글로벌경영연구
第 21 卷 1 號
2009年 8月


# 카드 불법사용 방지를 위한 가상자기띠형 IC 카드 설계

조 준 서

# A Design of Virtual Magnetic Line Strip type IC Card for Credit Card Fraud Prevention

*Abstract*

*There are two types of credit cards according to the type of recording information on a card; magnetic line strip credit card and IC card. Since it does not have functions for security or ID checking, the magnetic strip type card may cause financial damage to a card holder or a financial organization that issues credit cards when it is lost, forged, or tampered. However, the IC card can be used with a relatively high security due to an ID checking function such as fingerprint recognition and due to password confirmation system by card reader.*

*In spite of all these advantages, the transition from the magnetic card to the IC card makes a slower progress than expected. The first obstacle to the transition is that a separate IC card reader must be provided since the IC card cannot be read by the magnetic strip card reader, but the introduction of the IC card reader is not progressive due to the high cost.*

*This paper proposed a method to provide an IC card configured to be read using a magnetic strip card reader, which encourages to introduce the IC cards more rapidly by making it unnecessary to replace the magnetic strip card readers with the new IC card readers of high cost as well as to provide an IC card the stored information of which cannot be read without the ID confirmation of the user using the high security functions of the IC card.*

* 한국외국어대학교 글로벌경영대학

# Ⅰ. 개요

현재 신용카드는 온라인 및 오프라인에서 가장 대표적인 지불결제 수단이다. <표 1>에서와 같이 그 사용규모는 2008년 현재 1100만건을 넘었고, 사용금액도 1조 2천억 원을 넘어 지속적으로 성장하고 있으며(한국은행, 2009), 여러 가지 부작용과 문제점도 적지 않은 것이 현실인데, 특히 오프라인 및 통신판매시장에서의 대표적 결제수단인 신용카드의 부정사용이 가장 큰 문제점으로 지적되고 있다. 즉, 신용카드는 후불 결제라는 메리트 때문에 인터넷 쇼핑몰은 물론 홈쇼핑몰을 포함한 모든 통신판매시장에서 가장 많이 이용되고 있으나, 그 동안 신용카드 결제 서비스와 관련된 보안장치가 미비한 관계로 신용카드 정보의 위·변조 및 도용 등 불법적 사용에 따른 소비자들의 피해가 자주 발생하고 이에 따라 전자상거래 자체에 대한 부정적 인식도 줄지 않았던 것이 사실이다. 또한 신용카드의 분실 및 도난에 의한 피해 역시 지속적으로 발생하고 있다.

따라서 오프라인상에서는 국내 카드사들이 주도가 되어 카드부정사용 방지 시스템 등을 도입하여 카드부정사용을 차단하기 위한 노력을 하고 있다(이종오, 2008; 이충훈, 2008). 또한 전자상거래에 따른 신용카드의 안전한 사용을 도모하

<표 1> 국내 카드 이용규모 현황(일평균)

(천건, 십억 원, %)

| | | 2006 | 2007 | 2008 | 증감률 |
|---|---|---|---|---|---|
| 건수 | 신용카드 | 8,574 | 9,514 | 11,332 | 19.1 |
| | 체크카드 | 901 | 1,400 | 2,029 | 44.9 |
| | 선불카드 | 42.1 | 52.5 | 56.8 | 8.2 |
| | 직불카드[1)] | 6.8 | 5.0 | 3.6 | -28.0 |
| | 합계 | 9,524 | 10,971 | 13,421 | 22.3 |
| 금액 | 신용카드 | 1,016 | 1,106 | 1,247 | 12.7 |
| | 체크카드 | 33.8 | 51.7 | 73.2 | 41.6 |
| | 선불카드 | 2.0 | 2.5 | 2.8 | 12.0 |
| | 직불카드[1)] | 0.31 | 0.22 | 0.16 | -27.6 |
| | 합계 | 1,052 | 1,160 | 1,323 | 14.1 |

주: [1)] 금융결제원 직불카드공동망 이용규모.
자료 : 전업카드사 및 겸영 은행.

기 위해 금융감독원은 전자상거래와 관련하여 인터넷 쇼핑몰 등에서의 신용카드 이용 시 공인인증제도를 반드시 도입하도록 하여 인터넷 상에서 카드소지자에 대한 본인확인을 강화하고, 해킹 등으로 인한 거래정보유출 및 데이터 위·변조 등의 방지책을 제시하고 있다. 그리고 2004년 4월부터는 30만원 이상의 거래의 경우 반드시 공인인증서를 사용하도록 하여 공인인증서를 통한 본인 확인이 없으면 신용카드 결제가 불가능하도록 함으로써 신용카드 도용이나 불법사용에 따른 피해를 줄일 수 있도록 하고 있다.

