



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0136100
(43) 공개일자 2010년12월28일

(51) Int. Cl.

H04L 9/32 (2006.01) G06F 21/00 (2006.01)

(21) 출원번호 10-2009-0054288

(22) 출원일자 2009년06월18일

심사청구일자 2009년06월18일

(71) 출원인

인하대학교 산학협력단

인천 남구 용현동 253 인하대학교

(72) 발명자

김유성

인천시 남구 용현3동 인하대학교 정보통신공학부

김상영

경기도 부천시 소사구 심곡본동 739-22번지 모던빌 503호

(뒷면에 계속)

(74) 대리인

특허법인무한

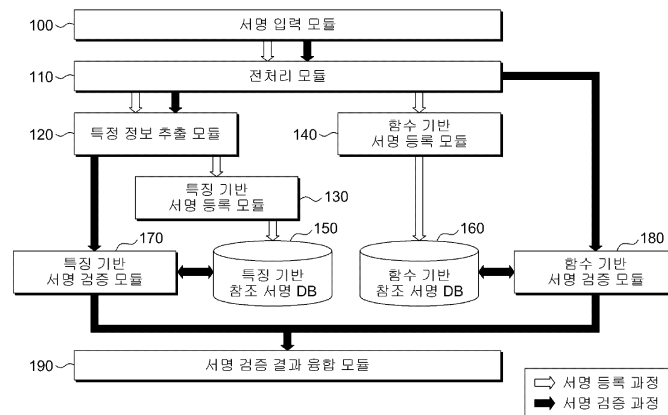
전체 청구항 수 : 총 9 항

(54) 다양한 응용을 위한 다기준 신뢰도 지원 하이브리드 온라인 서명검증 시스템 및 그 방법

(57) 요약

다양한 응용을 위한 다기준 신뢰도 지원 하이브리드 온라인 서명검증 시스템 및 그 방법을 개시한다. 다기준 신뢰도 지원 하이브리드 온라인 서명검증 시스템은 참조서명에서 추출된 벡터와 입력서명에서 추출된 벡터 간의 거리인 특징기반 서명검증의 거리 계산 값을 산출하는 특징기반 서명검증 모듈; 상기 참조서명과 입력서명의 입력 시간 흐름에 따라 상기 참조서명과 입력서명의 차이를 누적한 거리인 함수기반 서명검증의 거리 계산 값을 산출하는 함수기반 서명검증 모듈; 및, 상기 특징기반 서명검증의 거리 계산 값과 함수기반 서명검증의 거리 계산 값을 직렬 또는 병렬로 융합하여 상기 입력서명의 진위를 판단하는 서명검증 결과융합 모듈을 포함한다.

대표도



(72) 발명자

이성규

경기도 부천시 소사구 괴안동 22-7

조성영

인천시 계양구 박촌동 한화꿈에그린아파트 108동
902호

특허청구의 범위

청구항 1

참조서명에서 추출된 벡터와 입력서명에서 추출된 벡터 간의 거리인 특징기반 서명검증의 거리 계산 값을 산출하는 특징기반 서명검증 모듈;

상기 참조서명과 입력서명의 입력 시간 흐름에 따라 상기 참조서명과 입력서명의 차이를 누적한 거리인 함수기반 서명검증의 거리 계산 값을 산출하는 함수기반 서명검증 모듈; 및,

상기 특징기반 서명검증의 거리 계산 값과 함수기반 서명검증의 거리 계산 값을 직렬 또는 병렬로 융합하여 상기 입력서명의 진위를 판단하는 서명검증 결과융합 모듈

을 포함하는 다기준 신뢰도 지원 하이브리드 온라인 서명검증 시스템.

청구항 2

제1항에 있어서,

상기 서명검증 결과융합 모듈은,

상기 특징기반 서명검증의 거리 계산 값을 상기 입력서명의 진위를 판단하는 하나의 기준인 특징기반 허용기준치와 비교하는 1차 검증 과정을 수행한 후, 상기 1차 검증 과정의 결과에 따라 상기 함수기반 서명검증의 거리 계산 값을 상기 입력서명의 진위를 판단하는 다른 기준인 함수기반 허용기준치와 비교하는 2차 검증 과정을 수행하는, 다기준 신뢰도 지원 하이브리드 온라인 서명검증 시스템.

청구항 3

제1항에 있어서,

상기 서명검증 결과융합 모듈은,

데이터 마이닝(data mining)을 이용하여 상기 참조서명에 대한 FRR(false rejection ratio)과 FAR(false acceptance ratio)을 산출하고 상기 산출된 FRR과 FAR에 따라 상기 입력서명의 진위를 판단하는 기준인 허용기준치를 설정하는, 다기준 신뢰도 지원 하이브리드 온라인 서명검증 시스템.

청구항 4

제1항에 있어서,

상기 서명검증 결과융합 모듈은,

상기 특징기반 서명검증의 거리 계산 값에 해당하는 FAR과 함수기반 서명검증의 거리 계산 값에 해당하는 FAR을 이용하여 상기 참조서명과 입력서명의 유사도를 산출하고 상기 산출된 유사도에 따라 상기 입력 서명의 진위를 판단하는, 다기준 신뢰도 지원 하이브리드 온라인 서명검증 시스템.

청구항 5

특징기반 서명검증 모듈과, 함수기반 서명검증 모듈과, 서명검증 결과융합 모듈을 포함한 하이브리드 온라인 서명검증 시스템의 다기준 신뢰도 지원 하이브리드 온라인 서명검증 방법에 있어서,

상기 특징기반 서명검증 모듈에서 참조서명에서 추출된 벡터와 입력서명에서 추출된 벡터 간의 거리인 특징기반 서명검증의 거리 계산 값을 산출하는 단계;

상기 함수기반 서명검증 모듈에서 상기 참조서명과 입력서명의 입력 시간 흐름에 따라 상기 참조서명과 입력서명의 차이를 누적한 거리인 함수기반 서명검증의 거리 계산 값을 산출하는 단계; 및,

상기 서명검증 결과융합 모듈에서 상기 특징기반 서명검증의 거리 계산 값과 함수기반 서명검증의 거리 계산 값을 직렬 또는 병렬로 융합하여 상기 입력서명의 진위를 판단하는 단계

를 포함하는 다기준 신뢰도 지원 하이브리드 온라인 서명검증 방법.

청구항 6

제5항에 있어서,

상기 입력서명의 진위를 판단하는 단계는,

상기 특징기반 서명검증의 거리 계산 값에 상기 입력서명의 진위를 판단하는 하나의 기준인 특징기반 허용기준치와 비교하는 단계와,

상기 특징기반 서명검증의 거리 계산 값이 상기 특징기반 허용기준치 이내이면 상기 함수기반 서명검증의 거리 계산 값을 상기 입력서명의 진위를 판단하는 다른 기준인 함수기반 허용기준치와 비교하는 단계와,

상기 함수기반 서명검증의 거리 계산 값이 상기 함수기반 허용기준치 이내이면 상기 입력서명을 진서명으로 판단하는 단계

를 포함하는, 다기준 신뢰도 지원 하이브리드 온라인 서명검증 방법.

청구항 7

제5항에 있어서,

상기 입력서명의 진위를 판단하는 단계는,

데이터 마이닝을 이용하여 상기 참조서명에 대한 FRR과 FAR을 산출하는 단계와,

상기 산출된 FRR과 FAR에 따라 상기 입력서명의 진위를 판단하는 기준인 허용기준치를 설정하는 단계와,

상기 특징기반 서명검증의 거리 계산 값과 함수기반 서명검증의 거리 계산 값을 상기 설정된 허용기준치와 비교하여 상기 입력서명의 진위를 판단하는 단계

를 포함하는, 다기준 신뢰도 지원 하이브리드 온라인 서명검증 방법.

청구항 8

제7항에 있어서,

상기 참조서명에 대한 FRR과 FAR을 산출하는 단계는,

상기 참조서명 간의 거리 중 최대 거리인 최대 진서명 거리를 산출하는 단계와,

상기 참조서명 간의 거리 중 최소 거리인 최소 진서명 거리를 산출하는 단계와,

상기 참조서명과 상기 참조서명을 위조한 가서명 간의 거리 중 최소 거리인 최소 가서명 거리를 산출하는 단계와,

상기 최대 진서명 거리와 최소 진서명 거리의 비율인 최소 진서명 거리비율을 산출하는 단계와,

상기 최대 진서명 거리와 최소 가서명 거리의 비율인 최소 가서명 거리비율을 산출하는 단계와,

상기 최소 진서명 거리비율을 이용하여 FRR을 산출하는 단계와,

상기 최소 가서명 거리비율을 이용하여 FAR을 산출하는 단계

를 포함하는, 다기준 신뢰도 지원 하이브리드 온라인 서명검증 방법.

