(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0062931
(43) 공개일자 2011년06월10일

(51) Int. Cl.
G06Q 40/00 (2006.01)
(21) 출원번호 10-2009-0119805
(22) 출원일자 2009년12월04일
심사청구일자 2009년12월04일

(71) 출원인
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
(72) 발명자
양대헌
인천광역시 남구 용현3동 인하대학교 하이테크센터 317호
김성호
충청남도 예산군 대술면 시산리 1구 94번지
(뒷면에 계속)
(74) 대리인
이원희

전체 청구항 수 : 총 7 항

(54) 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법

(57) 요 약

본 발명은 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법에 관한 것으로, 해결하고자 하는 기술적 과제는 멀웨어를 통한 계좌 이체 정보의 변조 위협에 대응할 수 있고, 계좌 이체에 대한 보안성을 향상시킬 수 있는 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법을 제공하는데 있다.

이를 위해 본 발명에 따른 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법은 사용자가 계좌 이체 시작을 은행 서버에 요청하고 상기 은행 서버가 계좌 이체 페이지를 사용자에게 디스플레이하는 계좌 이체 준비단계와, 사용자가 상기 계좌 이체 페이지에 이체 정보를 입력하여 상기 은행 서버에 전송하는 이체 정보 전송단계와, 은행 서버가 상기 이체 정보에 해당하는 내용의 캡차와 상기 이체 정보에 해당하지 않는 내용의 캡차를 모두 포함하는 이체 승인 요청 페이지를 생성하여 사용자에게 디스플레이하는 이체 승인 요청단계와, 사용자가 상기 이체 승인 요청 페이지에서 상기 이체 정보에 해당하는 캡차를 선택한 후, 승인 정보를 입력하여 상기 은행 서버에 전송하는 이체 승인 완료단계 및 은행 서버가 상기 사용자가 선택한 캡차와 승인 정보를 확인하여 계좌 이체를 수행하는 계좌 이체 수행단계를 포함하는 것을 특징으로 한다.

대 표 도 - 도3

(72) 발명자

강전일

충청남도 공주시 옥룡동 284-1

김기태

인천광역시 연수구 옥련동 우성아파트 103-1509

맹영재

인천광역시 남구 용현3동 인하대학교 하이테크센터 307호

특허청구의 범위

청구항 1

사용자가 계좌 이체 시작을 은행 서버에 요청하고, 상기 은행 서버가 계좌 이체 페이지를 사용자에게 디스플레이하는 계좌 이체 준비단계;

사용자가 상기 계좌 이체 페이지에 이체 정보를 입력하여 상기 은행 서버로 전송하는 이체 정보 전송단계;

은행 서버가 상기 이체 정보에 해당하는 내용의 캡차와 상기 이체 정보에 해당하지 않는 내용의 캡차를 모두 포함하는 이체 승인 요청 페이지를 생성하여 사용자에게 디스플레이하는 이체 승인 요청단계;

사용자가 상기 이체 승인 요청 페이지에서 상기 이체 정보에 해당하는 캡차를 선택한 후, 승인 정보를 입력하여 상기 은행 서버에 전송하는 이체 승인 완료단계; 및

은행 서버가 상기 사용자가 선택한 캡차와 승인 정보를 확인하여 계좌 이체를 수행하는 계좌 이체 수행단계를 포함하는 것을 특징으로 하는 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법.

청구항 2

제 1항에 있어서,

상기 캡차는 실시간으로 갱신되는 것을 특징으로 하는 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법.

청구항 3

제 1항에 있어서,

상기 캡차는 순서에 관계없이 무작위로 섞여 있는 것을 특징으로 하는 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법.

청구항 4

제 1항에 있어서,

상기 캡차는 왜곡된 문자열 및 노이즈를 포함하는 것을 특징으로 하는 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법.

청구항 5

제 1항에 있어서,

상기 캡차는 동일 색상의 문자열을 포함하는 것을 특징으로 하는 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법.

