



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년05월11일
(11) 등록번호 10-1033973
(24) 등록일자 2011년05월02일

(51) Int. Cl.

H04W 12/06 (2009.01) H04L 9/32 (2006.01)

(21) 출원번호 10-2009-0029447

(22) 출원일자 2009년04월06일

심사청구일자 2009년04월06일

(65) 공개번호 10-2010-0111069

(43) 공개일자 2010년10월14일

(56) 선행기술조사문헌

KR1020060092472 A*

KR1020060036279 A

KR1020070080021 A

KR1020060131155 A

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

인하대학교 산학협력단

인천 남구 용현동 253 인하대학교

(72) 발명자

양대현

서울 서초구 서초동 삼풍 APT 3동 405호

강전일

충남 공주시 옥룡동 284-1번지

맹영재

서울시 광진구 자양1동 226-12호

(74) 대리인

이원희

전체 청구항 수 : 총 9 항

심사관 : 이현규

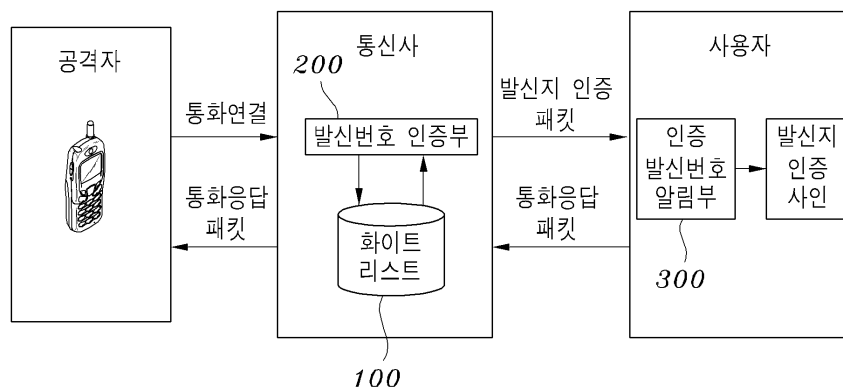
(54) 화이트 리스트를 이용한 보이스 피싱 방지 시스템 및 방법

(57) 요약

본 발명은 화이트 리스트를 이용한 보이스 피싱 방지 시스템 및 방법에 관한 것으로, 해결하고자 하는 기술적 과제는 사용자가 보이스 피싱에 속지 않고 스스로 통화의 진위여부를 판단할 수 있도록 하는 보이스 피싱 방지 시스템 및 방법을 제공하는데 그 목적이 있다.

이를 위해 본 발명에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템은 기관들의 전화번호가 저장되어 유지되는 화이트 리스트와, 상기 화이트 리스트 상의 전화번호와 발신지의 발신번호를 비교하되 상기 발신번호가 상기 화이트 리스트 상의 전화번호와 동일하면 발신지 인증 패킷을 수신자 단말기에 전송하는 발신번호 인증부 및 상기 발신지 인증 패킷에 대응하는 발신지 인증 사인을 상기 수신자 단말기에 전달하는 인증발신번호 알람부를 포함하는 것을 특징으로 한다.

대표도 - 도2



특허청구의 범위

청구항 1

기관들의 전화번호가 저장되어 유지되는 화이트 리스트;

상기 화이트 리스트 상의 전화번호와 발신지의 발신번호를 비교하되, 상기 발신번호가 상기 화이트 리스트 상의 전화번호와 동일하면 발신지 인증 패킷을 수신자 단말기에 전송하는 발신번호 인증부; 및

상기 발신지 인증 패킷에 대응하는 발신지 인증 사인을 상기 수신자 단말기에 전달하는 인증발신번호 알림부를 포함하고,

상기 발신지 인증 사인은 디스플레이 장치를 이용한 텍스트나, 아이콘 또는 애니메이션으로 이루어지거나, 진동으로 이루어지거나, 음향으로 이루어지는 것을 특징으로 하는 화이트 리스트를 이용한 보이스 피싱 방지 시스템.

청구항 2

기관들의 전화번호가 저장되어 유지되는 화이트 리스트;

상기 화이트 리스트 상의 전화번호와 수신지의 수신번호를 비교하되, 상기 수신번호가 상기 화이트 리스트 상의 전화번호와 동일하면 수신지 인증 패킷을 발신자 단말기에 전송하는 수신번호 인증부; 및

상기 수신지 인증 패킷에 대응하는 수신지 인증 사인을 상기 발신자 단말기에 전달하는 인증수신번호 알림부를 포함하는 것을 특징으로 하는 화이트 리스트를 이용한 보이스 피싱 방지 시스템.