청구항 9

제5항에 있어서,

상기 입력서명의 진위를 판단하는 단계는,

상기 특징기반 서명검증의 거리 계산 값에 해당하는 FAR를 추출하는 단계와,

상기 함수기반 서명검증의 거리 계산 값에 해당하는 FAR를 추출하는 단계와,

상기 특징기반 서명검증의 거리 계산 값에 해당하는 FAR과 함수기반 서명검증의 거리 계산 값에 해당하는 FAR을 이용하여 상기 참조서명과 입력서명의 유사도를 산출하는 단계와,

상기 산출된 유사도에 따라 상기 입력 서명의 진위를 판단하는 단계를 포함하는, 다기준 신뢰도 지원 하이브리드 온라인 서명검증 방법.

명세서

발명의 상세한 설명

기술 분야

[0001] 본 발명의 실시예들은 온라인 서명검증 시스템에 관한 것으로, 더욱 상세하게는 특징기반 서명검증 기법과 함수기반 서명검증 기법을 융합한 다기준 서명검증 신뢰도를 지원하는 하이브리드 온라인 서명검증 시스템 및 그 방법에 관한 것이다.

배경 기술

[0002] 디지털 펜 또는 테이블릿의 관련 기술의 발전에 따라 온라인 서명검증을 필요로 하는 분야 및 응용(은행거래, 카드거래, 전자문서결재 등)이 크게 증가하고 있다. 본인 여부를 판단하기 위한 생체인식기술과 같은 목적으로 온라인 서명검증에서는 사람이 직접 디지털 펜 또는 테이블릿을 이용하여 입력한 서명의 진본 여부를 판단하여 서명을 입력한 사람이 본인인가를 확인한다. 따라서, 온라인 서명검증에서는 서명검증의 정확성 및 신속성이 중요하다.

[0003] 서명 검증에서 발생할 수 있는 인식 오류는 위조서명 인증 오류(false acceptance error)와 진서명 거부 오류(false rejection error)의 2가지 유형이 존재한다. 만일, 서명검증의 정확성을 개선하기 위한 목적으로 위조서명 인증 오류의 비율(false acceptance ratio: FAR)을 낮추고자 서명검증의 신뢰도 기준을 높게 설정하면 일반적으로 서명검증을 실시하기 위한 소요시간이 증가하고, 또한 진서명 거부 오류의 비율(false rejection ratio: FRR)이 증가하여 사용자 본인의 진서명을 위조서명으로 분류하여 사용자에게 불편을 초래하게 된다. 온라인 서명검증을 이용하는 여러 응용에서 같은 신뢰도 기준을 사용한다면 상대적으로 낮은 신뢰도를 필요로 하는 응용에서는 불필요하게 높은 FRR을 갖게 되고, 상대적으로 높은 신뢰도를 필요로 하는 응용에서는 불필요하게 높은 FAR를 갖는 문제가 존재하게 된다.

[0004] 따라서, 다양한 서명검증의 응용을 지원하기 위해서는 각 응용 서비스의 중요도 및 사용자 서명의 복잡도에 따라 다르게 서명검증의 신뢰도를 지원할 수 있는 다기준 신뢰도 지원의 온라인 서명검증 시스템 및 체계적인 다기준 신뢰도 설정 방법이 필요하다.

[0005] 기존의 온라인 서명검증 시스템에서 사용하는 방법은 크게 특징기반 서명검증 기법과 함수기반 서명검증 기법으로 나눌 수 있다. 특징기반 서명검증 기법은 참조서명을 대표하는 전체론적인 벡터와 입력서명을 대표하는 전체론적인 벡터간의 다차원 공간에서의 거리를 기반으로 입력서명의 진위를 판단하는 방법이고, 함수기반 서명검증 기법은 서명시간의 흐름에 따라 참조서명과 입력서명간의 지역적인 특징 비교의 결과를 누적시킨 거리를 기반으로 입력서명의 진위를 판단하는 방법이다. 서명검증의 신속성과 정확성을 증진하기 위한 목적으로 두 기법을 융합하여 사용한 하이브리드 시스템들이 존재한다.

발명의 내용

해결 하고자하는 과제

[0006] 본 발명의 일실시예는 온라인 서명검증을 필요로 하는 응용의 서비스 내용 및 중요도와 사용자 서명의 복잡도에 따라 시스템 관리자 및 사용자가 동적으로 서명검증의 신뢰도를 선택할 수 있는 특징기반 서명검증 기법과 함수기반 서명검증 기법을 융합한 다기준 서명검증 신뢰도를 지원하는 하이브리드 온라인 서명검증 시스템 및 그 방법을 제공한다.

[0007] 본 발명의 일실시예는 서명검증 입력도구를 이용한 실제 서명검증 데이터를 활용하여 데이터 마이닝 기술로 이상적인 다기준 신뢰도를 설정할 수 있는 하이브리드 온라인 서명검증 시스템 및 그 방법을 제공한다.

과제 해결수단

[0008] 본 발명의 일실시예에 따른 다기준 신뢰도 지원 하이브리드 온라인 서명검증 시스템은 참조서명에서 추출된 벡터와 입력서명에서 추출된 벡터 간의 거리인 특징기반 서명검증의 거리 계산 값을 산출하는 특징기반 서명검증

모듈; 상기 참조서명과 입력서명의 입력 시간 흐름에 따라 상기 참조서명과 입력서명의 차이를 누적한 거리인 함수기반 서명검증의 거리 계산 값을 산출하는 함수기반 서명검증 모듈; 및, 상기 특징기반 서명검증의 거리 계산 값과 함수기반 서명검증의 거리 계산 값을 직렬 또는 병렬로 융합하여 상기 입력서명의 진위를 판단하는 서명검증 결과융합 모듈을 포함한다.

[0009] 본 발명의 일실시예에서 상기 서명검증 결과융합 모듈은 상기 특징기반 서명검증의 거리 계산 값을 상기 입력서명의 진위를 판단하는 하나의 기준인 특징기반 허용기준치와 비교하는 1차 검증 과정을 수행한 후, 상기 1차 검증 과정의 결과에 따라 상기 함수기반 서명검증의 거리 계산 값을 상기 입력서명의 진위를 판단하는 다른 기준인 함수기반 허용기준치와 비교하는 2차 검증 과정을 수행한다.

[0010] 본 발명의 일실시예에서 상기 서명검증 결과융합 모듈은 상기 특징기반 서명검증의 거리 계산 값에 해당하는 FAR과 함수기반 서명검증의 거리 계산 값에 해당하는 FAR을 이용하여 상기 참조서명과 입력서명의 유사도를 산출하고 상기 산출된 유사도에 따라 상기 입력 서명의 진위를 판단한다.

[0011] 본 발명의 일실시예에 따른 다기준 신뢰도 지원 하이브리드 온라인 서명검증 방법은 특징기반 서명검증 모듈과, 함수기반 서명검증 모듈과, 서명검증 결과융합 모듈을 포함한 하이브리드 온라인 서명검증 시스템의 다기준 신뢰도 지원 하이브리드 온라인 서명검증 방법에 있어서, 상기 특징기반 서명검증 모듈에서 참조서명에서 추출된 벡터와 입력서명에서 추출된 벡터 간의 거리인 특징기반 서명검증의 거리 계산 값을 산출하는 단계; 상기 함수기반 서명검증 모듈에서 상기 참조서명과 입력서명의 입력 시간 흐름에 따라 상기 참조서명과 입력서명의 차이를 누적한 거리인 함수기반 서명검증의 거리 계산 값을 산출하는 단계; 및, 상기 서명검증 결과융합 모듈에서 상기 특징기반 서명검증의 거리 계산 값과 함수기반 서명검증의 거리 계산 값을 직렬 또는 병렬로 융합하여 상기 입력서명의 진위를 판단하는 단계를 포함한다.

[0012] 본 발명의 일실시예에서 상기 입력서명의 진위를 판단하는 단계는 상기 특징기반 서명검증의 거리 계산 값을 상기 입력서명의 진위를 판단하는 하나의 기준인 특징기반 허용기준치와 비교하는 단계와, 상기 특징기반 서명검증의 거리 계산 값이 상기 특징기반 허용기준치 이내이면 상기 함수기반 서명검증의 거리 계산 값을 상기 입력서명의 진위를 판단하는 다른 기준인 함수기반 허용기준치와 비교하는 단계와, 상기 함수기반 서명검증의 거리 계산 값이 상기 함수기반 허용기준치 이내이면 상기 입력서명을 진서명으로 판단하는 단계를 포함한다.