이와 같은 안전대책과 관련해서 신용카드사들도 자체적으로 ISP(Internet Secure Payment)서비스, 안심클릭 서비스, 모바일 크레딧(Mobile Credit) 서비스와 같은 신용카드 안전결제를 위한 다양한 시스템을 도입하는 등 신용카드의 부정사용을 방지하기 위한 노력을 하고 있다(김현희, 2008). 이러한 노력들의 결과로 지난 2003년 4만 968건에 달했던 위·변조 및 도난·분실 신용카드 부정사용이 2004년 2만 5522건, 2005년 2만 2667건, 2006년 2만 925건, 2007년 1만 9113건, 2008년 2만 762건에 그쳤다(매일경제, 2009).

위에서 언급한 대부분의 카드는 카드에 정보를 수록하는 방법에 따라 크게 마그네틱 선(Magnetic Strip, MS)을 이용하는 방식의 마그네틱카드와 내장된 집적회로(Integrated Circuit, IC) 칩을 이용하는 방식의 IC 카드가 있다.

현재 가장 많이 사용하고 있는 마그네틱 카드에는 보안성과 본인확인 기능이 없으므로, 카드의 분실가 분실될 경우나, 카드가 위조/변조되어 사용되는 경우에는 카드 소지자나 카드 발행 금융기관에 큰 피해를 발생시키고 있다. 그러나 IC 카드인 경우에는 카드 자체에 지문인식기능과 같은 본인확인 기능이나, 카드 리더기를 통한 비밀번호 확인 작업을 통하여 상대적으로 안전하게 카드를 사용할 수 있다.

그러나 이러한 IC 카드의 장점에도 불구하고, 기존의 IC 카드는 자기띠 카드의 리더기로는 읽을 수 없으므로 그에 적합한 별도의 IC 카드 리더기가 설치되어야 하는데, 설치비용의 부담 때문에 IC 카드 리더기의 설치가 활발하게 진행되지 못하고 있으며, 따라서 마그네틱 카드에서 IC 카드로의 교체작업은 계획보다 느리게 진행되고 있다.

그러므로 기존의 인프라 구조에 급격한 변화없이 자연스럽게 IC 카드의 보급률을 높는 방법으로는 IC 카드를 기존의 마그네틱 카드 리더기에서도 정보를 읽을 수 있도록 하는 장치를 고안하는데 있다. 그러나, 단순히 IC 카드에 마그네틱 선을 부착하는 것은 IC 카드의 장점인 보안성을 전혀 이용하지 못하여, 기존의 마그네틱 카드의 단점이 그대로 노

출되어 있다.

본 연구는 직접회로(IC: Integrated Circuit) 칩을 내장하는 IC 카드에 관한 것으로서 보다 상세하게는 기존의 자기 띠 카드용 리더기에서도 카드 정보의 판독이 가능한 IC 카드에 관한 것이다. 본 연구에서는 사용자 인증 장치를 내장하여 사용자 확인시에만 정보를 외부에서 읽을 수 있도록 하는 자체 보안기능을 구비한 마그네틱/IC 겸용의 카드를 제시하고자 한다.

# Ⅱ. 연구배경

신용카드에는 카드에 정보를 수록하는 방법에 따라 크게 “자기 띠”(MS: Magnetic Strip) 방식을 이용하는 자기띠 신용카드와 직접회로(IC: Integrated Circuit) 칩을 내장하는 IC 카드가 있다. IC 카드의 IC 칩은 메모리와 연산기능이 가능한 프로세서 등을 가지고 있으며, 이러한 IC 칩을 이용하여 디지털 서명 등의 보안기능이나 접근제어 기능 등의 기능을 수행할 수 있고, 카드결제, 현금인출과 같은 결제 금융서비스는 물론 포인트 서비스, 전자승차권 등과 같은 서비스를 제공할 수 있다. 자기띠 카드에는 보안성과 본인확인 기능이 전혀 없으므로, 카드가 분실될 경우나, 카드가 위조/변조되어 사용되는 경우에는 카드 소지자나 카드 발행 금융기관에 큰 피해를 발생시킨다. 그러나 IC 카드인 경우에는 카드 자체에 지문인식기능과 같은 본인확인 기능이나, 카드 리더기를 통한 비밀번호 확인 작업을 통하여 상대적으로 안전하게 카드를 사용할 수 있다(김학범, 2006; 이충훈, 2008). 이러한 IC 카드의 다양한 기능과 안전성으로 인하여 IC 카드는 차세대 카드 사업의 주류가 될 것으로 기대되고 있으며, 전 세계적으로 카드의 종류가 자기띠 카드에서 IC 카드로 점점 교체되어가고 있는 추세이다(장병환, 2006).

