

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0139718

(43) 공개일자 2024년09월24일

(51) 국제특허분류(Int. Cl.)

H04L 9/32 (2006.01)

(52) CPC특허분류

H04L 9/3231 (2013.01)

H04L 9/3228 (2013.01)

(21) 출원번호 10-2023-0033753

(22) 출원일자 2023년03월15일

심사청구일자 2023년03월15일

(71) 출원인

인하대학교 산학협력단

인천광역시 미추홀구 인하로 100(용현동, 인하대학교)

(72) 발명자

이문규

인천광역시 연수구 컨벤시아대로42번길 95, 1005동 1403호(송도동, 더샵 엑스포)

권희용

인천광역시 미추홀구 인주대로 148, 102동 1814호(용현동, 효성해링턴타워인하)

(74) 대리인

양성보

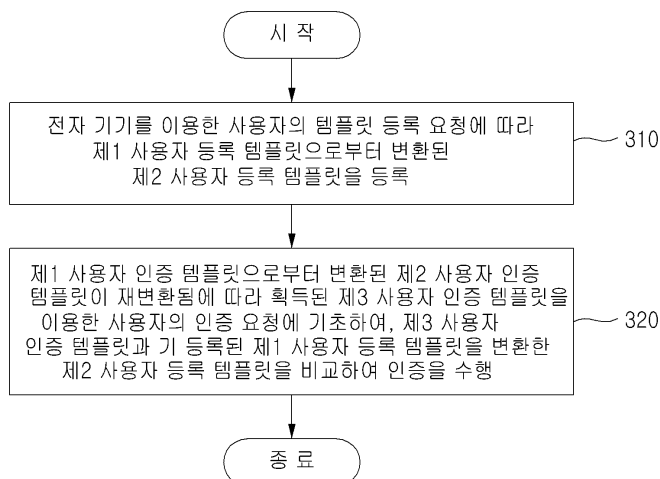
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 생체정보 기반 OTP 인증 방법

(57) 요약

생체정보 기반 OTP 인증 방법이 개시된다. 일 실시예에 따른 인증 시스템에 의해 수행되는 생체정보 기반의 일회용 비밀번호(One-Time Password; OTP) 인증 방법은, 전자 기기를 이용한 사용자의 템플릿 등록 요청에 따라 제1 사용자 등록 템플릿으로부터 변환된 제2 사용자 등록 템플릿을 등록하는 단계; 및 제1 사용자 인증 템플릿으로부터 변환된 제2 사용자 인증 템플릿을 재변환함에 따라 획득된 제3 사용자 인증 템플릿을 이용한 사용자의 인증 요청에 기초하여, 상기 제3 사용자 인증 템플릿과 기 등록된 제1 사용자 등록 템플릿을 변환한 제2 사용자 등록 템플릿을 비교하여 인증을 수행하는 단계를 포함할 수 있다.

대표도 - 도3



이 발명을 지원한 국가연구개발사업

과제고유번호 1711179347
 과제번호 RS-2022-00155915
 부처명 과학기술정보통신부
 과제관리(전문)기관명 정보통신기획평가원
 연구사업명 인공지능융합혁신인재양성
 연구과제명 인공지능융합혁신인재양성(인하대학교)
 기 여 율 1/3
 과제수행기관명 인하대학교 산학협력단
 연구기간 2023.01.01 ~ 2023.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호 1711170542
 과제번호 2022-0-01047
 부처명 과학기술정보통신부
 과제관리(전문)기관명 정보통신기획평가원
 연구사업명 데이터프라이버시글로벌선도기술연구개발(R&D)
 연구과제명 실수연산 기반의 동형암호를 활용한 통계 분석 알고리즘 및 모듈 개발
 기 여 율 1/3
 과제수행기관명 (주)크립토탭
 연구기간 2022.04.01 ~ 2024.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호 1711194266
 과제번호 RS-2023-00209294
 부처명 과학기술정보통신부
 과제관리(전문)기관명 한국연구재단
 연구사업명 중견연구(후속)
 연구과제명 블록체인 상의 기밀성 제공을 위한 기능성 양자내성암호 응용 및 연산 최적화 기술

개발

기 여 율 1/3
 과제수행기관명 인하대학교
 연구기간 2023.03.01 ~ 2026.02.28

명세서

청구범위

청구항 1

인증 시스템에 의해 수행되는 생체정보 기반의 일회용 비밀번호(One-Time Password; OTP) 인증 방법에 있어서, 전자 기기를 이용한 사용자의 템플릿 등록 요청에 따라 제1 사용자 등록 템플릿으로부터 변환된 제2 사용자 등록 템플릿을 등록하는 단계; 및

제1 사용자 인증 템플릿으로부터 변환된 제2 사용자 인증 템플릿을 재변환함에 따라 획득된 제3 사용자 인증 템플릿을 이용한 사용자의 인증 요청에 기초하여, 상기 제3 사용자 인증 템플릿과 기 등록된 제1 사용자 등록 템플릿을 변환한 제2 사용자 등록 템플릿을 비교하여 인증을 수행하는 단계

를 포함하는 일회용 비밀번호 인증 방법.

청구항 2

제1항에 있어서,

상기 등록하는 단계는,

상기 사용자로부터 입력 인터페이스를 통해 제1 사용자 등록 템플릿(U)이 획득되고, 템플릿 변환 함수(F)에 사용될 변환 파라미터(p)가 생성 및 저장되고, 상기 템플릿 변환 함수(F)에 상기 변환 파라미터(p)를 사용하여 제1 사용자 등록 템플릿(U)이 변환됨에 따라 제2 사용자 등록 템플릿(U')이 획득되고, 상기 사용자로부터 상기 획득된 제2 사용자 등록 템플릿(U')이 전달됨을 수신하고, 상기 수신된 제2 사용자 등록 템플릿(U')을 사용자의 인증 정보로써 등록하는 단계

를 포함하는 일회용 비밀번호 인증 방법.

청구항 3

제2항에 있어서,

상기 제1 사용자 등록 템플릿(U)은,

전자 기기를 이용한 생체정보 기반 인증 방식을 위해 상기 전자 기기의 생체정보 수집 장치를 통해 획득된 사용자의 생체정보에 기반하여 사용자 생체정보의 템플릿이 획득된 것인, 일회용 비밀번호 인증 방법.

청구항 4

제2항에 있어서,

상기 변환함수는,

임의의 벡터를 회전시키는 변환을 수행하는 것으로,

상기 제1 사용자 등록 템플릿(U)이 n (n 은 자연수)-차원 벡터로 표현될 때, 상기 변환 파라미터(p)를 씨드(seed)로 하여 임의의 n (n 은 자연수) 개의 정보를 각각 생성한 후, 상기 벡터의 n (n 은 자연수) 개의 요소에 따라 상기 생성된 정보만큼 각 요소를 변환하는 것인, 일회용 비밀번호 인증 방법.