청구항 6

제 1항에 있어서,

상기 캡차는 서로 연결된 문자열을 포함하는 것을 특징으로 하는 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법.

청구항 7

제 1항에 있어서,

상기 캡차는 배경색에 연속된 그러데이션이 삽입되는 것을 특징으로 하는 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법에 관한 것으로서, 계좌 이체 정보의 변조로 인한 피해를 방지할 수 있는 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법에 관한 것이다.

배 경 기 술

[0002] 인터넷이 발달되면서 은행에서는 인터넷뱅킹 서비스를 제공하여 사용자들에게 편의를 제공하고 있다. 인터넷뱅킹의 다양한 이점으로 인하여 많은 사용자들이 서비스를 이용하고 있고, 그 규모는 점차 성장하고 있다.

[0003] 한편, 클라이언트에 키로거, 백도어, 루트킷 등을 설치하거나, 인터넷뱅킹을 이용하는 웹브라우저에 악의적인 브라우저 확장 프로그램들(browser helper Object, browser extension, toolbar)을 설치하여 인터넷뱅킹의 안전성을 위협하고 있다.

[0004] 이러한 위협에 대응하기 위하여 인터넷뱅킹 서비스를 제공하는 은행의 웹사이트에서는 인터넷뱅킹 서비스 이용시에 각종 보안 프로그램들의 설치를 유도하여 클라이언트의 보안성을 강화하고 있으며, 또한, 추가적인 인증 기술, 예를 들어, PIN, 공인인증서, 스마트카드, OTP, 보안카드를 사용하고 있다.

[0005] 그러나, 인터넷뱅킹 서비스를 이용하는 클라이언트가 이미 멀웨어에 장악당했다면 설치된 보안 프로그램이 올바르게 수행되지 않을 수 있는 문제점이 있다.

[0006] 도 4는 멀웨어 공격 예상 시나리오를 나타내는 도이다.

[0007] 안전하지 않은 인터넷 뱅킹 환경, 즉, 감염된 컴퓨터 상에서 공격자는 사용자에게 보여지는 정보와 실제로 발생하는 계좌 이체 정보를 동시에 수정함으로써 사용자를 속일 수 있다.

[0008] 구체적으로, 도 4에 도시된 바와 같이, 사용자가 계좌 이체 정보를 전송할 때, 계좌 이체 정보들 중 특정 정보, 예를 들어, 이체할 계좌 번호 또는 액수를 악의적으로 변조하여 은행 서버로 전송할 수 있다.

[0009] 상기 은행 서버에서는 변조된 이체 정보를 바탕으로 이체 승인 요청 페이지를 생성하여 사용자에게 전송할 수 있고, 이때, 상기 이체 승인 요청 페이지에는 사용자가 의도하지 않은 정보들이 있기 때문에, 멀웨어는 사용자를 기만할 목적으로 이체 승인 요청 페이지를 사용자가 입력한 이체 정보를 바탕으로 재구성할 수 있다.

[0010] 사용자가 멀웨어에 의해 변조된 이체 승인 요청 페이지를 볼 때, 변조된 페이지는 원래 사용자가 의도한 계좌 이체 정보와 일치하므로, 추가적으로 필요한 보안 정보, 즉, OTP, 보안 카드 숫자를 입력한 후 상기 은행 서버로 전송할 수 있다.

[0011] 상기한 바와 같이, 멀웨어가 클라이언트를 장악하면 계좌 이체에 관련된 정보들을 변조할 수 있으므로, 사용자 피해를 유발할 수 있는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

[0012] 본 발명은 상기한 바와 같은 문제를 해결하기 위해 안출된 것으로, 멀웨어를 통한 계좌 이체 정보의 변조 위협에 대응할 수 있는 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법을 제공하는데 그 목적이 있다.

