

종이 영수증 기술을 이용한 전자 투표 시스템의 동향

강서일·이덕규·이임영
(순천향대학교)

목 차

1. 서 론
2. 전자 투표 시스템의 개요
3. 전자 투표 시스템 발전단계
4. 종이 영수증 기술의 개요
5. 종이 영수증 기술 종류
6. 종이 영수증 발급 업계 동향
7. 전자 투표 시스템과 종이 영수증 기술 발전방향
8. 결 론

1. 서 론

투표는 민주주의에 있어, 국민의 의견을 반영할 수 있는 중요한 수단 중 하나다. 투표의 과정에는 유권자의 투표권 확인, 투표용지 수령, 투표용지의 기표 단계로 세분화 되고, 개표의 단계는 기표된 투표용지의 취합, 투표용지 기표 확인, 개표 내용 발표 과정으로 세분화 된다. 이러한 단계를 거쳐 한 번의 투표가 실시된다. 그러므로 투표는 공정, 정확해야 함에도 불구하고 투표 방식에 있어 투표 결과에 영향을 미치는 경우가 발생하기도 한다. 기존 투표 방법은 도장으로 기표하는 방식으로 개표에 있어 도장을 잘 못 찍은 경우나 다른 쪽 면에 묻어서 유권자의 귀중한 한 표가 무효표 처리될 수 있다. 이러한 무효표 처리가 투표의 결과에도 영향을 줄 수 있다. 예로 미국의 2000년 플로리다 지역 대

선에서 펀치 카드 시스템을 이용하는 투표 방식에 있어 구멍이 반 정도 뚫린 표를 무효표 처리함으로 인해 근소한 표차이로 후보자의 당락이 결정되었다. 이와 같은 문제가 발생하자 무효표를 줄일 수 있는 방안이 필요하게 되었으며 전자 투표 시스템이 관심을 받게 되었다. 전자 투표 시스템은 투표와 개표의 과정에 있어 전자 기기를 이용하는 방식이다.

전자 기기를 이용하는 방식으로는 여러 방법이 있으나 그중 펀치 카드, 광학 OMR 방식은 기존투표용지를 나누어 주고 투표하는 행위와 동일하다. 이와 같은 방식은 투표를 실시한 이후 개표에 있어 전자 기기를 이용하여 빠르게 개표를 실시할 수 있다. 그러나 이 방식은 투표용지의 기표에 있어 무효표를 발생할 수 있는 문제점을 내포하고 있다. 다른 전자 기기를 이용하는 방식에서의 가장 큰 문제점으로는 사용

자의 신뢰성 부분과 투표 값에 대한 검증 부분이다. 이와 같은 문제점을 해결하고자 대두된 것이 종이 영수증 기술이다. 본 논문에서는 전자 투표 시스템의 발전단계를 살펴보고, 전자투표의 형태를 본 후, 전자 투표 시스템에 대한 논의와 컴퓨터를 이용한 전자 투표 시스템에서 종이 영수증 기술에 대하여 알아보겠다.

2. 전자 투표 시스템의 개요

전자 투표 시스템이란 전자적 기기를 이용하는 방식으로 2002년 4월 VoteHere사의 네트워크 투표 시스템의 표준 공개 문서에서는 전자 투표 시스템을 전자 데이터를 기록, 저장 및 디지털 정보화한 것을 이용하는 것으로 정의가 내려져 있다. 이와 같이 전자 투표 시스템을 넓은 의미로 본다면 전자 기기를 이용하는 모든 투표 시스템이 전자 투표 시스템으로 포함될 수 있다. 국내의 중앙 선거관리위원회에서는 전자투표사업으로 기존의 종이 투표에서 터치 스크린의 전자기기를 이용하는 방식을 추진하고 있으며, 단계적인 발전을 통해 인터넷을 이용한 원격 투표 서비스까지 제공하는 것이 목표다.

전자 투표 시스템은 데이터로 유권자가 선택한 결과를 입력하기 때문에 유권자의 투표 결과가 무효표를 포함되는 것을 줄일 수 있다. 또한 개표 과정에 전자 기기가 빠른 결과를 산출할 수 있다. 무효표를 줄일 수 있게 되는 이유는 유권자의 기표하는 방식은 개표를 진행하는 요원들의 기표 해석에 따라 무효표로 처리될 수 있지만 데이터의 경우 정확하게 기록되기 때문이다.

전자 투표 시스템은 투표 방식에 따라 분류를 할 수 있으며 독립적인 투표 기기를 설치하여 운영하는 방식과 네트워크를 이용한 인터넷 투표 방식으로 나눌 수 있다. 네트워크를 이용한 인터넷 투표 방식은 통신망에 따라 유선과

무선으로 나눌 수 있다.

독립적인 투표 기기의 경우 유권자는 투표 기기가 설치되어 있는 장소에 방문하여 투표를 실시한다. 투표한 결과는 기기 안에 저장되어 보관되거나 집계소에 전송되는 방식 두 가지를 선택한다. 기기 안에 저장되는 방식의 경우 투표가 종료된 후에 집계소로 이동하여 저장된 데이터를 가지고 개표를 진행하며, 전송 방식의 경우 집계소에 모인 데이터를 투표 완료된 이후에 개표를 진행한다.

인터넷을 이용한 전자 투표 시스템은 전자 투표 시스템에 인터넷을 연결하여 유권자가 투표를 할 수 있도록 하는 것이다. 이와 같은 시스템의 특징은 유권자가 어디에 있더라도 인터넷만 연결되면 투표 시간동안 언제든지 투표할 수 있다.

전자 투표 시스템에 있어서는 많은 역할을 전자 기기가 인력을 대신하여 하고 있다. 개표의 확인이나 투표 값의 데이터도 모두 전자 기기가 저장 보관하고 결과를 확인할 수 있는 장치도 모두 전자 기기로 구성되어있다. 데이터는 다음과 같은 특징을 가진다.

- 데이터는 새로 생성할 수 있다.
- 데이터의 수정을 할 수 있다.
- 데이터를 복제할 수 있다.
- 데이터를 삭제할 수 있다.

위와 같은 특성으로 많은 기록에 전자 데이터를 사용하고 있다. 간편하게 데이터를 생성, 수정, 삭제할 수 있으므로 사용에 대한 편리를 제공한다. 하지만 투표의 경우에는 일반 데이터 처럼 생성, 수정, 삭제가 된다면 유권자의 정당한 권리가 박탈되는 결과가 발생할 것이다. 그러므로 전자 투표 시스템은 한번 작성된 투표 데이터에 대해서는 데이터의 특성을 제공해서는 안 된다. 만약 부정행위로 투표값 변경이 발