청구항 5

제1항에 있어서,

상기 인증을 수행하는 단계는,

상기 사용자로부터 입력 인터페이스를 통해 제1 사용자 인증 템플릿(V)이 획득되고, 템플릿 변환 함수(F)에 변환 파라미터(p)를 사용하여 상기 제1 사용자 인증 템플릿(V)이 변환됨에 따라 제2 사용자 인증 템플릿(V')이 획득되고, 상기 템플릿 변환 함수(F)에 사용될 재변환 파라미터(p')가 생성되고, 상기 템플릿 변환 함수(F)에 상

기 재변환 파라미터(p')를 사용하여 상기 제2 사용자 인증 템플릿(V')이 재변환됨에 따라 제3 사용자 인증 템플릿(V'')이 획득되고, 상기 사용자로부터 상기 획득된 제3 사용자 인증 템플릿(V'')이 전달됨에 따라 사용자의 인증 요청을 수신하는 단계

를 포함하는 일회용 비밀번호 인증 방법.

청구항 6

제5항에 있어서,

상기 인증을 수행하는 단계는,

상기 템플릿 변환 함수(F)에 사용될 재변환 파라미터(p')를 생성하고, 상기 템플릿 변환 함수(F)에 상기 재변환 파라미터(p')를 사용하여 기 등록된 제1 사용자 등록 템플릿(R')이 변환됨에 따라 제2 사용자 등록 템플릿(R'')을 획득하고, 상기 제3 사용자 인증 템플릿(V'')을 상기 제2 사용자 등록 템플릿(R'')과 비교하여 인증을 수행하고, 상기 인증을 수행한 사용자 인증 결과를 상기 사용자에게 전달하는 단계

를 포함하는 일회용 비밀번호 인증 방법.

청구항 7

제5항에 있어서,

상기 제1 사용자 인증 템플릿(V)은,

전자 기기를 이용한 생체정보 기반 방식을 위해 상기 전자 기기의 생체정보 수집 장치를 통해 획득된 사용자의 생체정보에 기반하여 사용자 생체정보의 템플릿이 획득된 것인, 일회용 비밀번호 인증 방법.

청구항 8

제6항에 있어서,

상기 인증을 수행하는 단계는,

상기 제3 사용자 인증 템플릿(V'')과 상기 제2 사용자 등록 템플릿(R'')의 유사도를 통해 획득된 측정값을 기 정의된 인증 임계값을 기준으로 허가 또는 거부를 포함하는 사용자 인증 결과를 도출하는 단계

를 포함하는 일회용 비밀번호 인증 방법.

청구항 9

제8항에 있어서,

상기 인증을 수행하는 단계는,

상기 제3 사용자 인증 템플릿(V'')에 대한 사용자 인증 결과가 허가일 경우, 사용자의 템플릿 갱신 요청에 따라 사용자 템플릿을 갱신하는 단계

를 포함하는 일회용 비밀번호 인증 방법.

청구항 10

제9항에 있어서,

상기 인증을 수행하는 단계는,

상기 사용자로부터 입력 인터페이스를 통해 제1 갱신 템플릿(N)이 획득되고, 템플릿 변환 함수(F)에 사용될 템플릿 갱신 파라미터(p'')가 생성 및 저장되고, 상기 템플릿 변환 함수(F)에 상기 템플릿 갱신 파라미터(p'')를 사용하여 제1 갱신 템플릿(N)이 변환됨에 따라 제2 갱신 템플릿(N')이 획득되고, 상기 사용자로부터 상기 제2 갱신 템플릿(N')과 상기 템플릿 갱신 파라미터(p'')의 해시값이 전달됨을 수신하는 단계

를 포함하는 일회용 비밀번호 인증 방법.

청구항 11

제10항에 있어서,

상기 인증을 수행하는 단계는,

상기 제3 사용자 인증 템플릿(V'')의 해시값에 대한 제2해시값을 계산하고, 상기 수신된 템플릿 갱신 파라미터(p'')의 해시값과 상기 제3 사용자 인증 템플릿(V'')으로부터 계산된 해시값에 대한 제2 해시값이 일치하는 경우, 상기 제2 갱신 템플릿(N')을 사용자의 새로운 템플릿으로 갱신하는 단계

를 포함하는 일회용 비밀번호 인증 방법.

청구항 12

인증 시스템에 있어서,

전자 기기를 이용한 사용자의 템플릿 등록 요청에 따라 제1 사용자 등록 템플릿으로부터 변환된 제2 사용자 등록 템플릿을 등록하는 등록부; 및

제1 사용자 인증 템플릿으로부터 변환된 제2 사용자 인증 템플릿을 재변환함에 따라 획득된 제3 사용자 인증 템플릿을 이용한 사용자의 인증 요청에 기초하여, 상기 제3 사용자 인증 템플릿과 기 등록된 제1 사용자 등록 템플릿을 변환한 제2 사용자 등록 템플릿을 비교하여 인증을 수행하는 인증부

를 포함하는 인증 시스템.

발명의 설명

기술 분야

[0001] 아래의 설명은 일회용 비밀번호 인증 기술에 관한 것이다.

배경 기술

[0003] 네트워크 및 모바일 기술의 발전으로 오프라인에서 존재하던 다양한 산업 및 어플리케이션들이 온라인으로 이동하였다. 또한 금융산업과 같은 개인의 재산과 관련된 서비스들이 온라인에서 서비스됨에 따라 개인의 식별은 온라인 서비스의 보안과 효율성을 위하여 매우 중요하게 여겨진다.

[0004] 개인을 식별하기 위한 절차로써 사용자 인증이 대부분의 서비스에서 채택되고 있다. 사용자 인증이란 서비스를 사용하는 사용자가 정당한 사용자인지 접근 자격을 검증하는 절차이다. 이러한 사용자 인증은 비밀번호(password) 등을 이용하는 지식 기반, 여권, 신분증 등을 이용하는 소유 기반, 지문, 필체 등을 이용하는 생체/행동 기반의 방식을 포함한다.

[0005] 비밀번호 등을 이용하는 지식 기반의 인증 방식은 가장 대중적으로 사용되어 오던 사용자 인증방식으로 사용이 간편하고, 비용이 저렴하며, 다양한 응용에 적용될 수 있다는 장점이 있다. 여권, 신분증 등을 이용하는 소유 기반의 인증 방식은 가장 강력한 보안성을 장점으로 하며, 최근에는 필요한 난수를 1회만 생성하여 인증하는 일회용 비밀번호(One-Time Password; OTP) 장치가 많이 사용되고 있다. 마지막으로, 지문, 필체 등을 이용하는 생체/행동 기반의 인증 방식은 인증을 위해 다른 도구를 별도 구비할 필요가 없고 분실 위험이 없으며, 비밀번호자와 같이 기억할 필요가 없다는 장점이 있다.

