

전자 선거 시범 시스템과 본인 인증 기술 적용 모델 분석

송영기·김유라·이병상·강환일
(현대정보기술)

목 차

1. 서 론
2. 전자 선거 시범 시스템의 구성
3. 본인 인증 기술 개요 및 처리 방안
4. 전자 선거 시스템의 본인 인증 모델
5. 결 론

1. 서 론

최근 중앙선거관리위원회는 2008년 18대 총선부터 전자투표제를 도입하기 위한 파일럿 시스템의 구축을 추진하고 있으며, 2012년 19대 총선부터는 유권자가 투표소에 가지 않더라도 개인용 컴퓨터와 노트북, 휴대전화, 휴대용 단말기 등을 통해서 선거를 치를 수 있는 소위 유니쿼터스(Ubiquitous, 언제 어디서나 서비스를 연결할 수 있는) 시대의 전자투표를 실시하겠다는 전략을 발표하였다. 그간 우리나라는 지방자치, 선거구 조정 및 다양한 형태의 국민 여론수렴의 창구로서 선거를 통한 민주주의를 실현해 나가고 있으며, 앞선 정보기술과 우수한 인프라, 낮은 투표율과 고비용의 선거 구조를 고려해 볼 때 전자투표 도입의 필요성이 지속적으로 제기되어 온 것이 사실이다.

특히 최근 선진 각국에서는 이러한 국민들의 정치 참여의, 실제적인 투표 참여율의 향상 및 객관적인 검토, 비용의 최소화를 고려하여 새로

운 방식의 전자 선거 시스템에 대한 계획 및 시범 시업을 추진하고 있다. 미국에서는 전자기록장치(Direct Recoding Electronic : 이하 DRE)나 재택 기반의 투표 시스템을 추진하고 있으며, 유럽에서는 스마트 카드를 이용하여 본인 인증 여부를 확인하는 TRUEVOTE 시스템을 추진하고 있다. TRUEVOTE 시스템의 경우 투표 전에 투표권자에게 스마트 카드를 배포하며, 인증 기관으로부터 인증된 공개키를 통해, 투표의 결과를 암호화하여 전송하고, 여기에 투표자의 확인자를 포함하여 전송한 후 그 결과를 수집하여 검표를 하게 되는 시스템이다.

이와 같이 전자 투표 시스템은 기존의 종이 방식에 비해, 보다 편리하고 쉽게 선거에 참여할 수 있다는 장점이 있지만, 선거의 기본적인 정신과 배치가 될 수 있는 점이 제기되고 있으며, 유럽에서는 투표의 투명성, 투표 과정의 제어 가능성 및 기밀성 유지, 그리고 투표자들이 언제 어디에서나 투표를 할 수 있기 때문에 가족의 구성원 및 투표 집단에 대해 영향을 미칠

수 있음이 지적되고 있다. 특히, 전자 투표 시스템에 대한 신뢰성이 확보되어야 하며, 본인 확인 인증 절차의 투명성 및 투표 결과에 따른 문제 제기의 간명화등이 해결되어야 할 과제로 지적되고 있다.

본 논문은 전자 선거 시범 시스템 개발을 통해 우리 나라가 추진하고 있는 전자 선거 시스템의 주요 기술 요소 및 추진 내용을 기술하고, 전자 선거 시스템의 투명성 제고를 위한 본인 인증에 대한 모델을 제시한다.

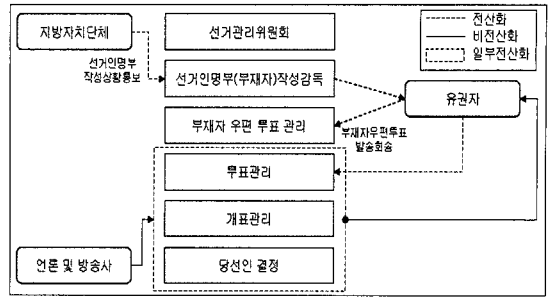
2. 전자 선거 시범 시스템의 구성

전자 투표 시범 시스템은 국민 정서와 정치 적의 합의를 위해 적절한 IT 기술을 접목시킴으로써, 기술적으로 무리가 없으며, 대국민 서비스를 극대화하여 국민 정서에 부합되어야 하며, 전자 선거에 대한 정치적인 합의가 도출될 수 있도록 하는 것을 목적으로 하여야 한다. 또한, 해외 전자 투표 실패 사례에 대한 적절한 대비가 이루어져야 하고, 상상 가능한 모든 실패 가능성에 대해서도 대비하여야 한다. 전 국민을 대상으로 하는 시스템이므로 IT 기술에 친숙하지 않은 투표자의 사용을 최대한 고려한 편의 장치를 제공할 수 있어야 한다.

현재 추진되고 있는 전자 선거 시범 시스템은 크게 4개의 하부 시스템으로 구성되어 있으며, 각각의 시스템들은 통합선거인명부확인시스템, 전자투표시스템, 전자개표시스템과 전자검표시스템으로 이루어져 있다.

이중에서 전자 선거 시스템의 주요 요구 사항에 따라 자체 제작을 통하여 구현된 시스템은 전자 투표기를 포함한 선거인명부확인시스템과 전자투표시스템의 2개 시스템이며, 전자개표시스템과 전자검표시스템은 일반 컴퓨터를 이용한 개, 검표과정을 구현한 시스템으로 이루어져 있다.