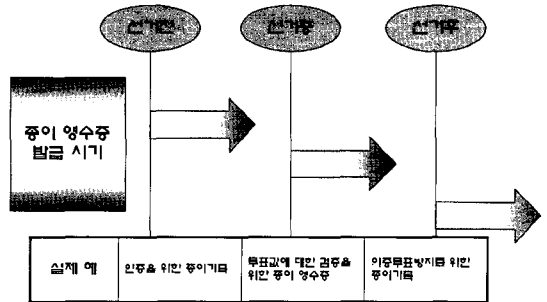
생되면 이를 발견할 수 있어야 하며, 또한 제 3자에 의한 부정행위를 막을 수 있는 방안도 제시되어야 한다. 그러므로 전자 투표 시스템은 보안 기술을 이용하여, 제 3자의 부정이나 데이터의 불법 수정을 막으며, 백업을 만들어 투표 결과를 유지하도록 한다. 하지만 이미 작성된 데이터를 가지고 개표를 한 이후에 다시 재개표를 한다고 하더라도 동일한 데이터를 적용하므로 동일한 결과가 나올 것이다. 그러므로 전자 투표 시스템에 있어서는 데이터가 수정, 삭제되기 이전의 데이터를 보관할 수 있는 방안이 요구되며, 데이터의 변형을 발견할 수 있는 방법으로는 검증 방안이 있어야 한다. 이러한 방안 중에 한 가지가 종이 영수증 기술이다. 종이 영수증 기술은 간략히 말한다면 데이터로 전자 투표 값을 보관하기도 하지만 종이에도 결과 값을 프린트하여 유지하도록 하는 것이다. 데이터가 수정, 삭제되면 프린트된 결과와 다른 결과가 발생함으로 인해 투표에 대한 부정행위를 알 수 있다.

종이 영수증은 발급 시기에 따라 각 특징을 지닌다. 본고에서 살펴보는 방법은 선거가 이뤄진 후 사용자에게 종이 영수증을 발급함으로써 사용자 선거 후 자신의 투표 값에 대한 검증이나 검표에 사용되는 것을 의미한다. 하지만 종이 영수증이 발급되는 형태를 보면 첫 번째로 선거 전에 발급되는 종지와 두 번째로 선거 중에 발행되는 종이 영수증, 마지막으로 선거가 모두 이뤄진 후에 발급되는 종이 영수증이 있다.

각각에 대해 살펴보면 선거전에 발급되는 종지는 선거 시에 사용자가 자신을 인증하기 위한 인증값이 포함된 영수증을 발급받고 이를 이용하여 선거가 이루어지는 형태를 말한다. 이와 같은 종이 영수증은 사용자의 인증값을 포함하고 있어 사용자 인증 및 선거 범위 등 여러 가지 제어가 가능하다. 두 번째인 선거 중에 발행되는 종이 영수증은 본고에서 살펴보고 있는 기

술로서 사용자의 선거 값을 출력하여 보관하고 있다가 사용자의 투표 값 검증 및 사후 검표 시에 이용되는 종이 영수증 기술이다. 이 기술은 현재 사용자의 투표 값을 그대로 출력하였을 경우 많은 문제점을 가지고 있어 출력되는 종이 영수증에 투표 값을 출력할 때 여러 암호 기술을 이용하여 출력하고 있다. 각각의 기술은 다음 6장에서 살펴해보도록 한다.

마지막으로 선거가 모두 이루어지고 난 후에 발급되는 종이 영수증은 사용자의 이중 투표를 방지책으로 사용되는 기술로서 인도에서는 사용자에게 지워지지 않는 잉크를 손가락에 묻힘으로써 또 다시 투표를 행하려 할 경우 잉크의 유무로써 제어하고 있다. 각각에 대해 그림으로 살펴보면 다음 (그림 1)과 같이 진행된다.



(그림 1) 종이 영수증 발급 시기에 따른 분류

3. 전자 투표 시스템 발전단계

본 장에서는 종이 영수증 기술에 대해 알아보기 이전에 전자 투표의 발전 단계를 기술하고자 한다. 기존의 투표소에서 실시하는 종이투표를 단지 전자기록에 의하여 대체하는 투표방식을 가장 초보단계로 보고 각 가정이나 사무실 등 자신이 원하는 장소에서 인터넷을 통하여 투표관리전산시스템에 접속하여 투표를 실시하는 단계를 가장 발달된 단계로 보아 투표자의 입장에서 편의성을 어느 정도 진전시키고 있는냐에 따라 그 발달정도를 나누어 본 것이다. 따라서

본 발전단계는 시스템이나 보안의 사항과는 무관하게 사용자 편의성 측면에서만 살펴보도록 한다.

3.1 기존 투표소 전자투표(제1단계)

선거인이 투표하기 전에 정당한 선거인임을 인증하기 위하여 선거공무원이 배치되는 전통적 투표소에서 전자투표기의 단말기를 통해 투표하는 것을 말한다. 기존의 선거방식과 기본적으로 비슷하나, 기존의 종이를 컴퓨터로 대체하는 방식이다. 따라서 유권자들은 자신이 속한 투표소에 직접 가서 그 안에 설치된 컴퓨터를 이용하여 투표를 하게 된다. 이는 미국에서 도입하고 있는 펀치카드, 터치 스크린 등의 전자기계를 이용하는 것과 기본적으로 동일하다. 그러나 컴퓨터에 익숙하지 않은 유권자들을 위하여 기존의 종이투표방식과 병행 실시하여 유권자들이 선택할 수 있도록 한다. 이 단계는 보다 발전된 단계의 전자투표가 도입될 수 있도록 유권자에게 컴퓨터에 대한 적응력을 높이는 데 주안점을 두는 것이 좋겠다.

3.2 간이 투표소 전자투표(제2~3단계)

3.2.1 선택한 투표소에서 투표(제2단계)

1단계 방식과 동일하나, 자신의 투표소를 선택할 수 있다는 점에서 보다 발전적이다. 따라서 유권자는 전국의 어느 투표소에 가셔도 자신의 선거인명부를 확인하여 투표할 수 있으므로 지리적 제한요건이 크게 완화된다.

이 단계에서는 모든 투표소에서 투표가 가능하므로 중복투표여부의 확인 작업이 가장 중요하다. 또한 국회의원선거 또는 지방선거의 경우 선거구마다 후보자가 다르므로 모든 선거구에 해당하는 투표양식이 제공되어야 하고, 전국의 모든 유권자에 대하여 선거인명부 확인이 가능하여야 한다. 아직 인터넷이 익숙하지 않은 유

권자들을 위하여 종이투표를 병행하여야 함은 전 단계와 같다.

이의 가장 큰 장점으로서는 장소의 제약이 완화되어 유권자의 투표참여를 크게 확대할 수 있다는 점이다. 예를 들면, 서울에 사는 유권자가 부산에 가셔도 투표할 수 있다. 또한 투표소 설치 장소도 크게 확대된다. 기존의 투표소 설비 장소 외에도 시내 중심가 등 어디나 설치가 가능하다.

따라서 기존의 학교, 관공서 중심이었던 투표소가 이제는 시내 유명 백화점, 할인점, 놀이공원, 유원지, 기차역, 대합실, 대학교 등 유권자가 많이 모이는 곳에도 설치가 가능하고, 전국의 PC방, 컴퓨터 판매점 등의 활용도 가능하다.

3.2.2 무인 투표소에서 투표(제3단계)

1·2단계에서와는 달리 3단계는 사람에 의해서 투표소가 관리되지 않는다는 것이 특징이다. 현재의 24시간 현금서비스처럼 특정한 장소에 정보통신망을 이용한 전자투표시스템을 설치해 놓으면 유권자는 미리 등록·인가된 전자카드나 비밀번호의 조합을 통하여 본인확인을 받은 후 투표를 할 수 있게 된다. 투표장소 또한 전 단계와 같이 임의의 선택이 가능하다.

