은 기존의 지문, 홍채, 손의 형태 및 개인용 ID 숫자(PIN)를 이용할 때 보다 더 안전성이 향상된 것으로 알려지고 있는데 이 시스템의 구현의 핵심은 역시 9000 Byte에 상당하는 영상을 큰 왜곡 없이 50 Byte로 180 : 1 압축하는 기법이다. 발표된 시스템에서 사용한 영상압축 기법은 자세히 알려져 있지 않으나 얼굴 영상에 최적화되어 사전 (a priori) 가정 및 지식을 이용한 Eastman Kodak 사의 고유 알고리즘인 것으로 추정된다. 또한 압축된 영상을 신장하여 얼굴 영상을 얻는 영상 신장(복원) 과정은 실시간 내에 이루어져야 하지만, 원래의 얼굴 영상을 압축하는 과정은 실시간내에 이루어질 필요는 없다는 조건을 최대로 반영한 압축 알고리즘을 사용한 것으로 추정된다. 이 시스템이 특히 50 Byte로 데이타의 양을 한정한 것은 크레딧 카드의 마그네틱 테이프상에 첫 번째 두 트랙은 이미 사용되고 있으므로 세 번째 트랙에 압축된 영상을 저장하고자 한 것이며, 이곳의 저장 용량이 바로 50 Byte에 해당된다. 영상압축 기술을 이용한 얼굴 영상 디스플레이 시스템의 안정성을 향상시키기 위해 Eastman Kodak 사는 랜덤하게 선택된 압축된 영상 데이타의 일부 (약 2~3 Byte)를 가맹점과 센터 사이의 확인 과정에서 센터로 전송하여 센터 내의 데이타 베이스에 저장된 원 영상의 내용과 비교하여 정합 여부를 확인하여 시스템의 안정성을

한층 향상시켰다. 새롭게 개발된 이 시스템은 은행과 가맹점에서 사용하던 기존의 터미널과 양립성이 있으며 1995년말까지는 상용화될 것으로 보인다.

4. 패턴 인식 장치의 구현

개인의 ID로 사용된 생체적 특징은 2-D 영상 정보이므로 처리하는데 많은 시간이 요구된다. 그러나 카드 속의 패턴 인식 및 확인 과정은 카드가 단말기 내에 삽입된 이후 가능한 한 실시간내에 이루어져야 한다. 따라서 패턴의 상관성 여부를 판단하기 위해 실시간 처리가 가능한 광학적 기구를 사용한다. 즉, 카드에 빛을 쪼이고 이것을 렌즈를 통과한 후 받아들임으로써 퓨리에 변환된 신호의 크기가 렌즈 뒤의 평면에 전달된다[그림 2 참조]. 또한 퓨리에 변환된 신호를 다시 한 번 렌즈를 통과시키므로써 역퓨리에 변환된 신호를 얻을 수 있다. 실제로 그림 3에서와 같은 조인트 변환 상관기(JTC, Joint Transform Correlator)는 상관관계를 구하는데 효율적으로 사용될 수 있다.

광학적 기구 이외에 실시간 패턴 매칭을 달성할 수 있는 방법은 신경망(Neural Network)을 이용하는 것이다. 신경망은 병렬 처리가 가능하고, 샘플로부터 학습될 수 있고, 또 한가지 보안상 패턴인식에 중요한 특성으로 입력 패턴의 일부가 왜곡(Distorted)되어도 패턴을 옳게 인식할 수 있다는 특성 때문에 보안용 패턴인식에 많이 사용될 것으로 예상된다. 예를 들어, 얼굴인식 시스템에서 입력된 얼굴 모양은 동일인인 경우도 입력되는 시점에 따라 머리 스타일이나, 안색, 볼륨 등이 다르게 입력될 수 있다. 이 경우 신경망을 이용하면 애초에 여러 가능한 입력의 변형으로 학습되었으므로 어느 정도의 입력 왜곡은 신경망에 의해 무시될 수 있다.

5. 결 론

지문, 홍채패턴, 얼굴모양 등 사람의 생체적 특징을 기본으로 하는 보안 시스템은 시스템의 구현 가격, 신뢰성(false rejection rate와 false acceptance rate), 실시간 실현 가능성 및 입력 패턴의 채취 용이성에 따라 서로 장단점을 보유하고 있으므로 응용 분야에 따라 적합한 특징을 선택해야 한다. 수표, 현금, 카드 및 여권에 부착된 비밀 패턴이나 로고 등은 육안으로 확인 확 수 없고, 복사기로 복제될 수 없는 위상 마스크 기법 등이 고려되어야 하며, 압축된 얼굴 영상을 카드의 마그네틱 테이프에 저장하는 방법도 효율적으로 사용될 수 있을 것이다. 디지탈 영상 처리를 위한 하드웨어의 가격이 싸지고 실시간 처리가 가능해지면서 여러 다양한 패턴 보호 기법이 사용될 수 있을 것으로 예상된다.

참 고 문 헌

[1] B. Javidi and J. L. Horner, "Optical pattern recognition for anti-counterfeiting and security systems", Optical processing & computing, pp 6-7, November 1994.

[2] B. Miller, "Vital Signs of Identity", IEEE Spectrum, pp 22-30, Feb. 1994.

[3] B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification", Optical Engineering, vol. 33, no 6, pp 1752-1756, June. 1994.

[4] T. E. Bell, "Invisible images ensure security", IEEE Spectrum, pp 17, April 1995.

[5] d. Sidlauskas, "Hand : give me five," IEEE Spectrum, pp 24-25, Feb. 1994.

[6] R. C. Fowler, "fingerprint : an old touchstone descriminalized", IEEE spectrum, pp 26, Feb. 1994.

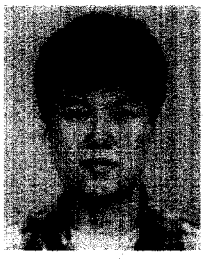
[7] J. E. Siedlarz, "IRIS : more detailed than a fingerprint", IEEE spectrum, pp 27, Feb. 1994.

[8] T. hutcheson, "FACE : smile, you're on candid camera", IEEE Spectrum pp. 28-29, Feb. 1994.

[9] Jacek M. Zurada, "Introdution to Artificial Neural Netwopk", Info Access Distribution Pte LTD., pp 186-195. 1992

[10] T. E. Bell, "A picture is worth 50 words. " IEEE Spectrum, pp 17, June 1995.

□ 著者紹介



김 구 영

1995년 동국대학교 전자공학과 졸업
현 동국대학교 전자공학과 대학원 석사 과정

원 치 선

1982년 고려대학교 전자공학과 졸업
1986년 매사추세츠대 (앰허스트) 석사
1990년 매사추세츠대 (앰허스트) 박사
1989년 ~ 1992년 LG전자 (현)영상미디어 연구소 선임연구원
1992년 ~ 현재 동국대학교 전자공학과 조교수

※ 주관심분야 : 디지탈 영상처리, 디지탈 비디오 전송 시스템