2.1 기존 시스템 업무처리절차



(그림 1) 기존 시스템 업무처리 절차

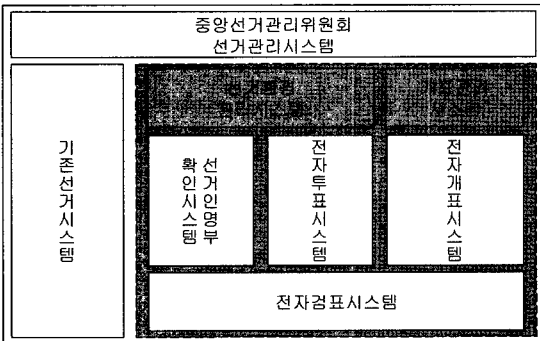
- 1) 선거인명부 작성 (공직선거 및 선거부정방지법 제 37조, 제 38조)
 - 선거를 실시하는 때에는 그때마다 구청장, 시장, 읍장, 면장이 작성
 - 주민전산망에 의해 선거인명부 및 부재자신고인명부를 생성, 출력하여 제책한 후 구,시,군 선거관리위원회 및 투표구선거관리위원회에 송부
- 2) 투표 (공직선거 및 선거부정방지법 제 147조, 제148조, 제157조, 제158조)
 - 선거일전일까지 각 투표소에 투표용지 수송
 - 명부에 등재된 사람은 주민등록지 각 투표구마다 설치된 지정된 투표소에서 투표를 하고 부재자 신고인은 부재자 투표소 또는 거소에서 투표
 - 선거인 본인여부를 확인하고 선거인명부에 서명, 날인
 - 투표용지를 받은 후 기표소에서 기표한 후 투표함에 투표지를 넣고 퇴장
- 3) 개표 (공직선거 및 선거부정방지법 제 173조, 제175조~제178조)
 - 투표마감 후 각 투표소의 투표함을 개표장으로 이송
 - 개표기에 의한 개표 후 후보자별 득표수를 중앙집계서버로 전송하여 집계
 - 집계자료를 인터넷홈페이지 게시 및 방송사 서버로 전송하여 공개

4) 당선인 결정

- 유효투표수의 다수를 얻은자를 당선인으로 결정

2.2 시범 시스템 구성

전체 전자 투표 시범시스템의 구성은 다음과 같다.



(그림 2) 시범 시스템 구성

자연스러운 전자선거 시스템으로의 전환을 위한 기존 선거관리시스템(이하 NECIS : National Election Commission Information System)과의 연계 가능성을 평가하기 위해 운영 중인 NECIS와는 별도로 NECIS의 Database Schema를 임시 장비에 설치하여 시스템을 구성하였다.

2.3 각 시스템 별 세부 구성

위에서 언급한 4개의 하부 시스템에 대한 구성을 간략히 정리하면 다음과 같다. 특히 하부 시스템의 구성을 할 때, 해외의 선거 시스템과의 비교를 통해 차별화를 하였으며, 각 시스템의 유기적인 인터페이스를 위한 고려를 하였으며, 시스템 소프트웨어의 확장성도 반영 하였다.

2.3.1 통합선거인명부확인시스템

통합선거인명부확인시스템은 중앙선거관리위원회 선거인명부를 지역에 관계없이 조회하여 투표소에서 선거인에 대한 본인여부 확인, 이중투표 여부 확인 기능을 수행할 수 있도록 구성

된 시스템이다. 또한 전자투표의 선거환경 설정, 선거인용 스마트카드 발급을 통하여 전자투표, 개표 및 검표 부문과 인터페이스 한다.

본 시스템을 통하여 각 투표구의 단말기는 선거인명부 DB와 연결되어 선거인명부를 조회함으로써 본인여부를 확인하고, DB서버에 선거인의 투표여부를 업데이트하며, 전자서명과 지문정보 획득 방식을 동시에 지원함으로써 이중투표 여부 확인 기능과 증빙 자료를 제공한다. 이를 위해 단말기와 전자서명기, 지문인식기, 스마트카드발급기, 모니터 등의 장치를 연결하여, 신속 정확하게 선거인명부를 조회하면서 인증과정을 거쳐서 선거인용 스마트카드를 발급하도록 구성한다.

■ 노트북 PC

통합선거인명부확인시스템에 연결되는 전자서명기, 지문인식기, 스마트카드 발급기 및 통합선거인명부확인 프로그램을 통합하므로 장치들의 연결을 위한 인터페이스 및 구동, 제어를 수행하는데 필요한 충분한 사양을 제공해야 한다.

통합선거인명부확인 프로그램에서 메인서버로부터 데이터 전송 및 데이터 처리가 원활히 이루어져야 하고, 투표소별 네트워크 연결 환경에 적용할 수 있는 사양을 제공해야 한다. 정전 사태 발생에 대비할 수 있어야 하고 선거인의 지문이나 서명 데이터를 저장할 수 있는 충분한 저장 공간을 제공하여야 한다.

■ 전자서명기

통합선거인명부확인 시스템에서 선거인의 이중투표 여부 확인 기능과 증빙 자료를 제공하기 위한 방안으로 전자서명기를 사용한다. 선거인 자신이 서명하는 동안 글씨를 확인할 수 있도록 전자서명기의 화면에 실시간으로 표시할 수 있어야 한다. 전자서명기의 LCD를 통해 사용자의 서명을 받은 후, 전자서명기의 LCD를 통해 명

부 확인 결과를 표시하여 선거인이 볼 수 있도록 한다.

■ 지문인식기

통합선거인명부확인 시스템에서 선거인의 이 중투표 여부 확인 기능과 증빙 자료를 제공하기 위한 방안으로 지문인식기를 사용한다. 지문 정보는 개인을 확인하기 위한 가장 안전한 수단 중에 하나고, 개인 정보와 관련이 있기 때문에 저장할 경우, 개인 사생활 침해 등의 문제가 없도록 암호화 및 변환을 통한 저장 방법을 택한다. 전 선거인의 지문이 지문인식기 유리면에 남아있어도 현재 선거인의 지문 인식에 영향을 주지 않는 안정적인 인식 알고리즘을 가지고 있어야 한다.