제 3단계에서는 공간 제약의 완화 외에 시간적 제약조건이 완화되어 투표시간을 유권자가 선택할 수 있는 장점이 있다.

3.3 인터넷 투표(제4단계)

선거인이 투표소가 아닌 PC나 디지털TV, 이동전화와 같은 첨단 기기를 이용하여 거소 또는 회사 등에서 투표하는 것을 말한다. 1, 2, 3단계의 장소 및 선거관리공무원의 통제성을 초월한 전자투표의 최종단계(궁극적 목표)로서 이는 인터넷 보급정도 및 이용정도가 어느 수준에 도달한 경우에만 가능하다. 또한 종이 영수증도 마지막 단계로서 우리가 살펴볼 기술이 이에 해당

한다. 종이 영수증은 선관위, 사용자의 부정 및 오용을 방지위한 해결책으로서 자세한 사항은 5장과 6장에서 기술하도록 한다.

4. 종이 영수증 기술의 개요

종이 영수증 기술은 투표 시스템 방식 중 하나의 방식이며, 이 기술은 전자 투표 시스템의 모든 기록이 데이터로 유지되는데 있어 검증 방안으로 프린트된 투표용지를 포함시킴으로 인해 투표 결과에 대한 재검표가 가능하도록 하는 것이다. 전자 투표 시스템에서 투표의 결과에 대해서 언급하는 요구 사항은 다음과 같다.

- 전자 투표 시스템을 검증할 수 있는 장치가 필요하다.
- 전자 투표 시스템의 개표 결과를 검증할 수 있는 방안이 필요하다.
- 유권자의 투표 내용을 검증할 수 있는 방안이 필요하다.
- 유권자가 투표한 내용에 대한 백업이 필요하다.
- 제 3자의 개입이나 부정 행위의 발생에 대한 검증이 필요하다.

이와 같이 전자 투표 시스템 자체에 대한 신뢰성을 얻기 위해서도 위에서 언급한 내용들이 필요하며, 이와 같은 필요성에 의해 보안 기술을 적용하게 된다. 종이 영수증 기술은 다음과 같은 특징을 가지고 있다.

- 유권자에 의해 기록된 투표용지 혹은 프린트 영수증은 유일하게 존재한다.
- 기록된 투표용지 혹은 프린트 영수증은 수정, 삭제가 어렵다.
- 유권자가 자신의 투표 내용을 검증할 수 있다.
- 유권자의 투표의 결과에 대하여 제3자가 개입할 여지를 줄일 수 있다.

- 전자 투표 시스템의 개표과정을 검증할 수 있는 또 다른 방안이 제시된다.

위의 특징에 의해 종이 영수증 기술은 전자 투표 시스템에서 보조의 역할을 수행할 수 있다. 전자 투표 시스템에서 활용되는 데이터가 각기 다른 방식의 두 종류의 데이터로 분할되어 다른 하나에서 문제가 발생한 경우 다른 방식으로 보완을 제공할 수 있다. 또한 감사 기록으로 이용할 수 있으며, 유권자 자신의 투표한 내용을 직접 검증할 수 있는 방안도 제공한다. 전자 투표 시스템에 있어 데이터의 조작이나 제 3자의 악의적인 공격이 있어 데이터가 변경되더라도 이미 투표용지로 프린트된 내용을 조작하기는 매우 어렵다.

이러한 종이 영수증은 다음과 같은 보안 요구사항을 만족하여야 한다. 이는 종이 영수증이 보안적인 측면에서 고려하였을 경우를 의미하는 것으로 단지 확인용으로 제공되는 종이 영수증에는 해당되지 않는다. 종이 영수증에 암호 값이나, 워터마킹이 삽입된 이미지 등 여러 보안 기술을 적용하였을 경우에 해당한다.

- **Completeness** : 검표시기에 사용자의 종이 영수증의 집계와 투표 결과의 정확한 집계가 이루어져야 한다.
- **Privacy** : 영수증과 사용자 사이의 익명성은 보장되어야 한다.
- **Unresuability** : 영수증은 중복 투표 행위를 방지할 수 있어야 한다.
- **Fairness** : 영수증을 분실하였을 경우에도 검표에 영향을 미치지 않도록 해야 한다.
- **Verifiability** : 종이 영수증에 대한 위조를 방지할 수 있어야 한다.
- **Soundness** : 부정 사용된 종이 영수증에 의한 방해를 견뎌내어야 한다.

5. 종이 영수증 기술 종류

다음은 종이 영수증 기술을 이용하는 방식으로 초기 단계의 종이 투표용지를 이용하는 기술과 암호 기술이 적용된 프린트 기술을 이용하는 방식으로 분류되어 다음과 같은 기술을 적용할 수 있다. 앞서 살펴본 초기의 전자투표에서 사용된 투표용지를 이용한 기술로는 펀치카드와 광학 마크가 있으며, 최근에 와서 암호화적인 기술을 적용하여 사용하는 프린트 기술로는 SRTI 방식과 VVPAT 방식, NV 방식, VoteHere사의 Scratch Ticket 방식, VHTI™ 방식 등이 있다.

5.1 펀치 카드 방식

펀치 카드 방식은 이미 오래 전부터 이용하는 방식으로 유권자가 투표용지를 받아서 펀치기기 앞으로 다가선다[13]. 유권자는 펀치기기를 자신의 선택한 후보자에 구멍이 뚫리도록 조작한다. 각각의 구멍을 맞추기 위해 조작하는 방법이 어려우며, 사용자에게 불편함을 제공한다. 개표에 있어서는 투표용지를 개표 기기에 통과시켜 개표를 할 수 있다. 하지만 개표 과정에 있어 무효표가 발생하게 되는데 개표 기기가 읽지를 못하고 통과시킨 표를 감시인원이 다시 확인한다. 투표용지의 확인 과정에서 무효표 처리에 논의가 되는 것이다. 미국의 2000년 대선에서는 문제가 된 부분이 펀치 기기가 구멍을 정확히 뚫지 못하고 반쪽 표시를 하였기 때문에 무효표가 발생하였고 이와 같은 무효표로 인해 후보자의 당락이 결정되었다.

5.2 OMR 카드 방식

OMR 카드 방식 또한 많이 사용하는 방식으로 유권자는 투표용지로 OMR 카드를 이용한다[13]. OMR 카드는 OMR 인식기를 통해 선택한 값을 입력 받을 수 있다. 유권자는 투표소에 들어가 OMR 카드를 받고 후보자에 대하여 마킹

을 한다. 이후 유권자는 투표함에 용지를 집어 넣으면 된다. 개표과정에서는 취합한 투표용지를 OMR 인식기로 읽어들이어 합산을 하면 된다. OMR 카드의 방식의 경우 유권자가 마킹을 하는 것에서 오류가 나지 않는다면 무효표로 처리될 확률이 적다.