## 1. 기존 연구

대표적으로 오프라인에서 사용되는 결제수단은 신용카드이다. 또한 상품을 전자적으로 결제하는 데에는 여러 가지 방법이 있으나 인터넷에서 가장 많이 쓰이는 결제의 수단 역시 신용카드이다. 전 세계의 은행들은 그들의 신용카드에 관한 공정을 효과이고도 안전하고 신속하게 하기 위해서 마그네틱 선을 가진 카드에 관한 기술에 많은 투자를 하고 있는 실정이다.

금융부분에서 소비자들이 가장 많이 사용하고 있는 결제 수단인 신용 카드는 사용의 광범위성과 더불어 특히 보안적인 문제가 제시되고 있다. 사용자가 안심하고 사용할 수 있도록 카드사에서 여러 방법으로 보안에 대한 노력이 진행되

어 오고 있다. 대표적인 예로 스마트카드와 슈퍼 IC 카드가 있다(Alder, 2002).

### 1.1 스마트 카드

스마트 카드는 EPS의 형태로서 화폐가치에 대한 정보를 담고 있는 마이크로칩을 가진 플라스틱 카드의 형태를 사용한다. 카드에 저장된 화폐의 가치는 현금과 같이 사용된다. 스마트 카드, 더 정확히 말하자면 stores value cards(SVCs)는 마그네틱 카드보다 더 많은 정보를 저장할 수 있고 더 많은 기능을 구현할 수 있다. 전 세계에는 6억개 이상의 스마트 카드가 사용되고 있는 것으로 알려져 있는데 마그네틱 카드나 마이크로칩을 담은 SVCs를 통해 사용되고 있다. 이들은 개인의 건강 정보나 신원 증명, 보안, 휴대폰에서의 전자 서명에 관한 정보를 담는 카드로 사용된다. 호주나 유럽에서는 Visa나 Mondex와 같이 스마트 카드가 현금 대신 쓰이고 있는데 이는 스마트 카드가 현재 EFTPOS나 ATM에서 쓰이고 있는 마크네틱 카드를 대체할 것으로 보인다.

스마트 카드는 실제로 매우 작은 컴퓨터로서, 전기를 공급하여 그것을 작동시킬 수 있는 다른 매체를 필요로 하게 된다. 스마트 카드는 작은 칩을 내장하고 있으며 대부분 플라스틱 재질이다. 이 칩은 전형적인 입/출력장치, 마이크로프로세서, ROM, RAM의 기능을 가지는 작은 컴퓨터처럼 작동한다. 스마트 카드나 SCVs는 지갑안의 모든 정보를 저장할 수 있다. 이는 대부분 카드안에 저장된 데이터나 화폐가치를 비즈니스 시스템으로 전송하는 형태로 작동하게 된다. 이때 별도의 인증이 필요하지 않다는 점이 다른 결제 시스템과 구별되는 특징이다.

스마트 카드는 또한 대학 성적 증명서나 개인 기록, 의료 정보, 의료 기록, 사회 보장 시스템 정보나 고용 정보 등 개인이나 조직에서 필요한 모든 정보를 담을 수 있다. 호주에서 SVC는 의료정보나 개인적인 CV는 물론 운전면허나 의료, 은행 카드 등으로 사용될 수 있었다. 그러나 이러한 개발은 보안이나 법적, 사회적, 그리고 정치적 문제와 관련되어 한계점을 드러내었다.

### 1.2 SuperIC Card(수퍼 IC 카드)

수퍼 IC 카드는 일본 및 세계 최대 금융회사인 MUFG(Mitsubishi-UFJ Financial Group-구, MTFG)가 2005년 10월 12일에 처음으로 발급을 시작한 IC 및 마그네틱 겸용 금융거래카드이다.

이 카드의 특징이자 강력한 보안 시스템인 손바닥 문양 인식 기능 덕분이다. 이 카드에는 예외 사용을 제외하고, 비밀번호 기능이 부여되어 있지 않다는 특징이 있다. MUFG 소속 ATM에서는 이 카드거래 시 비밀번호를 쓸 수 없게

되어 있으며, 비밀번호 대신 손바닥을 이용해 본인 인증을 한다.

MTFG 및 UFJ ATM기의 경우, 입력 패드 우측의 핸드스캐너를 확인하고, 핸드스캐너 바로 밑에 세워져 있는 핸드스탠더에 손목을 대고 손바닥 아랫면을 핸드스캐너로 향한다. 약 3~7초 후 거래 프로세스로 이동한다.