■ 스마트카드(전자투표권) 발급기

전자투표권은 선거인에게 발급하여 전자투표를 1회 실시 할 수 있는 권한 부여 방식이어야 한다. 선거인에 해당하는 선거 및 선거구 정보, 전자투표기내에 저장된 소속 선거구의 후보자 조합의 이미지를 현출시키게 하는 기능 및 투표 완료 후 저장된 정보를 소거하는 기능을 갖춰야 한다.

■ 관리자 스마트카드

관리자권한을 부여한 스마트 카드로 통합선거인명부확인시스템과 전자투표시스템을 관리할 수 있는 권한을 부여할 수 있어야 한다. 복제를 방지할 수 있는 고유 아이디를 키로 가지고 있어야 한다. 보안성 확보를 위해 접촉식 스마트카드를 사용하여야 한다. 투표소에 방문하여 투표자가 투표하는 경우 관리자 카드가 반드시 존재하는 경우에만 투표를 할 수 있게 한다.

■ 선거인 스마트카드

선거권한을 부여한 스마트 카드로 통합선거인명부확인시스템에서 발급되어 전자투표시스

템을 사용할 수있는 권한을 줄 수 있어야 한다. 복제를 방지할 수 있는 고유 아이디를 키로 가지고 있어야 한다. 선거인이 전자투표기에서 투표 후 선거인 정보가 소거될 수 있어야 한다. 보안성 확보를 위해 접촉식 스마트카드를 사용하여야 한다.

2.3.2 전자투표시스템

전자투표시스템은 통합선거인명부확인시스템으로부터 투표권을 인증받은 유권자에게 제공된 선거인용 스마트카드로 전자투표시스템의 사용권한을 부여하여 유권자가 투표하도록 하는 시스템이다. 후보자의 정보를 전자화된 이미지 형태로 터치스크린 모니터에 표시, 유권자가 손으로 선택하여 투표하며, 시각 장애우를 위하여 점자키패드 및 음성 지원 장치를 장착하여 터치스크린 모니터로 투표하는 것과 동일한 효력을 갖도록 한다. 유권자가 후보자를 선택하면 선택 정보를 전자투표기 본체에 전자화된 정보로 저장되며, 동시에 유권자가 자신이 선택한 후보자를 프린터에서 출력된 인쇄물을 통해 확인해 볼 수 있도록 한다. 이 인쇄물은 카세트 방식의 투표 기록지로서 전자검표시스템에서 개표 결과의 검증을 위해 사용된다. 시각 장애우의 경우, 음성 지원 장치로 확인해 볼 수 있도록 한다. 신호 표시기를 설치하여 투표자에 의해 발생할 수 있는 장애 및 투표기 자체 발생 장애를 모니터링할 수 있도록 하여 투표 진행요원이 즉시 조치할 수 있도록 한다. 투표 종료 시에는 저장된 투표 정보를 CD 및 USB 메모리로 저장하여 전자개표시스템에서 개표할 수 있는 자료로 제공한다. 만약의 정전 사태에 대비하여 전원을 사용하는 모든 장치를 UPS에 연결하도록 한다.

■ 전자투표기 본체

터치스크린 모니터, 프린터, 점자 키패드, 이

어폰, 신호 표시기, CD 저장기, 스마트카드 리더기, UPS 등 전자투표시스템 장치들을 통합할 수 있는 인터페이스 및 구동, 제어를 수행하는데 필요한 충분한 사양을 제공하여야 한다. 전자투표 진행 및 투표 데이터를 수집, 저장하는 장치이므로 투표에 지연이 발생하지 않는 충분한 처리 속도와 수집된 데이터가 저장될 충분한 공간을 보장하여야 한다. 온라인 실시간으로 연결된 통합선거인명부확인시스템과 별도로 독립적으로 운영하여 온라인상으로 투표조작의 가능성을 배제할 수 있는 구조이어야 한다. 사용권이 없는 자가 프로그램을 조작하여 후보자별 득표수를 임의로 배분할 수 없도록 하는 등 원본 프로그램의 훼손을 방지할 수 있어야 한다.

■ 터치스크린 모니터

선거인 스마트카드에 기록되어있는 선거인 정보를 분석하여 해당 선거의 후보자들을 스크린에 표시하는 출력 장치인 동시에, 스크린에 표시된 후보자들 중 원하는 후보자를 선거인이 손으로 선택하여 전자투표기 본체에 전달하는 입력 장치다. 선거인과 직접적으로 인터페이스하면서 선거인에게 후보자 정보를 전달하고 선거인으로부터 후보자 선택 정보를 전달받는 입출력 장치이므로 주변 환경이나 선거인의 신체 조건 즉, 외부 빛이나 선거인의 보는 각도, 선거인 신장에 따라 달라지는 시야각이 충분히 고려되어야 하며, 기온, 습도 등의 환경적인 요인에 의해 이상동작을 하지 않는 충분한 안전성을 보장하여야 한다. 외부적 충격, 각종 물질에 의한 화면 오염 및 손상으로부터 터치스크린이 이상동작을 하지 않는 충분한 내구성을 보장하여야 한다.

■ 프린터

프린터는 전자투표기와 별도로 설치되어야 한다. 투표결과는 추후 쉽게 검증이 가능하도록

선거인이 선택한 후보자의 기호, 성명, 바코드 등을 출력하도록 프린터를 설치하여야 하되 동시선거를 대비하여 선거별로 구분하여 출력할 수 있어야 한다. 출력되는 투표결과는 선거인 본인이 확인하기 쉽도록 활자크기를 가급적 선명하게 하고 선거인이 볼 수 있도록 투명창을 제공하여야 한다. 투표기와 탈, 부착 및 투표기록지 공급이 용이하여야 하며 소모품 또는 부품의 교체가 용이하여야 한다.