위의 펀치 카드 방식과, OMR 카드 방식은 투표에 있어 투표용지를 이용하는 방식으로 감사나 유권자의 투표내용 확인에서 투표용지를 활용할 수 있다.

5.3 VVPAT 방식

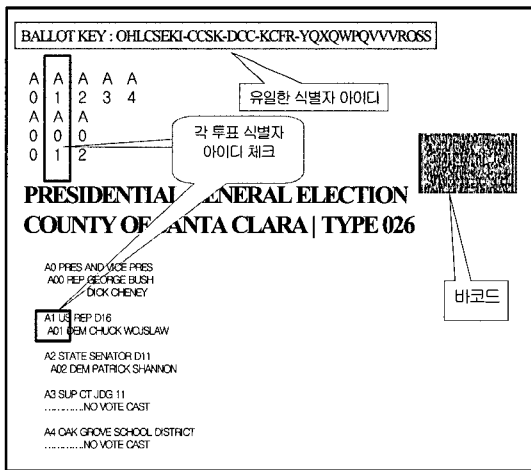
VVPAT(Voter Verified Paper Audit Trail) 방식은 독립기기를 이용하는 투표 시스템 있어 투표에 대한 프린트 영수증을 제공하는 것이다. 유권자는 독립기기가 설치된 투표 장소에 가서 투표를 실시한다. 유권자가 투표를 완료하고 나면 자신의 투표한 결과를 프린트하여 제공해주는 영수증을 받을 수 있다. 이 영수증을 제출하는 방식과 영수증 자체가 투표함에 자동적으로 들어가는 방식 두 가지가 있다. 둘 다 영수증의 결과를 가지고 투표 장소를 벗어나지는 못한다[2]. 현재 하나의 예로 AccuPoll사의 VVPAT는 종이에 투표의 기록을 남기는 방식으로 사용되고 투표용지로는 펀지지 크기를 이용하고 있다. 프린트 시스템으로는 잉크젯을 이용하고 있으며, 프린트되는 내용에는 워터마크 혹은 특수한 용지를 이용하고 이용한다. 독립 기기 시스템은 투표에 대한 데이터를 저장하는 것과 투표 영수증을 출력하여 저장하는 것 이렇게 두 가지로 나누어 관리된다. 투표 영수증으로 출력되는 내용은 (그림 2)와 같다.

- 유권자의 식별자 아이디 : 투표하는 유권자마다 식별자를 부여하여 차후 검증이 가능하도록 제공
- 전자 기록과 일치하는 바코드 : 데이터의 내용

과 투표용지의 내용이 매칭 되도록 정보를 바코드를 제공한다. 이로 인해 종이 영수증과 전자 데이터를 검증할 수 있다.

- 투표 내용 : 자신이 선택한 투표의 내용이 그대로 프린트됨으로 인해 유권자는 투표내용을 검증하기 쉽도록 하였다. 또한 선택한 내용과 앞에 코드 두 개가 일치하도록 하여 선택한 내용이 올바른 것임을 검증하도록 하였다.

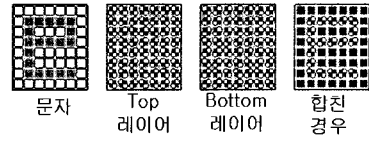
이 방식은 투표내용을 그대로 출력함으로써 유권자는 쉽게 자신의 투표 내용을 확인할 수 있으며, 전자적으로 저장되는 데이터와 동일한 정보를 가지고 있는지 매칭할 수 있는 방안을 제공해주고 있다.



(그림 2) AccuPoll사의 VVPAT의 종이 영수증

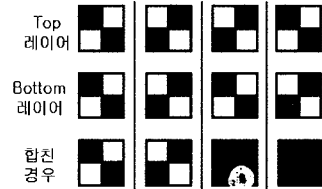
5.4 SRTI방식

David Chaum의 SRTI방식(Secret-ballot Receipt and Transparent Integrity)은 투표의 결과를 두 개의 종이에 나누어 프린트하도록 하였다[1]. 두 개로 표현하는 방법으로 상위(Top)레이어와 하위(Bottom)레이어를 이용하였고 한 문자를 표현하는데 있어 상위와 하위 레이어를 합치면 하나의 문자가 생성할 수 있다(그림 3 참조).



(그림 3) 문자 표현 방법

문자 표현 방법은 아래 (그림 4)의 방법을 이용한다.



(그림 4) 상위 레이어와 하위 레이어 표현방법

(그림 4)와 같이 상위 레이어와 하위 레이어에서 같은 방향으로 블랙이 존재하면 동일 방향의 그림이 나오고 서로 다른 방향으로 점이 존재하면 붉은색으로 채워진다. 이와 같은 프린트를 제공하기 위해서는 다음과 같은 수식을 이용한다.

$$R^t \oplus W^b = B^t$$

$$R^b \oplus W^t = B^b$$

위의 수식은 XOR을 이용하여 각각의 적색과 백색이 겹치거나 겹치지 않도록 출력하는 방법을 제시하였다. R은 붉은색을 W는 흰색을 B는 겹친 색을 나타내며, t는 상위 레이어로 b는 하위 레이어를 표시한다. 위의 수식으로 인해 상위 레이어와 하위 레이어에 프린트 될 색이 정해진다. 프린트되는 수식이 4개를 하나의 마크로 보면 다음과 같이 확장된다.

$$L^t_{i,2j-(i \bmod 2)} = R^t_{ij}$$

$$L^t_{i,2j-(i+1 \bmod 2)} = W^t_{ij}$$

$$L^b_{i,2j-(i+1 \bmod 2)} = R^b_{ij}$$

$$L^b_{i,2j-(i \bmod 2)} = W^b_{ij}$$

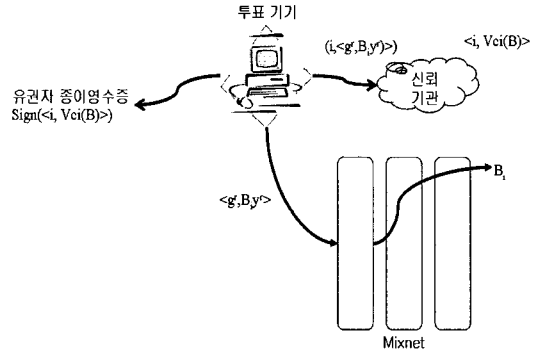
여기서 i, j 는 행렬을 표시하며, L 은 각 내용의 프린트 값이 된다. 그럼으로 프린트 값이 출력되면 이에 따른 색이 정해지고 각각의 행과 열값으로 인해 프린트된다. 영수증에 프린트 되는 값으로는 투표에서 사용한 임의 선택 값과 각각의 신뢰기관의 공개키로 암호화 된 값, 그리고 서명 값이 된다. 암호화 된 값을 상위와 하위 레이어로 프린트하여 하나는 버리고 다른 하나는 유권자가 선택하여 보관하게 된다. 이때 유권자가 보관하는 투표용지는 암호화된 값의 나머지 반(상위 혹은 하위 레이어)으로 보이기 때문에 어떠한 값인지는 알 수 없게 된다. 하지만 검증 과정에서는 나머지 반을 사용자가 신뢰기관 혹은 검증기관에 제공함으로써 나머지 반을 저장하고 있는 신뢰기관 혹은 검증기관 데이터에서는 검증이 가능하다. 이 기술에서는 투표의 내용을 그대로 프린트하는 것이 아니고 암호화 된 값을 프린트함으로써 보관하는 영수증에서 어느 후보자를 선택하였는지 알 수 없으며, 각각의 데이터가 무엇인지 알 수 없도록 하였다.