청구항 3

제 2항에 있어서,

상기 수신지 인증 사인은 디스플레이 장치를 이용한 텍스트나, 아이콘 또는 애니메이션으로 이루어지는 것을 특징으로 하는 화이트 리스트를 이용한 보이스 피싱 방지 시스템.

청구항 4

제 2항에 있어서,

상기 수신지 인증 사인은 진동으로 이루어지는 것을 특징으로 하는 화이트 리스트를 이용한 보이스 피싱 방지 시스템.

청구항 5

제 2항에 있어서,

상기 수신지 인증 사인은 음향으로 이루어지는 것을 특징으로 하는 화이트 리스트를 이용한 보이스 피싱 방지 시스템.

청구항 6

발신지의 발신번호와 화이트 리스트 상의 전화번호를 비교하여 동일 여부를 판단하는 발신번호 판단단계;

상기 발신번호가 상기 화이트 리스트 상의 전화번호와 동일하면 발신지 인증 패킷을 수신자 단말기에 전송하는 발신번호 인증단계; 및

상기 발신지 인증 패킷에 대응하는 발신지 인증 사인을 상기 수신자 단말기에 전달하는 인증발신번호 알림단계를 포함하고,

상기 인증발신번호 알림단계의 발신지 인증 사인은 디스플레이 장치를 이용한 텍스트나, 아이콘 또는 애니메이션으로 이루어지거나, 진동으로 이루어지거나, 음향으로 이루어지는 것을 특징으로 하는 화이트 리스트를 이용한 보이스 피싱 방지 방법.

청구항 7

제 6항에 있어서,

상기 발신번호 판단단계 이전에 기관들의 변경되거나 추가된 전화번호를 상기 화이트 리스트 상에 업데이트하는 화이트 리스트 업데이트단계를 포함하는 것을 특징으로 하는 화이트 리스트를 이용한 보이스 피싱 방지 방법.

청구항 8

수신지의 수신번호와 화이트 리스트 상의 전화번호를 비교하여 동일 여부를 판단하는 수신번호 판단단계;

상기 수신번호가 상기 화이트 리스트 상의 전화번호와 동일하면 수신지 인증 패킷을 발신자 단말기에 전송하는 수신번호 인증단계; 및

상기 수신지 인증 패킷에 대응하는 수신지 인증 사인을 상기 발신자 단말기에 전달하는 인증수신번호 알림단계를 포함하는 것을 특징으로 하는 화이트 리스트를 이용한 보이스 피싱 방지 방법.

청구항 9

제 8항에 있어서,

상기 수신번호 판단단계 이전에 기관들의 변경되거나 추가된 전화번호를 상기 화이트 리스트 상에 업데이트하는 화이트 리스트 업데이트단계를 포함하는 것을 특징으로 하는 화이트 리스트를 이용한 보이스 피싱 방지 방법.

명세서

발명의 상세한 설명

기술분야

[0001] 본 발명은 화이트 리스트를 이용한 보이스 피싱 방지 시스템 및 방법에 관한 것으로서, 보이스 피싱으로 인한 피해를 방지할 수 있는 화이트 리스트를 이용한 보이스 피싱 방지 시스템 및 방법에 관한 것이다.

배경기술

[0002] 피싱은 일반 사용자들의 보안의식이 높지 않다는 사실에서 시작한다. 전화상으로 이루어지는 보이스 피싱은 발신자인 공격자가 전화상으로 유명한 기관, 예를 들어, 은행이나, 우체국 등이라고 밝혔을 때, 이를 사용자가 의심 없이 받아들이는 것이다. 이러한 형태는 해당 기관의 내부 보안수준과는 관계없이 외부에서 사용자를 속이는 공격 방법이다.

[0003] 공격자가 사용자를 속이는 과정은 매우 간단하다. 즉, 전화를 걸고, 어떤 기관임을 사칭하며 소개하는 것이 사용자를 속이는 과정의 전부이다. 사용자의 전화기에 발신지의 전화번호가 표시되기는 하지만 이 번호가 진정으로 해당 기관의 전화번호인지는 모르는 것이다.

[0004] 이처럼, 상기 보이스 피싱은 생각해내기 쉽고 공격에 소요되는 비용도 저렴한 만큼 공격자의 접근성이 좋은 공격 방법이지만, 아직까지 보이스 피싱에 대한 적절한 대응책은 찾아보기 힘들다. 그 때문에 보이스 피싱은 보안기술이 발달한 오늘날에도 오히려 그 피해 사례가 증가하고 있다.