[0013] 본 발명의 일실시예에서 상기 입력서명의 진위를 판단하는 단계는 데이터 마이닝을 이용하여 상기 참조서명에 대한 FRR과 FAR을 산출하는 단계와, 상기 산출된 FRR과 FAR에 따라 상기 입력서명의 진위를 판단하는 기준인 허용기준치를 설정하는 단계와, 상기 특징기반 서명검증의 거리 계산 값과 함수기반 서명검증의 거리 계산 값을 상기 설정된 허용기준치와 비교하여 상기 입력서명의 진위를 판단하는 단계를 포함한다.

[0014] 이때, 상기 참조서명에 대한 FRR과 FAR을 산출하는 단계는 상기 참조서명 간의 거리 중 최대 거리인 최대 진서명 거리를 산출하는 단계와, 상기 참조서명 간의 거리 중 최소 거리인 최소 진서명 거리를 산출하는 단계와, 상기 참조서명과 상기 참조서명을 위조한 가서명 간의 거리 중 최소 거리인 최소 가서명 거리를 산출하는 단계와, 상기 최대 진서명 거리와 최소 진서명 거리의 비율인 최소 진서명 거리비율을 산출하는 단계와, 상기 최대 진서명 거리와 최소 가서명 거리의 비율인 최소 가서명 거리비율을 산출하는 단계와, 상기 최소 진서명 거리비율을 이용하여 FRR을 산출하는 단계와, 상기 최소 가서명 거리비율을 이용하여 FAR을 산출하는 단계를 포함한다.

[0015] 본 발명의 일실시예에서 상기 입력서명의 진위를 판단하는 단계는 상기 특징기반 서명검증의 거리 계산 값에 해당하는 FAR을 추출하는 단계와, 상기 함수기반 서명검증의 거리 계산 값에 해당하는 FAR을 추출하는 단계와, 상기 특징기반 서명검증의 거리 계산 값에 해당하는 FAR과 함수기반 서명검증의 거리 계산 값에 해당하는 FAR을 이용하여 상기 참조서명과 입력서명의 유사도를 산출하는 단계와, 상기 산출된 유사도에 따라 상기 입력 서명의 진위를 판단하는 단계를 포함한다.

효 과

[0016] 본 발명의 일실시예에 따르면, 응용 서비스의 중요도 및 사용자 서명의 복잡도에 따라 동적으로 적절한 신뢰도 기준을 선택하여 사용자 인증을 수행함으로써 온라인 서명검증의 응용별로 적절한 서명검증의 정확성을 확보할 수 있으며 개인별 또는 서명입력 환경에 따라 동적으로 서명검증의 방법 및 신뢰도 기준을 다르게 정할 수 있다.

[0017] 본 발명의 일실시예에 따르면, 사용자 서명의 복잡도에 따라 사용자 개인별 서명검증 신뢰도를 선택함으로써 사용자 인증을 받도록 지원하는 응용, 서비스 타입/내용 및 서비스 중요도에 따라 사용자 인증 신뢰도를 선택하는

응용, 사용자가 사전에 등록한 환경에서는 서명검증 신뢰도를 낮게 지원하고 사용자가 사전 등록하지 않은 환경에서는 높은 서명검증 신뢰도로 사용자 인증을 하도록 자동으로 조정하는 기능을 제공하는 응용 등에서 시스템 자동 또는 사용자 선택적으로 서명검증의 신뢰도를 동적으로 조절할 수 있도록 하여 환경에 적합한 서명검증 보안성을 제공할 수 있다.

발명의 실시를 위한 구체적인 내용

- [0018] 이하에서, 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다. 그러나, 본 발명이 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.
- [0019] 도 1은 본 발명의 일실시예에 따른 하이브리드 온라인 서명검증 시스템의 내부 구성을 도시한 것이다. 도 1을 참조하여, 본 발명의 일실시예에 따른 하이브리드 온라인 서명검증 시스템에서의 참조서명의 등록 과정과 입력서명의 검증과정을 설명한다.
- [0020] 서명 입력모듈(100)은 서명을 입력받는 기능을 수행하는 것으로, 디지털 펜 또는 테이블릿 등으로 서명을 입력받는 입력 장치 및 구동 소프트웨어 모듈을 의미한다.
- [0021] 전처리 모듈(110)은 입력된 서명 정보를 전처리 과정을 통해 서명 입력 시간, 또는 서명의 크기에 따라 정규화하는 기능을 수행한다.
- [0022] 특징정보 추출 모듈(120)은 서명의 진위를 판단하기 위해 주요하게 활용될 수 있는 특징 정보를 원시 서명 정보로부터 추출하는 기능을 수행한다. 여기서, 특징 정보는 문자 인식 및 이미지 인식 분야 등에서 활용되는 특징 정보를 참조하여 시스템 개발자가 경험적으로 선정할 수 있으며 데이터 마이닝 기법의 속성 선택 기법 등을 활용하여 분별력이 높은 구분 특징을 선정할 수 있다.
- [0023] 특징기반 서명등록 모듈(130)은 특징기반 서명검증에 활용되는 속성정보의 추출 값들(즉, 특징 정보)을 특징기반 참조서명 DB(150)에 저장하고, 함수기반 서명등록 모듈(140)은 함수기반 서명검증에 활용되는 속성정보의 추출 값들(즉, 특징 정보)을 함수기반 참조서명 DB(160)에 저장한다.
- [0024] 특징기반 서명검증 모듈(170)은 서명의 전체적인 형태 및 전체적인 속도, 시간 등을 특징 정보로 활용한 다차원 벡터를 구성하여 참조서명과 입력서명과의 다차원 벡터간의 거리를 계산하는 기능을 수행한다.
- [0025] 함수기반 서명검증 모듈(180)은 동적 타임 워핑 거리 함수(dynamic time warping distance function) 계산식 등을 이용하여 참조서명과 입력서명의 입력 시간 흐름에 따른 차이의 누적 거리를 계산하는 기능을 수행한다.
- [0026] 서명검증 결과융합 모듈(190)은 특징기반 서명 검증의 거리 계산 값과 함수기반 서명검증의 거리 계산 값을 적절한 형태에 따라 융합하고 입력서명의 진본 여부를 판단하는 기능을 수행한다. 서명검증 결과융합 모듈(190)은 다양한 응용을 지원하기 위해 특징기반 서명검증 모듈(170)과 함수기반 서명검증 모듈(180)의 결과 값들을 직렬 또는 병렬로 융합할 수 있으며 직렬로 융합하는 경우에도 다기준 서명검증 신뢰도를 지원하여 응용에 적합한 서명검증의 보안성을 확보할 수 있도록 지원한다.
- [0027] 도 2는 본 발명의 일실시예에 따른 하이브리드 온라인 서명검증 시스템에서의 직렬 융합을 통한 서명검증 과정을 설명하기 위한 도면이다.
- [0028] 본 발명의 일실시예에 따른 하이브리드 온라인 서명검증 시스템은 특징기반 서명검증 모듈(170)과 함수기반 서명검증 모듈(180)을 통해 참조서명과 입력서명과의 거리($D_{feature}$, $D_{function}$)를 산출한다(S201).
- [0029] 상세하게는, 특징기반 서명검증 모듈(170)은 사용자의 등록된 참조서명을 찾기 위해 특징기반 참조서명 DB(150)에서 서명자 ID로 k개의 참조 서명($k=5$)을 검색한 후, 수학적 식 1을 통해 참조서명의 특징 정보들과 검증용 입력서명의 특징 정보들 간의 거리($D_{feature}$)를 계산한다.

수학적 식 1

$$D_{feature} = \sum_{n=1}^N \min(CD(R_{k,n}, C_n))$$

[0030]

[0031] 여기서, k는 각 참조 서명($k=1\sim5$)을 의미하며, $R_{k,n}$ 은 k번째 참조서명의 n번째 특징 정보, C_n 은 입력서명의 n번째

제 특징 정보를 의미한다. 그리고, CD는 참조 서명의 특징 정보와 입력서명의 특징 정보 간의 거리를 계산하는 방법으로 수학식 2와 같은 캔버라 거리(Canberra Distance)를 이용하여 산출한다. 이때, 여러 참조서명의 특징 정보들과 입력서명의 특징 정보의 거리 중 최소값을 취하는 이유는 입력서명의 특징 정보와 가장 근접한 참조서명의 특징 정보를 비교하기 위함이다. 캔버라 거리를 계산하는 방식은 값의 범주(range)와 단위(unit)가 서로 다른 특징 정보들을 정규화 시키는 효과를 갖는다.