■ 투표기록지 카세트

선거인이 선택한 후보자, 선거 정보, 전자투표시스템의 상태 로그 등의 정보가 기록되는 카세트 방식의 기록지로, 선거인이 투표 직후 확인할 수 있는 물리적인 결과 기록 데이터가 제공되어야 한다. 전자투표가 종료된 후 전자검표를 위한 데이터로 사용할 수 있도록 쉽게 탈, 부착이 가능하여야 한다. 외부 환경에 의해 투표기록지가 오염되지 않도록 투표기록지를 보호할 수 있는 구조이어야 한다. 운반, 보관 등이 용이하도록 공간활용도가 높고 컴팩트한 구조이어야 한다.

이외에도 시각 장애우가 후보자를 선택, 확인, 취소할 수 있도록 하기 위한 점자로 된 키패드 10인 이상의 후보자 등록 시에는 점자키보드를 이용한 후보선택에 오류가 발생하지 않도록 방지설계를 제공하며, 시각 장애우가 투표를 진행할 수 있도록 음성 정보를 이어폰으로 제공하여야 한다. 표대기 중, 투표진행 중, 투표완료, 장애 발생 등 투표기 상태를 외부에서 쉽게 확인하여 즉시 조치할 수 있도록 하여야 한다. 해당 투표기의 투표결과를 CD로 저장할 수 있어야 한다. 선거인이 발급받은 스마트 카드를 읽어 전자투표기를 사용할 수 있는 권한을 부여할 수 있어야 한다. 선거인의 정보를 읽어 해당 후보자를 현출시킬 수 있어야 한다. UPS를 통해 정전 등 무전원 사태에 대비할 수 있어야 한다.

2.3.3 전자개표시스템

전자개표시스템은 전자투표시스템으로부터 획득한 투표결과저장매체(CD)의 데이터를 읽어 개표를 진행하는 시스템이다. 투표결과저장매체(CD)로부터 얻은 데이터로 후보자별 득표현황을 집계, 조회, 확인하여 중앙선관위 DB에 전송할 수 있어야 한다. 관리자 스마트카드에 의해 개표가 시작, 진행될 수 있도록 한다.

■ 전자개표기 본체

전자개표시스템에 연결되는 전자개표기 모니터, 스마트카드 리더기, CD 저장기를 연결하여 개표를 진행하는 PC다. 이 PC는 상기 장치들의 연결을 위한 인터페이스 및 구동, 제어를 수행하는데 필요한 충분한 사양을 제공하여야 한다. 관리자 스마트카드에 의해 전자개표기의 사용 권한이 부여되어야 하며, 투표결과 저장매체를 개표시스템에 입력하여 자동으로 개표를 실시할 수 있어야 한다. 선거관리전산시스템(NECIS)과 연계 운영할 수 있어야 한다.

■ 전자개표기 모니터

전자개표기 본체와 연결하여 개표 과정을 확인할 수 있는 모니터다. 전자개표 프로그램 실행 시 화면 디스플레이 및 사용자의 제어가 용이한 화면 크기이어야 한다.

■ 스마트카드 리더기

관리자 스마트카드에 의해 개표가 시작, 진행될 수 있도록 한다.

2.3.4 전자검표시스템

전자검표시스템은 개표결과에 이의 제기 또는 분쟁의 발생 시 전자투표시스템에서 인쇄/출력된 투표기록지의 바코드 내용을 검표스캐너를 이용하여 채취하고 본 시스템에서 바코드의 판독결과 및 이미지를 화면에 디스플레이하고

그 결과를 다양한 방법으로 집계하여 투표결과를 검증하는 시스템이다. 또한 전자검표시스템은 개표소에서 전자 개표한 결과를 검증하기 위해 사용한다.

■ 전자검표기 본체

전자검표시스템에 연결되는 검표 모니터, 고속 스캐너를 연결하여 투표 기록지의 데이터를 수집하고 검증하는 PC다.

■ 고속스캐너

전자투표기에서 기록된 특수재질의 투표기록지를 스캔할 수 있어야 한다. 투표기록지에 기록된 바코드 정보를 해독하여 신속한 검표의 결과를 제공할 수 있어야 한다. 특수 재질의 투표기록지에 대한 고속, 저속, 반복, 수동 검표가 가능하여야 한다. 투표기록지와 비접촉식으로 설계하여 용지의 마모 및 훼손을 방지하여야 한다. 400DPI, 256 Level Gray 이미지로 1D 바코드 및 2D 바코드의 대용량 데이터 인식이 가능하도록 한다.

지금까지는 전자 선거 시스템의 시범 시스템의 주요 구성에 대한 자세히 살펴 보았으며, 다음 장에서는 본인 인증에 대해 살펴 보도록 한다.

3. 본인 인증 기술 개요 및 처리 방안

3.1 본인 인증 기술 개요

정보통신기술의 급속한 발달과 정보통신망 확산과 더불어 병행되는 문제로 신원절도나 사기를 통한 보안문제가 심각한 수준에 이르고 있다. 또한 개인뿐만 아니라 대부분의 회사나 금융 기관, 정부 기관 등이 인터넷과 인트라넷에 의존적이고, 이로 인해 해커나 산업 스파이에게 신원절도를 통해 기밀 정보의 노출 위험이 도사

리고 있다. 이는 개인이나 기업의 재산에 막대한 손실을 가져다준다. 현재 일상의 대부분에서 본인 확인을 통한 후 실생활이나 업무 처리를 가능하게 하는 것도 본인 인증의 문제가 중요 관심사이자 곧바로 개인 및 기업 나아가 국가의 보안과 직결되기 때문이다.