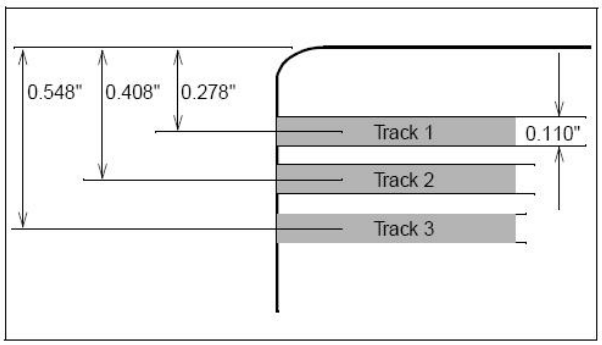
이 카드의 장점은 위변조가 아예 불가능하여 안전하다는 것, 비밀번호를 기억해야 할 필요가 없다는 것, VISA브랜드로 이용할 수 있다는 것, Platinum 서비스 발급이 가능하다는 것이다. 반면에 단점은 해당 은행 소속 ATM기 중에도 아직 사용할 수 없는 기계가 많다는 것과 타 은행권에서 가끔 오류가 난다는 것, 그리고 인식 불가능 국가가 많다는 것이다.

## 2. 기존 카드방식

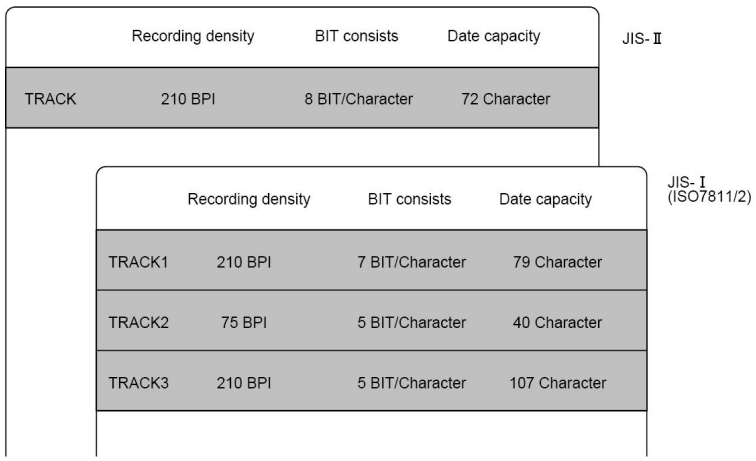
현재 많이 사용하고 있는 자기띠형 신용카드는 [그림 1]에 도시된 바와 같이 자기띠에 세 개의 트랙을 포함한다. 이들 각 트랙에는 카드 정보가 기록되어 있다. 자기띠의 트랙에 정보를 수록하는 방법은 표준화 되어 있으며, [그림 2]에 도시된 바와 같이 세 개 트랙에 정보를 수록하는 데이터의 길이와 문자표준 및 문자의 집적도 등에 관한 표준은 ISO 7811/2-1985 이며, 또한 하나의 트랙에 정보를 수록하는 표준도 존재한다. 자기띠 카드의 카드 정보 기록은 이러한 표준에 따라 이루어진다.

# Ⅲ. 지문인증을 이용한 마그네틱/IC 겸용 카드 설계

본 연구는 보안인증이 가능한 직접회로(Integrated Circuit, IC) 칩을 내장하는 IC 카드에 관한 것으로서 기존의 자기띠 카드용 리더기에서도 카드 정보의 판



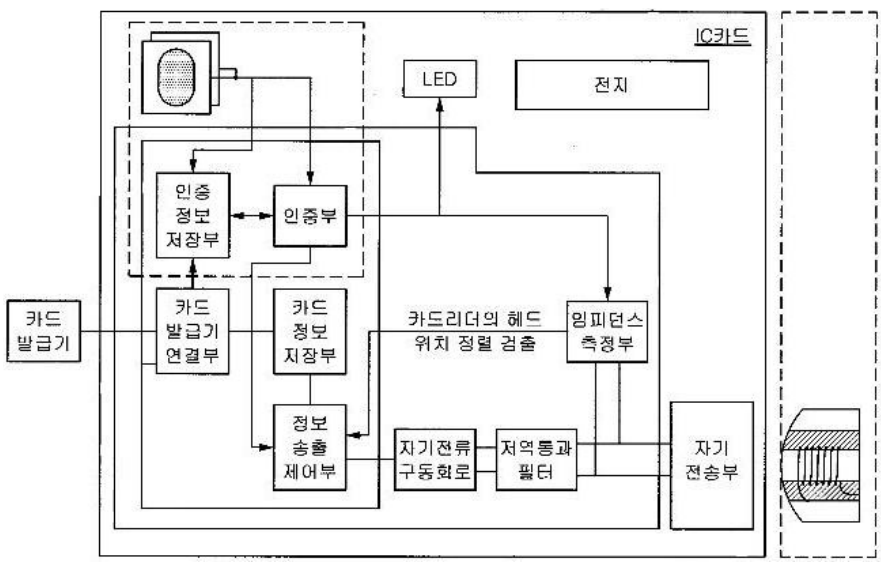

[그림 1] 기존카드 자기띠 트랙




[그림 2] 카드정보 표준

독이 가능한 IC 카드에 관한 것이다.