[0005] 도 6에 도시된 바와 같이, 2009년 3월 경찰청의 자료에 따르면 최근 2년 6개월 동안 보이스 피싱 발생 건수는 513%가 증가했고, 그 피해액도 748%가 증가한 것으로 분석되었다. 보이스 피싱 발생 대비 검거율은 2006년 52.6%에서 2007년 69.4%로 다소 증가했다가 2008년 64.8%로 다시 감소세로 돌아섰다.

[0006] 이 통계를 미루어보아 지능화되는 보이스 피싱 수법에 대한 경찰이 대응이 미흡하다고 추정이 가능하다. 실제로, 최근에 발생한 공문서 위조를 이용한 보이스 피싱과 유괴를 가장한 보이스 피싱은 그 방법이 점차 지능

화되고 있다는 것을 보여준다.

- [0007] 또한, 2008년에는 노인만을 대상으로 한 보이스 피싱 일당이 적발된 사례가 있었다. 노인의 경우 타 계층에 비해 상대적으로 낮은 교육 수준, 심리적 불안, 신체적 노쇠 등으로 대응 능력이 부족해 피해가 발생해도 적극적으로 대처하지 못하는 경향이 있다는 점을 악용한 것이다. 이 일당에게 피해를 본 노인들 가운데는 평생 모은 재산을 한꺼번에 빼앗긴 사례도 적지 않아서 보이스 피싱의 대책이 일반적인 교육 수준에서 머무르면 이와 같은 피해사례가 줄어들지 않을 수 있다는 것을 보여준다.
- [0008] 도 7에 도시된 바와 같이, 2008년 경기도내 노인 782명을 상대로 노인 소비실태에 대한 설문조사를 벌인 결과 응답자 중 37.5%가 보이스피싱 사기를 접했으며 임시매장 상술, 무료관광 상술 등에 속아 제품을 구입한 경험도 각각 36.8%, 32.6%에 달했다.
- [0009] 보이스 피싱이 가능한 이유는 지인을 제외한 상대방에 대한 인증이 간단한 pretexting에만 의존하고 있기 때문이다. 공격자는 속이는 성공률을 높이기 위해서 상대방에 대한 전화기록, 신용카드 내역, 각종 고지서, 프로젝트와 관련된 정보 등을 다양한 경로를 통해 입수하고 이를 pretexting에 활용할 수 있다.
- [0010] 이때, 피해자와 공격자 사이에는 팬옵티콘(panopticon)이 발생하게 되어 피해자는 공격자가 어떤 정보를 요구하는 행위에 대해 의심을 하지 않게 되는 것이다.
- [0011] 유출된 개인정보가 보이스 피싱에 악용된다는 점을 우려하여 KISA는 2007년에 보이스피싱 피해 예방 10계명을 제시하였다. 하지만 우리의 실생활에서 개인정보는 빈번히 노출되어 있는 실정이다. 길거리에 주차되어 있는 차에서 그 예를 어렵지 않게 찾아볼 수 있다. 주차된 자동차를 통해서 차량의 모델, 차번호, 주차와 관련된 연락을 받기 위해 차 주인이 남겨놓은 전화번호를 얻을 수 있고, 차가 주차된 곳이 주택가일 경우에는 차 주인의 집 주소를 추가로 예측할 수 있다.
- [0012] 또한, 집으로 배달되는 각종 고지서도 개인정보를 얻어내기에 충분하며, 기관을 대상으로 하는 보이스 피싱을 이용하여 개인정보를 얻어낼 수도 있다. 기관에서 물어보는 몇 개의 질문을 통과하면 그것이 가능해 지는데, 그 질문들은 주민등록번호나 전화번호, 주소 등으로 비교적 알아내기 어렵지 않은 정보들이다.
- [0013] 지금처럼 개인정보가 인증의 수단으로 사용되는 방법으로는 적절한 인증체계를 구축하는 것이 쉽지 않다. 공격자의 개인정보 수집단계에 대한 대응방법이 개개인의 보안의식에 의존하고 있으며 이는 잠재적으로 노출될 가능성이 있기 때문이다.
- [0014] 개인정보가 노출되는 것을 방지하기 위해서 극단적으로는 암호 프로토콜의 적용을 생각해 볼 수 있다. 모든 정보들에 대한 권한을 설정하고 어떤 정보에 대한 요구가 있을 때 매번 접근 권한을 확인하는 것이다. 하지만 어떤 정보가 요구될지 모르는 상태에서 정보들에 대한 권한을 정의한다고 하는 것은 모순이 될 수 있고 사람들에게 매번 암호확적인 응답을 강요하는 단계도 현실적이지 않다.
- [0015] 개인정보를 이용한 pretexting 이외에 다른 인증방법이 실생활에 이용되고 있다. 발신지 전화번호 표시가 그것이다. 하지만 지금의 발신지 전화번호에 대한 인증은 순전히 개개인의 몫으로만 유지되고 있다. 그것도 어떤 한 기관이 사용자에게 자주 발신하는 등의 경로를 통해 사전에 사용자의 신뢰를 얻고, 사용자가 그 번호를 외우고 있는 경우로 국한된다.
- [0016] 사람이 모든 중요 기관들에 대한 번호를 사전에 기억하고 있는 것은 불가능하기 때문에 전화번호 자체를 이용한 인증은 한계가 존재한다.

