(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년11월12일
(11) 등록번호 10-1198716
(24) 등록일자 2012년11월01일

(51) 국제특허분류(Int. Cl.)
G06Q 20/00 (2008.03)
(21) 출원번호 10-2010-0090748
(22) 출원일자 2010년09월15일
심사청구일자 2010년09월15일
(65) 공개번호 10-2012-0028731
(43) 공개일자 2012년03월23일
(56) 선행기술조사문헌
JP2009064400 A*
KR1020070117420 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
양대헌
인천광역시 남구 소성로 71, 하이테크센터 317호 (용현동, 인하대학교)
맹영재
인천광역시 남구 소성로 71, 하이테크센터 307호 (용현동, 인하대학교)
(뒷면에 계속)
(74) 대리인
이원희

전체 청구항 수 : 총 10 항 심사관 : 박장환

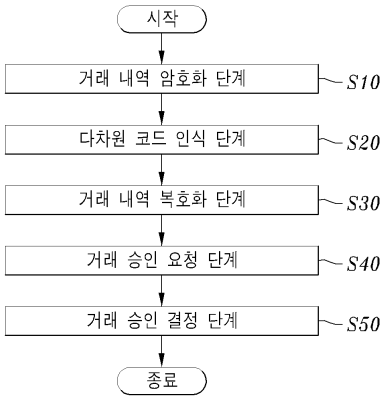
(54) 발명의 명칭 **다차원 코드를 이용한 전자금융거래 승인방법**

(57) 요 약

본 발명은 다차원 코드를 이용한 전자금융거래 승인방법에 관한 것으로, 해결하고자 하는 기술적 과제는 전자금융거래를 승인함에 있어서 사용자의 편의성을 향상시킬 수 있고 비용 부담을 감소시킬 수 있는 다차원 코드를 이용한 전자금융거래 승인방법을 제공하는데 있다.

이를 위해 본 발명에 따른 다차원 코드를 이용한 전자금융거래 승인방법은 서버가 거래 내역(T)을 암호화한 후 상기 거래 내역(T)의 암호값을 다차원 코드로 표현하여 클라이언트에게 전송하는 거래 내역 암호화 단계와, 사용자가 카메라가 구비된 단말기를 구동시키고 공인인증서 패스워드를 입력한 후 상기 카메라를 통하여 클라이언트로부터 수신된 다차원 코드를 인식하는 다차원 코드 인식 단계와, 상기 단말기가 상기 다차원 코드로 표현된 암호화된 거래 내역(T)을 복호화한 후 화면에 디스플레이하는 거래 내역 복호화 단계와, 사용자가 상기 거래 내역(T)을 확인하고 상기 서버로 승인을 요청하는 경우 상기 단말기가 사용자 응답의 해시값을 생성하고 상기 해시값을 암호화한 후 상기 서버에 전송하는 거래 승인 요청 단계 및 상기 서버가 수신된 사용자 응답의 해시값을 복호화하여 상기 사용자 응답의 해시값과 스스로 생성한 해시값을 비교한 후 거래의 정상 승인여부를 결정하는 거래 승인 결정 단계를 포함하는 것을 특징으로 한다.

대 표 도 - 도1



(72) 발명자

신동오

인천광역시 남구 소성로 71, 하이테크센터 307호
(용현동, 인하대학교)

변제성

인천광역시 남구 소성로 71, 하이테크센터 307호
(용현동, 인하대학교)

강전일

인천광역시 남구 소성로 71, 하이테크센터 307호
(용현동, 인하대학교)

김성호

인천광역시 남구 소성로 71, 하이테크센터 307호
(용현동, 인하대학교)

이 발명을 지원한 국가연구개발사업

과제고유번호	41473-01
부처명	교육과학기술부
연구사업명	기본연구
연구과제명	인지기반 온라인 금융 서비스와 DDoS 대응 시스템
주관기관	인하대학교
연구기간	2010.05.01 ~ 2013.04.30