수학식 2

$$CD(R_{k,n}, C_n) = \frac{|R_{k,n} - C_n|}{|R_{k,n}| + |C_n|}$$

[0032]

[0033] 함수기반 서명검증 모듈(180)은 사용자의 등록된 참조서명과 검증용으로 입력된 입력서명간의 유사도를 판단하기 위해 입력서명의 특징 정보들과 함수기반 참조서명 DB(160)에 있는 참조서명들의 특징 정보들 간의 누적 거리를 계산한다. 거리 계산은 동적 프로그램(dynamic program)의 한 종류인 동적 타임 워핑(Dynamic Time Warping) 알고리즘을 사용할 수 있다. 참조 서명들의 특징 정보들과 입력서명의 특징 정보들 간의 누적 거리($D_{function}$)를 계산하는 방법은 수학식 3과 같다.

수학식 3

$$D_{function} = \sum_{m=1}^M \frac{\min(DTW(R_{k,m}, C_m))}{D(m)_{reference}}$$

[0034]

[0035] 여기서, M은 함수기반 서명검증에서 사용하는 지역적인 특징 정보의 개수($M=4$)이고, $DTW(R_{k,m}, C_m)$ 은 k번째 참조서명($k=1 \sim 5$)의 m번째 특징 정보 $R_{k,m}$ 과 입력서명의 m번째 특징 정보 C_m 사이의 거리를 동적 타임 워핑 알고리즘을 통해 구한 값이다. 이 때, 각 참조서명의 특징 정보들과 입력서명의 특징 정보 사이의 거리 중 최소값을 취하는 이유는 입력서명의 특징 정보와 가장 근접한 참조서명의 특징 정보를 비교하기 위함이다. 그리고, 동적 타임 워핑 알고리즘으로 구하는 거리는 특징기반 서명검증에서 하나의 값으로 정해진 특징 정보들 간의 거리와는 달리 서명 입력시간에 따른 서명의 지역적인 속성을 점 대 점으로 비교하여 누적한 값이기 때문에 전체 거리 값의 편차가 클 수 있다. 따라서, 각 사용자에 대한 상대적인 거리를 구할 필요가 있다. 이를 위하여, 함수기반 서명검증 모듈(180)은 수학식 4와 같은 방법으로 참조서명들 간의 거리($D(m)_{reference}$)를 계산하여 참조서명과 입력서명간의 거리를 참조서명들 간의 거리로 나누어서 정규화한다.

수학식 4

$$D(m)_{reference} = \max(DTW(R_{i,m}, R_{j,m}))$$

[0036]

[0037] 여기서, $D(m)_{reference}$ 는 특징정보 부분집합에 포함된 m번째 특징 정보로, 각 특징정보에 대해 참조 서명들간의 거리를 동적 타임 워핑 알고리즘으로 구한 값 중 최대값을 의미한다. $DTW(R_{i,m}, R_{j,m})$ 은 i번째 참조 서명의 m번째 특징 정보 $R_{i,m}$ 과 j번째 참조 서명의 m번째 특징 정보 $R_{j,m}$ 사이의 거리를 동적 타임 워핑 알고리즘을 통해 구한 값이다. 이때, i와 j는 같지 않다. 참조 서명들 간의 거리의 최대값으로 나누어 준 이유는 참조 서명들 간의 오차의 최대 허용범위에 대한 비율로 누적거리를 정규화하기 위함이다.

[0038] 다시 도 2에서, 본 발명의 일실시예에 따른 하이브리드 온라인 서명검증 시스템은 서명검증 결과융합 모듈(190)에서 특징기반 서명검증 기법과 함수기반 서명검증 기법의 직렬 융합을 통해 입력서명에 대한 검증을 수행한다.

[0039] 상세하게, 직렬 융합 방법에서는 1차 검증 단계(S202)에서 특징기반 서명검증을 위해 참조서명과 입력서명과의 거리($D_{feature}$)를 허용 기준($\Theta_{feature}$)(이하, '특징기반 기준'이라 칭함)과 비교하여 특징기반 기준($\Theta_{feature}$)보다 크

면 등록된 참조 서명과의 거리가 허용치를 벗어난 경우이므로 거짓 서명으로 판정한다. 한편, 참조서명과 입력 서명과의 거리($D_{feature}$)가 특징기반 기준($\Theta_{feature}$) 이내일 경우에는 2차 검증 단계(S203)에서 함수기반 서명검증 기법으로 참조서명과 입력서명과의 거리($D_{function}$)를 허용 기준($\Theta_{function}$)(이하, '함수기반 기준'이라 칭함)과 비교한다. 참조서명과 입력서명과의 거리($D_{function}$)가 함수기반 기준($\Theta_{function}$) 이내이면 진서명으로 인증하고 다른 경우에는 거짓 서명으로 판정한다.

[0040] 본 발명의 일실시예는 특징기반 서명검증 기법과 함수기반 서명검증 기법을 직렬로 연결한 직렬 융합 방법을 사용하는 것으로, 일반적으로 특징기반 서명검증 기법이 함수기반 서명검증 기법보다 검증 속도가 빠르기 때문에 서명의 전체적인 형태 및 특성상 사용자의 등록된 참조서명과 확연하게 차이가 나는 입력서명을 빠르게 위조서명으로 판정할 수 있는 장점이 있다. 즉, 함수기반 서명 검증에서는 사용자의 등록된 참조서명과 입력서명과의 거리를 계산하기 위해 서명 입력시간에 따른 특징 비교의 차이를 누적하여 두 서명간의 차이를 나타내는 누적 거리를 계산하기 때문에 전체적인 형태 및 특성을 비교하여 거리로 표현하는 특징기반 서명 검증 기법보다 검증 시간이 오래 걸린다. 따라서, 본 발명의 일실시예에 따른 직렬 융합 방법은 1차 검증단계(S202)인 특징기반 서명검증을 성공적으로 통과한 입력서명에 대해서만 2차 검증단계(S203)에서 서명 검증시간이 오래 걸리는 함수기반 서명검증을 수행하기 때문에 확실한 위조서명을 직렬 융합의 1차 단계 검증만으로 빠르게 검출해 낼 수 있는 장점을 갖게 된다.

[0041] 본 발명의 일실시예에 따른 하이브리드 온라인 서명검증 시스템은 특징기반 서명검증 기법과 함수기반 서명검증 기법에서 사용하는 특징기반 기준 값($\Theta_{feature}$)과 함수기반 기준 값($\Theta_{function}$)에 따라서 입력된 검증용 입력서명이 진서명/가서명으로 판정되는 정도를 조절할 수 있다. 특징기반 기준 값($\Theta_{feature}$)과 함수기반 기준 값($\Theta_{function}$)을 어떻게 정하는지가 온라인 서명검증 시스템의 정확성에 영향을 주는 중요한 파라미터가 될 수 있다.

[0042] 본 발명의 일실시예는 서명검증의 신뢰도를 설정하기 위해 데이터 마이닝 기술을 이용한다.

[0043] 데이터 마이닝 기술을 적용하기 위하여 온라인 서명검증을 이용하는 사용자로부터 진서명을 수집하고 진서명을 모방한 가서명을 수집한 후 수집된 진서명과 가서명을 학습 데이터로 활용한다. 이때, 진서명과 가서명의 개수는 다를 수 있다.

[0044] 도 3은 학습 데이터의 일례로, 70명의 사용자($u_1 \sim u_{70}$) 각각에 대하여 진서명 30개를 수집하고 각 진서명을 정교하게 모방한 가서명 30개를 수집한 것이다. 실제 온라인 서명검증을 위해 수집된 학습 데이터에서 각 사용자(u_1)의 진서명 중 참조서명으로 사용하기 위한 참조용 진서명(301)을 k 개($k=5$) 선택하고 다른 나머지 진서명(25개)을 학습용 진서명(302)으로 사용한다. 그리고, 해당 사용자(u_1)의 진서명을 모방한 가서명 30개는 전문위조 서명(303)으로 활용하고 다른 사용자($u_2 \sim u_{70}$)의 진서명 중에서 임의로 30개를 택해서 랜덤위조 서명(304)으로 활용한다. 이때, 전문위조 서명(303)과 랜덤위조 서명(304)을 학습용 가서명으로 사용하게 되는데, 학습용 가서명으로 전문위조 서명(303)만을 사용하거나, 필요에 따라서는 전문위조 서명(303)과 랜덤위조 서명(304)을 임의로 혼합하여 학습용 가서명으로 사용할 수 있다. 이하에서는, 전문위조 서명(303)과 랜덤위조 서명(304)이 혼합된 학습용 가서명을 '전문+랜덤 위조서명'이라 칭한다.