5.5 NV 방식

NV(Neff Voting)방식은 유권자가 자신의 일련번호(i)와 후보자의 코드를 부여 받는다[4]. 투표 전체 메시지(VC_i)는 유권자가 선택한 값(B_i)와 B_i 의 해쉬값을 나타낸다. BR 은 유권자의 일련 번호와 VC_i 를 투표기기가 서명하여 제공하는 값이 된다. 투표의 내용은 신뢰기관에 제공되는 방법으로는 ElGamal방식의 암호화를 이용한다. 유권자는 랜덤(r)을 선택하여 g^r 을 생성하고 신뢰기관의 공개키에 r 을 적용한다. 신뢰기관은 g^r 에 자신의 개인키를 연산하면 투표 값을 얻을 수 있다.

유권자에게 프린트되어 제공되는 종이 영수증은 서명된 값으로 값을 보고는 투표의 결과를 알 수는 없다. 투표기기의 서명으로 인해 정당한

투표용지임을 증명할 수 있다. 이와 같은 프린트 기술을 이용함으로써 인해 투표의 결과에 따른 검증과정에서 신뢰기관이 개입할 수 있어 유권자의 검증을 확인해 줄 수 있다.



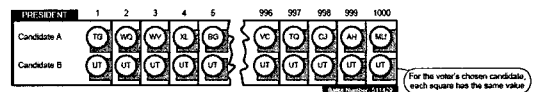
(그림 5) Neff Voting의 흐름도

5.6 Scratch Ticket 방식

VoteHere 사의 Scratch Ticket 방식으로 자신의 투표 값 위에 scratch할 수 있는 표면을 씌워서 제공하는 것이다[20]. 즉석 복권은 표면 아래에 미리 정해진 글씨를 새겨 넣고 그 위에 특수한 코팅을 입힌 것을 의미한다. 그러나 본 방식에서는 사용자가 원하는 글씨를 적어 넣고 그 위에 특수한 기계를 이용하여 표면을 코팅하여 제출하는 것을 의미한다.

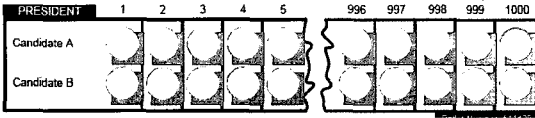
본 방식의 단계를 살펴보면 다음과 같다.

- 1단계: 투표자는 후보자 B를 선택
- 2단계: 투표기기는 투표 값에 대해 scratch ticket 과 유사한 것을 제작한다. 투표자가 선택한 각각의 원에는 동일한 값을 기입하고 선택하지 않은 원(후보자 A)에는 랜덤 값을 기입한다(그림 6 참조).



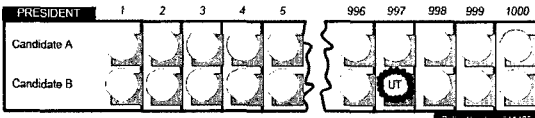
(그림 6) 사용자에 의해 생성된 값 기입

- 3단계: 투표기계는 각각의 원 위에 투표 값을 감출 수 있도록 생성한다(그림 7 참조).



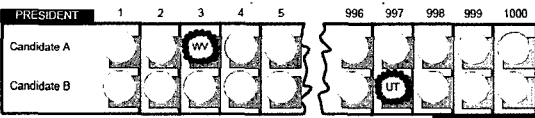
(그림 7) 사용자 생성 값 위에 특수 코팅

- 4단계: 투표기계는 투표자가 선택한 후보자 B에 대해 임의로 선택한 원 안에서의 “UT” 코드를 볼 것을 요청한다.
- 5단계: 후보자 B를 선택한 투표자는 1000 개의 원 중에서 하나를 선택하여 긁고, 선택한 “UT”를 확인한다. 만약 “UT”라고 확인하지 못하면 투표기계의 잘못이 된다(그림 8 참조).



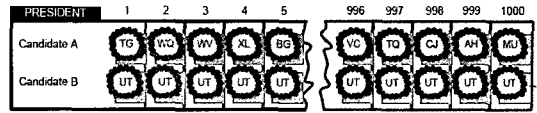
(그림 8) 사용자가 선택하여 코팅을 제거한 값

또한 투표자는 자신의 프라이버시를 보장하기 위해서 투표하지 않은 후보자 A의 원을 긁음(그림 9 참조)



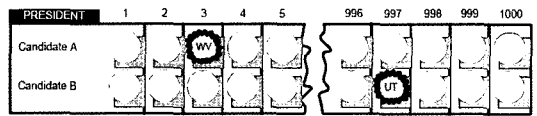
(그림 9) 사용자 프라이버시 보호를 위한 다른 후보자 선택

- 6단계: 자신이 가지고 있는 투표 값을 이용하여 시험하고 투표용지는 투표함에 제출한다.
- 7단계: 개표결과를 표로 만들기 위해 투표 번호는 각각의 투표와 섞는다(그림 10 참조).



(그림 10) 사용자 선택 값이 B 후보자임을 확인

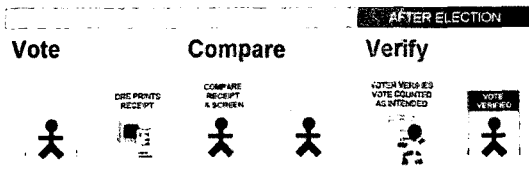
- 8단계: 원의 다른 부분을 긁어내고 후보자의 열이 모두 동일한 코드로 되어있음을 확인한다(그림 11 참조).



(그림 11) 개표를 위한 투표 번호 취함
[VoteHere사의 Scratch Ticket]

5.7 VHTi™ 방식

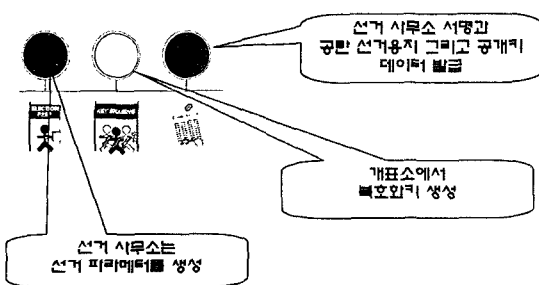
VoteHere사의 VHTi™는 선거 신임을 보증하며 투표자의 프라이버시를 보호하면서 투표의 검표를 할 수 있도록 한다[20]. 또한 투표자에 대한 단대단 보안과 보기 기능을 제공하는데 선거 사무소에서 수행하는 행위에 대해 단대단 보안을 제공할 수 있도록 설계되어있다. VHTi™는 발전 단계로써 초기에는 가장 간단한 종이 영수증을 제공하였고 현재에 와서는 사용자의 식별자값과 암호값을 통하여 종이 영수증 자체에 대한 보안도 강화하고 있는 실정이다. VHTi™에서의 투표과정을 살펴보면 가장 간단한 단계는 3단계로 이뤄진다. 투표자는 어떤 전자 투표 기계 앞에서 일반적인 투표를 한다. 확인된 모니터에 투표자가 선택한 투표 값을 확인시켜 주고 비교할 수 있는 종이 영수증을 출력한다. 선거 후에 투표자의 투표 값이 올바르게 반영되었는지 정부의 홈페이지에 접속하여 확인하고 검증하는 과정을 거친다. 이러한 과정이 가장 기본적인 과정으로 (그림 12)와 같이 이뤄진다.