[0013] 본 발명의 다른 목적은, 은행 서버로부터 전송받은 이체 승인 요청 페이지에 신뢰성을 부여하여 계좌 이체에 대한 보안성을 향상시킬 수 있는 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법을 제공하는데 있다.

과제 해결수단

[0014] 상기한 바와 같은 목적을 달성하기 위해 본 발명에 따른 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법은 사용자가 계좌 이체 시작을 은행 서버에 요청하고 상기 은행 서버가 계좌 이체 페이지를 사용자에게 디스플레이하는 계좌 이체 준비단계와, 사용자가 상기 계좌 이체 페이지에 이체 정보를 입력하여 상기 은행 서버로 전송하는 이체 정보 전송단계와, 은행 서버가 상기 이체 정보에 해당하는 내용의 캡차와 상기 이체 정보에 해당하지 않는 내용의 캡차를 모두 포함하는 이체 승인 요청 페이지를 생성하여 사용자에게 디스플레이하는 이체 승인 요청단계와, 사용자가 상기 이체 승인 요청 페이지에서 상기 이체 정보에 해당하는 캡차를 선택한 후, 승인 정보를 입력하여 상기 은행 서버에 전송하는 이체 승인 완료단계 및 은행 서버가 상기 사용자가 선택한 캡차와 승인 정보를 확인하여 계좌 이체를 수행하는 계좌 이체 수행단계를 포함하는 것을 특징으로 한다.

[0015] 또한, 상기 캡차는 실시간으로 갱신될 수 있다.

[0016] 또한, 상기 캡차는 순서에 관계없이 무작위로 섞여 있을 수 있다.

[0017] 또한, 상기 캡차는 왜곡된 문자열 및 노이즈를 포함할 수 있다.

[0018] 또한, 상기 캡차는 동일 색상의 문자열을 포함할 수 있다

[0019] 또한, 상기 캡차는 서로 연결된 문자열을 포함할 수 있다.

[0020] 또한, 상기 캡차는 배경색에 연속된 그러데이션이 삽입될 수 있다.

효 과

[0021] 상기한 바와 같이 본 발명에 따른 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법은 멀웨어를 통한 계좌 이체 정보의 변조 위협에 대응할 수 있는 효과가 있다.

[0022] 또한, 본 발명에 따른 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법은 은행 서버로부터 전송받은 이체 승인 요청 페이지에 신뢰성을 부여하여 계좌 이체에 대한 보안성을 향상시킬 수 있는 효과가 있다.

발명의 실시를 위한 구체적인 내용

[0023] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세히 설명한다. 우선, 도면들 중 동일한 구성요소 또는 부품들은 가능한 한 동일한 참조부호를 나타내고 있음에 유의해야 한다. 본 발명을 설명함에 있어서 관련된 공지 기능 혹은 구성에 대한 구체적인 설명은 본 발명의 요지를 모호하게 하지 않기 위해 생략한다.

[0024] 도 1은 본 발명의 일 실시예에 따른 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법의 블록도이다.

[0025] 본 발명의 일 실시예에 따른 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법은 도 1에 도시된 바와 같이, 계좌 이체 준비단계(S10)와, 이체 정보 전송단계(S20)와, 이체 승인 요청단계(S30)와, 이체 승인 완료단계(S40)

및 계좌 이체 수행단계(S50)를 포함한다.

[0026] 상기 계좌 이체 준비단계(S10)는 사용자가 계좌 이체 시작을 은행 서버에 요청하고, 상기 은행 서버가 계좌 이체 페이지를 사용자에게 디스플레이하는 단계이다.

[0027] 구체적으로, 상기 계좌 이체 준비단계(S10)에서는 사용자가 인터넷 뱅킹 서비스를 제공하는 은행의 웹사이트에 접속하여 계좌 이체를 선택한다. 그러면, 상기 은행의 웹사이트는 계좌 이체 페이지를 사용자에게 디스플레이하며 사용자의 이체 정보 입력을 요청한다.