[그림 3]은 가상자기띠형 IC 카드의 구성을 기능적으로 구분하여 나타낸 구성도이다. IC 카드는 카드발급기 연결부, 카드정보저장부, 사용자 인증수단, 정보 송출제어부, 임피던스 측정부, 자기전류 구동 회로, 저역통과필터, LED 램프, 전지, 그리고 자기전송부 등과 같은 구성요소




[그림 3] IC 카드 기능적 구성도

를 갖는다.

IC 카드의 각 구성요소들의 연결관계와 기능 및 역할은 다음과 같다.

## 1. 카드발급기

IC 카드 발급회사가 갖추는 장비로서, 본 연구에 따른 IC 카드와 전기적 또는 자기적으로 연결되는 인터페이스를 갖고 있고 카드의 정보를 송출하여 발급하려는 IC 카드로 제공하는 기능을 갖춘 카드발급기이다. 또한, 카드 리셋신호를 IC 카드에 제공하여 카드소유자의 지문정보나 비밀번호가 기준 인증정보로서 IC 카드에 미리 등록되도록 제어하는 기능을 가진다. 기존의 자기식 카드발급기에 이러한 기능들을 더 부여하여 카드발급기를 구성하며, 전기적, 자기적 연결 인터페이스는 일반적으로 널리 알려져 있는 표준기술을 사용한다.

## 2. 카드발급기 연결부

IC 카드 발급회사의 카드발급기에 대한 인터페이스를 제공한다. 즉, 카드발급기로부터 카드사용자의 카드정보를 전달 받아 카드정보저장부에 저장되도록 한다. 또한 카드발급기 연결부는 카드발급기가 제공하는 카드소유자의 기준 인증정보를 수신하여 인증정보저장부에 저장되도록 한다.

## 3. 카드정보저장부

카드발급기가 카드발급기 연결부를 통해 제공하는 신용카드 또는 기타 용도의 카드 정보를 저장하여 소실되지 않도록 보관한다. 또한, 정보 송출 제어부의 요청에 응하여 보관중인 카드 정보를 제공한다.

## 4. 사용자 인증수단

IC 카드의 정당한 소유자로 인증된 사용자만이 그 카드를 사용할 수 있도록 한다. 사용자 인증수단은 이를 위한 구성요소로서, IC 카드의 사용자가 입력한 인증정보를 그 IC 카드의 기준 인증정보와 비교하여 양자가 일치하는 경우에만 그 사용자의 IC 카드 사용이 허락되도록 하는 인증방식을 채용한다. 여기서 기준 인증정보는 IC 카드의 정당소유자의 지문정보나 카드소유자가 정한 비밀번호가 그 예가 될 수 있다. 이 경우, 사용자 입력 인증정보는 그 IC 카드의 사용자가 카드사용 시 입력하는 그의 지문정보나 비밀번호가 된다. 사용자 인증수단은 지문인증수단과 비밀번호인증수단 중 어느 하나 또는 이들 둘 다를 채용한 구성일 수 있다.

### 4.1 지문인증수단

지문인증수단은 지문센서, 인증정보저

장부, 사용자인증부로 구성된다. 이러한 구성에 의해, IC 카드 소유자의 지문정보를 기본 인증정보로서 IC 카드에 등록하고, IC 카드 사용 시 사용자의 지문정보를 이용하여 그 사용자를 인증한다.

- 지문센서는 IC 카드를 소유자나 사용자가 특정 손가락 끝 지문을 지문센서 사용 방법에 정해진 방법으로 지문센서에 접촉하게 되면 지문센서는 그 사용자의 지문을 디지털 데이터 형태의 지문정보로 변환한다. 지문센서가 획득한 IC 카드 소유자의 지문정보는 기본 인증정보로 등록하기 위해 인증정보저장부에 제공된다. 또한 지문센서가 획득한 IC 카드 사용자의 지문정보는 그 사용자에 대한 인증을 위해 사용자인증부에 제공된다.
- 인증정보저장부는 불휘발성 메모리소자로 구성되며, IC 카드 소유자의 기준 인증정보를 저장한다.

이처럼 기준 인증정보를 IC카드에서 직접 채취하여 등록할 수도 있고, 카드회사의 카드발급기를 통해 기준 인증정보를 제공받을 수도 있다.