[0006] 상기 서술된 것과 같이 각각의 인증 방식들은 각자의 장점을 가지나, 단점 또한 존재한다. 지식 기반의 인증 방식은 도청과 같은 공격으로 인해 외부로 노출되기 쉽고, 노출된 비밀번호를 사용한 재생 공격(replay attack)에 취약하다는 단점이 있다. 소유 기반의 인증 방식은 인증을 위해 추가적인 물품 또는 디바이스를 소유하고 있어야 한다는 단점이 있다. 생체/행동 기반의 인증 방식은 지식 기반의 인증 방식과 같이 서버에 등록된 생체 또는 행동의 템플릿(Template)이 노출되는 경우 재생 공격에 취약하다. 또한 노출된 템플릿으로부터 개인의 생체 또는 행동 정보가 유출될 수 있고 비밀번호자와 달리 생체 또는 행동 정보를 변경하기 어렵다는 단점이 있어 비밀번호자의 노출보다 더 치명적으로 여겨진다. 이와 같은 단점들로 인해 더 안전하고 편리한 사용자 인증 방식을 제공하기 위한 연구들이 진행되고 있다.

발명의 내용

해결하려는 과제

- [0008] 종래의 인증 방식들의 단점을 보완하여 재생 공격을 방지하고 사용자의 프라이버시를 보장하는 생체정보 기반 일회용 비밀번호 인증 방법을 제공할 수 있다.

과제의 해결 수단

- [0010] 인증 시스템에 의해 수행되는 생체정보 기반의 일회용 비밀번호(One-Time Password; OTP) 인증 방법은, 전자 기기를 이용한 사용자의 템플릿 등록 요청에 따라 제1 사용자 등록 템플릿으로부터 변환된 제2 사용자 등록 템플릿을 등록하는 단계; 및 제1 사용자 인증 템플릿으로부터 변환된 제2 사용자 인증 템플릿을 재변환함에 따라 획득된 제3 사용자 인증 템플릿을 이용한 사용자의 인증 요청에 기초하여, 상기 제3 사용자 인증 템플릿과 기 등록된 제1 사용자 등록 템플릿을 변환한 제2 사용자 등록 템플릿을 비교하여 인증을 수행하는 단계를 포함할 수 있다.
- [0011] 상기 등록하는 단계는, 상기 사용자로부터 입력 인터페이스를 통해 제1 사용자 등록 템플릿(U)이 획득되고, 템플릿 변환 함수(F)에 사용될 변환 파라미터(p)가 생성 및 저장되고, 상기 템플릿 변환 함수(F)에 상기 변환 파라미터(p)를 사용하여 제1 사용자 등록 템플릿(U)이 변환됨에 따라 제2 사용자 등록 템플릿(U')이 획득되고, 상기 사용자로부터 상기 획득된 제2 사용자 등록 템플릿(U')이 전달됨을 수신하고, 상기 수신된 제2 사용자 등록 템플릿(U')을 사용자의 인증 정보로써 등록하는 단계를 포함할 수 있다.
- [0012] 상기 제1 사용자 등록 템플릿(U)은, 전자 기기를 이용한 생체정보 기반 인증 방식을 위해 상기 전자 기기의 생체정보 수집 장치를 통해 획득된 사용자의 생체정보에 기반하여 사용자 생체정보의 템플릿이 획득된 것일 수 있다.
- [0013] 상기 변환함수는, 임의의 벡터를 회전시키는 변환을 수행하는 것으로, 상기 제1 사용자 등록 템플릿(U)이 n (n 은 자연수)-차원 벡터로 표현될 때, 상기 변환 파라미터(p)를 씨드(seed)로 하여 임의의 n (n 은 자연수) 개의 정보를 각각 생성한 후, 상기 벡터의 n (n 은 자연수) 개의 요소에 따라 상기 생성된 정보만큼 각 요소를 변환하는 것일 수 있다.
- [0014] 상기 인증을 수행하는 단계는, 상기 사용자로부터 입력 인터페이스를 통해 제1 사용자 인증 템플릿(V)이 획득되고, 템플릿 변환 함수(F)에 변환 파라미터(p)를 사용하여 상기 제1 사용자 인증 템플릿(V)이 변환됨에 따라 제2 사용자 인증 템플릿(V')이 획득되고, 상기 템플릿 변환 함수(F)에 사용될 재변환 파라미터(p')가 생성되고, 상기 템플릿 변환 함수(F)에 상기 재변환 파라미터(p')를 사용하여 상기 제2 사용자 인증 템플릿(V')이 재변환됨에 따라 제3 사용자 인증 템플릿(V'')이 획득되고, 상기 사용자로부터 상기 획득된 제3 사용자 인증 템플릿(V'')이 전달됨에 따라 사용자의 인증 요청을 수신하는 단계를 포함할 수 있다.
- [0015] 상기 인증을 수행하는 단계는, 상기 템플릿 변환 함수(F)에 사용될 재변환 파라미터(p')를 생성하고, 상기 템플릿 변환 함수(F)에 상기 재변환 파라미터(p')를 사용하여 기 등록된 제1 사용자 등록 템플릿(R')이 변환됨에 따라 제2 사용자 등록 템플릿(R'')을 획득하고, 상기 제3 사용자 인증 템플릿(V'')을 상기 제2 사용자 등록 템플릿(R'')과 비교하여 인증을 수행하고, 상기 인증을 수행한 사용자 인증 결과를 상기 사용자에게 전달하는 단계를 포함할 수 있다.
- [0016] 상기 제1 사용자 인증 템플릿(V)은, 전자 기기를 이용한 생체정보 기반 인증 방식을 위해 상기 전자 기기의 생체정보 수집 장치를 통해 획득된 사용자의 생체정보에 기반하여 사용자 생체정보의 템플릿이 획득된 것일 수 있다.
- [0017] 상기 인증을 수행하는 단계는, 상기 제3 사용자 인증 템플릿(V'')과 상기 제2 사용자 등록 템플릿(R'')의 유사도를 통해 획득된 측정값을 기 정의된 인증 임계값을 기준으로 허가 또는 거부를 포함하는 사용자 인증 결과를 도출하는 단계를 포함할 수 있다.
- [0018] 상기 인증을 수행하는 단계는, 상기 제3 사용자 인증 템플릿(V'')에 대한 사용자 인증 결과가 허가일 경우, 사

용자의 템플릿 갱신 요청에 따라 사용자 등록 템플릿을 갱신하는 단계를 포함할 수 있다.