[0028] 상기 이체 정보 전송단계(S20)는 사용자가 상기 계좌 이체 페이지에 이체 정보를 입력하여 상기 은행 서버로 전송하는 단계이다.

[0029] 이때, 상기 이체 정보는 수신 계좌, 이체 금액, 수신인 등 다양한 정보가 포함될 수 있다.

[0030] 상기 이체 승인 요청단계(S30)는 은행 서버가 상기 이체 정보에 해당하는 내용의 캡차와 상기 이체 정보에 해당하지 않는 내용의 캡차를 모두 포함하는 이체 승인 요청 페이지를 생성하여 사용자에게 디스플레이하는 단계이다.

[0031] 일반적으로, 상기 캡차(CAPTCHA, Completely Automated Public Turing test to tell Computers and Humans Apart)는 컴퓨터와 사람을 구별할 수 있게 해주는 튜링 테스트로, 주로 자동화된 봇(bot 또는 automated software agent)을 차단할 때에 사용된다.

[0032] 예를 들어, 캡차는 봇에 의한 웹 서비스의 자동 가입, 블로그 댓글에 스팸광고, 자동 투표, 게시판 글의 자동 등록 등을 차단하는데 사용된다.

[0033] 도 3은 본 발명의 일 실시예에 따른 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법에서 이체 승인 요청 페이지를 나타내는 도이다.

[0034] 은행 서버가 상기 이체 승인 요청 페이지를 생성할 때, 도 3에 도시된 바와 같이, 이체 정보에 해당하는 내용과 이체 정보와 관련이 없는 더미 정보를 바탕으로 다수의 캡차를 생성하여 순서에 관계없이 무작위로 섞어 나타낼 수 있다.

[0035] 이때, 상기 캡차는 문맥 기반의 이미지 캡차로 이루어질 수 있고, 다수, 예를 들어 25개의 캡차 중에 일부, 예를 들어 5개만이 이체 정보와 관련이 있을 수 있다.

[0036] 한편, 야후!의 EZ-gimpy, 윈도우라이브 핫메일, 구글 Gmail 등의 캡차에 대하여 이미지 프로세싱 기법이나 인공지능 기법을 이용하여 캡차를 읽어냄으로서 보안 위협이 보고된 바 있다.

[0037] 따라서, 상기 이미지 프로세싱 기법이나 인공 지능 기법을 이용하여 캡차를 읽어내는 보안 위협에 대응하기 위해 보다 안전한 캡차를 생성하는 것이 필요하다.

[0038] 구체적으로, 상기 캡차는 왜곡된 문자열 및 노이즈를 포함할 수 있고, 동일 색상의 문자열을 포함할 수 있다.

[0039] 또한, 상기 캡차는 서로 연결된 문자열을 포함할 수 있고, 배경색에 연속된 그러데이션이 삽입될 수 있다.

[0040] 문맥 기반의 캡차는 사용자가 해당 문맥, 즉, 이체 정보를 사전에 인지하고 있기 때문에, 가독성이 현저하게 낮은 캡차를 생성하여도 사용자는 이체 정보와 관련된 캡차를 선택하는데 어려움이 없고, 가독성이 낮은 캡차를

이용할 수 있다는 점은 안전한 캡차를 생성하는데 중요한 요소가 될 수 있다.

[0041] 한편, 계좌 이체를 1회 진행한다면 도 3에 도시된 바와 같이, 25개의 캡차가 필요하고, 이때, 캡차를 재사용한다면 공격자는 캡차 이미지를 모아 확률적으로 캡차의 문자열을 추측할 수 있다. 따라서, 상기 캡차는 상기 이체 승인 요청 페이지를 생성할 때마다 실시간으로 갱신될 수 있다.

[0042] 상기한 바와 같이, 본 발명에 따른 캡차는 무작위로 캡차를 선택하는 공격자나 캡차를 부분 수정하는 공격자에 대해 보안성을 향상시킬 수 있다.