이를 통해 일상생활 특히 금융거래나 회사의 기밀 정보가 오가는 온라인 연동 시스템에서 본인 인증이 얼마나 중요하고, 적절하고 정확한 본인 확인을 통한 본인 인증이 필요한지 알 수 있다. 이러한 문제를 해결하기 위해서 각 분야별 대응되는 엄격한 기준과 방법에 의한 본인인증 기술이 중요하다.

본인인증이라 함은 자신이 정당한 이용자인지, 정당한 권한을 갖고 있는 사람인지의 여부를 확인하는 것이다. 이러한 본인 인증 방법으로는 오래전부터 사용하여, 일반인들에게 익숙한 ID, 비밀번호와 같은 정보를 이용하는 방법과 주민등록증, 여권, 운전면허증, 신용카드와 같이 매체를 이용하는 방법이 있다. 그리고, 인터넷 기반의 전자 금융서비스에서 많이 사용되는 공개키 방식의 암호기술을 이용한 공인인증서와 같은 방법이 있다.

이러한 방법에 더불어 보안의 개념을 강화해 개인의 생체를 이용하여 본인임을 인증하는 생체인증 기술이 최근에는 주목을 받고 있다.

이와 같은 본인인증에 대한 기술은 응용 시스템과 적용되는 환경에 따라 요구되는 보안 수준 및 비용이 달라지며, 좀 더 강력한 본인인증을 위해서는 몇 가지 본인인증 기술을 병행하여 사용한다.

본 절에서는 본인인증에 대한 기술들을 소개하고자 한다. 궁극적으로 본 논문에서 전자선거 시범시스템에 적용될 수 있는 최적의 적절한 본인인증 기술로 어떤 방법이 사용될 수 있는지 고찰하고자 한다.

3.2 본인 인증 기술 종류

3.2.1 정보를 이용한 기술

ID나 비밀번호, PIN 번호와 같은 정보를 이용한 기술은 서비스 이용자가 서비스 제공자에게 등록된 특정 문자나 숫자 정보를 제시하여 이것이 등록된 정보와 일치하는지 여부를 판단하는 방법으로 본인확인을 하는 기술을 말한다. 본인을 인증하는 기술로 고전적이고 가장 사용자에게 친숙한 방법으로 정보나 매체를 이용하는 방법이 있다.

정보를 이용하는 기술은 사용자 측면에서는 일반적이고 사용자 친숙성이라는 장점이 있는 반면에 정보에 대한 기억성뿐만 아니라 관리자 측면에서 안정성이나 정보에 대한 비밀성을 유지해야하는 문제가 따른다.

요즘, 안전하게 정보를 이용하여 본인을 인증하고자 문자와 숫자를 혼합한 6자리 이상의 비밀번호를 사용하던지, 비밀번호 오류 입력 횟수를 모니터링하여 일정 횟수를 초과하면 시스템 사용을 불가하게 하는 방법이 있다. 또한 일회용 비밀번호를 두어 거래 시 마다 매번 다른 번호를 사용하는 것으로 고정적인 비밀번호의 단점을 보완할 수 있는 장점이 있는 반면에 별도의 일회용 비밀번호 생성장치가 필요하다. 다른 방법으로는 보안카드에 기록된 번호를 이용한다는 측면에서 일회용 비밀번호 장치보다 비용 측면에서는 유리하지만 안정성은 떨어진다.

이러한 정보를 이용하는 본인인증 기술은 정보를 생성, 유지, 관리하는데 안정성을 지키는 게 기술의 핵심이다.

3.2.2 매체를 이용하는 기술

매체를 이용하여 본인임을 인증하는 기술은 주민등록증이나 여권, 운전면허와 같은 순수한 신분확인용으로 사용되는 매체와 카드(신용카드, 직불카드, 현금카드)처럼 금융거래를 목적으

로 본인임을 증명하기 위해 사용되는 매체가 있다. 이는 정보를 이용하는 본인 인증 기술처럼 사용자들에게 친숙하고 고전적인 본인 인증 방법이다. 그런데 이러한 방법은 매체의 분실 및 위·변조에 의해서 개인이나 기업에 금전적으로 심각한 영향을 끼친다.

매체를 이용하는 기술의 핵심은 매체의 복제를 차단하고, 그러한 매체로부터 정보를 유출할 수 없어야 한다.

요즘 활발히 논의 되고 있는 스마트카드는 이러한 매체를 이용하는 본인 인증 시 문제점을 해결할 수 있는 좋은 열쇠가 될 수 있다. 칩을 삽입한 전자주민등록증이나, 전자여권, 전자 운전면허카드, 신용카드 등이 있을 수 있다.

이런 스마트카드는 IC 칩의 복제가 불가능할 뿐만 아니라, 칩은 자체적으로 연산기능을 갖고 있어서 기존의 일반 카드보다 안정성 측면에서 월등히 높다고 할 수 있다. 더 나아가 스마트카드에 공인인증서나 생체정보를 보강하여 강력한 본인인증 기능을 수행할 수 있다.

스마트카드에 생체인증 기술을 접목하는 방법으로는 생체 정보를 IC 칩에 저장하여 인식 처리는 단말기에서 수행하는 Store-on-Card 방식과 생체 정보 저장뿐만 아니라 인식처리까지 IC 칩 내에서 수행하는 Mach-on-Card 방식이 있다.

Store-on-Card 방식에서는 인식 처리가 단말기 내의 프로세서에서 수행되기 위하여 그 생체 정보가 단말기로 전송될 때 정보 누출의 위험성이 있어, 개인의 생체 정보를 IC 칩 내에 저장할 뿐만 아니라 IC 칩 내의 프로세서를 이용하여 인식 처리까지 수행함으로써 개인의 정보가 외부로 유출되지 않는 Mach-on-Card 기술 개발이 현재 활발히 진행 중이다.