발명의 내용

해결 하고자하는 과제

- [0017] 본 발명은 상기한 바와 같은 문제를 해결하기 위해 안출된 것으로, 사용자가 보이스 피싱에 속지 않고 스스로 통화의 진위여부를 판단할 수 있도록 하는 보이스 피싱 방지 시스템 및 방법을 제공하는데 그 목적이 있다.
- [0018] 본 발명의 다른 목적은, 공격자에 의한 통화 연결시 사용자가 발신번호를 확인하는 과정에서 발신기관의 진위여부를 판단할 수 있도록 하는 보이스 피싱 방지 시스템 및 방법을 제공하는 것이다.
- [0019] 본 발명의 또 다른 목적은, 사용자에게 의한 통화 연결시 사용자가 수신번호를 확인하는 과정에서 수신기관의 진위여부를 판단할 수 있도록 하는 보이스 피싱 방지 시스템 및 방법을 제공하는 것이다.

과제 해결수단

- [0020] 상기한 바와 같은 목적을 달성하기 위해 본 발명에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템은 기관들의 전화번호가 저장되어 유지되는 화이트 리스트와, 상기 화이트 리스트 상의 전화번호와 발신지의 발신번호를 비교하되 상기 발신번호가 상기 화이트 리스트 상의 전화번호와 동일하면 발신지 인증 패킷을 수신자 단말기에 전송하는 발신번호 인증부 및 상기 발신지 인증 패킷에 대응하는 발신지 인증 사인을 상기 수신자 단말기에 전달하는 인증발신번호 알림부를 포함하는 것을 특징으로 한다.
- [0021] 또한, 상기 발신지 인증 사인은 디스플레이 장치를 이용한 텍스트나, 아이콘 또는 애니메이션 등으로 이루어질 수 있다.
- [0022] 또한, 상기 발신지 인증 사인은 진동으로 이루어질 수 있다.
- [0023] 또한, 상기 발신지 인증 사인은 음향으로 이루어질 수 있다.
- [0024] 또한, 본 발명에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템은 기관들의 전화번호가 저장되어 유지되는 화이트 리스트와, 상기 화이트 리스트 상의 전화번호와 수신지의 수신번호를 비교하되 상기 수신번호가 상기 화이트 리스트 상의 전화번호와 동일하면 수신지 인증 패킷을 발신자 단말기에 전송하는 수신번호 인증부 및 상기 수신지 인증 패킷에 대응하는 수신지 인증 사인을 상기 발신자 단말기에 전달하는 인증수신번호 알림부를 포함할 수 있다. 이때, 상기 수신지 인증 사인은 디스플레이 장치를 이용한 텍스트나, 아이콘 또는 애니메이션 등으로 이루어질 수 있고, 진동으로 이루어질 수 있으며, 음향으로 이루어질 수 있다.
- [0025] 또한, 본 발명에 따른 화이트 리스트를 이용한 보이스 피싱 방지 방법은 발신지의 발신번호와 화이트 리스트 상의 전화번호를 비교하여 동일 여부를 판단하는 발신번호 판단단계와, 상기 발신번호가 상기 화이트 리스트 상의 전화번호와 동일하면 발신지 인증 패킷을 수신자 단말기에 전송하는 발신번호 인증단계 및 상기 발신지 인증 패킷에 대응하는 발신지 인증 사인을 상기 수신자 단말기에 전달하는 인증발신번호 알림단계를 포함할 수 있다.
- [0026] 또한, 상기 발신번호 판단단계 이전에 기관들의 변경되거나 추가된 전화번호를 상기 화이트 리스트 상에 업데이트하는 화이트 리스트 업데이트단계를 포함할 수 있다.
- [0027] 또한, 본 발명에 따른 화이트 리스트를 이용한 보이스 피싱 방지 방법은 수신지의 수신번호와 화이트 리스트 상의 전화번호를 비교하여 동일 여부를 판단하는 수신번호 판단단계와, 상기 수신번호가 상기 화이트 리스트 상의 전화번호와 동일하면 수신지 인증 패킷을 발신자 단말기에 전송하는 수신번호 인증단계 및 상기 수신지 인증 패킷에 대응하는 수신지 인증 사인을 상기 발신자 단말기에 전달하는 인증수신번호 알림단계를 포함할 수 있다. 이때, 상기 수신번호 판단단계 이전에 기관들의 변경되거나 추가된 전화번호를 상기 화이트 리스트 상에 업데이트하는 화이트 리스트 업데이트단계를 포함할 수 있다.