[0043] 구체적으로, 멀웨어는 은행 서버로부터 전송된 캡차 전체를 새롭게 만들어 사용자에게 보여주고, 자신은 은행으로부터 전송된 캡차를 무작위로 선택하여 이를 은행 서버로 전송할 수 있다.

[0044] 그러나, 이러한 공격이 성공할 확률은 $1/(25\times\cdots\times21)=1.56\times10^{-7}$으로 현실적으로 성공하기에 매우 낮다.

[0045] 또한, 멀웨어는 수정된 이체 정보를 사용자에게 발각되지 않기 위해 이체 승인 요청 페이지에서 자신이 수정했던 이체 정보에 해당하는 캡차를 최소 2개(계좌번호, 수신자) 이상 구분하여 해당 부분의 캡차 이미지를 수정할 수 있다.

[0046] 그러나, 멀웨어가 캡차 이미지의 문자열을 읽을 수 있는 가능성이 상당히 낮으므로, 멀웨어는 무작위로 2개 이상의 캡차 이미지를 선택할 수 밖에 없다. 이러한 확률은 $1/(25\times24)=1.67\times10^{-7}$부터 1.67×10^{-7}에 해당한다.

[0047] 이 경우, 멀웨어는 배경과 글자를 분라하고, 이를 다시 사용자가 알아챌 수 없도록 정교하게 다시 제작해야 하는 어려움이 있다. 이때, 사용자가 해당 캡차에 이상이 있음을 인지할 수 있다면, 공격은 실패하게 된다.

[0048] 도 2는 본 발명의 일 실시예에 따른 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법 중 이체 승인 완료단계의 블록도이다.

[0049] 상기 이체 승인 완료단계(S40)는 사용자에 의해서 입력된 캡차 선택 정보를 다른 이체 정보와 함께 서명하여 이를 은행 서버로 전송하는 단계이다.

[0050] 상기 이체 승인 완료단계(S40)는 도 2에 도시된 바와 같이, 해당 캡차 선택공정(S41) 및 승인 정보 입력공정(S42)을 포함한다.

[0051] 상기 해당 캡차 선택공정(S41)은 사용자가 상기 이체 승인 요청 페이지에서 상기 이체 정보에 해당하는 캡차를 선택하는 공정이다.

[0052] 상기 해당 캡차 선택공정(S41)에서 사용자는 자신이 입력하였던 이체 정보에 해당하는 캡차 이미지를 마우스나 키보드를 이용하여 선택할 수 있다.

[0053] 상기 승인 정보 입력공정(S42)은 사용자가 상기 이체 승인 요청 페이지에서 승인 정보를 입력하여 상기 은행 서버에 전송하는 공정이다.

[0054] 이때, 상기 승인 정보는 서명, OTP나 보안카드의 정보, 인증서의 암호 등 다양한 정보가 포함될 수 있다.

[0055] 상기 계좌 이체 수행단계(S50)는 은행 서버가 상기 사용자가 선택한 캡차와 승인 정보를 확인하여 계좌 이체를 수행하는 단계이다.

[0056] 상기 계좌 이체 수행단계(S50)에서 은행 서버는 서명을 확인하고, 캡차 선택 정보가 올바르다면 이체를 수행한

다. 이때, 캡차 선택 정보는 캡차 이미지가 선택되는 순서를 포함한다.

[0057] 이상과 같이 본 발명에 따른 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법을 예시한 도면을 참조로 하여 설명하였으나, 본 명세서에 개시된 실시예와 도면에 의해 본 발명이 한정되는 것은 아니며, 본 발명의 기술사상 범위내에서 당업자에 의해 다양한 변형이 이루어질 수 있음은 물론이다.

도면의 간단한 설명

[0058] 도 1은 본 발명의 일 실시예에 따른 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법의 블록도.