특허청구의 범위

청구항 1

서버가 거래 내역(T)을 대칭키(k) 또는 공인인증서의 공개키(upk) 중 어느 하나를 사용하여 암호화한 후 상기 거래 내역(T)의 암호값을 QR 코드 또는 해독할 수 있는 임의의 이미지 파일로 이루어지는 다차원 코드로 표현하여 클라이언트에게 전송하는 거래 내역 암호화 단계;

사용자가 카메라가 구비된 단말기를 구동시키고 공인인증서 패스워드를 입력한 후 상기 카메라를 통하여 클라이언트로부터 수신된 다차원 코드를 인식하는 다차원 코드 인식 단계;

상기 단말기가 상기 다차원 코드로 표현된 암호화된 거래 내역(T)을, 대칭키(k) 또는 공인인증서의 공개키(upk) 중 어느 하나를 사용하여 복호화한 후 화면에 디스플레이하는 거래 내역 복호화 단계;

사용자가 상기 거래 내역(T)을 확인하고 상기 서버로 승인을 요청하는 경우 상기 단말기가 사용자 응답의 해시값을 생성하고 상기 해시값을 암호화한 후 상기 서버에 전송하는 거래 승인 요청 단계; 및

상기 서버가 수신된 사용자 응답의 해시값을 복호화하여 상기 사용자 응답의 해시값과 스스로 생성한 해시값을 비교한 후 거래의 정상 승인여부를 결정하는 거래 승인 결정 단계를 포함하는 것을 특징으로 하는 다차원 코드를 이용한 전자금융거래 승인방법.

청구항 2

제 1항에 있어서,

상기 거래 내역 암호화 단계는,

상기 거래 내역(T)을 임의로 생성한 대칭키(k)를 이용하여 암호화하는 경우,

상기 대칭키(k)를 사용자 공인인증서의 공개키(upk)를 이용하여 암호화한 후, 상기 거래 내역(T) 및 대칭키(k)의 암호값을 각각 다차원 코드로 표현하는 것을 특징으로 하는 다차원 코드를 이용한 전자금융거래 승인방법.

청구항 3

제 2항에 있어서,

상기 거래 내역 복호화 단계는,

상기 단말기가 사용자 공인인증서의 비밀키(usk)를 이용하여 상기 다차원 코드의 문자열 중 대칭키(k)를 복호화하고, 상기 대칭키(k)를 이용하여 상기 거래 내역(T)을 복호화한 후 화면에 디스플레이하는 것을 특징으로 하는 다차원 코드를 이용한 전자금융거래 승인방법.

청구항 4

제 1항에 있어서,

상기 거래 내역 암호화 단계는,

상기 거래 내역(T)을 사용자 공인인증서의 공개키(upk)를 이용하여 암호화한 후 다차원 코드로 표현하는 것을 특징으로 하는 다차원 코드를 이용한 전자금융거래 승인방법.

청구항 5

제 4항에 있어서,

상기 거래 내역 복호화 단계는,

상기 단말기가 사용자 공인인증서의 비밀키(usk)를 이용하여 상기 거래 내역(T)을 복호화한 후 화면에 디스플레이하는 것을 특징으로 하는 다차원 코드를 이용한 전자금융거래 승인방법.

청구항 6

제 1항에 있어서,

상기 거래 내역 암호화 단계는,

상기 서버와 단말기가 유효한 대칭키(k)를 공유하는 경우, 상기 거래 내역(T)을 대칭키(k)를 이용하여 암호화한 후 다차원 코드로 표현하는 것을 특징으로 하는 다차원 코드를 이용한 전자금융거래 승인방법.

청구항 7

제 6항에 있어서,

상기 거래 내역 복호화 단계는,

상기 단말기가 상기 대칭키(k)를 이용하여 상기 거래 내역(T)을 복호화한 후 화면에 디스플레이하는 것을 특징으로 하는 다차원 코드를 이용한 전자금융거래 승인방법.