효과

- [0028] 상기한 바와 같이 본 발명에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템 및 방법에 의하면 기관의

전화번호를 사용자 대신 컴퓨터가 직접 확인하고 단말기 상으로 그 기관의 진위여부를 알림으로써 보이스 피싱의 피해를 방지할 수 있는 효과가 있다.

[0029] 또한, 공격자에 의한 통화 연결시 사용자가 발신번호를 확인하는 과정에서 발신기관의 진위여부를 판단할 수 있는 효과가 있다.

[0030] 또한, 사용자에게 의한 통화 연결시 사용자가 수신번호를 확인하는 과정에서 수신기관의 진위여부를 판단할 수 있는 효과가 있다.

발명의 실시를 위한 구체적인 내용

[0031] 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.

[0032] 도 1은 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템을 이용하여 발신지의 발신번호가 화이트 리스트에 있는 경우와 그렇지 않은 경우의 비교예를 보여주는 도이고, 도 2 및 도 3은 각각 본 발명에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템의 구성도이다. 또한, 도 4a 및 도 4b는 각각 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 방법의 블록도이고, 도 5a 및 도 5b는 각각 본 발명의 제 2실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 방법의 블록도이다.

[0033] 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템은 도 1 및 도 2에 도시된 바와 같이, 화이트 리스트(100)와, 발신번호 인증부(200) 및 인증발신번호 알림부(300)를 포함한다.

[0034] 상기 화이트 리스트(100)는 각 기관, 예를 들어, 금융기관, 택배회사, 우체국, 정부기관 등의 전화번호 목록이 저장되어 유지되는 통신사의 데이터 베이스이다.

[0035] 여기서, 상기 기관은 전화번호 인증을 위해 전화번호를 공개하여야 할 의무를 가진 기관을 의미한다.

[0036] 또한, 상기 화이트 리스트(100)는 상기 기관들의 기존의 전화번호가 변경되거나, 새로운 전화번호가 추가될 때, 업데이트될 수 있음은 물론이다.

[0037] 상기 발신번호 인증부(200)는 보이스 피싱자(이하, '공격자' 라 함)가 전화통화 연결시, 상기 화이트 리스트(100) 상의 전화번호와 발신지의 발신번호를 비교한다.

[0038] 이후, 상기 발신번호가 상기 화이트 리스트 상의 전화번호와 동일하면 특별 신호인 발신지 인증 패킷을 수신자 단말기, 즉, 임의 사용자의 단말기에 전송한다.

[0039] 상기 인증발신번호 알림부(300)는 상기 발신지 인증 패킷에 대응하는 발신지 인증 사인을 상기 수신자 단말기에 전달한다.

[0040] 이때, 상기 발신지 인증 사인은 상기 수신자 단말기가 사용할 수 있는 모든 사인이 포함될 수 있다.

[0041] 구체적으로, 상기 발신지 인증 사인은 OLED 등의 디스플레이 장치를 이용한 텍스트나, 아이콘 또는 애니메이션 등으로 이루어질 수 있고, 특별한 느낌의 진동으로 이루어질 수 있으며, 음향으로 이루어질 수 있다.

[0042] 사용자는 상기 발신지 인증 사인을 확인한 후, 통화 응답에 따라 통화 응답 패킷을 전송하여 전화연결을 완료할 수 있다.