[0019] 상기 인증을 수행하는 단계는, 상기 사용자로부터 입력 인터페이스를 통해 제1 갱신 템플릿(N)이 획득되고, 템플릿 변환 함수(F)에 사용될 템플릿 갱신 파라미터(p'')가 생성 및 저장되고, 상기 템플릿 변환 함수(F)에 상기 템플릿 갱신 파라미터(p'')를 사용하여 제1 갱신 템플릿(N)이 변환됨에 따라 제2 갱신 템플릿(N')이 획득되고, 상기 사용자로부터 상기 제2 갱신 템플릿(N')과 상기 템플릿 갱신 파라미터(p'')의 해시값이 전달됨을 수신하는 단계를 포함할 수 있다.

[0020] 상기 인증을 수행하는 단계는, 상기 제3 사용자 인증 템플릿(V'')의 해시값에 대한 제2해시값을 계산하고, 상기 수신된 템플릿 갱신 파라미터(p'')의 해시값과 상기 제3 사용자 인증 템플릿(V'')으로부터 계산된 해시값에 대한 제2 해시값이 일치하는 경우, 상기 제2 갱신 템플릿(N')을 사용자의 새로운 템플릿으로 갱신하는 단계를 포함할 수 있다.

[0021] 인증 시스템은, 전자 기기를 이용한 사용자의 템플릿 등록 요청에 따라 제1 사용자 등록 템플릿으로부터 변환된 제2 사용자 등록 템플릿을 등록하는 등록부; 및 제1 사용자 인증 템플릿으로부터 변환된 제2 사용자 인증 템플릿을 재변환함에 따라 획득된 제3 사용자 인증 템플릿을 이용한 사용자의 인증 요청에 기초하여, 상기 제3 사용자 인증 템플릿과 기 등록된 제1 사용자 등록 템플릿을 변환한 제2 사용자 등록 템플릿을 비교하여 인증을 수행하는 인증부를 포함할 수 있다.

발명의 효과

[0023] 변환된 사용자 템플릿을 서버에 등록하는 과정과 변환된 템플릿을 재변환하여 인증을 수행하는 과정을 통해, 공격자에 의한 재생 공격이 불가능하고 사용자의 생체정보 프라이버시를 보장하는 인증을 수행할 수 있다

도면의 간단한 설명

[0025] 도 1은 일 실시예에 있어서, 사용자와 서버 간 생체정보 기반 일회용 비밀번호 인증의 개괄적인 동작을 설명하기 위한 도면이다.

도 2는 일 실시예에 있어서, 인증 시스템의 구성을 설명하기 위한 블록도이다.

도 3은 일 실시예에 있어서, 생체정보 기반 일회용 비밀번호 인증 방법을 설명하기 위한 흐름도이다.

도 4는 일 실시예에 있어서, 사용자 템플릿을 등록하는 과정을 설명하기 위한 도면이다.

도 5는 일 실시예에 있어서, 인증을 수행하는 과정을 설명하기 위한 도면이다.

도 6은 일 실시예에 있어서, 사용자 템플릿을 갱신하는 과정을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0026] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0028] 도 1은 일 실시예에 있어서, 사용자와 서버 간 생체정보 기반 일회용 비밀번호 인증의 개괄적인 동작을 설명하기 위한 도면이다.

[0029] 도 1은 사용자 인증 방식의 인증 모델을 나타낸 것이다. 실시예에서 제안하는 사용자 인증 방식에는 사용자(110)와 서비스를 제공하는 서버(100)가 포함된다. 서버(100)는 변환된 사용자 템플릿을 등록하는 과정 및 변환된 사용자 템플릿을 재변환하여 인증을 수행하는 과정을 포함할 수 있다.

[0030] 도 2는 일 실시예에 있어서, 인증 시스템의 구성을 설명하기 위한 블록도이고, 도 3은 일 실시예에 있어서, 생체정보 기반의 일회용 비밀번호 인증 방법을 설명하기 위한 흐름도이다.

[0031] 인증 시스템(100)의 프로세서는 등록부(210) 및 인증부(220)를 포함할 수 있다. 이러한 프로세서의 구성요소들은 인증 시스템에 저장된 프로그램 코드가 제공하는 제어 명령에 따라 프로세서에 의해 수행되는 서로 다른 기능들(different functions)의 표현들일 수 있다. 프로세서 및 프로세서의 구성요소들은 도 3의 생체정보 기반

의 일회용 비밀번호 인증 방법이 포함하는 단계들(310 내지 320)을 수행하도록 인증 시스템을 제어할 수 있다. 이때, 프로세서 및 프로세서의 구성요소들은 메모리가 포함하는 운영체제의 코드와 적어도 하나의 프로그램의 코드에 따른 명령(instruction)을 실행하도록 구현될 수 있다.

[0032] 프로세서는 생체정보 기반의 일회용 비밀번호 인증 방법을 위한 프로그램의 파일에 저장된 프로그램 코드를 메모리에 로딩할 수 있다. 예를 들면, 인증 시스템에서 프로그램이 실행되면, 프로세서는 운영체제의 제어에 따라 프로그램의 파일로부터 프로그램 코드를 메모리에 로딩하도록 인증 시스템을 제어할 수 있다. 이때, 프로세서는 등록부(210) 및 인증부(220) 각각은 메모리에 로딩된 프로그램 코드 중 대응하는 부분의 명령을 실행하여 이후 단계들(310 내지 320)을 실행하기 위한 프로세서의 서로 다른 기능적 표현들일 수 있다.

[0033] 단계(310)에서 등록부(210)는 전자 기기를 이용한 사용자의 템플릿 등록 요청에 따라 제1 사용자 등록 템플릿으로부터 변환된 제2 사용자 등록 템플릿을 등록할 수 있다. 등록부(210)는 사용자로부터 입력 인터페이스를 통해 제1 사용자 등록 템플릿(U)이 획득되고, 템플릿 변환 함수(F)에 사용될 변환 파라미터(p)가 생성 및 저장되고, 템플릿 변환 함수(F)와 변환 파라미터(p)를 사용하여 제1 사용자 등록 템플릿(U)이 변환됨에 따라 제2 사용자 등록 템플릿(U')이 획득되고, 사용자로부터 획득된 제2 사용자 등록 템플릿(U')이 전달됨을 수신하고, 수신된 제2 사용자 등록 템플릿(U')을 사용자의 인증 정보로써 등록할 수 있다.