- 사용자인증부는 지문센서로부터 현재 IC 카드를 사용하고자 하는 사용자의 지문정보를 전달받아 그 지문정보를 인증정보저장부에 미리 기준 인증정보로서 저장된 지문정보와 비교하여, 양자가 일치하는 지 여부에 따라 현재 사용자의 인증을 결정한다. 지문센서가 제공한 지문정보와 인증정보저장부에 저장된 지문정보 간에 미리 설정된 수준의 상관도(correlation)가 있다고 인정되면 양 지문이 일치하는 것으로 간주하여, 현재 사용자를 인증한다. 현재 사용자가 인증되면, 사용자인증부는 정보송출제어부에 인증신호를 제공한다. 인증신호의 입력에 응하여 정보송출제어부 내의 정보송출버퍼가 활성화된다. 그리고 그 시점부터 IC 카드는 사용가능한 상태에 놓이게 된다.

사용자인증부는 또한 그 인증신호를 LED 램프에도 제공함으로써 LED 램프가 점등되도록 한다. 사용자는 LED 램프가 켜지면 그 IC 카드는 사용가능한 상태에 있는 것으로 인식할 수 있게 된다. 사용자인증부는 일정 시간이 지나면 지문인증을 취소하는 신호를 정보송출제어부와 LED 램프에 각각 제공하여 정보송출버퍼를 비활성화 하고 LED 램프도 소등되도록 한다.

### 4.2 비밀번호 인증수단

비밀번호를 이용한 인증은 지문정보를 비밀번호로 대체한 점에서 다를 뿐, IC 카드 발급 시 비밀번호를 기준 인증정보로

미리 등록해두고, IC 카드 사용 시 비밀번호를 입력받아 미리 등록된 비밀번호와의 일치 여부를 확인하여 사용자 인증을 하는 절차는 지문을 이용한 경우와 같다.

IC 카드에 설치되는 비밀번호 인증수단은 지문센서 대신에 비밀번호입력부를 구비한다. 인증정보저장부와 사용자인증부를 각각 비밀번호저장부와 비밀번호인증부로 기능하도록 구성한다. 지문과 비밀번호를 동시에 인증정보로 이용하는 경우에는, 지문센서와 비밀번호입력부를 함께 구비함과 아울러, 인증정보저장부와 사용자 인증부 각각이 지문 인증 기능과 비밀번호 인증 기능을 함께 갖추도록 구성한다.

## 5. LED 램프

사용자가 자신의 지문이나 비밀번호가 인증되었는지 여부를 시각적으로 확인할 수 있도록 하기 위해 제공된 수단이다.

## 6. 자기전송부

자기카드 리더기의 자기헤드가 검출할 수 있도록 카드정보를 자기정보로 전송해주는 역할을 한다. 즉, 자기구동전류를 흐르게 하여 자기띠 카드에 관한 표준에서 정하고 있는 트랙들의 위치에 대응하는 지점에서 자기구동전류의 극성변화에 대응되는 시변자기를 발생시키는 것에 의해 카드정보를 자기정보로 전송한다.

즉, 자기전송부는 카드 기판 내부의 소정지점에 각각 배치된 상기 트랙의 개수만큼의 자기코일을 포함하며, 자기코일 각각의 양팔은 자기전류구동부의 출력단에 각각 별도로 연결된다. 또한 자기전송부는 카드 기판의 소정 위치에 트랙의 개수에 대응되는 개수만큼 배치되며 자기발생코일 및 다수의 자기발생코일마다 스트립라인이 그 내부를 관통하고 각 스트립라인은 서로 교차되지 않게 대략 원형, 타원형 또는 다각형을 그리면서 소정 지점 근처까지 연장되되 각 스트립라인의 양끝이 소정 지점에서 소정 간격만큼 이격되어 이를 통해 시변자기가 송출되도록 구성된, 트랙의 개수에 대응되는 개수의 자성물질 자기회로를 포함하며, 자기발생코일 각각의 양팔은 자기전류구동회로의 출력단에 각각 별도로 연결된다.

## 7. 정보송출제어부

카드정보저장부에 저장되어 있는 카드정보를 읽어 들여 그 정보를 순시적으로 변화하는 전류정보로 환산하고 그 전류정보를 자기전류구동회로에 순차적으로 제공한다. 이때 여러 개의 자성 트랙이 있은 자기띠의 경우 각 트랙 정보를 동시에 각각의 전류 정보로 환산하여 보