청구항 8

제 1항에 있어서,

상기 거래 내역 복호화 단계는,

상기 사용자의 보안수단이 보안카드인 경우 보안카드에 대한 질문을 화면에 디스플레이하는 것을 특징으로 하는 다차원 코드를 이용한 전자금융거래 승인방법.

청구항 9

제 1항에 있어서,

상기 거래 승인 요청 단계는,

상기 사용자 응답의 해시값을 상기 서버의 공개키(spk)를 이용하여 암호화한 후 상기 서버에 전송하는 것을 특징으로 하는 다차원 코드를 이용한 전자금융거래 승인방법.

청구항 10

제 1항에 있어서,

상기 거래 승인 요청 단계는,

상기 사용자 응답의 해시값을 임의로 생성한 대칭키(k)를 이용하여 암호화한 후 상기 서버에 전송하는 것을 특징으로 하는 다차원 코드를 이용한 전자금융거래 승인방법.

청구항 11

삭제

청구항 12

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 다차원 코드를 이용한 전자금융거래 승인방법에 관한 것으로서 전자금융거래의 문서변조 공격에 대응할 수 있는 다차원 코드를 이용한 전자금융거래 승인방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로, 문서변조 공격은 문서에 대한 무결성이 제공되지 않을 때 가능한 공격으로 화면에는 사용자가 거래하고자 하는 화면을 보여주되 사용자가 입력하는 비밀은 건드리지 않은 상태에서 공격자의 의도대로 거래를 완료시키는 공격 방법이다.

[0003] 이는 사용자의 눈을 속인다는 점에서 피싱 또는 파밍과 비슷하다고 볼 수 있으나 비밀을 단순히 얻어내는 형태의 공격이 아니고 사용자의 의심 없이 입력된 비밀을 악용한다는 점에서 더욱 지능화된 공격이라 할 수 있다.

[0004] 도 4는 공격자가 문서를 위조하는 과정을 나타내는 도이다.

[0005] 공격자는 도 4에 도시된 바와 같이, 자신의 문서 위에 문서 원본 중 내용 부분만을 겹치도록 만들고 이렇게 변조된 문서를 사용자에게 보여준다. 이후, 문서의 내용에 이상이 없음을 확인한 사용자는 문서에 사인을 하게 되고, 사인된 문서를 받은 공격자는 겹친 부분을 떼어 내어 사용자가 사인한 위조된 문서를 가지게 된다.

[0006] 상술한 바와 같이, 문서변조 공격은 사용자 자신이 거래하고자 하는 내용을 눈으로 확인하고 비밀을 입력하기 때문에 공격자가 사용자의 눈을 속일 수 있으면 사용자의 의심 없이 비밀을 얻어낼 수 있는 문제점이 있다.

[0007] 이하, MITB(Man In The Browser) 공격에 대응하는 방법인 전화승인 서비스, 트랜잭션 서명기법, ZTIC, ArcotVPS, MS 워터 마크에 대해 설명한다.

[0008] 상기 전화승인 서비스는 사용자의 전화기와 그 통신 채널의 보안성에 의존하여 사용자가 구리선을 이용한 유선전화기를 사용하는 경우, 공격자가 ARS응답을 사용자 대신 할 수 있기 때문에 MITM 공격에 취약한 문제점이 있다.

[0009] 또한, 상기 트랜잭션 서명기법은 공인인증서를 사용하여 부인방지를 제공하나 추가적인 장치를 소지해야 하고 결과적으로 추가 발급된 장치의 보안성에 의존하여 사용자가 부분적인 거래 내역을 장치에 입력해야 하기 때문에 사용자 편리성이 부족한 문제점이 있다.

[0010] 더불어, 상기 ZTIC는 상기 트랜잭션 서명기법과 동일하게 추가적인 장치를 소지해야 하고 결과적으로 추가 발급된 장치의 보안성에 의존하며, 상기 ArcotVPS 및 MS 워터 마크은 캡차를 인식하고 사용자가 수동적으로 입력해야 하기 때문에 편의성이 높지 않은 문제점이 있다.