(그림 12) VHTiTM의 가장 기본적인 투표절차

다음은 VHTiTM의 현재 제공되고 있는 기술에 대해 살펴보도록 하겠다. 현재 제공되고 있는 VHTiTM기술은 공개키 방식을 이용하여 진행하고 있으며 절차는 다음 (그림 13)과 같이 이뤄진다.

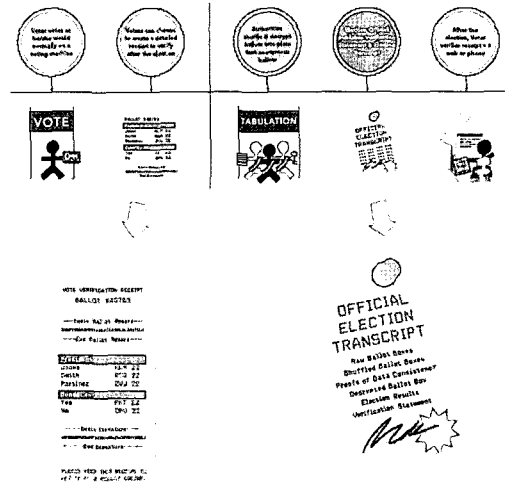
- 1단계 : 선거 사무소에서 투표자 각각의 선거 파라미터를 생성하여 이를 개표소에 전달하게 된다.
- 2단계 : 선거 파라미터를 선거 사무소로부터 전달받은 개표소는 이를 이용하여 투표자 각각의 복호화키를 생성한다.
- 3단계 : 각각의 투표자에게 투표용지를 발급하기 전에 선거 사무소의 서명과 공란 선거 용지(이때 선거용지는 종이 가 아닌 데이터로서 보관하게 된다), 투표자에게 발급할 공개키 데이터를 발급한다.



(그림 13) 초기 선거 절차

- 4단계 : 선거단계로서 투표자는 투표 기계 상에서 일반적으로 투표를 진행하게 된다. 이때 기계에서는 투표자가 검증

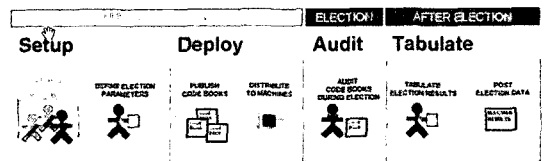
을 위해 영수증을 제공하고 투표자는 선택하여 출력하게 된다.



(그림 14) 종이 영수증 발급과 검증 절차

- 5단계 : 선거가 모두 이루어진 후의 단계로서 선거 후에 투표자는 자신의 영수증을 통해 웹이나 전화기로 검증 가능하게 되며, 투표 복사본은 신뢰기관에 보관하게 된다.

전제적인 그림은 (그림 15)를 참조한다.



(그림 15) 종이 영수증 발급 전체 투표 절차 [VoteHere사의 VHTiTM]

6. 종이 영수증 발급 업계 동향

종이 영수증 발급의 업계동향에 살펴보도록 한다. 다음 3개 업체는 대표적인 업체로서 사용자의 입력에 따른 출력물을 제공하게 된다. 출력물을 제공할 때 현재는 일반적인 확인용으로

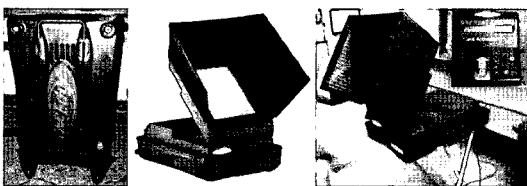
〈표 1〉 종이 영수증기술 비교

기술		내용	특징	보안 요구 사항	
투표 용지 기술	펀치 카드	펀치기 이용	펀치 카드에 구멍을 뚫어 투표	무효표 발생의 확률이 높음	조작의 어려움이 존재
	OMR 카드	OMR카드의 마크	OMR카드의 마크	OMR인식기를 이용한 개표 방식	기표의 오류 및 인식 오류 발생 확률이 존재
프린트 기술	VVPAT 방식	이미지 워터마킹 특수 용지 이용	투표자의 식별자 투표 내용	종이 영수증 제출 유권자는 소유 불가 전자적 기록에 대한 감사로 이용	종이 영수증 관리
	SRTI 방식	두 개 레이어 이용 암호 기술 적용	투표자의 식별자 암호화된 투표 내용 서명 값	유권자가 직접 소유 2개의 레이어 중 택	매매 방지 이중 투표 방지
	NV 방식	서명된 암호문 프린트 제공	투표 값에 대한 신뢰기관의 서명제공	유권자가 직접 소유 서명 값을 프린트	매매 방지
	VHTI™ 방식	스크래치 방식	사용자가 기입한 문자위에 특수한 막으로 코팅	사용자만 알 수 있음 부정 발생 통제 가능	스크래치가 임의적으로 제거되면 취소

서 제공하고 있으나 6장에서 살펴본 기술을 접목하여 종이 영수증에 대한 보안을 제공할 수 있을 것이라 사료된다.

6.1 Sequoia Voting Systems Inc.

다음의 Sequoia Voting Systems사의 AVC Edge에 대해 살펴보도록 한다[21]. 이 시스템의 특징은 사용자 인증에 있어 스마트카드를 이용하여 사용자를 인증하고 투표자의 투표 값을 메모리에 보관하고 투표 후에 내용을 제공하는 특징을 가지고 있다.



(그림 16) AVC/Edge 모델
[Electronic Voting Machine Information Sheet]

시스템의 흐름을 살펴보면 스마트카드를 이용하여 투표를 실시하며, 사용기기로는 터치스크린 방식을 이용한다.

- 1) 두 개의 플래쉬 메모리 카드를 이용하여 투표의 내용을 기록하고
- 2) 스마트카드는 한번만 투표에 사용할 수 있다.
- 3) 투표 후에 투표의 내용을 프린트하여 제공한다.

종이로 프린트되는 내용은 유리를 통해서 보여지며, 프린트된 내용이 틀리면 터치 스크린을 통해서 다시 작성할 수 있다. 투표를 끝낸 후에 스마트카드를 돌려받으면 투표는 완료된다. 특징으로 두 개의 카드가 서로 다른 기능을 하는 것으로 하나는 관리자 카드로 스마트 카드가 되며 각각의 기계마다 사용하는 것으로 투표시마다 리셋이 된다. 다른 하나는 PCMCIA카드로 플래쉬 메모리에 투표한 내용을 저장하고 있다. 두 개의 서로 다른 카드를 이용하는 것이 가장 큰 특징이 된다.