낸다. 이러한 전류정보의 자기전류구동회로에 대한 제공은 IC 카드가 카드리더기에 삽입되어 IC 카드의 자기전송부와 카드리더기의 자기 헤드가 자기적으로 결합되는 순간에 이루어진다. 이러한 자기적 결합은 자기 전송부의 위치와 자기헤드의 위치가 정렬이 이루어진 경우에 얻어진다. 자기 헤드와 자기 전송부간의 정렬 여부는 임피던스 측정부가 제공하는 카드리어기의 자기헤더 정렬검출신호에 의해 확인된다. 정보송출제어부는 이 정렬검출신호로부터 자기 헤드와 자기 전송부간의 상대 위치를 파악할 수 있다. 예컨대, 정보송출제어부는 그 측정된 임피던스 값이 설정된 범위에 들어올 때 카드리더기의 자기헤드와 자기전송부의 헤드가 정렬된 것으로 판단하고, 이들 양자가 정렬되었음이 확인될 때, 상기 전류 정보를 자기전류구동회로로 송출을 시작한다. 또한 IC 카드의 사용이 인증된 사용자에게만 허용이 되도록 구성된 경우, 정보송출제어부는 사용자인증부가 인증신호를 제공해 줄 때 카드정보의 송출이 활성화 되도록 제어한다.

## 8. 임피던스 측정부

IC 카드는 카드리더기의 자기헤드와 자기전송부의 헤드가 정렬되는지 여부를 검출하여 그 정렬검출신호를 정보송출제어부에 제공하는 정렬검출수단으로 구성된다. 이 정렬검출수단은 자기전송부의 임피던스를 측정하는 임피던스 측정부로 구현된다. 임피던스 측정부는 지문 인증이 유효한 순간부터 자기전송부의 임피던스를 측정하여 카드리더기의 자기 헤드와 자기전송부 헤드가 일치하는 순간을 검출한다. 이를 위해 임피던스 측정부는 자기전송부에 전류를 흘려서 자기전송부의 임피던스를 측정한다. 자기 헤드와 자기전송부 헤드 간의 위치 정렬 여부는 자기전송부의 임피던스 측정 결과의 변이를 검출함으로써 감지한다. 즉, 자기 헤드는 자성 물질이므로 가까워지면 자기전송부 헤드의 임피던스가 증가하는데, 특히 자기 헤드가 자기전송부와 정렬이 되는 경우에는 임피던스는 크게 증가한다. 임피던스 측정부는 그 임피던스의 변화를 검출하여 그에 대응하는 정렬검출신호로 변환하여 정보송출제어부로 전달한다.

## 9. 자기전류 구동 회로

정보송출제어부로부터 제공받은 펄스신호를 자기전송부의 구동에 필요한 아날로그신호 형태의 자기구동전류로 변환한다. 예컨대 펄스신호의 진폭이 변경되는 것에 대응하여 자기구동전류의 극성이 변경되도록 하는 방식으로 전류신호를 발생킨다. 아울러, 이 자기구동전류는 카드리더기의 자기 헤드에 충분한

자기정보가 유도되도록 하는 데 필요한 크기의 전류로 증폭된다. 자기전류 구동회로는 자기전송부에 대한 전류원으로서 기능하므로, 저역통과필터, 자기전송부 및 카드리더기의 자기 헤드와 임피던스 매칭을 하여 자기전송부에서 최대한의 자기신호가 유도되도록 한다.

## 10. 저역통과필터

자기전류 구동회로가 제공하는 자기구동 전류는 저역통과필터를 통해 자기전송부로 전달된다. 저역통과필터는 자기전류 구동회로와 자기전송부 사이에 위치하여, 자기전류 구동회로가 임피던스 측정부의 고주파 성분으로부터 차폐되도록 한다.

## 11. 전지

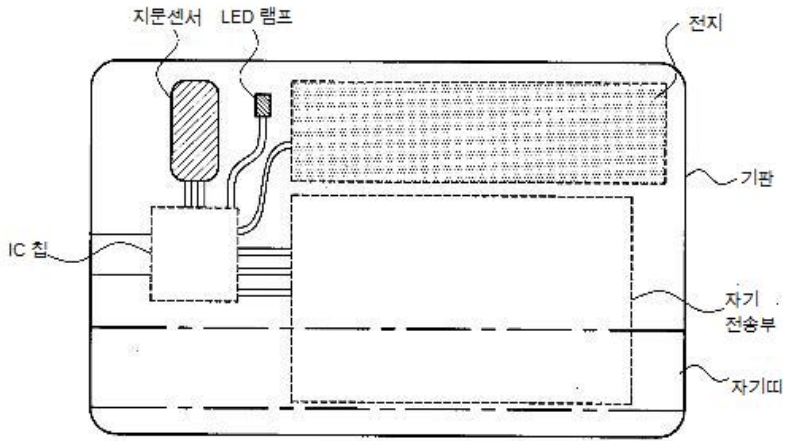
일회용 전지 또는 이차 전지를 이용한다. 이차전지의 경우 전극에 의한 충전 또는 자기코일 유도에 의한 충전이 가능하다. 전지를 2차전지로 구현하는 경우에는 충전회로가 별도로 필요로 하다.