[0045] 도 4는 데이터 마이닝 기법을 이용한 FAR과 FRR 설정 방법의 전 과정을 설명하기 위한 도면이다. 여기서, 학습 데이터에 대한 서명들간의 거리 계산 방법은 서명검증 방법 즉, 특징기반 서명검증 기법 또는 함수기반 서명검증 기법에 따라 상기에서 설명한 $D_{feature}$ 와 $D_{function}$ 계산식을 이용할 수 있다.

[0046] 먼저, 각 사용자 별로 선택한 참조용 진서명들간의 거리(D_r)를 계산하여(S401) 최대값을 $\max_D_r$ 이라 정의한다. 참조용 진서명들과 학습용 진서명들간의 거리(D_g)를 계산하여(S402) 최소값을 $\min_D_g$ 라고 정의하며 참조용 진서명들과 학습용 가서명들간의 거리(D_f)를 계산하여(S403) 최소값을 $\min_D_f$ 라고 정의한다.

[0047] 각 사용자 별로 $\frac{\min_D_g}{\max_D_r}$ 을 계산하여 이를 해당 사용자의 '최소 진서명 거리비율'이라고 정의하고 모든 사용

자의 최소 진서명 거리비율을 오름차순으로 정렬한다(S404). 각 사용자 별로 $\frac{\min_D_f}{\max_D_r}$ 을 계산하여 이를 해

당 사용자의 '최소 가서명 거리비율'이라고 정의하고 모든 사용자의 최소 가서명 거리비율을 오름차순으로 정렬한다(S405).

[0048] 그리고, 모든 사용자의 최소 진서명 거리비율 리스트에 대해 임의로 임계값을 0에서부터 차례로 올렸을 때 최소 진서명 거리비율이 해당 임계값보다 커서 진서명으로 인정받지 못하는(즉, 진서명 거부 오류(false reject error)) 사용자의 비율을 계산하여 해당 임계값에서의 FRR(false rejection ratio)로 정의한다(S406). 같은 방법으로, 모든 사용자의 최소 가서명 거리비율 리스트에 대해 임의로 임계값을 0에서부터 차례로 올렸을 때 최소 가서명 거리비율이 해당 임계값보다 작아서 진서명으로 잘못 인정되는(즉, 위조서명 인증 오류(false acceptance error)) 사용자의 비율을 계산하여 해당 임계값에서의 FAR(false acceptance ratio)로 정의한다(S407).

[0049] 따라서, 본 발명의 일실시예는 서명검증의 신뢰도를 설정하기 위해 데이터 마이닝 기술을 이용하여 산출된 FRR과 FAR을 특징기반 기준 값($\Theta_{feature}$)과 함수기반 기준 값($\Theta_{function}$)으로 활용할 수 있다.

[0050] 온라인 서명검증을 필요로 하는 응용에서는 응용서비스의 내용 및 중요도에 따라 다른 서명검증 신뢰도를 사용할 수 있다. 예를 들면, 중요한 서비스를 제공하기 위해 본인 인증을 하는 경우에는 높은 서명검증 신뢰도를 이용해야 하며 중요하지 않은 서비스를 제공하는 경우에는 서명검증이 형식적이거나 아예 서명검증을 하지 않고 입력된 서명을 이미지로 저장하는 것으로 만족할 수도 있을 것이다. 또한, 사용자의 서명의 복잡도에 따라 다른 서명검증 신뢰도를 사용할 수 있다. 예를 들면, 위조가 어려운 정도의 복잡한 서명을 사용하는 사용자를 위해서는 낮은 신뢰도로 서명검증을 하고 위조가 쉬운 정도의 간단한 서명을 사용하는 사용자를 위해서는 높은 신뢰도로 서명검증을 실시할 수도 있다. 따라서, 본 발명의 일실시예에서는 온라인 하이브리드 서명검증 시스템에서 특징기반 서명검증 기법과 함수기반 서명검증 기법을 직렬로 융합시키고 각 기법에서 사용하는 기준 값 $\Theta_{feature}$ 와 $\Theta_{function}$ 를 다르게 설정하도록 허용함으로써 응용에 따라서 또는 사용자 등록 서명의 복잡도에 따라서 다른 신뢰도 기준으로 서명검증을 할 수 있도록 지원한다.

[0051] 일례로, 본 발명의 일실시예에서는 다양한 응용의 서명검증을 지원하기 위한 체계적인 다기준 서명검증 신뢰도로 표 1과 같이 보안등급 0단계에서부터 7단계까지 총 8개의 신뢰도 기준을 설정할 수 있다. 다기준 서명검증 신뢰도는 임의로 설정한 것이 아니라 온라인 서명검증 데이터 집합을 대상으로 데이터 마이닝 기법을 활용하여 도 3과 도 4를 참조로 설명한 방법을 이용하여 체계적으로 설정한 신뢰도 기준 값들이다.

표 1

[0052]

보안등급	$\Theta_{feature}$	$\Theta_{function}$	설정 기준
㉠	∞	∞	서명검증을 실행하지 않음
①	1.192	∞	특징기반 서명검증 기법만을 이용하여 전문+랜덤 위조서명을 학습용 가서명으로 이용하여 FRR=0인 최소의 거리 값을 $\Theta_{feature}$ 으로 설정하여 직렬융합의 첫 번째 단계만 수행
②	1.192	1.024	직렬융합의 첫 번째 단계의 기준으로 ①의 $\Theta_{feature}$ 값을 사용하고 두 번째 단계의 함수기반 신뢰도 기준 값을 위해 전문+랜덤 위조서명을 학습용 가서명으로 사용한 EER의 거리 값을 $\Theta_{function}$ 으로 사용
③	1.192	0.967	직렬융합의 첫 번째 단계의 기준으로 ①의 $\Theta_{feature}$ 값을 사용하고 두 번째 단계의 함수기반 신뢰도 기준 값을 위해 전문 위조 서명만을 학습용 가서명으로 사용한 EER의 거리 값을 $\Theta_{function}$ 으로 사용
④	1.192	0.866	직렬융합의 첫 번째 단계의 기준으로 ①의 $\Theta_{feature}$ 값을 사용하고 두 번째 단계의 함수기반 신뢰도 기준 값을 위해 전문 위조 서명만을 학습용 가서명으로 이용하여 FAR=7이 되는 최소 거리 값을 $\Theta_{function}$ 으로 사용
⑤	1.192	0.697	직렬융합의 첫 번째 단계의 기준으로 ①의 $\Theta_{feature}$ 값을 사용하고 두 번째 단계의 함수기반 신뢰도 기준 값을 위해 전문 위조 서명만을 학습용 가서명으로 이용하여 FAR=2가 되는 최소 거리 값을 $\Theta_{function}$ 으로 사용

⑥	1.192	0.637	직렬융합의 첫 번째 단계의 기준으로 ①의 $\theta_{feature}$ 값을 사용하고 두 번째 단계의 함수기반 신뢰도 기준 값을 위해 전문 위조 서명만을 학습용 가서명으로 이용하여 FAR=1이 되는 최소 거리 값을 $\theta_{function}$ 으로 사용
⑦	1.192	0.510	직렬융합의 첫 번째 단계의 기준으로 ①의 $\theta_{feature}$ 값을 사용하고 두 번째 단계의 함수기반 신뢰도 기준 값을 위해 전문 위조 서명만을 학습용 가서명으로 이용하여 FAR=0이 되는 최소 거리 값을 $\theta_{function}$ 으로 사용