- [0043] 한편, 가짜 전화번호를 남겨놓은 가짜 지로용지를 임의의 사용자에게 전달하는 것과 유사하게, 공격자는 임의의 사용자에게 메시지를 이용하여 기관의 가짜 전화번호로 발신하도록 유도하는 공격을 할 수 있다.
- [0044] 이를 방지하기 위한 본 발명의 제 2실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템을 이하에서 상세히 설명한다.
- [0045] 본 발명의 제 2실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템은 도 1 및 도 3에 도시된 바와 같이, 화이트 리스트(400)와, 수신번호 인증부(500) 및 인증수신번호 알림부(600)를 포함한다.
- [0046] 상기 화이트 리스트(400)는 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템의 화이트 리스트와 그 구성 및 내용이 동일하다.
- [0047] 상기 수신번호 인증부(500)는 메시지에 남겨진 기관을 사칭한 가짜 전화번호로 발신하는 임의의 사용자(이하 '사용자' 라 함)가 전화통화 연결시, 상기 화이트 리스트(400) 상의 전화번호와 수신지의 수신번호, 즉, 가짜 전화번호를 비교한다.
- [0048] 이후, 상기 수신번호가 상기 화이트 리스트(400) 상의 전화번호와 동일하면 특별 신호인 수신지 인증 패킷을 발신자 단말기, 즉, 사용자의 단말기에 전송한다.
- [0049] 상기 인증수신번호 알림부(500)는 상기 수신지 인증 패킷에 대응하는 수신지 인증 사인을 상기 발신자 단말기에 전달한다.
- [0050] 이때, 상기 수신지 인증 사인은 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템의 발신지 인증 사인과 동일하게, 디스플레이 장치를 이용한 텍스트나, 아이콘 또는 애니메이션 등으로 이루어질 수 있고, 특별한 느낌의 진동으로 이루어질 수 있으며, 음향으로 이루어질 수 있다.
- [0051] 사용자는 상기 수신지 인증 사인을 확인한 후, 통화 연결에 따라 통화 연결 패킷을 전송하여 전화연결을 완료할 수 있다.
- [0052] 이하, 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 방법을 상세히 설명한다.
- [0053] 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 방법은 도 4a에 도시된 바와 같이, 발신 번호 판단단계(S20)와, 발신 번호 인증단계(S30) 및 인증발신번호 알림단계(S40)를 포함한다.
- [0054] 상기 발신 번호 판단단계(S20)는 공격자가 전화통화 연결시, 발신지의 발신번호와 화이트 리스트 상의 전화번호를 비교하여 동일 여부를 판단하는 단계이다.
- [0055] 이때, 상기 화이트 리스트는 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템의 화이트 리스트와 그 구성 및 내용이 동일하다.
- [0056] 상기 발신 번호 인증단계(S30)는 상기 발신번호가 상기 화이트 리스트 상의 전화번호와 동일하면 특별 신호인 발신지 인증 패킷을 수신자 단말기, 즉, 사용자의 단말기에 전송하는 단계이다.
- [0057] 상기 인증발신번호 알림단계(S40)는 상기 발신지 인증 패킷에 대응하는 발신지 인증 사인을 상기 수신자 단말기, 즉 사용자의 단말기에 전달하는 단계이다.
- [0058] 이때, 상기 발신지 인증 사인은 상기 수신자 단말기가 사용할 수 있는 모든 사인이 포함될 수 있다.

- [0059] 따라서, 사용자는 상기 발신지 인증 사인을 확인한 후, 통화에 대한 응답여부를 결정할 수 있다.
- [0060] 한편, 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 방법은 도 4b에 도시된 바와 같이, 상기 발신번호 판단단계(S20) 이전에 화이트 리스트 업데이트단계(S10)를 포함할 수 있다.
- [0061] 상기 화이트 리스트 업데이트단계(S10)는 기관들의 기존의 전화번호가 변경되거나, 새로운 전화번호가 추가될 때, 상기 화이트 리스트 상에 변경 또는 추가된 전화번호를 업데이트하는 단계이다.
- [0062] 이하, 본 발명의 제 2실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 방법을 상세히 설명한다.
- [0063] 본 발명의 제 2실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 방법은 도 5a에 도시된 바와 같이, 수신 번호 판단단계(S60)와, 수신 번호 인증단계(S70) 및 인증수신번호 알림단계(S80)를 포함한다.
- [0064] 상기 수신 번호 판단단계(S60)는 사용자가 기관을 사칭한 가짜 전화번호로 전화통화 연결시, 수신지의 수신번호, 즉, 가짜 전화번호와 화이트 리스트 상의 전화번호를 비교하여 동일 여부를 판단하는 단계이다.
- [0065] 이때, 상기 화이트 리스트는 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템의 화이트 리스트와 그 구성 및 내용이 동일하다.
- [0066] 상기 수신 번호 인증단계(S70)는 상기 수신번호가 상기 화이트 리스트 상의 전화번호와 동일하면 특별 신호인 수신지 인증 패킷을 발신자 단말기, 즉, 사용자의 단말기에 전송하는 단계이다.
- [0067] 상기 인증수신번호 알림단계(S80)는 상기 수신지 인증 패킷에 대응하는 수신지 인증 사인을 상기 발신자 단말기, 즉 사용자의 단말기에 전달하는 단계이다.
- [0068] 이때, 상기 수신지 인증 사인은 상기 발신자 단말기가 사용할 수 있는 모든 사인이 포함될 수 있다.
- [0069] 따라서, 사용자는 상기 수신지 인증 사인을 확인한 후, 통화에 대한 계속여부를 결정할 수 있다.
- [0070] 한편, 본 발명의 제 2실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 방법은 도 5b에 도시된 바와 같이, 상기 수신번호 판단단계(S60) 이전에 화이트 리스트 업데이트단계(S50)를 포함할 수 있다.
- [0071] 상기 화이트 리스트 업데이트단계(S50)는 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템의 화이트 리스트 업데이트단계와 동일하다.
- [0072] 즉, 상기 화이트 리스트 업데이트단계(S50)는 기관들의 기존의 전화번호가 변경되거나, 새로운 전화번호가 추가될 때, 상기 화이트 리스트 상에 변경 또는 추가된 전화번호를 업데이트하는 단계이다.
- [0073] 이상과 같이 본 발명에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템 및 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