[0059] 도 2는 본 발명의 일 실시예에 따른 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법 중 이체 승인 완료단계의 블록도.

[0060] 도 3은 본 발명의 일 실시예에 따른 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법에서 이체 승인 요청 페이지를 나타내는 도.

[0061] 도 4는 멀웨어 공격 예상 시나리오를 나타내는 도.

[0062] < 도면의 주요 부분에 대한 부호의 설명 >

[0063] S10:계좌 이체 준비단계

[0064] S20:이체 정보 전송단계

[0065] S30:이체 승인 요청단계

[0066] S40:이체 승인 완료단계

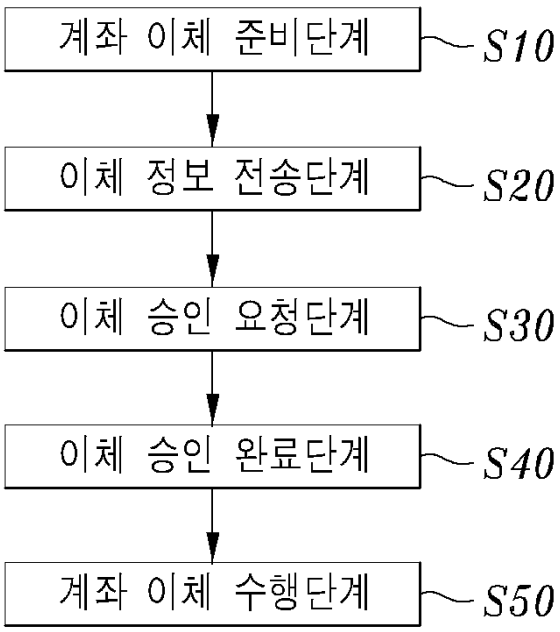
[0067] S41:해당 캡차 선택공정

[0068] S42:승인 정보 입력공정

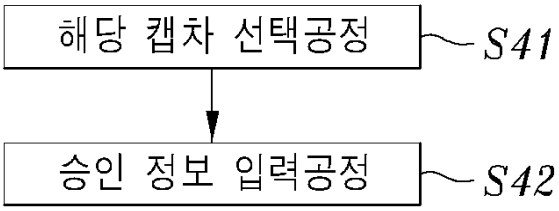
[0069] S50:계좌 이체 수행단계

도면

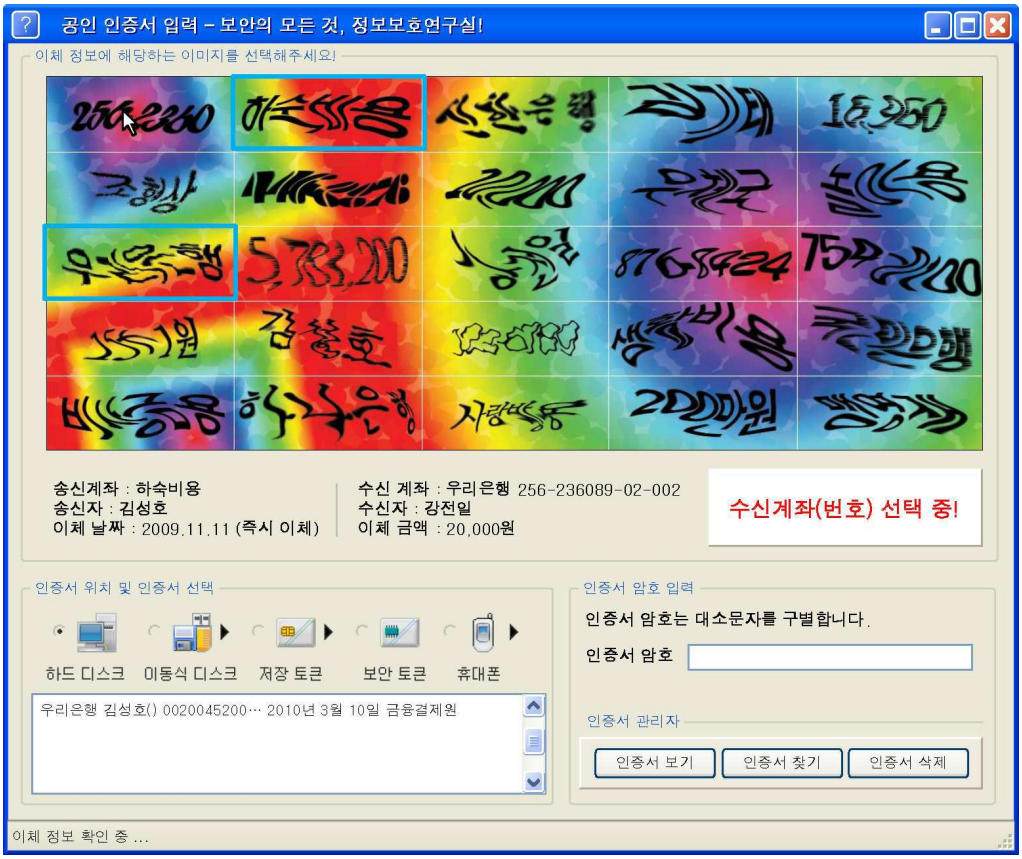
도면1