- [0053] 보안등급 0단계에서는 검증용 입력서명에 대해서 실제 검증 과정을 수행하지 않고도 진서명으로 인증하는 단계이며, 보안등급 1단계에서는 직렬 융합의 첫 번째 단계인 특징기반 서명 검증 단계만 수행하는 단계이며, 보안등급 2단계에서는 이후 특징기반 서명 검증을 위한 신뢰도 기준은 보안등급 1단계와 같게 설정하고 두 번째 함수기반 서명검증 단계의 서명검증 신뢰도 기준을 보안등급 7단계까지 점차적으로 높여가는 방법으로 다기준을 설정한 것이다. 표 1에서 FAR은 위조서명 인증 오류의 비율(false acceptance ratio)을 의미하며 FRR은 진서명 거부 오류의 비율(false rejection ratio)을 의미한다. EER(equal error ratio)은 위조서명 인증 오류의 비율과 진서명 거부 오류의 비율이 같은 지점을 의미한다.
- [0054] 설정된 다기준 서명검증 신뢰도의 각 보안등급 선정 이유 및 활용가능 분야를 정리하면 다음과 같다.
- [0055] 보안등급 ⑥: 검증을 위해 입력된 검증용 입력서명에 대해서 서명검증을 실시하지 않고 모두 인증과정을 통과한 것으로 인정한다. 즉, 직렬 융합에서 무조건 첫 번째 단계와 두 번째 단계를 통과한 것으로 해석하여 입력된 검증용 입력서명이 모두 진서명으로 인위적으로 판정되도록 하는 보안등급으로서 이는 보안검증을 위한 실제 서명검증이 필요 없고 입력된 서명을 단순히 저장하는 응용에서 활용할 수 있다.
- [0056] 보안등급 ①: 직렬 융합에서 2차 검증과정을 거치지 않고 1차 검증과정만 통과하면 진서명으로 판정하는 보안등급으로서 서명의 전체적인 형태 및 특징만 유사하면 진서명으로 인정을 하는 보안등급이다. 즉, 직렬융합의 첫 번째 단계인 특징기반 서명검증 기법에서는 위조서명을 빠르게 기각시키는 것이 주요 목적이므로 가능한 진서명 거부 오류(false reject error)가 발생하지 않도록 하기 위해 FRR=0인 최소 거리 값을 $\theta_{feature}$ 값으로 활용한다(도 5 참조). 이 보안등급은 서명의 전체적인 형태 및 글로벌 특징들로만 유사도를 비교하는 특징기반 서명 검증기법만을 이용하여 빠르게 온라인 서명의 진위를 판단하는 응용에서 활용할 수 있다.
- [0057] 보안등급 ②: 직렬융합의 1, 2차 검증과정을 모두 사용하는 보안등급 중 가장 낮은 신뢰도를 갖는 보안등급으로 보안등급 ①의 $\theta_{feature}$ 값으로 특징기반 서명검증을 수행하고 이를 통과한 서명에 대해서는 추가적으로 함수기반 서명검증을 수행한다. 함수기반 서명검증 기법의 기준 $\theta_{function}$ 값은 전문위조 서명과 랜덤위조 서명을 임의로 혼합한 '전문+랜덤 위조 서명'을 학습용 가서명으로 사용하여 구한 FRR과 FAR이 같아지는 지점(EER)의 거리 값으로 설정한다(도 6 참조). 이 보안등급은 서명의 전체적인 형태 및 글로벌 특징들만으로 유사도를 비교하는 특징기반 서명 검증기법을 통과한 서명에 대해서 서명 시간의 흐름에 따른 특징을 비교하여 좀 더 정확하게 입력서명의 진위 여부를 판단하려는 응용에서 사용할 수 있다.
- [0058] 보안등급 ③: 보안등급 ②와 유사하지만 함수기반 서명검증 기법의 기준 $\theta_{function}$ 값을 설정하기 위한 학습용 가서명으로 전문위조 서명만을 이용하여 FRR과 FAR이 같아지는 지점(EER)의 거리 값으로 설정한다. 학습용 가서명에 전문위조 서명만을 포함시키므로 랜덤위조 서명을 포함시킨 경우보다 FAR이 높아지므로 ERR지점이 낮아지는 효과가 있다(도 6 참조). 즉, 좀 더 정확한 함수기반 서명 검증을 통해 직렬융합의 2차 검증과정을 실시할 필요가 있는 응용에서 사용할 수 있다.
- [0059] 보안등급 ④: 보안등급 ③과 유사하지만 함수기반 서명검증 기법의 기준 $\theta_{function}$ 값을 설정하기 위한 학습용 가서명으로 전문위조 서명만을 이용하여 FAR이 7%인 지점의 거리 값으로 설정한다(도 6 참조). FAR을 7%로 설정한 근거는 도 3에서 설명한 바와 같이 수집된 서명검증 데이터 집합(서명 시간 t에 따른 좌표 값 (x,y)와 압력 값 p로 원시 데이터 구성)에 대해 현재까지 개발된 다양한 데이터 마이닝 기법을 이용하여 분류할 때 실험 결과에 의하면 정확도가 최대 93% 정도 값을 갖는 것으로 조사된다. 따라서, 허용 오류 정도를 7%로 설정한 것이다. 이 보안등급은 서명검증을 위해 사용되는 서명 입력장치가 서명시간에 따른 좌표 값과 압력 값을 제공하는 경우에 사용하면 적당하다.
- [0060] 보안등급 ⑤: 보안등급 ④와 유사하지만 함수기반 서명검증 기법의 기준 $\theta_{function}$ 값을 설정하기 위한 학습용 가

서명으로 전문위조 서명만을 이용하여 FAR이 2%인 지점의 거리 값으로 설정한다(도 6 참조). FAR을 2%로 설정한 근거는 서명검증 알고리즘의 성능을 비교하기 위해 사용되는 이상적인 서명검증 데이터 집합(서명시간 t에 따른 좌표 값 (x,y), 압력 값 p, 펜의 각도, 펜의 기울기로 구성된 SVC 2004 데이터)에 대해 현재까지 개발된 다양한 데이터 마이닝 기법을 이용하여 분류할 때 실험 결과에 의하면 정확도가 최대 98% 정도 값을 갖는 것으로 조사된다. 따라서, 허용 오류 정도를 2%로 설정한 것이다. 이 등급은 서명 시간에 따른 좌표 값과 압력 값 이외로 펜의 각도 및 기울기 등을 제공할 수 있는 서명 입력장치를 사용하는 응용을 위한 서명검증 신뢰도로 사용할 수 있다.

[0061] 보안등급 ⑥: 보안등급 ⑤와 유사하지만 함수기반 서명검증 기법의 기준 $\Theta_{function}$ 값을 설정하기 위한 학습용 가 서명으로 전문위조 서명만을 이용하여 FAR이 1%인 지점의 거리 값으로 설정한다(도 6 참조). FAR을 1%로 설정한 근거는 현재까지 연구되어 실제로 개발된 서명검증 알고리즘들의 정확성 목표가 99%정도이다. 따라서, 허용 오류 정도를 1%로 설정한 것이다. 이 등급은 현재의 서명검증 기술이 목표로 하는 신뢰도 수치이므로 높은 서명검증 신뢰도를 필요로 하는 응용에서 사용할 수 있다.

[0062] 보안등급 ⑦: 보안등급 ⑥과 유사하지만 함수기반 서명검증 기법의 기준 $\Theta_{function}$ 값을 설정하기 위한 학습용 가 서명으로 전문위조 서명만을 이용하여 FAR이 0%인 지점의 거리 값으로 설정한다(도 6 참조). FAR이 0%라는 의미는 위조서명을 잘못 분류하여 진서명으로 인증하는 경우가 확률적으로 발생하지 않음을 의미하는 기준이므로 특징기반 서명검증으로는 FRR=0인 지점을 기준으로 사용하고 함수기반 서명검증에서는 FAR=0인 지점을 기준으로 사용함으로써 완벽한 정확성을 갖는 서명검증 기준이라고 할 수 있다. 따라서, 이 등급에서는 서명의 일관성이 떨어지는 사용자 본인도 쉽게 통과하지 못하는 서명검증 신뢰도이다. 즉, 매우 중요한 서비스를 제공하여 사용자 본인 확인이 중요한 응용에서 사용할 수 있다.

[0063] 도면 7은 특징기반 서명검증 기법에 의한 거리 값과 함수기반 서명검증 기법에 의한 거리 값을 융합해서 사용자의 참조서명과 검증용 입력서명간의 유사도 값(0 ~100)을 출력하는 병렬 융합 과정을 표현한 것이다.

[0064] 먼저, 특징기반 서명검증 기법과 함수기반 서명검증 기법에 따른 참조서명과 입력서명과의 거리($D_{feature}$, $D_{function}$)를 산출한다(S701). 참조서명과 입력서명과의 거리($D_{feature}$, $D_{function}$)를 산출하는 과정은 도 2를 참조로 설명한 수학적 1 내지 수학적 4에 의한 산출 방식과 동일하다.

[0065] 그리고, 특징기반 서명검증을 위해 참조서명과 입력서명과의 거리($D_{feature}$)에 해당하는 $FAR_{feature}$ 값을 추출하고(S702) 함수기반 서명검증을 위해 참조서명과 입력서명과의 거리($D_{function}$)에 해당하는 $FAR_{function}$ 값을 추출한다(S703).