[0011] 한편, 특허출원번호 " 10-2009-0119805 " 로 출원된 " 문맥 기반의 캡차를 이용한 인터넷 계좌 이체 방법 " 에서는 사용자가 캡차를 읽고 입력하는 형태가 아닌 선택하는 용도로 사용하기 때문에 더욱 복잡도가 높은 캡차를 이용할 수 있으나, 공격자가 직접 공격에 실시간으로 참여하는 경우에는 캡차가 제 역할을 하지 못하기 때문에 보안성을 담보할 수 없고 사용자는 여러 개의 캡차를 인식해야 하기 때문에 편의성이 높지 않은 문제점이 있다.

발명의 내용

해결하려는 과제

[0012] 본 발명은 상기한 바와 같은 과제를 해결하기 위해 발명된 것으로, 전자금융거래를 승인함에 있어서 사용자의 편의성을 향상시킬 수 있고 비용 부담을 감소시킬 수 있는 다차원 코드를 이용한 전자금융거래 승인방법을 제공하는데 그 목적이 있다.

과제의 해결 수단

[0013] 상기한 바와 같은 목적을 달성하기 위해 본 발명에 따른 다차원 코드를 이용한 전자금융거래 승인방법은 서버가 거래 내역(T)을 암호화한 후 상기 거래 내역(T)의 암호값을 다차원 코드로 표현하여 클라이언트에게 전송하는 거래 내역 암호화 단계와, 사용자가 카메라가 구비된 단말기를 구동시키고 공인인증서 패스워드를 입력한 후 상기 카메라를 통하여 클라이언트로부터 수신된 다차원 코드를 인식하는 다차원 코드 인식 단계와, 상기 단말기가 상기 다차원 코드로 표현된 암호화된 거래 내역(T)을 복호화한 후 화면에 디스플레이하는 거래 내역 복호화 단계와, 사용자가 상기 거래 내역(T)을 확인하고 상기 서버로 승인을 요청하는 경우 상기 단말기가 사용자 응답의 해시값을 생성하고 상기 해시값을 암호화한 후 상기 서버에 전송하는 거래 승인 요청 단계 및 상기 서버가 수신된 사용자 응답의 해시값을 복호화하여 상기 사용자 응답의 해시값과 스스로 생성한 해시값을 비교한 후 거래의 정상 승인여부를 결정하는 거래 승인 결정 단계를 포함하는 것을 특징으로 한다.

[0014] 또한, 상기 거래 내역 암호화 단계는 상기 거래 내역(T)을 임의로 생성한 대칭키(k)를 이용하여 암호화하고, 상기 대칭키(k)를 사용자 공인인증서의 공개키(upk)를 이용하여 암호화한 후, 상기 거래 내역(T) 및 대칭키(k)의 암호값을 각각 다차원 코드로 표현할 수 있다. 이때, 상기 거래 내역 복호화 단계는 상기 단말기가 사용자 공인인증서의 비밀키(usk)를 이용하여 상기 다차원 코드의 문자열 중 대칭키(k)를 복호화하고, 상기 대칭키(k)를 이용하여 상기 거래 내역(T)을 복호화한 후 화면에 디스플레이할 수 있다.

[0015] 또한, 상기 거래 내역 암호화 단계는 상기 거래 내역(T)을 사용자 공인인증서의 공개키(upk)를 이용하여 암호화한 후 다차원 코드로 표현할 수 있다. 이때, 상기 거래 내역 복호화 단계는 상기 단말기가 사용자 공인인증서의 비밀키(usk)를 이용하여 상기 거래 내역(T)을 복호화한 후 화면에 디스플레이할 수 있다.

[0016] 또한, 상기 거래 내역 암호화 단계는 상기 서버와 단말기가 유효한 대칭키(k)를 공유하는 경우, 상기 거래 내역(T)을 대칭키(k)를 이용하여 암호화한 후 다차원 코드로 표현할 수 있다. 이때, 상기 거래 내역 복호화 단계는 상기 단말기가 상기 대칭키(k)를 이용하여 상기 거래 내역(T)을 복호화한 후 화면에 디스플레이할 수 있다.