- [0074] 도 1은 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템을 이용하여 발신지의 발신번호가 화이트 리스트에 있는 경우와 그렇지 않은 경우의 비교예를 보여주는 도.
- [0075] 도 2는 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템의 구성도.
- [0076] 도 3은 본 발명의 제 2실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 시스템의 구성도.

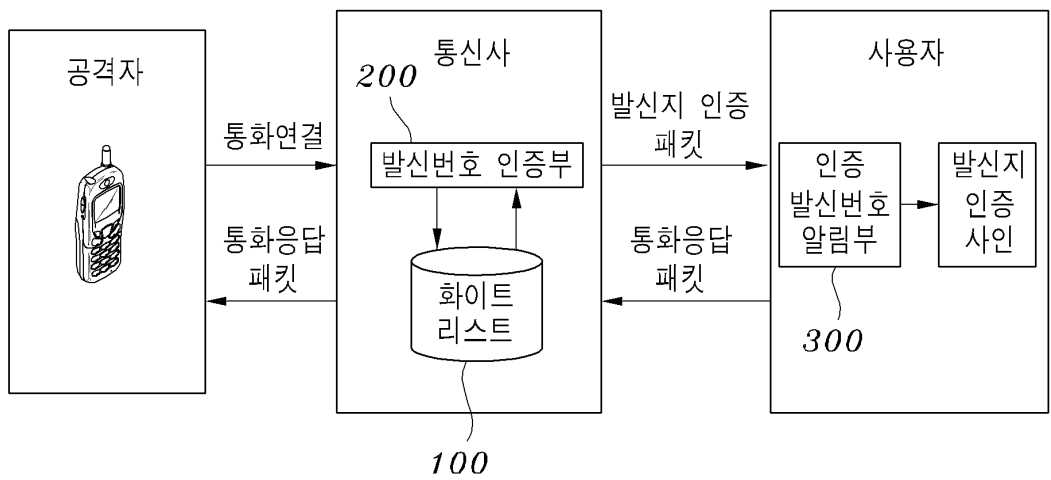
- [0077] 도 4a는 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 방법의 일 블록도.
- [0078] 도 4b는 본 발명의 제 1실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 방법의 다른 블록도.
- [0079] 도 5a는 본 발명의 제 2실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 방법의 일 블록도.
- [0080] 도 5b는 본 발명의 제 2실시예에 따른 화이트 리스트를 이용한 보이스 피싱 방지 방법의 일 블록도.
- [0081] 도 6은 2009년 3월에 발표된 경찰청 내부자료의 보이스 피싱 발생 및 검거 현황을 나타내는 도.
- [0082] 도 7은 2008년 경기도내 노인 782명을 상대로 노인 소비실태에 대한 설문조사의 결과를 나타내는 도.
- [0083] < 도면의 주요 부분에 대한 부호의 설명 >
- [0084] 100,400:화이트 리스트
- [0085] 200:발신번호 인증부
- [0086] 300:인증발신번호 알람부
- [0087] 500:수신번호 인증부
- [0088] 600:인증수신번호 알람부
- [0089] S10,S50:화이트 리스트 업데이트 단계
- [0090] S20:발신번호 판단단계
- [0091] S30:발신번호 인증단계
- [0092] S40:인증발신번호 알람단계
- [0093] S60:수신번호 판단단계
- [0094] S70:수신번호 인증단계
- [0095] S80:인증수신번호 알람단계