3.2.3 공개키기반구조(PKI)를 이용하는 기술

PKI는 기본적으로 인터넷과 같이 안전이 보장되지 않은 공중망 사용자들이, 신뢰할 수 있

는 기관에서 부여된 한 쌍의 공개키와 개인키를 사용함으로써, 안전하게 데이터나 자금을 교환할 수 있게 해준다. 공개키 암호기술을 이용하여 구현되는 인증서(Digital Certificate)는 온라인 상에서 사용할 수 있는 하나의 디지털 신분증이다.

인증서는 일반 기업이 발행하는 사설 인증서와 정부의 허가를 받은 공인 인증서가 있지만, 1999년 전자서명법 시행 이후 인터넷뱅킹이나 중요 전자상거래에서는 공인인증서의 이용이 의무화되었다.

PKI는 인터넷 상에서 메시지 송신자를 인증하거나 메시지를 암호화하는데 있어 가장 보편적인 방법인 공개키 암호문을 사용한다. 전통적인 암호문은 대개 메시지의 암호화하고 해독하는데 사용되는 비밀키를 만들고, 또 공유하는 일들이 관여된다.

이러한 비밀키나 개인키 시스템은, 만약 그 키를 다른 사람들이 알게 되거나 도중에 가로채어질 경우, 메시지가 쉽게 해독될 수 있다는 치명적인 약점을 가지고 있다. 이러한 이유 때문에, 기업 간 전자상거래, 전자 지불, 행정 민원 등 사이버 공간에서 전자문서를 이용한 전자 거래 시 공개키 암호화와 PKI 방식이 선호되고 있는 것이다.

더 나아가 강력한 신분확인을 위해 스마트카드 내에 PKI를 구축하여 보안 서비스를 제공할 수 있다.

3.2.4 생체인식 기술

생체인식 기술은 사람 개개인 마다 다르게 가진 생체정보(지문, 얼굴, 홍채, 손 모양, 정맥, 음성)를 추출하여 기존에 저장된 데이터와 비교해서 본인임을 확인하고 인증하는 기술을 말한다. 생체인식은 ID카드나 비밀번호와는 달리 개인의 고유 신호를 이용하기 때문에 도난이나 분실의 염려가 없고 위조 및 변조가 어렵기 때문

에 보안 분야에서 각광을 받고 있다. 또한, 금융 서비스·통신·정보보안·의료·치안관리·전자상거래 등의 분야에서도 활발하게 응용 모델이 발전되고 있다.

생체인식이 대두된 가장 큰 이유는 보안성과 편리성이라고 할 수 있다. 즉, 기존의 열쇠, 출입카드 등의 경우 도용, 분실, 복제 등의 여지가 많아 상대적으로 보안성이 낮고, 반드시 휴대를 해야 하며 비밀번호를 외우는 등의 수고가 필요하다는 단점을 가지고 있다.

이에 반해 생체인식은 인간이 가진 생체정보를 이용하므로 시스템의 신뢰성에 따라 정도의 차이는 있지만 자기 자신이 아니면 안되는 탁월한 보안성과 별도의 장치를 가지고 다니거나 외울 필요가 없는 편리성을 동시에 만족시킬 수 있다는 장점이 있다.

본 절에서는 각 생체 인식에 대한 기술을 간단히 소개하고자 한다.

정맥인증은 손등이나 손목 혈관의 형태를 인식하는 방법으로, 적외선을 혈관에 투시하여 혈관의 형태에 따라 신분확인을 한다. 이 방식의 경우 복제가 거의 불가능하여 높은 보안성을 갖지만 하드웨어 구성이 복잡하고 전체 시스템 비용이 많이 들어 활용할 수 있는 범위가 제한되는 단점이 있다.

손바닥 인증은 사람의 손바닥에 분포되어 있는 손금을 이용하는 것으로 개개인의 손금은 모두 독특한 패턴을 가지고 있다는 점에서 착안된 기술이다.

음성인식은 사람의 억양과 음의 높낮이가 서로 다르다는 특성에 기인한 방식으로 마이크 등을 통해 전달된 음성의 특징을 분석한 후 가장 근접한 것을 찾아내는 방식으로 다른 생체인식과 달리 멀리 떨어진 곳에서도 전화를 이용하여 신분을 확인할 수 있고, 사용하기 위한 별도의 교육이 필요하지 않으며 시스템 가격이 저렴하다는 장점이 있다. 하지만 감기나 기타 요인에

의해 목이 쉬었을 때나, 의도적으로 타인의 목소리를 흉내내거나 주변환경에 큰 소음이 있을 경우에는 오인식을 할 수 있다는 단점이 있다.

얼굴인증은 기계에 접촉하지 않고 카메라를 입력된 얼굴 형상을 데이터베이스와 비교하는 방식으로, 가장 거부감이 없는 생체 인증이지만 사용자의 표정이 바뀌거나 주위 조명의 영향을 많이 받는다는 단점이 있다.

홍채인증은 사람마다 고유한 특성을 가진 눈동자 바깥의 홍채 패턴을 이용한 것으로 데이터의 정확성, 안정성, 사용 편리성, 처리 속도 면에서 지문 또는 망막인식에 비해 가장 발전한 보안시스템이다. 홍채는 통상 생후 1~2년 내에 고유한 패턴이 형성된 후 평생 변하지 않으며, 어느 정도 떨어진 상태에서 홍채패턴을 인식하는 비접촉 방식으로 거부감이 거의 없다.