[0066] 특징기반 서명검증 기법의 검증결과($FAR_{feature}$)와 함수기반 서명검증 기법의 검증결과($FAR_{function}$)를 이용하여 서명진위 판단을 위한 참조서명과 입력서명 간의 유사도를 산출한다(S704). 이때, 참조서명과 입력서명 간의 유사도(Similarity)는 수학적 5와 같이 정의할 수 있다.

수학적 5

$$Similarity = \frac{(1 - FAR_{feature}) + (1 - FAR_{function})}{2}$$

[0067]

[0068] 본 발명의 일실시예는 특징기반 서명검증 기법의 검증결과($FAR_{feature}$)와 함수기반 서명검증 기법의 검증결과($FAR_{function}$)를 통합하여 하나의 유사도 값으로 사용자에게 제시하므로 두 기법의 서명검증 결과를 보완적으로 사용할 수 있는 융합 방법이며, 입력서명이 사용자의 등록된 참조서명과 어느 정도 유사한지를 보고 서명의 진위 여부를 퍼지(fuzzy) 단계로 표현하려는 응용에 적합하다.

[0069] 도 8과 도 9는 본 발명의 일실시예에 따른 다기준 신뢰도 지원 하이브리드 온라인 서명검증 시스템을 위한 사용자 인터페이스의 일례를 도시한 것이다.

[0070] 온라인 서명검증을 필요로 하는 응용의 특성 및 서비스 중요성, 또는 사용자 서명의 복잡성 및 반복 일관성 정도에 따라 신뢰도에 따른 서명의 진위 판단 결과를 출력하는 인터페이스(도 8) 또는 입력서명과 등록된 참조서명과의 유사도 값을 출력하는 인터페이스(도 9)를 구성할 수 있다. 다기준 서명검증 신뢰도를 기준으로 하는

경우에는 신뢰도 버튼(801)을 선택하고 유사도를 기준으로 fuzzy한 결정을 하고자 할 때는 유사도 버튼(901)을 선택한다. 이러한 버튼 선택은 사용자가 매뉴얼 방식으로 선택할 수도 있고 상황 파악을 한 후에 시스템이 동적으로 자동으로 설정할 수도 있다. 또한, 다기준 신뢰도를 선택한 경우(도 8)에는 적절한 보안등급을 관리자가 설정할 수도 있으며 시스템이 환경에 따라 동적으로 보안등급을 선택할 수도 있다. 유사도를 선택한 경우(도 9)에는 출력된 유사도 값에 따라 입력서명의 진위 여부를 fuzzy하게 결정할 수 있다.

[0071] 본 발명의 일실시예는 특정기반 서명검증 기법과 함수기반 서명검증 기법을 융합하여 다기준 신뢰도를 지원할 수 있으며 시스템에 의한 자동 또는 사용자 선택적으로 서명검증의 신뢰도를 동적으로 조절할 수 있도록 함으로써 온라인 서명검증의 응용 환경에 적합한 서명검증의 정확성 및 보안성을 지원할 수 있다.

[0072] 본 발명의 실시예들은 다양한 컴퓨터로 구현되는 동작을 수행하기 위한 프로그램 명령을 포함하는 컴퓨터 판독 가능 매체를 포함한다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광 기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0073] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0074] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

도면의 간단한 설명

[0075] 도 1은 본 발명의 일실시예에 따른 하이브리드 온라인 서명검증 시스템의 내부 구성을 도시한 것이다.

[0076] 도 2는 본 발명의 일실시예에 따른 하이브리드 온라인 서명검증 시스템에서의 직렬 융합을 통한 서명검증 과정을 설명하기 위한 도면이다.

[0077] 도 3은 다기준 신뢰도를 설정하기 위하여 활용되는 학습 데이터를 설명하기 위한 도면이다.

[0078] 도 4는 데이터 마이닝 기술을 이용한 다기준 신뢰도 설정 방법을 설명하기 위한 도면이다.

[0079] 도 5와 도 6은 보안등급에 따른 다기준 서명검증 신뢰도 설정 과정을 설명하기 위한 도면이다.

[0080] 도 7은 본 발명의 일실시예에 따른 하이브리드 온라인 서명검증 시스템에서의 병렬 융합을 통한 서명검증 과정을 설명하기 위한 도면이다.

[0081] 도 8과 도 9는 본 발명의 일실시예에 따른 다기준 신뢰도 지원 하이브리드 온라인 서명검증 시스템을 위한 사용자 인터페이스의 일례를 도시한 것이다.