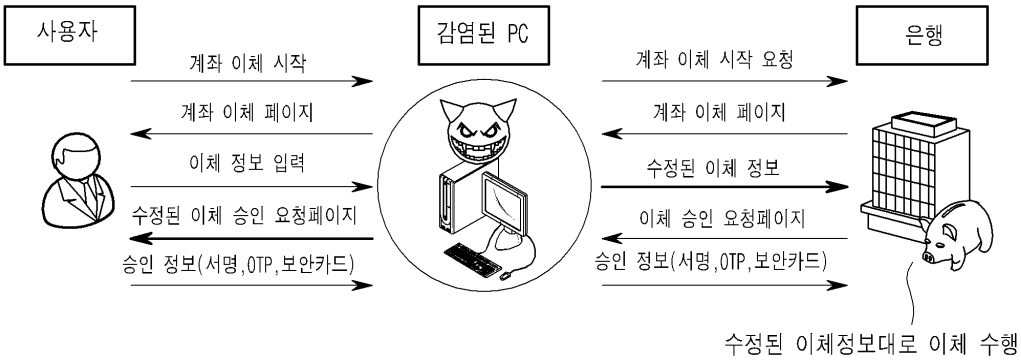
도면2


해당 캡차 선택공정
S41
승인 정보 입력공정
S42

도면3


공인 인증서 입력 – 보안의 모든 것, 정보보호연구실!
이체 정보에 해당하는 이미지를 선택해주세요!
송신계좌 : 하숙비용
송신자 : 김성호
이체 날짜 : 2009.11.11 (즉시 이체)
수신 계좌 : 우리은행 256-236089-02-002
수신자 : 강전일
이체 금액 : 20,000원
수신계좌(번호) 선택 중!
인증서 위치 및 인증서 선택
하드 디스크
이동식 디스크
저장 토큰
보안 토큰
휴대폰
우리은행 김성호() 0020045200… 2010년 3월 10일 금융결제원
인증서 암호 입력
인증서 암호는 대소문자를 구별합니다.
인증서 암호
인증서 관리자
인증서 보기
인증서 찾기
인증서 삭제
이체 정보 확인 중 …

도면4


사용자
감염된 PC
은행
계좌 이체 시작
계좌 이체 페이지
이체 정보 입력
수정된 이체 승인 요청페이지
승인 정보(서명,OTP,보안카드)
계좌 이체 시작 요청
계좌 이체 페이지
수정된 이체 정보
이체 승인 요청페이지
승인 정보(서명,OTP,보안카드)
수정된 이체정보대로 이체 수행