[0017] 또한, 상기 거래 내역 복호화 단계는 상기 사용자의 보안수단이 보안카드인 경우 보안카드에 대한 질문을 화면에 디스플레이할 수 있다.

[0018] 또한, 상기 거래 승인 요청 단계는 상기 사용자 응답의 해시값을 상기 서버의 공개키(spk)를 이용하여 암호화한 후 상기 서버에 전송할 수 있다.

[0019] 또한, 상기 거래 승인 요청 단계는 상기 사용자 응답의 해시값을 임의로 생성한 대칭키(k)를 이용하여 암호화한 후 상기 서버에 전송할 수 있다.

[0020] 또한, 상기 다차원 코드는 QR 코드로 이루어질 수 있다.

[0021] 또한, 상기 다차원 코드는 해독할 수 있는 임의의 이미지 파일로 이루어질 수 있다.

발명의 효과

[0022] 상기한 바와 같이 본 발명에 따른 다차원 코드를 이용한 전자금융거래 승인방법에 의하면, 보급률이 뛰어난 휴대용 단말기를 이용하여 전자금융거래 승인을 할 수 있으므로 추가적인 장치의 발급이 필요하지 않아 비용 부담을 감소시키고 거래 내역 확인 후 승인 여부만을 결정하면 되기 때문에 사용자 편의성을 향상시키는 효과가 있다.

도면의 간단한 설명

[0023] 도 1은 본 발명의 일 실시예에 따른 다차원 코드를 이용한 전자금융거래 승인방법의 블록도.

도 2는 본 발명의 일 실시예에 따라 다차원 코드인 QR 코드를 이용하여 전자금융거래를 승인하는 과정을 나타내는 도.

도 3은 본 발명의 일 실시예에 따라 사용자가 단말기의 화면을 통해 거래 내역을 확인하는 모습을 나타내는 도.

도 4는 공격자가 문서를 위조하는 과정을 나타내는 도.

발명을 실시하기 위한 구체적인 내용

[0024] 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.

[0025] 도 1은 본 발명의 일 실시예에 따른 다차원 코드를 이용한 전자금융거래 승인방법의 블록도이다.

[0026] 본 발명의 일 실시예에 따른 다차원 코드를 이용한 전자금융거래 승인방법은 도 1에 도시된 바와 같이, 거래 내역 암호화 단계(S10)와, 다차원 코드 인식 단계(S20)와, 거래 내역 복호화 단계(S30)와, 거래 승인 요청 단계(S40) 및 거래 승인 결정 단계(S50)를 포함한다.

[0027] 도 2는 본 발명의 일 실시예에 따라 다차원 코드인 QR 코드를 이용하여 전자금융거래를 승인하는 과정을 나타내는 도이다.

[0028] 상기 거래 내역 암호화 단계(S10)는 도 2에 도시된 바와 같이, 서버가 거래 내역(T)을 암호화한 후 상기 거래 내역(T)의 암호값을 다차원 코드로 표현하여 클라이언트에게 전송하는 단계로, 상기 다차원 코드는 QR 코드로 이루어지거나 해독할 수 있는 임의의 이미지 파일로 이루어질 수 있다.

[0029] 상기 거래 내역(T)은 전자금융거래의 종류에 따라 다양해질 수 있는데, 예를 들면, 전자금융거래가 인터넷뱅킹 계좌이체인 경우 상기 거래 내역(T)은 이체금액, 수신자 은행명, 수신자 계좌번호, 수신자명 등이 될 수 있고, 전자금융거래가 주식거래인 경우 상기 거래 내역(T)은 종목명, 종목코드, 주문유형, 주문수량, 주문단가, 수수료 등이 될 수 있으며, 전자금융거래가 전자결제인 경우 상기 거래 내역(T)은 품목명, 가격, 수량, 구매옵션 등이 될 수 있다.