[0034] 단계(320)에서 인증부(220)는 제1 사용자 인증 템플릿으로부터 변환된 제2 사용자 인증 템플릿을 재변환함에 따라 획득된 제3 사용자 인증 템플릿을 이용한 사용자의 인증 요청에 기초하여, 제3 사용자 인증 템플릿과 기 등록된 제1 사용자 등록 템플릿을 변환한 제2 사용자 등록 템플릿을 비교하여 인증을 수행할 수 있다. 인증부(220)는 사용자로부터 입력 인터페이스를 통해 제1 사용자 인증 템플릿(V)이 획득되고, 템플릿 변환 함수(F)에 변환 파라미터(p)를 사용하여 제1 사용자 인증 템플릿(V)이 변환됨에 따라 제2 사용자 인증 템플릿(V')이 획득되고, 템플릿 변환 함수(F)에 사용될 재변환 파라미터(p')가 생성되고, 템플릿 변환 함수(F)에 재변환 파라미터(p')를 사용하여 제2 사용자 인증 템플릿(V')이 재변환됨에 따라 제3 사용자 인증 템플릿(V'')이 획득되고, 사용자로부터 획득된 제3 사용자 인증 템플릿(V'')이 전달됨에 따라 사용자의 인증 요청을 수신할 수 있다. 인증부(220)는 템플릿 변환 함수(F)에 사용될 재변환 파라미터(p')를 생성하고, 템플릿 변환 함수(F)에 재변환 파라미터(p')를 사용하여 기 등록된 제1 사용자 등록 템플릿(R')이 변환됨에 따라 제2 사용자 등록 템플릿(R'')을 획득하고, 제3 사용자 인증 템플릿(V'')을 제2 사용자 등록 템플릿(R'')과 비교하여 인증을 수행하고, 인증을 수행한 사용자 인증 결과를 사용자에게 전달할 수 있다. 인증부(220)는 제3 사용자 인증 템플릿(V'')과 제2 사용자 등록 템플릿(R'')의 유사도를 통해 획득된 측정값을 기 정의된 인증 임계값을 기준으로 허가 또는 거부를 포함하는 사용자 인증 결과를 도출할 수 있다. 예를 들면, 인증부(220)는 제3 사용자 인증 템플릿(V'')과 제2 사용자 등록 템플릿(R'')의 평균 제곱 오차(Mean squared error, MSE)를 이용한 유사도 측정을 통해 획득된 측정값을 기 정의된 인증 임계값을 기준으로 허가 또는 거부를 포함하는 사용자 인증 결과를 도출할 수 있다.

[0035] 또한, 인증부(220)는 제3 사용자 인증 템플릿(V'')에 대한 사용자 인증 결과가 허가일 경우, 사용자의 템플릿 갱신 요청에 따라 사용자 등록 템플릿을 갱신할 수 있다. 인증부(220)는 사용자로부터 입력 인터페이스를 통해 제1 갱신 템플릿(N)이 획득되고, 템플릿 변환 함수(F)에 사용될 템플릿 갱신 파라미터(p'')가 생성 및 저장되고, 템플릿 변환 함수(F)에 템플릿 갱신 파라미터(p'')를 사용하여 제1 갱신 템플릿(N)이 변환됨에 따라 제2 갱신 템플릿(N')이 획득되고, 사용자로부터 제2 갱신 템플릿(N')과 템플릿 갱신 파라미터(p'')의 해시값이 전달됨을 수신할 수 있다. 인증부(220)는 제3 사용자 인증 템플릿(V'')의 해시값에 대한 제2해시값을 계산하고, 수신된 템플릿 갱신 파라미터(p'')의 해시값과 제3 사용자 인증 템플릿(V'')으로부터 계산된 해시값에 대한 제2 해시값이 일치하는 경우, 제2 갱신 템플릿(N')을 사용자의 새로운 템플릿으로 갱신할 수 있다.

[0036] 도 4는 일 실시예에 있어서, 사용자 템플릿을 등록하는 과정을 설명하기 위한 도면이다.

[0037] 도 4에서는 전자 기기를 이용한 사용자의 템플릿 등록 요청에 따라 상기 사용자로부터 등록을 위한 사용자 템플릿(제1 사용자 등록 템플릿)으로부터 변환된 사용자 템플릿(제2 사용자 등록 템플릿)을 등록하는 동작에 대하여 설명하기로 한다.

[0038] 사용자(110)는 사용자(110)의 입력 인터페이스(interface)를 통해 등록을 위한 제1 사용자 등록 템플릿(U)을 획득할 수 있다(획득 단계(Acquisition) ①). 사용자(110)는 템플릿 변환 함수(F)에 사용될 변환 파라미터(p)를 생성 및 저장할 수 있다(설정 단계(Setup) ②). 사용자(110)는 템플릿 변환 함수(F)에 변환 파라미터(p)를 사용하여 제1 사용자 등록 템플릿(U)을 제2 사용자 템플릿(U')으로 변환할 수 있다(변환 단계(Transformation) ③). 다시 말해서, 사용자(110)는 템플릿 변환 함수(F)에 변환 파라미터(p)를 사용하여 제1 사용자 등록 템플릿(U)을 변환함에 따라 제2 사용자 템플릿(U')을 획득할 수 있다. 사용자(110)는 제2 사용자 등록 템플릿(U')

을 서버(100)로 전달하여 템플릿 등록을 요청할 수 있다(전송 단계(Send) ④). 서버(100)는 사용자(110)로부터 제2 사용자 등록 템플릿(U')이 전달됨을 수신하고, 수신된 제2 사용자 등록 템플릿(U')을 등록할 수 있다(등록 단계(Enrollment) ⑤).

[0039] 이때, 사용자(110)가 자신의 템플릿을 변환하여 서버에 등록하는 과정의 일례로, 사용자(110)의 생체정보를 이용한 인증 방식이 사용될 수 있다. 예를 들면, 스마트 폰과 같은 이동형 단말을 이용한 얼굴 인증 방식이 사용될 수 있다. 획득 단계 ①에서, 사용자(110)는 이동형 단말의 카메라를 통해 사용자(110)의 얼굴 이미지를 획득하고, 획득된 얼굴 이미지에 기반하여 사용자 얼굴의 템플릿(U)을 획득할 수 있다. 설정 단계 ②에서, 사용자(110)는 템플릿 변환 함수(F)에 사용될 변환 파라미터(p)를 생성 및 저장할 수 있다. 일례로, 변환 파라미터 p는 다음과 같이 생성될 수 있다.

[0040] 수학적 식 1:

$$p = \text{Hash}(r)$$

[0041]

[0042] 이때, Hash는 해시함수, r은 임의의 난수를 의미한다.

[0043] 변환 단계 ③에서, 사용자(110)는 템플릿 변환 함수(F)에 제1 사용자 등록 템플릿(U)과 변환 파라미터(p)를 사용하여 다음과 같이 변환된 제2 사용자 등록 템플릿(U')을 획득할 수 있다.