6.2 AccuPoll Inc.

투표에 사용되는 키는 한번 사용하고 나면 리셋 된다[15]. 유권자는 투표가 끝나면 그 내용을 프린트하여 유권자에게 제공한다. 유권자는 프린트된 내용을 확인하고 나서 프린트된 용지를 투표함에 넣는다. 이외에 주요한 특징으로는

CD-ROM을 이용하여 투표 결과를 저장할 수도 있다. 카드에 투표에 사용되는 키가 입력되어 있는 것이 가장 큰 특징이다.



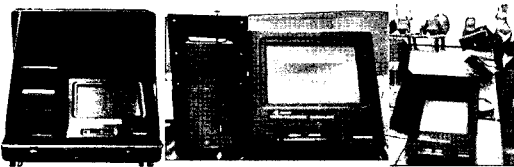
(그림 17) AVS/1000 모델
[Electronic Voting Machine Information Sheet]

본 시스템의 절차를 보면 스마트카드 내에 투표키를 저장하여 이용한다.

- 1) 스마트카드를 투표 기기에 투입한다.
- 2) 유권자는 후보자를 선택한다.
- 3) 투표 기기는 두 개로 기록하는데 하나는 플래시 메모리이고 다른 하나는 저장하드다.

6.3 Avante International Technology Inc.

프린트의 내용을 검사하고 나서 투표의 내용이 저장되는 방식이 특징이며, 프린트 내용이 잘못 되었으면 다시 터치스크린을 통해 결정값을 수정할 수 있다. 스마트카드에 식별자 아이디가 입력되어 있는 것이 가장 큰 특징이다 [21].



(그림 18) Vote-Trakker/EVC-308SPR 모델
[Electronic Voting Machine Information Sheet]

본 시스템의 방식에 대해 살펴보면 스마트카드를 이용하는 방식으로 스마트카드에는 식별자 아이디가 입력되어 있다.

- 1) 유권자는 터치 스크린을 통해 투표를 한다.
- 2) 투표 기기는 기록에 대하여 프린트를 제공한다.
- 3) 프린트의 내용을 검토하고 나서 투표의 내용이 정확하다고 하면 프린트에 기기의 바코드가 프린트되면서 플래시 메모리와 저장 하드에 입력된다.
- 4) 투표가 모두 완료되면 하드의 내용을 CD로 저장한다. CD로 저장된 내용은 집계소로 운반되어 개표를 한다.

7. 전자 투표 시스템과 종이 영수증 기술 발전 방향

7.1 전자 투표 시스템 발전 방향

전자 투표 시스템은 현재 도입에 있으며, 활용하는데 있어 유권자들의 전자 기기 자체에 대한 신뢰성이 우려가 발생하고 있다. 투표는 서론에서 언급한 것처럼 유권자의 의견을 나타내는 가장 기본적인 수단이 된다. 이와 같은 방식에 있어 전자 투표 시스템의 도입은 IT 인프라의 발전과 전자 정부를 구축하는데 있어 중요한 이슈가 되고 있으며, 현재 많은 나라에서는 활용을 하고 있다. 우리 나라도 앞으로 전자 투표 시스템을 도입하는데 있어 다음과 같은 사항을 고려하여 전자 투표 시스템을 도입되어야 할 것이다.

- 전자 투표 시스템의 신뢰성
- 전자 투표 시스템의 개표 검증
- 유권자의 투표 내용에 대한 검증
- 전자 데이터에 대한 감사자료 필요
- 유권자의 편리성 제공

전자 투표 시스템을 활용하기 위해서는 무엇보다 우선되어야 할 것이 유권자들의 신뢰성이다. 유권자들이 전자 투표 시스템에 대하여 신뢰하기 위해서는 안전성에 대한 설명도 필요하

지만 자신들의 투표에 대한 검증을 제공함으로써 투표 시스템에 대한 신뢰성을 높일 수 있다. 이때 검증 방안은 여러 기술이 제공될 수 있다. 암호학적 기술을 이용하여 제공할 수 있고, 시스템 내부의 검증 방안을 제공할 수 있다. 하지만 유권자는 전체적인 시스템을 이해하기 어렵고 직접 자신이 투표하는 결과가 어떻게 처리되는지 보기를 원한다면, 종이 영수증 기술이 여러 방안 중에 좋은 방안이 될 수 있다. 종이 영수증은 유권자기 기준에 하던 방식을 이용하는 방법과 비슷하며, 유권자 자신이 검증을 할 수 있는 방안을 제시할 수도 있기 때문이다. 이와 같이 종이 영수증 방식은 투표 시스템의 검증과 신뢰성을 높일 수 있는 방안이 되며, 다른 한편으로는 기록을 오프라인으로 보관할 수 있는 방안이 될 수 있다. 투표에 대한 절차가 모두 전자적으로 처리되더라도 종이로 보관을 하면 자신이 선택한 초기 값과 투표 값에 대한 변경에 대해 검증할 수 있으며, 전자 투표 시스템이 신뢰성을 얻는데 있어 도움을 줄 것으로 사료된다. 종이 영수증을 기술을 부가한다고 해서 전자 기기를 이용하는 편리성이 없어지는 것은 아니다.

7.2 종이 영수증 발전 방향

위에서 살펴보았듯이 전자 투표는 기존 종이 전자 투표의 불편성을 제거하기 위해 개발되었으나 완전한 전자 투표는 보안적인 측면에서 여러 가지 문제점을 가질 수 있다. 그래서 최근에는 종이 영수증에 대한 두 가지 의견이 지배적으로 대두되고 있다. 첫째로는 종이 영수증 장치의 무의미론을 제기하는 집단이고 둘째로는 종이 영수증의 의미론을 제기하는 집단이다. 각각의 집단은 암호화적인 문제와 정책적인 문제 등으로 의견을 제시하고 있다.

우선 종이 영수증 장치의 무의미론을 제기하는 입장에서 살펴보면 다음과 같다. 첫 번째로

종이기록장치의 무의미론 집단에서 살펴보면, 종이기록 장치는 재검표에 아무런 도움을 주지 못한다고 제기하고 있다. 이는 종이 영수증이 사용자에게 제공되기 때문에 문제 발생 시 사용자의 영수증이 회수가 불가능하기 때문에 이러한 문제점을 제기하게 되었다. 두 번째 사항은 투표 결과 값이 다른 3 자에게 유출되어 결과가 사전에 계산된다면 투표에 대한 신뢰도를 떨어뜨리는 것이 된다고 하고 있지만, 종이 영수증의 필요성을 제기하는 쪽에서는 영수증에 암호 기술을 이용하여 제공하기 때문에 문제가 발생하지 않는다고 반박하고 있다. 세 번째 사항은 기존 전자투표에 대한 신뢰도 문제를 제기하는데 종이 영수증을 이용하게 됨으로써 기존 전자 투표 전체에 대한 신뢰도가 하락할 수 있다는 문제점을 제기한다. 네 번째 사항으로는 종이 기록 장치가 없더라도 공격자나 내부자로 인해 투표 값이 변할 이유가 없다고 하고 있으나 필요성을 제기하는 집단에서는 정부가 문제를 발생시킨다면 문제는 항상 존재한다고 제기하고 있다. 다섯 번째 사항은 내부자라 할지라도 검증 가능한 원시기록을 알 수 없기 때문에 네 번째 사항은 안전하다고 할 수 있으나 원시기록을 관리하는 측과의 공모를 방지할 수 없다는 문제점이 남게 된다. 마지막으로 다섯 번째 사항은 인증기준의 향상, 철저한 시험, 향상된 투표절차, 투표요원의 훈련 등으로 해결 가능하다는 것이다.