[0030] 상술한 바와 같이, 전자금융거래의 종류에 따른 거래내역과 암호화할 데이터는 하기의 [표 1]와 같다.

표 1

전자금융거래	거래내역 T	
인터넷뱅킹 계좌이체	거래내역	이체금액, 수신자 은행명, 수신자 계좌번호, 수신자명 등
	추가정보	사용자의 보안수단이 보안카드인 경우 이를 사용하기 위한 질문 (수신자가 정보제공에 동의한 경우)수신자에 대한정보가 서버에 존재하는 경우 수신자를 식별할 수 있는 부분정보(전화번호, 이메일 주소 등)
주식거래	거래내역	종목명, 종목코드, 주문유형, 주문수량, 주문단가, 수수료 등
	추가정보	거래하고자 하는 주식의 CI(Company Identity)
전자결제	거래내역	품목명, 가격, 수량, 구매옵션 등
	추가정보	품목의 이미지 또는 품목의 브랜드 이미지

[0031]

[0032] 상기 거래 내역 암호화 단계(S10)는 상기 거래 내역(T)을 임의로 생성한 대칭키(k)를 이용하여 암호화하고, 상기 대칭키(k)를 사용자 공인인증서의 공개키(upk)를 이용하여 암호화한 후, 상기 거래 내역(T) 및 대칭키(k)의 암호값을 각각 다차원 코드로 표현하여 상기 클라이언트에게 전송할 수 있다.

[0033] 또한, 상기 거래 내역 암호화 단계(S10)는 상기 거래 내역(T)을 사용자 공인인증서의 공개키(upk)를 이용하여 암호화한 후 다차원 코드로 표현하여 상기 클라이언트에게 전송할 수 있다.

[0034] 즉, 상기 거래 내역 암호화 단계(S10)에서는 상기 거래 내역(T)을 임의로 생성한 대칭키(k)를 이용하여 암호화하지 않고 단순히 사용자 공인인증서의 공개키(upk)만을 이용하여 암호화할 수 있다.

[0035] 더불어, 상기 거래 내역 암호화 단계(S10)는 상기 서버와 단말기가 유효한 대칭키(k)를 공유하는 경우, 상기 거래 내역(T)을 대칭키(k)를 이용하여 암호화한 후 다차원 코드로 표현하여 상기 클라이언트에게 전송할 수 있다.

[0036] 즉, 상기 거래 내역 암호화 단계(S10)에서는 상기 거래 내역(T)을 임의로 생성한 대칭키(k)를 이용하여 암호화하지 않고 사전에 서버와 단말기 사이에 유효한 대칭키(k)를 공유한 다음 상기 거래 내역(T)을 대칭키(k)를 이용하여 암호화할 수 있다.

[0037] 상기 다차원 코드 인식 단계(S20)는 사용자가 카메라가 구비된 단말기를 구동시키고 공인인증서 패스워드를 입력한 후 상기 카메라를 통하여 클라이언트로부터 수신된 다차원 코드를 인식하는 단계이다.

[0038] 구체적으로, 사용자는 상기 다차원 코드 인식 단계(S10)에서 카메라가 달리 단말기(예를 들면, 휴대폰)의 프로그램(예를 들면, 스마트폰의 경우 앱)을 구동시키고, 공인인증서 패스워드를 입력한 이후에 카메라를 통해 상기 다차원 코드를 인식할 수 있다.

[0039] 일반적으로, 거래 내역을 사용자에게 전달하는 방법은 사람이 직접 개입되는 과정이니 만큼 최대한 인식능력을 이용하도록 할 수 있는데, 여기서 인식능력이란 사람의 이미지를 읽는 능력을 의미하며 문자열을 읽는 것보다 이미지를 인식하는 것이 더 편리하다는 사실에 기초한다.

[0040] 예를 들어, 인터넷뱅킹 계좌이체의 경우, 수신자의 전화번호를 거래 내역에 포함시켜 단말기에 전송하면 이 전화번호를 통해 단말기에 등록되어 있는 수신자의 사진을 보여주어 사용자에게 수신자를 인식하도록 유도할 수 있고, 추가 정보가 이미지인 경우에는 이미지를 문자열로 인코딩하여 전송할 수 있다.