[0044] 수학적 식 2:

$$U' = F(U, p)$$

[0045]

[0046] 일례로, 템플릿 변환 함수(F)는 초구면 좌표계(Hyperspherical Coordinates) 상의 임의의 벡터를 회전시키는 변환을 수행할 수 있다. 구체적으로, 템플릿 변환 함수(F)는 제1 사용자 등록 템플릿(U)이 초구면 좌표계 상의 n(n은 자연수)-차원 벡터로 표현될 때, 변환 파라미터(p)를 씨드(seed)로 하여 임의의 n(n은 자연수) 개의 각도 정보 $\alpha_1, \alpha_2, \dots, \alpha_n$ 를 각각 생성한 후, n(n은 자연수) 개의 축에 따라 생성된 각도 정보만큼 축을 기준으로 회전시킬 수 있다. 다시 말해서, 즉, 1 번 축을 회전축으로 제1 사용자 등록 템플릿(U)을 α_1 만큼 회전, 2 번 축을 회전축으로 제1 사용자 등록 템플릿(U)을 α_2 만큼 회전, 쯤, n 번 축을 회전축으로 제1 사용자 등록 템플릿(U)을 α_n 만큼 회전시켜, 제2 사용자 등록 템플릿(U')을 생성할 수 있다.

[0047] 전송 단계 ④에서, 사용자(110)는 제2 사용자 등록 템플릿(U')을 서버(100)로 전달하여 사용자(110)의 템플릿으로 등록을 요청할 수 있다.

[0048] 등록 단계 ⑤에서, 서버(100)는 사용자(110)로부터 제2 사용자 등록 템플릿(U')을 수신하고, 수신된 제2 사용자 등록 템플릿(U')을 사용자의 인증 정보로써 등록할 수 있다.

[0049] 도 5는 일 실시예에 있어서, 인증을 수행하는 과정을 설명하기 위한 도면이다.

[0050] 사용자(110)는 입력 인터페이스를 통해 인증을 위한 제1 사용자 인증 템플릿(V)을 획득할 수 있다(획득 단계(Acquisition) ①). 사용자(110)는 템플릿 변환 함수(F)에 변환 파라미터(p)를 사용하여 제1 사용자 인증 템플릿(V)을 제2 사용자 인증 템플릿(V')으로 변환할 수 있다(재구성(Reconstruction) 단계 ②). 다시 말해서, 사용자(110)는 템플릿 변환 함수(F)에 변환 파라미터(p)를 사용하여 제1 사용자 인증 템플릿(V)을 변환함에 따라 제2 사용자 인증 템플릿(V')을 획득할 수 있다. 사용자(110)는 템플릿 변환 함수(F)에 사용될 재변환 파라미터(p')를 생성할 수 있다(설정(Setup) 1 단계 ③). 사용자(110)는 템플릿 변환 함수(F)에 재변환 파라미터(p')를 사용하여 제2 사용자 인증 템플릿(V')을 제3 사용자 인증 템플릿(V'')으로 재변환할 수 있다(변환(Transformation) 1 단계 ④). 다시 말해서, 사용자(110)는 템플릿 변환 함수(F)에 재변환 파라미터(p')를 사용하여 제2 사용자 인증 템플릿(V')을 재변환함에 따라 제3 사용자 인증 템플릿(V'')을 획득할 수 있다. 사용자(110)는 제3 사용자 인증 템플릿(V'')을 서버(100)로 전달하여 사용자 인증을 요청할 수 있다(전송(Send) 1 단계 ⑤).

[0051] 서버(100)는 템플릿 변환 함수(F)에 사용될 재변환 파라미터(p')를 생성할 수 있다(설정(Setup 2) 단계 ⑥). 서버(100)는 템플릿 변환 함수(F)에 재변환 파라미터(p')를 사용하여 기 등록된 제1 사용자 등록 템플릿(R')을

제2 사용자 등록 템플릿(R'')으로 변환할 수 있다(변환(Transformation) 2 단계 ⑦). 다시 말해서, 서버(100)는 템플릿 변환 함수(F)에 재변환 파라미터(p')를 사용하여 기 등록된 제1 사용자 등록 템플릿(R')을 변환함에 따라 제2 사용자 등록 템플릿(R'')을 획득할 수 있다. 이때, 정상적인 사용자라면, 기 등록된 제1 사용자 등록 템플릿(R')은 템플릿 등록 단계에서 서버(100)가 저장했던 제1 사용자 등록 템플릿(U')과 동일하다. 서버(100)는 제2 사용자 등록 템플릿(R'')을 제3 사용자 인증 템플릿(V'')과 비교하여 인증을 수행할 수 있다(검증(Verification) 단계 ⑧). 서버(100)는 인증을 수행한 인증 결과를 사용자(110)에게 전달할 수 있다(전송(Send) 2 단계 ⑨).

[0052] 이때, 사용자(110)가 자신의 템플릿을 재변환하여 서버(100)에 인증을 수행하는 과정의 일례로 사용자(110)의 생체정보를 이용한 인증 방식이 사용될 수 있다. 예를 들면, 스마트 폰(smart phone)과 같은 이동형 단말을 이용한 얼굴 인증 방식이 사용될 수 있다.

[0053] 획득 단계 ①에서, 사용자(110)는 이동형 단말의 카메라를 통해 사용자(110)의 얼굴 이미지를 획득하고, 획득된 얼굴 이미지에 기반하여 사용자 얼굴의 템플릿(V), 즉, 제1 사용자 인증 템플릿(V)을 획득할 수 있다. 재구성 단계 ②에서, 사용자(110)는 템플릿 변환 함수(F)에 제1 사용자 인증 템플릿(V)과 변환 파라미터(p)를 사용하여 다음과 같이 변환된 제2 사용자 인증 템플릿(V')을 생성할 수 있다.

[0054] 수학적 식 3:

$$V' = F(V, p)$$

[0055] 설정 1 단계 ③에서, 사용자(110)는 템플릿 변환 함수(F)에 사용될 재변환 파라미터(p')를 생성할 수 있다. 재변환 파라미터(p')는 사용자(110)와 서버(100)가 모두 알고 있는 값으로 생성되어야 하며, 일례로 재변환 파라미터(p')는 다음과 같이 생성될 수 있다.

[0057] 수학적 식 4:

$$p' = \text{Hash}(s)$$

[0058] 이때, Hash는 해시 함수, s 는 사용자(110)와 서버(100)가 모두 알고 있는 값이다. 예를 들면, s 는 사용자(110)와 서버(100) 간에 동기화된 타임스탬프(timestamp) 또는 인증 시도 횟수 카운터(counter)가 개별적으로 또는 조합되어 사용될 수 있다.

[0060] 변환 1 단계 ④에서, 사용자(110)는 템플릿 변환 함수(F)에 변환된 제2 사용자 인증 템플릿(V')과 재변환 파라미터(p')를 사용하여 다음과 같이 재변환된 제3 사용자 인증 템플릿(V'')을 생성할 수 있다.