지문인증은 진피부분이 손상되지 않는 한 평생 변하지 않는 특성을 갖고 있다. 지문인식시스템의 원리는 지문의 융선과 골, 단점 등 지문 이미지의 특징점을 파악하여 저장된 원본데이터와 일치하는지를 비교하는 것이다.

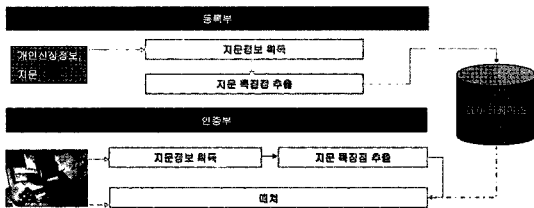
이런 각각의 생체 인증의 방법이 나와 있지만, 그 중 지문 인증 기술이 생체인증 시장의 50% 이상을 차지하고 있을 정도로 보편적으로 많이 사용되고 있다. 지문 인증 기술이 널리 사용되고 있는 것은 가격대비 경쟁력이 뛰어나기 때문이다. CPU의 기술적인 발전으로 가격이 크게 하락한 데다 지문은 오랫동안 연구대상이 되어왔기 때문에 상대적으로 기술적인 접근이 쉽고 안정화된 단계에 이르렀기 때문이다. 또한 지문의 불변성과 채집성이 용이하여 신원확인 용으로 특히 지문이 가장 널리 사용된다.

현재, 지문 인증 기술은 사용자의 인증을 위해 출입 관리, 근태관리, 도어락 등 상용 분야와 지문 감시, 외국인 출입 관리 시스템 등의 공공 분야에 주로 이용되고 있다. 특히 생체 인증 여권 등 국제적으로 지문 정보를 활용한 응용 분

야가 확대되고 있는 실정이다. 또한 최근에는 PC의 주변 장치로써 PC 보안뿐만 아니라 온라인 연동 시스템(그룹웨어, 메일 및 결제 등)에 적용되어 편리성 및 보안성을 요구하는 분야에 적용되고 있다.

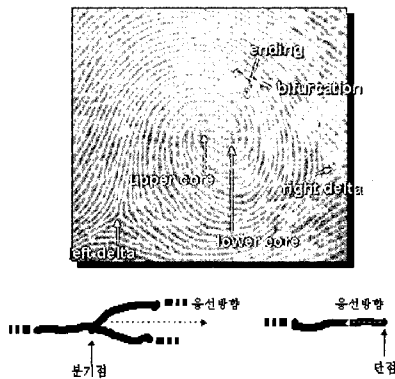
3.3 지문인증을 이용한 본인 인증 기술 처리 방안

본 논문에서는 전자선거시범시스템에서 본인 인증을 위하여 지문 인증 기술을 적용하는 모델을 보여주고자 하므로 지문 인증 기술에 국한된 처리 방안을 논한다.



(그림 3) 지문 인증의 기본 구조

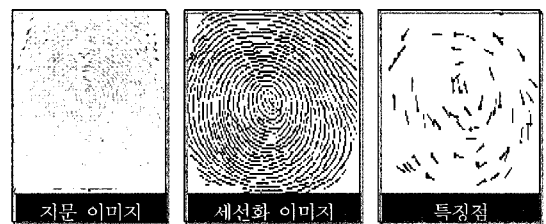
지문 인증의 기본 구조는 (그림 3)과 같이 크게 등록부와 인증부로 이루어져 있으며, 등록부에서는 획득된 지문 영상을 데이터베이스에 등록하고, 인증부에서는 이미 등록된 지문 정보와 신원을 확인하고자 하는 지문 정보 간의 매칭 모듈을 통한 본인을 인증하는 부분이다.



(그림 4) 지문 특징점 정보

지문 알고리즘은 지문영상을 획득하는 “획득”부분과 획득된 지문영상의 품질을 향상시키는 “품질향상”부분 그리고 지문영상에서 패턴인식 방법을 이용하여 특징점 정보를 추출해내는 “특징점 추출”, 추출된 특징 정보를 이용해 동일인인지를 판단하는 “매칭” 단계로 이루어진다.

특징점 추출 단계 이전까지를 전처리 과정이라고 하는데, 전처리를 위해서 먼저 수행되는 부분으로 지문의 구조적 정보를 추출하게 되는데 지문의 구조적 정보라 함은 먼저 획득된 지문영상에서 지문영역과 배경영역을 추출하는 단계를 거친다. 구조적 정보추출의 두 번째로는 지문 용선들의 흐름정보(방향)를 얻어내는 것이다. 이러한 구조적 정보를 추출한 후, 획득된 지문영상의 품질은 동일한 사람의 지문이라 하더라도 획득 당시의 환경적 특성이나 신체적 특성에 따라 지문영상이 달라진다. 이와 같은 이유로 지문영상을 향상시켜주는 단계가 필요한 것이다. 이렇게 향상된 지문을 가지고 특징점을 추출하게 된다.



(그림 5) 지문이미지에서 특징점 추출

매칭 단계 이전에 지문 분류 과정을 수행함으로써, 이는 지문 데이터베이스에서 중요한 인덱싱 정보를 제공하는 역할을 한다. 정밀하고 정확한 분류를 통해 지문 매칭 시간을 단축시켜주는 효과를 준다. 분류 방법에는 코어(core), 델타(delta)의 위치 정보를 이용하는 5분류 방법(헨리 방식 분류법 : FBI 표준)과 5분류 방법에 용선의 개수 정보를 이용하는 10분류 방법(합부

르크 방식 분류법)이 있다.

마지막으로 지문이미지로부터 추출된 특징점을 이용하여 동일인인지의 판단을 하는 매칭 과정으로 이루어진다. 지문 매칭의 방법은 이미지 기반, 그래프 기반으로 한 방법인 있지만 높은 처리 속도, 작은 템플릿 크기, 최고 등급의 데이터 보안 제공을 요구하는 최상의 자동 지문 매칭 방법은 특정점 기반의 매칭 방법이다.