[0041] 상기 거래 내역 복호화 단계(S30)는 상기 단말기가 상기 다차원 코드로 표현된 암호화된 거래 내역(T)을 복호화

한 후 화면에 디스플레이하는 단계로, 상기 사용자의 보안수단이 보안카드인 경우 보안카드에 대한 질문을 화면에 디스플레이할 수 있다.

[0042] 구체적으로, 상기 거래 내역 암호화 단계(S10)가 상술한 바와 같이, 거래 내역(T)을 대칭키(k)를 이용하여 암호화하고 상기 대칭키(k)를 사용자 공인인증서의 공개키(upk)를 이용하여 암호화한 후 상기 거래 내역(T) 및 대칭키(k)의 암호값을 각각 다차원 코드로 표현한 경우에, 상기 거래 내역 복호화 단계(S30)는 상기 단말기가 사용자 공인인증서의 비밀키(usk)를 이용하여 상기 다차원 코드의 문자열 중 대칭키(k)를 복호화하고, 상기 대칭키(k)를 이용하여 상기 거래 내역(T)을 복호화한 후 화면에 디스플레이할 수 있다. 이때, 상기 거래 내역(T)에 이미지가 포함되어 있다면 이미지 또한 디스플레이할 수 있다.

[0043] 또한, 상기 거래 내역 암호화 단계(S10)가 상술한 바와 같이, 상기 거래 내역(T)을 사용자 공인인증서의 공개키(upk)를 이용하여 암호화한 후 다차원 코드로 표현한 경우에, 상기 거래 내역 복호화 단계(S30)는 상기 단말기가 사용자 공인인증서의 비밀키(usk)를 이용하여 상기 거래 내역(T)을 복호화한 후 화면에 디스플레이할 수 있다.

[0044] 더불어, 상기 거래 내역 암호화 단계(S10)가 상술한 바와 같이, 상기 서버와 단말기가 유효한 대칭키(k)를 사전에 공유한 후 상기 거래 내역(T)을 대칭키(k)를 이용하여 암호화한 다음 다차원 코드로 표현한 경우, 상기 거래 내역 복호화 단계(S30)는 상기 단말기가 상기 대칭키(k)를 이용하여 상기 거래 내역(T)을 복호화한 후 화면에 디스플레이할 수 있다.

[0045] 도 3은 본 발명의 일 실시예에 따라 사용자가 단말기의 화면을 통해 거래 내역을 확인하는 모습을 나타내는 도이다.

[0046] 상기 거래 승인 요청 단계(S40)는 사용자가 도 3에 도시된 바와 같이, 상기 거래 내역(T)을 확인하고 상기 서버로 승인을 요청하는 경우 상기 단말기가 사용자 응답의 해시값을 생성하고 상기 해시값을 암호화한 후 상기 서버에 전송하는 단계이다.

[0047] 구체적으로, 상기 거래 승인 요청 단계(S40)에서는 상기 단말기가 상기 사용자 응답의 해시값을 상기 서버의 공개키(spk)를 이용하여 암호화한 후 상기 서버에 전송하거나, 상기 서버의 공개키(spk)를 이용하지 않는 환경이라면 임의로 생성한 대칭키(k)를 이용하여 상기 사용자 응답의 해시값을 암호화한 후 상기 서버에 전송할 수 있다. 이때, 사용자의 보안수단(보안카드 또는 One Time Password)이 있는 경우, 사용자의 응답은 해당 보안수단이 될 수 있다.

[0048] 상기 거래 승인 결정 단계(S50)는 상기 서버가 수신된 사용자 응답의 해시값을 복호화하여 상기 사용자 응답의 해시값과 스스로 생성한 해시값을 비교한 후 거래의 정상 승인여부를 결정하는 단계이다.