[0061] 수학적 식 5:

$$V'' = F(V', p')$$

[0062] 전송 1 단계 ⑤에서, 사용자(110)는 제3 사용자 인증 템플릿(V'')을 서버(100)로 전달하여 사용자 인증을 요청할 수 있다.

[0064] 설정 단계 ⑥에서, 서버(100)는 템플릿 변환 함수(F)에 사용될 재변환 파라미터(p')를 생성할 수 있다. 재변환 파라미터(p')는 수학적 식 4와 동일한 방법으로 생성될 수 있다.

[0065] 검증 단계 ⑦에서, 서버(100)는 템플릿 변환 함수(F)에 기 등록된 제1 사용자 등록 템플릿(R')과 재변환 파라미터(p')를 사용하여 다음과 같이 변환된 제2 사용자 등록 템플릿(R'')을 생성할 수 있다. 이때, 제1 사용자 등록 템플릿(R')은 템플릿 변환 함수(F)에 변환 파라미터(p)를 사용하여 템플릿 등록을 위한 사용자 템플릿(R)을 변환한 것일 수 있다.

[0066] 수학적 식 6:

$$R'' = F(R', p')$$

[0067] 검증 단계 ⑧에서, 서버(100)는 사용자(110)로부터 전달받은 재변환된 사용자 템플릿, 즉, 제3 사용자 인증 템플릿(V'')을 기 등록된 제1 사용자 등록 템플릿(R')으로부터 변환된 제2 사용자 등록 템플릿(R'')과 비교하여

인증을 수행할 수 있다.

[0069] 실시예에서 제시하는 인증 방식은 사용자 템플릿 간의 유사도를 측정하는 방법을 사용할 수 있다. 일례로, 사용자 템플릿 간의 평균 제곱 오차(Mean squared error, MSE)가 다음의 식과 같이 계산되어 인증에 사용될 수 있다.

[0070] 수학적식 7:

$$D = MSE(V'', R'') = \frac{1}{n} \sum_{i=1}^n (V_i'' - R_i'')^2$$

[0071] 이때, n은 템플릿의 길이, V_i'' 과 R_i'' 는 각각 제3 사용자 인증 템플릿(V'')과 제2 사용자 등록 템플릿(R'')의 i 번째 요소를 의미한다. 이후, 서버(100)는 제3 사용자 인증 템플릿(V'')과 제2 사용자 등록 템플릿(R'')의 평균 제곱 오차(D)를 사용하여 다음과 같은 기준으로 사용자 인증 결과를 도출할 수 있다.

[0073] 수학적식 8:

$$R = \begin{cases} \text{Accept,} & \text{if } D < \theta \\ \text{Reject, otherwise} \end{cases}$$

[0074] 이때, θ 는 서버(100)에 정의된 인증 임계값을 의미한다.

[0075] 전송 단계 ⑨에서, 서버(100)는 사용자 인증 결과를 사용자(110)에게 전달할 수 있다. 사용자 인증 결과는 수학적식 8에 따라 사용자 인증에 성공한 경우 허가(Accept), 실패하는 경우 거부(Reject)가 전달될 수 있다.

[0076] 실시예에 따르면, 변환된 사용자 템플릿을 서버에 등록하는 과정과 변환된 템플릿을 재변환하여 인증을 수행하는 과정을 통해, 공격자에 의한 재생 공격이 불가능하고 사용자의 생체 정보 프라이버시를 보장하는 인증을 수행할 수 있다.

[0077] 도 6은 일 실시예에 있어서, 사용자 템플릿을 갱신하는 과정을 설명하기 위한 도면이다.

[0078] 서버(100)에 등록된 변환된 사용자 템플릿은 공격자에 의해 서버(100)에 저장된 사용자 템플릿이 유출되거나 인증에 사용되는 변수가 임계 값을 초과하는 등의 문제로 사용자 등록 템플릿의 갱신을 필요로 할 수 있다. 이 경우, 사용자(110)는 서버(100)에 사용자 등록 템플릿의 갱신을 요청하고, 서버(100)는 사용자 등록 템플릿의 갱신을 수행할 수 있다.

[0079] 일례로, 사용자 등록 템플릿을 변경하기 위해, 사용자(110)는 제3 사용자 인증 템플릿(V'')을 서버(100)에 전달하여 사용자 인증을 시도하고, 서버(100)는 제3 사용자 인증 템플릿(V'')에 대한 인증 결과가 허가(Accept)인 경우, 도 4의 사용자 템플릿을 등록하는 과정과 유사하게 서버(100)에 저장된 사용자 템플릿을 갱신할 수 있다.

[0080] 먼저, 획득 단계 ①에서 사용자(110)는 입력 인터페이스를 통해 제1 갱신 템플릿(N)을 획득할 수 있다. 설정 단계 ②에서, 사용자(110)는 템플릿 변환 함수(F)에 사용될 템플릿 갱신 파라미터(p'')를 저장할 수 있다. 이때, 변경되는 템플릿 갱신 파라미터(p'')는 사용자(110)와 서버(100)가 공유하는 정보를 사용하여 생성한다. 예를 들어, 사용자(110)와 서버(100)가 인증을 위해 공유한 제3 사용자 인증 템플릿(V'')으로부터 템플릿 갱신 파라미터(p'')를 다음과 같이 계산할 수 있다.

[0081] 수학적식 9:

$$p'' = \text{Hash}(V'')$$

[0082] 변환 단계 ③에서, 사용자(110)는 템플릿 변환 함수(F)에 템플릿 갱신 파라미터(p'')를 사용하여 제1 갱신 템플릿(N)을 다음과 같이 제2 갱신 템플릿(N')으로 변환할 수 있다. 다시 말해서, 사용자(110)는 제1 갱신 템플릿(N)을 변환함수에 따라 제2 갱신 템플릿(N')을 획득할 수 있다.

[0083] 수학적식 10:

$$N' = F(N, p'')$$

[0087] 전송 단계 ④에서, 사용자(110)는 변환된 제2 갱신 템플릿(N')과 템플릿 갱신 파라미터(p'')의 해시값을 서버(100)로 전달하여 템플릿 갱신을 요청할 수 있다.

[0088] 수학적 식 11:

[0089] $H = Hash(p'')$

[0090] 이후, 서버(100)는 갱신 과정 초기에 인증을 위해 수신된 제3 사용자 인증 템플릿(V'')에 대한 해시값에 대한 제2 해시값을 계산할 수 있다.

[0091] 수학적 식 12:

$$H' = Hash(Hash(V''))$$

[0092]

[0093] 서버(100)는 수신된 템플릿 갱신 파라미터(p'')의 해시값과 제3 사용자 인증 템플릿(V'')으로부터 계산된 해시값에 대한 제2 해시값을 비교하여 수신된 템플릿 갱신 파라미터(p'')의 해시값과 제3 사용자 인증 템플릿(V'')으로부터 계산된 해시값에 대한 제2 해시값이 일치하는 경우, 제2 갱신 템플릿(N')을 사용자의 새로운 템플릿으로 갱신할 수 있다.