이때 매칭은 지문인증 목적에 따라서, 획득된 지문과 데이터베이스 내에 등록된 그 사람의 지문과 동일한지를 비교하는 1:1 매칭과 획득한 지문의 조건 정보로 대량의 지문 데이터베이스에서 해당하는 후보 지문을 찾아내어 비교 대조하는 1:N 매칭으로 나뉜다. 일반적으로 전자 상거래나 금고키 등의 응용분야에서 신분확인용으로 1:1 매칭이 사용되고, 범죄현장에서 유류 지문을 이용하여 기 구축된 데이터베이스 내에서 범인 후보를 색출해 내는 범죄 수사용으로 1:N 매칭이 사용된다.

이러한 지문 인증의 성능을 평가하는 대표적인 방법으로는 타인수락율(FAR), 본인거부율(FRR)이 있다. 일반적으로 보안을 목적으로 하는 곳에서는 타인수락율이 0%에 가까워야 하지만, 범죄 수사를 목적으로 용의자 색출을 하는 경우에는 본인거부율이 0%에 가까워야 한다. 이렇듯 사용 용도에 따라서 사용자가 해당 응용 시스템에 맞는 다양한 단계의 보안 레벨을 결정할 수가 있다.

4. 전자 선거 시스템의 본인 인증 모델

앞절에서 살펴본바와 같이 본인 인증의 기술은 전자 선거 시스템의 투명성 확보, 부인 방지, 본인 확인 등을 위해 매우 필수적인 기술 중 하나다. 본 절에서는 전자 선거 시스템에서 본인 인증 모델에 대해 지문 정보를 이용한 본인 검증의 방법에 대해 제안한다.

최근 전 세계적으로 지문 정보가 저장된 전자 여권, 선원 증명서, 전자 주민증의 발급 등의 기술 적용이 활발해 지고 있으며, 이를 활용한 전자 투표에서의 모델을 개발하여 제안하고자 한다. 지문 정보의 등록 과정은 유권자에 대한 지문 정보를 투표 시 활용하는 방법으로, 개인이 투표이전 자신의 정보를 등록하는 과정이다. 본 제안에서는 현재 우리 나라는 성인인 경우 주민증의 발급을 위해서 지문 정보를 등록하는 과정이 있기 때문에 이를 이용하는 모델을 제안한다. 이를 경우 본인 여부 확인을 하는 과정만을 처리하면 되므로, 투표 시스템에서 주민 번호와 지문 확인을 통해 간단히 처리할 수 있다.

5. 결 론

지금까지 전자 선거 시범 시스템의 구성과 각 세부 시스템에 대해 살펴 보았다. 그리고 전자 선거 시스템의 도입 및 확대를 위한 본인 확인의 방법으로 지문 인식을 통한 투표자 확인 방법에 대해서도 살펴보았다.

선거 시스템은 가장 안전하고, 투명한 선거 절차를 모두 수용할 수 있어야 하며, 모든 유권자가 편리하게 사용할 수 있어야 한다. 시범 시스템의 개발은 이러한 점에서 구미 선진국에서 시도된 선거 시스템의 단순 IT 도입뿐만 아니라, 투표에서 검표에 이르기까지 다양한 기술을 접목하여, 보다 선진화된 선거 관리 시스템의 개발을 추진하였다.

또한 우리 나라의 특수한 사항을 감안하여, 전자 정부와 연계된 선거 시스템에서 본인 여부 확인 방법을 제안함으로써, 향후 보다 개선된 선거 관리 시스템의 개발에 도움이 될 것이며, 이러한 국내 적용 모델을 기반으로 전자 선거 분야에서 국내 산업의 해외 수출도 가능할 것으로 예상된다.

참고문헌

- [1] 전자투표제의 효율적 도입을 위한 커뮤니케이션 전략, 김신동 박동진 한림대학교
- [2] OpenCable Application Platform Specification: OC-SP-OCAP1.0-111-040604, June 2004.
- [3] ATSC Data Broadcast Specification, Doc, A/90, July 2000.
- [4] ATSC T3/S17, ATSC DASE(Digital TV Application Software Environment) Standard, Feb 2001.
- [5] ARIB STD-B24 Version 1.2, June 2000.
- [6] ITU-R SG 6, TTA 저널, 제83호, pp.198~203, 2002년 10월.
- [7] ETRI, 매체별 호환성 확보를 위한 데이터방송 표준화, 2003년 6월.

저자약력



송 영 기

1998년 국립 경상대학교 제어 계측공학과(석사)
 1998년~1999년 기아정보시스템(주)연구소
 2003~현재 산자부 생체 인식 표준화(SC37) 분과 위원
 2004년~현재 현대정보기술(주) 유비쿼터스 사업부 Bio ID팀 팀장



김 유 라

1999년 전남대학교 전자계산학과(석사)
 1999년~2001년 디오티크 연구원
 2001~현재 현대정보기술(주) 유비쿼터스 사업부 Bio ID 대리



이 병 상

1995년 동국대학교 전자계산학과(학사)
 1995년~1997년 한국컴퓨터(주) 유닉스사업부
 1997년~2002년 한진정보통신(주) 항공사업부
 2002년~현재 현대정보기술(주) 공공기술부 전자투표 시범시스템 개발 프로젝트 매니저



강 환 일

1980년 서울대 전자공학과 졸업.
 1982년 한국과학기술원 전기 및 전자공학과 졸업.
 1992년 미국위스콘신 매디슨 대학 전기 및 전자공학과 졸업.
 1996년~현재 명지대 정보공학과 교수