한편, 카드발급기 연결부, 카드정보저장부, 사용자 인증수단, 정보송출제어부는 디지털회로부이고, 임피던스 측정부, 자기전류 구동 회로, 저역통과필터, 전지의 충전회로는 아날로그회로부이다. 디지털회로부는 예컨대 CPU나 마이크로프로세서 등과 같은 싱글칩 또는 ASIC 칩으로 구현될 수 있다. 이 경우 아날로그회로부는 별도의 아날로그 회로로 구현된다. 디지털회로부와 아날로그회로부를 전부 ASIC으로 구현할 수도 있는데, 이 경우 이들 디지털회로부와 아날로그회로부는 단일의 ASIC 칩에 통합될 수도 있을 것이다.

이러한 구성을 갖는 IC 카드는 기존의 자기띠 카드용 카드리더기에서도 읽혀질 수 있는 자기정보를 발생시킨다. 그러므로 기존의 자기띠 카드용 카드리더기로 구축된 환경에서도 곧바로 사용될 수 있는 카드라는 장점을 갖는다.

본 연구가 제안하고자 하는 IC 카드는 IC 카드의 기능을 가지고 있으며, 종래의 자기띠 카드 리더기의 수정 없이 위와 같은 종래의 카드리더기의 정보 판독 방법을 그대로 활용할 수 있다는 데 주요한 특징이 있다. 기존의 자기띠 카드리더기를 그대로 활용하기 위한 방안이 단순히 IC 신용카드에 자기띠를 부착하는 것이라면, IC 카드의 장점인 보안성을 전혀 이용하지 못하여 기존의 자기띠 카드의 단점을 그대로 노출하는 것이 되므로 부적절하다. 보안성의 유지와 종래의 자기띠 카드리더기의 활용가능성을 동시에 충족시킬 필요가 있다.

[그림 4]는 가상자기띠형 IC 카드의 개략적인 레이아웃을 나타낸다. 그림에서 IC 칩은 상기 아날로그회로부와 디지털




[그림 4] IC카드구조도

회로부를 합한 것을 나타낸다. 예컨대 플라스틱 기판에 전지와 자기전송부, 아날로그회로부와 디지털회로부 등은 매입되고, 지문센서와 LED램프는 기판의 외부로 노출되게 설치된다. 이러한 배치에 의하면, 자기전송부가 형성하는 자기회로에 의해 IC 카드의 하단에는 마치 자기띠가 배치된 것과 비슷한 개념의 가상자기띠가 존재하는 것처럼 된다. 물론 가상자기띠는 물리적으로 존재하는 것은 아니다.

## Ⅳ. 결론

본 연구에서 IC칩을 내장하는 자기 띠 카드용 리더기에서도 카드 정보의 판독이 가능하며, 사용자 인증 장치를 내장하여 사용자 확인시에만 정보를 외부에서 읽을 수 있도록 하는 자체 보안기능을 구비한 마그네틱/IC 겸용의 카드를 제시하였다. 이 카드는 IC 카드의 기능을 가지고 있으며, 종래의 자기띠 카드 리더기의 수정 없이 위와 같은 종래의 카드 리더기의 정보 판독 방법을 그대로 활용할 수 있다는 데 주요한 특징이 있다.

제시한 IC 카드는 지속적으로 발생하고 있는 신용카드 등 카드의 부정사용 및 신용카드정보 유출 및 이로 인한 위·변조 사고를 감소시키거나 예방할 수 있으리라 기대한다.

## 참고문헌

[1] 김학범, 금융 IC 카드 보안과 EMV 인증, 한국정보보호학회지, 제16권, 제5호(2006).

[2] 김현희, 모바일지급결제 서비스 신규 비즈니스 모델 및 주요 이슈, 지급결제와 정보기술, (2008).
[3] 매일경제, (2009).
[4] 이종오, 신용카드 POS가맹점의 카드회원 신용정보 보안상 문제점 및 대응방안, 계간 신용카드 제45호(2008).
[5] 이충훈, 생체인식을 이용한 신용카드 결제 시스템의 연구, 건국대 정보통신대학원, (2008).
[6] 장병환, 카드기반 지급결제 수단의 이용현황 및 전망, 지급결제와 정보기술, (2006).
[7] 한국은행, 2008년도 지급결제 제도 운영관리 보고서, (2009).
[8] Alder, E., “Smart Card Technology-Hong Kong, Legal Issues in Smart Card Technology,” Computer Law and Security Report, Vol.18, No.2 (2002), pp.120-123.