[0049] 상술한 바와 같이, 본 발명은 MITB 공격에 대응하기 위해 다차원 코드를 활용하여 승인과정을 안전하게 한 보안방법으로, 전자금융거래 승인을 위해 보급률이 높은 휴대용 단말기를 이용하므로 추가적인 장치 발급으로 인한 비용 부담이 없고, 다차원 코드 인식을 통해 거래 내역을 단말기로 전달하기 때문에 사용자 편의성이 높은 장점이 있다.

[0050] 이상과 같이 본 발명에 따른 다차원 코드를 이용한 전자금융거래 승인방법을 예시한 도면을 참조로 하여 설명하였으나, 본 명세서에 개시된 실시예와 도면에 의해 본 발명이 한정되는 것은 아니며, 본 발명의 기술사상 범위 내에서 당업자에 의해 다양한 변형이 이루어질 수 있음은 물론이다.

부호의 설명

[0051] S10:거래 내역 암호화 단계

S20:다차원 코드 인식 단계

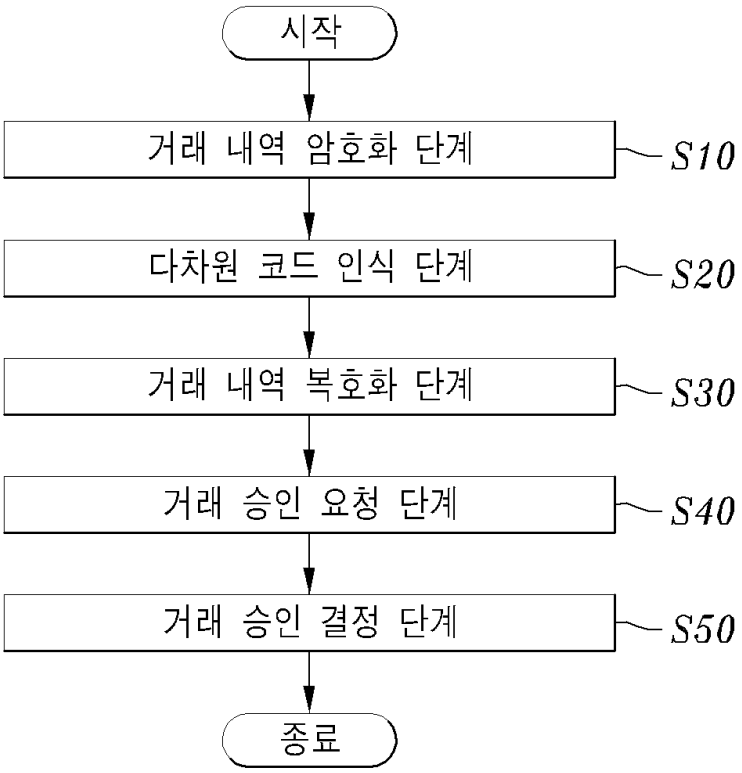
S30:거래 내역 복호화 단계

S40:거래 승인 요청 단계

S50:거래 승인 결정 단계

도면

도면1



도면2


T : 거래내역, H : 일방향 해시함수
upk, usk : 사용자의 공개키 및 비밀키
spk, ssk : 서버의 공개키 및 비밀키
사용자
공인인증서 패스워드
T_e, k_e = Decode(QR);
k= Dec_{usk}(k_e);
T = Dec_k(T_e);
거래내역 T
보안카드 또는 OTP
휴대폰
QR code
클라이언트
QR code
서버
k= Rand();
T_e = Enc_k(T);
k_e = Enc_{upk}(k);
QR = Encode(T_e, k_e);
Enc_{spk}(H_k(보안카드 또는 OTP))
ssk로 복호화
보안카드 또는 OTP를
생성, 해시 후 비교
데이터의 간접적인 전달
데이터의 직접적인 전달

도면3


3,500
신동오
우리은행
235-346346-62-235
3,500
신동오
slide to confirm

도면4


문서원본
위조된 문서
변조된 문서와
사용자의 사인
사인된
공격자의
위조된 문서