도면

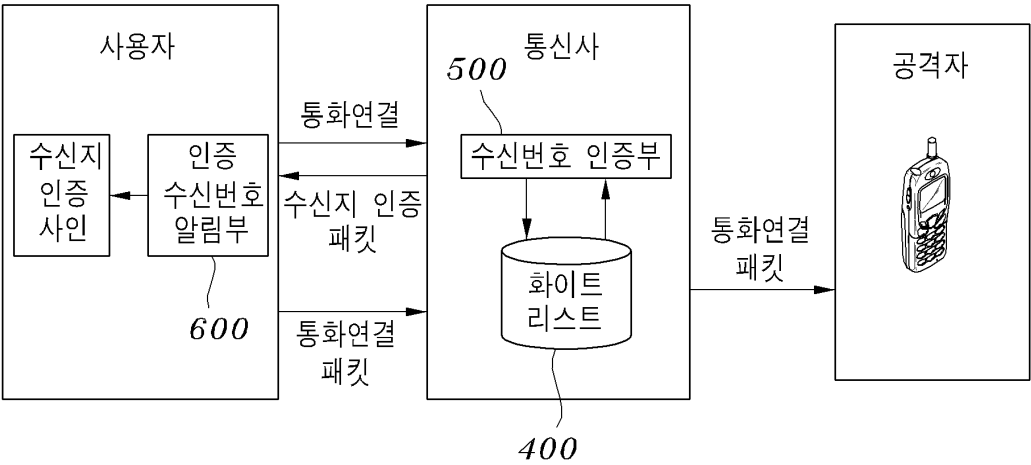
도면1



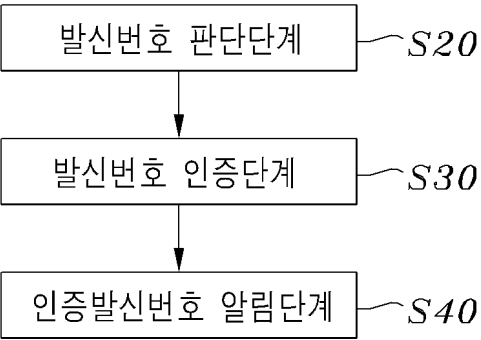
도면2



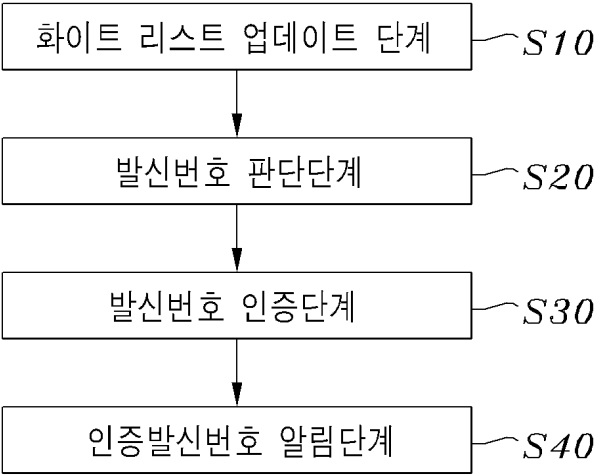
도면3



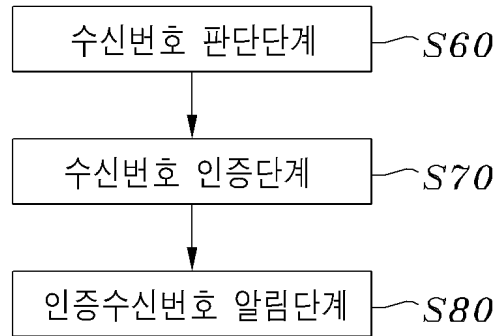
도면4a



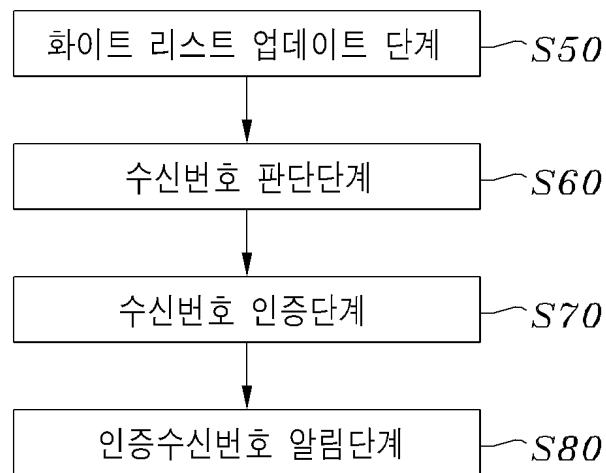
도면4b



도면5a



도면5b



도면6

구분	발생건수	피해액	검거건수	검거인원
계	1만3038 건	1332 억원	8457 건	8194 명
2006. 6~12월	1480 건	106 억원	779 건	83 명
2007. 1~12월	3969 건	433 억원	2757 건	2221 명
2008. 1~12월	7589 건	793 억원	4921 건	5890 명

도면7