종이 영수증의 의미론 집단에서 살펴보면 다음과 같다. 첫 번째 사항은 종이 영수증으로 인해 재검표를 올바르게 수행할 수 있다는 것이다. 이것은 사용자가 온라인 상에서 잘못된 투표결과가 전송되어 잘못된 개표를 보였을 때 유용하게 사용될 수 있다. 두 번째 사항은 종이 영수증 장치 없이 상위 기관에서 임의적으로 투표의 결과를 부정할 수 없도록 종이 영수증 장치가 보완책이 될 수 있다는 것이다. 이것은

종이 영수증을 제공하지 않았을 경우 사용자의 투표 값을 부정 생성하여 이용할 수 있는 문제 점을 효율적으로 방지하는 경우를 의미한다. 마지막으로 세 번째 사항은 종이 영수증의 부재는 익명으로 하는 거래와 동일하다고 볼 수 있으며, 이러한 문제는 자신의 값이 변경되거나 수정되더라도 초기의 자신이 제출한 투표 값을 알 수 없으므로 종이 영수증은 필수사항이라는 것이다.

8. 결 론

전자 투표 시스템에 있어 가장 중요한 것은 유권자가 투표한 내용이 정확히 전달되는 것이며, 이와 같은 방법을 제시하여 시스템을 모두 설계하였을 것이다. 하지만 시스템 자체의 오류도 존재할 수 있지만, 제 3자의 부정이 있을 수 있으며, 유권자의 자신의 투표에 대한 요구도 발생할 수 있다. 이와 같은 사항으로 인해 검증할 수 있는 방안이 필요하며, 검증방법에는 보안 기술을 적용하여 제시하는 방안이 제안되어져 있다. 하지만 데이터로 모든 것을 처리하면 데이터의 특성은 2장에서 언급한 것처럼 수정, 삭제가 가능하며, 관리자가 악의적인 목적을 가지고 수정할 수 있으며, 유권자의 투표 결과가 포함되었다는 것을 보여줄 수 있는 방안이 없기 때문에 4장에서 언급한 것처럼 종이 영수증 기술이 나타나게 되었다. 종이 영수증 기술은 전자 투표 시스템의 한 방안으로 데이터로 저장되는 것 이외에 다른 자료가 되는 것이다. 종이 영수증의 특징으로 인해 데이터에서 제공하지 못하는 기술을 제공해 줄 수 있으며, 이와 같은 기능은 유권자가 전자 투표 시스템에 신뢰성을 가질 수 있게 도움을 줄 것이다. 특히 유권자의 투표 내용을 보이지 않고 저장되는 데이터보다 바로 앞에 프린트되어 자신이 직접 볼 수 있는 것이 더욱 신뢰성을 제공할 수 있다. 그러므로

앞으로 전자 투표 시스템을 도입하는 방안으로는 종이 영수증 기술을 적용한 시스템에 대한 검토의 논의해야 할 것이다.

참고문헌

- [1] David Chaum, "Secret-Ballot Receipts and Transparent Integrity", Courtesy advance draft, 2002, 3
- [2] David Chaum, "Secret Ballot Receipts: True Voter-Verifiable Elections", RSA Laboratories, Vol.7, No.2, 2004
- [3] Donald P.Moynihan, "Building Secure Elections: E-Voting, Security and Systems Theory", ABI/INFORM Global, 2004. 9
- [4] Dennis Vadura, Frank Wiebe, what is a meaningful "Voter Verified Paper Audit Trail?", 2003. 12
- [5] Margaret McGaley, J. Paul Gibson, "Electronic Voting: A Safety Critical System", Technical Report, NUIM-CS-TR2003-02, 2003. 3
- [6] Michael Ian Shamos, "Paper v. Electronic Voting Records-An Assessment", election-tech.org, 2004. 4
- [7] Susan King Roth, "Disenfranchised by design: voting systems and the election process" Information design Journal, Vol.9, No.1, 1998
- [8] Safevote, "Voting Ssystem Requirements", Safevote, Inc. and The Bell, 2001. 2
- [9] Pedro A.D. Rezendé, "Electronic Voting Systems-Is Brazil Ahead of its Time?", RSA Laboratories, Vol.7, No.2, 2004
- [10] Ron Rivest, "Neff Voting", Advanced Topics in Cryptography, 2004. 3
- [11] Wen-shenq Juang, Student Member and

Chin-Laung Lei, "A Secure and Practical Electroni Voting Scheme for Real World Environments", IEICE TRANS. FUNDAMENTALS.

- [12] 고선규, "일본의 지역 전자투표 추진현황", 국제 컨퍼런스, 2005. 3.
- [13] 김재광, "전자투표의 도입에 따른 관련 법 제 정비 방안", 한국법제 연구원
- [14] 김혁, "e-Governance 구현을 위한 전자 투표(e-voting)의 가능성과 한계", 한국전산원
- [15] <http://accupoll.com>, AccuPoll
- [16] <http://www-db.stanford.edu/pub/keller/2004/electronic-voting-machine.pdf> Arthur Keller, "A PC-Based Open-Source Voting Machine with an Accessible Voter-Verifiable Paper Ballot"
- [17] <http://realex.nist.gov/conferences/voting/dayone/session2.3/index.htm>, David Dill. NIST Voting Standards Symposium, 2003. 12.
- [18] <http://citeseer.ist.psu.edu/cache/papers/cs/31785>, Ronald L. Rivest, "Electronic Voting"
- [19] <http://theory.lcs.mit.edu/~cis/theses/DuRette-bachelors.pdf> Brandon William DuRette, "Multiple Administrators for Electronic Voting"
- [20] <http://votehere.net>, VoteHere
- [21] <http://verifiedvoting.org>, VerifiedVoting

저자약력



강 서 일

2003년 순천향대학교 정보기술 공학부 졸업
 2004년~2005년 순천향대학교 전산학과 석사
 2005년~현재 순천향대학교 전산학과 박사 과정
 관심분야: 전자 투표, 전자 화폐, 전자 상거래



이 덕 규

2001년 순천향대학교 컴퓨터공학과 졸업
 2003년 순천향대학교 전산학과 석사
 2003년~현재 순천향대학교 전산학과 박사과정
 관심분야: Broadcast Encryption, DRM, EKE



이 임 영

1981년 홍익대학교 전자공학과 졸업
 1986년 오사카대학 통신공학전공 석사
 1989년 오사카대학 통신공학전공 박사
 1989년~1994년 한국전자통신연구원 선임연구원
 1994년~현재 순천향대학교 정보기술공학부 교수
 관심분야: 암호이론, 정보이론, 컴퓨터 보안