[0082] <도면의 주요 부분에 대한 부호의 설명>

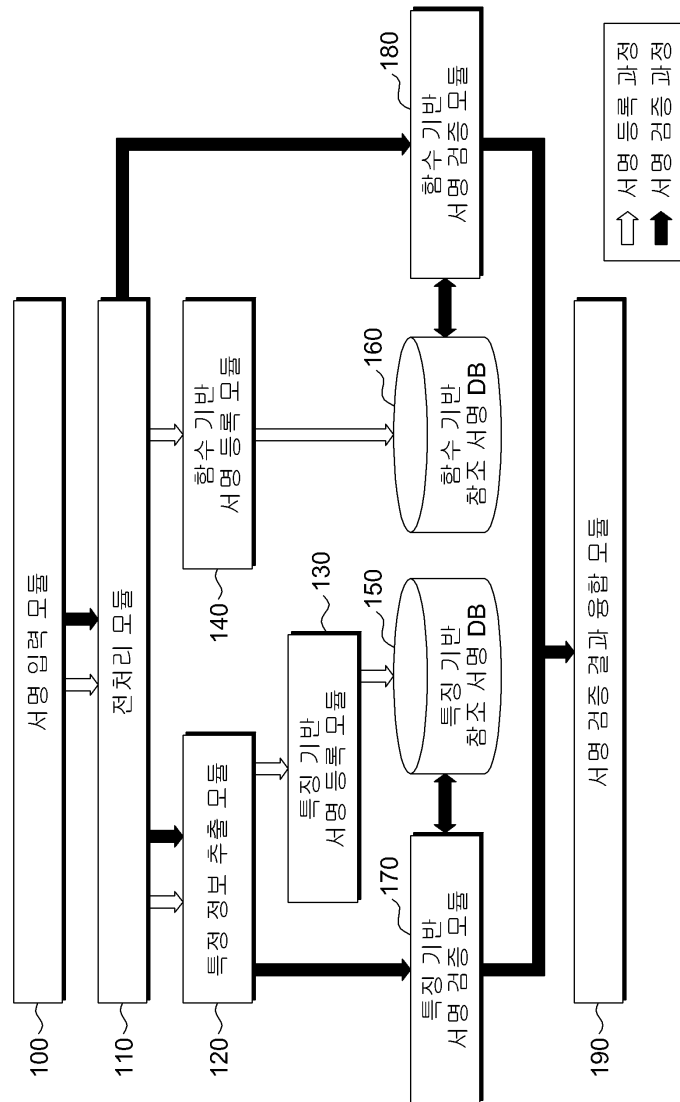
[0083] 170: 특징기반 서명검증 모듈

[0084] 180: 함수기반 서명검증 모듈

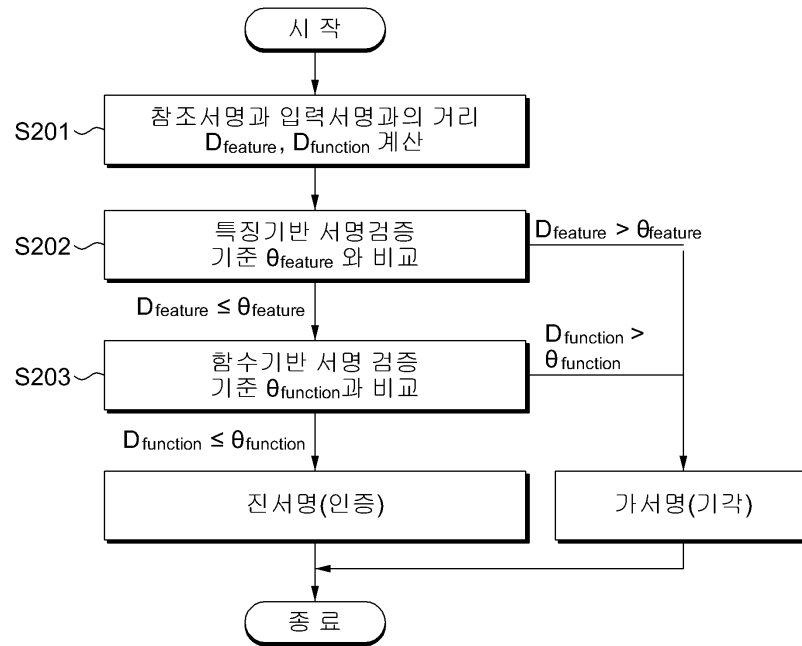
[0085] 190: 서명검증 결과융합 모듈

도면

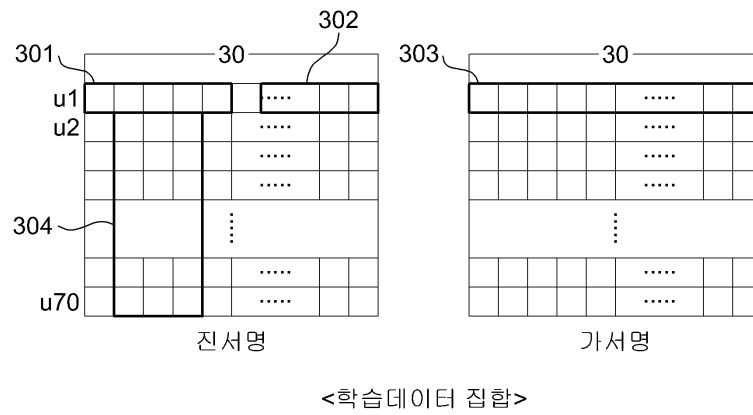
도면1



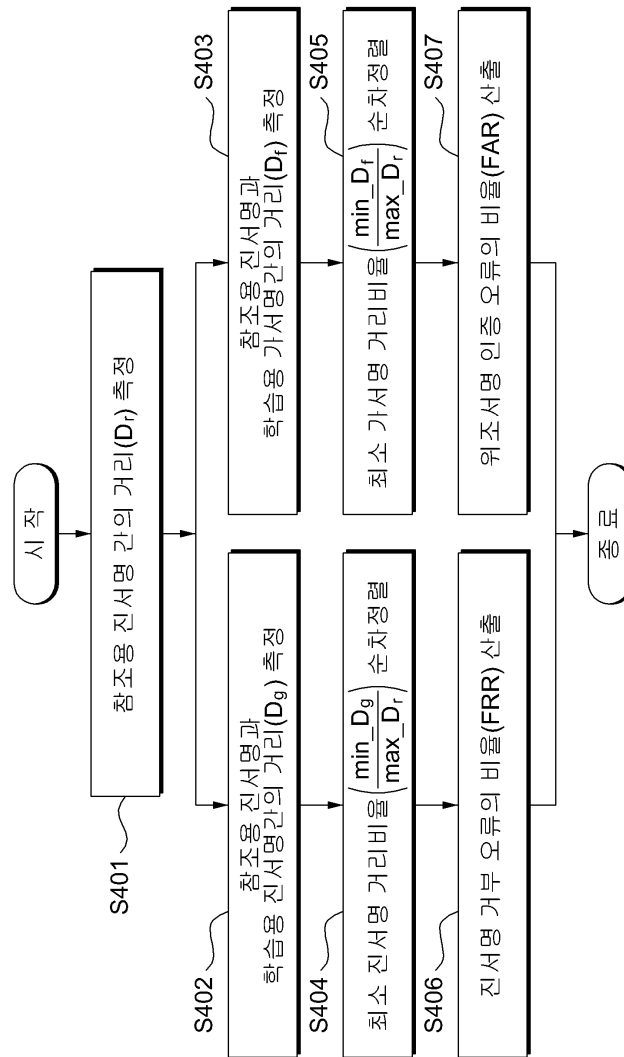
도면2



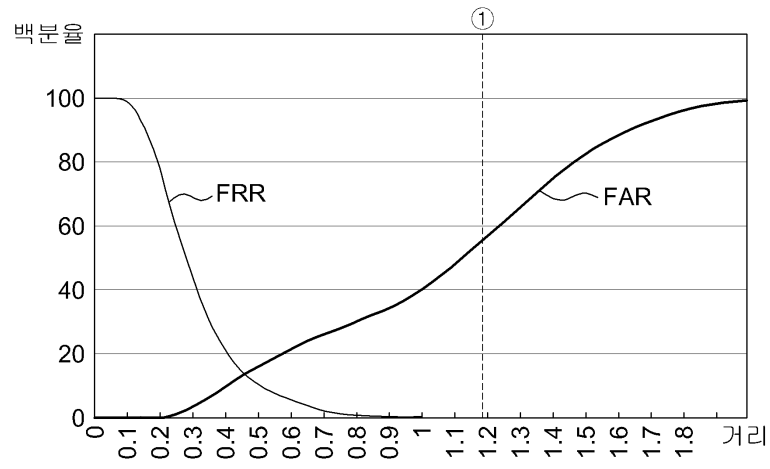
도면3



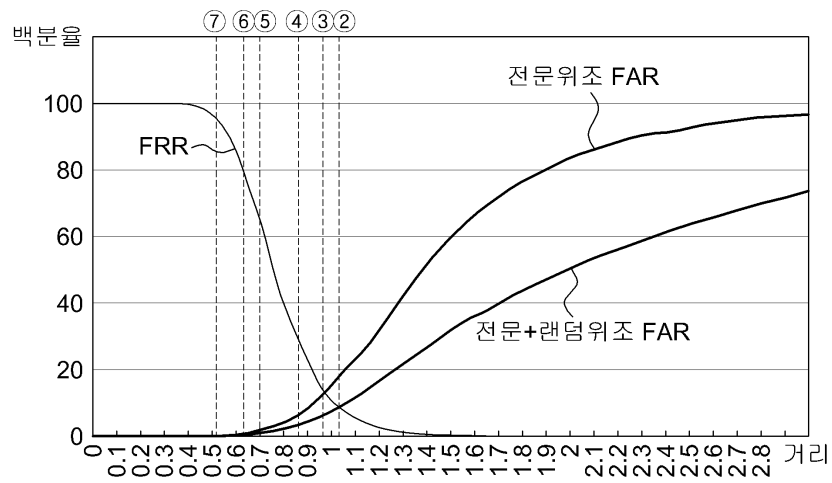
도면4



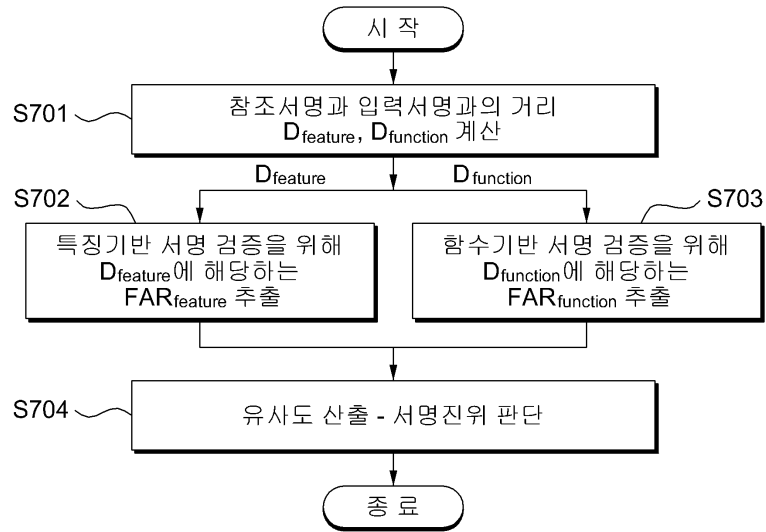
도면5



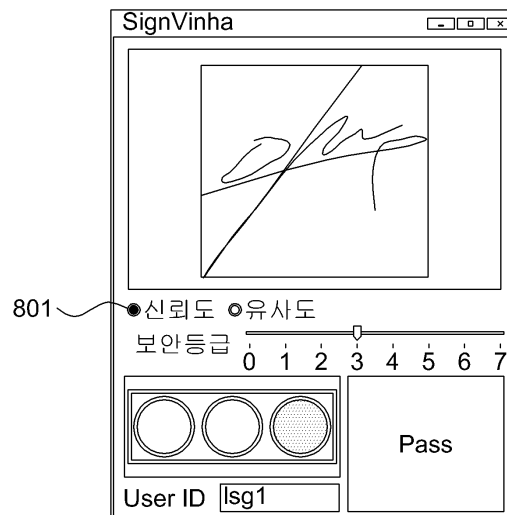
도면6



도면7



도면8



도면9