[0094] 상기 기술된 것과 같이 지식 기반의 사용자 인증 방식은 비밀번호 등이 외부로 노출되기 쉽고, 노출된 비밀번호를 사용한 재생 공격에 취약하다는 단점이 있었으나, 실시예에서 제안된 사용자 인증은 매 인증 시도마다 수학적 식 (4)에 의해 재변환 파라미터(p')를 생성하고 템플릿을 변환하여 인증이 수행되므로 공격자가 도청 등을 통해 인증에 사용되는 템플릿을 획득하더라도 재생 공격을 수행할 수 없다. 또한, 생체/행동 기반의 인증 방식은 등록된 생체 또는 행동의 템플릿이 노출됨에 따라 개인의 생체 또는 행동 정보가 유출될 수 있다는 단점이 있고 비밀번호와 달리 생체 또는 행동 정보를 변경할 수 없다는 단점이 있었으나, 실시예에서는 사용자가 자신의 생체 또는 행동 정보 템플릿을 서버에 등록하는 과정에서 템플릿을 변환하여 등록을 함에 따라 공격자가 서버의 사용자 템플릿을 획득하더라도 이로부터 사용자의 원본 템플릿을 획득할 수 없다. 또한, 사용자는 기존에 사용된 변환 파라미터와 다른 변환 파라미터를 사용하여 템플릿을 변환하여 사용할 수 있다.

[0095] 상기 기술된 것과 같이 본 발명은 일회성 정보를 사용한 일회용 비밀번호의 한 종류로써, 기존 사용자 인증 방식들의 단점을 해소하여 더 안전하고 편리한 사용자 인증을 제공할 수 있다.

[0096] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0097] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0098] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등

을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 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 광기록 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.

[0099] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

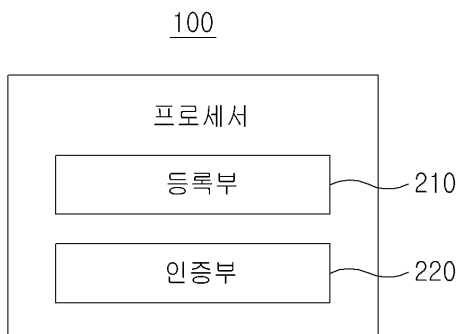
[0100] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

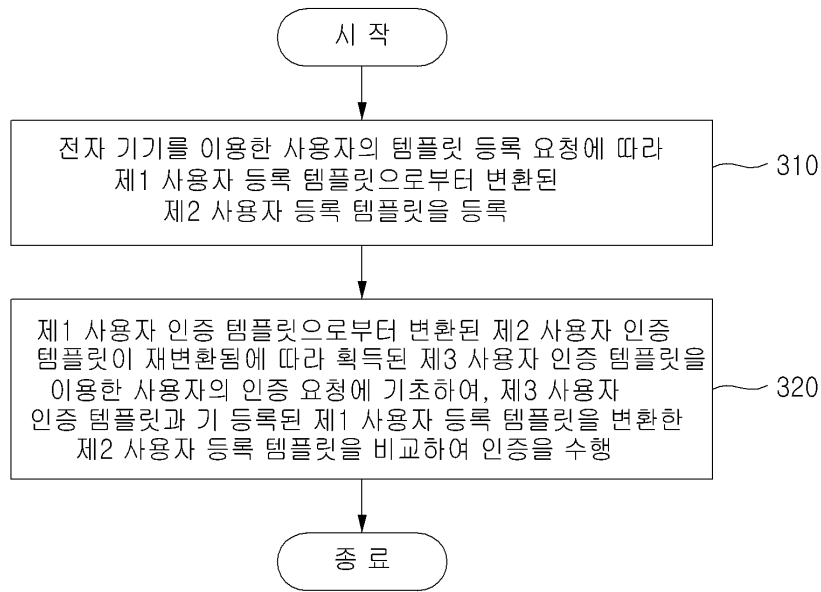
도면1



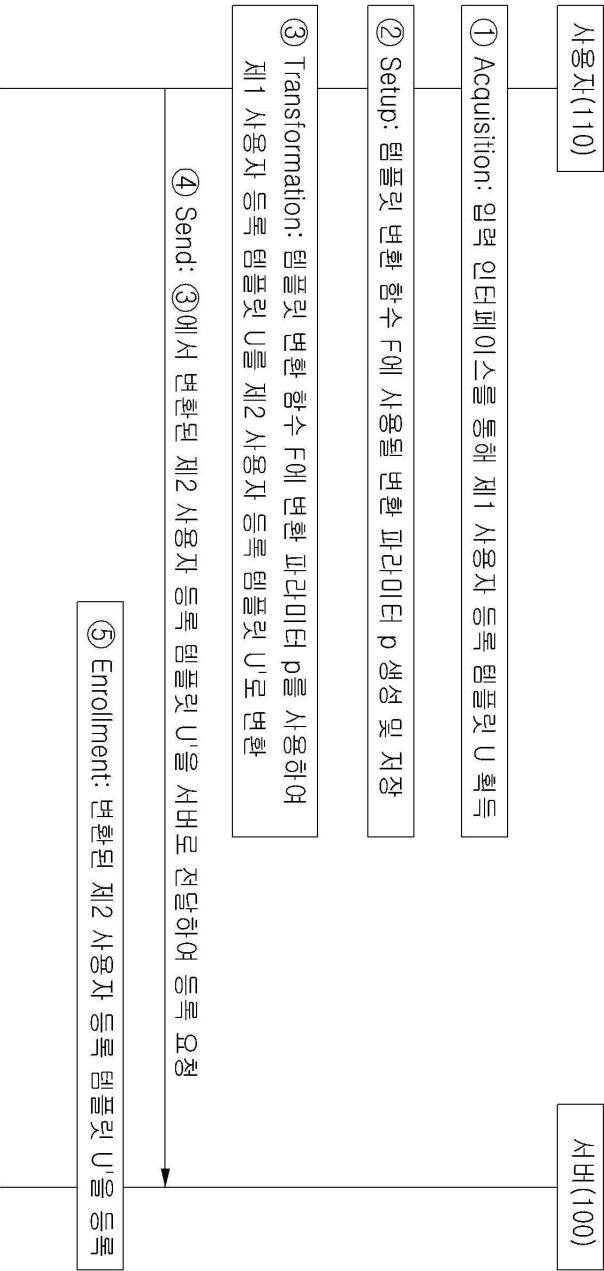
도면2



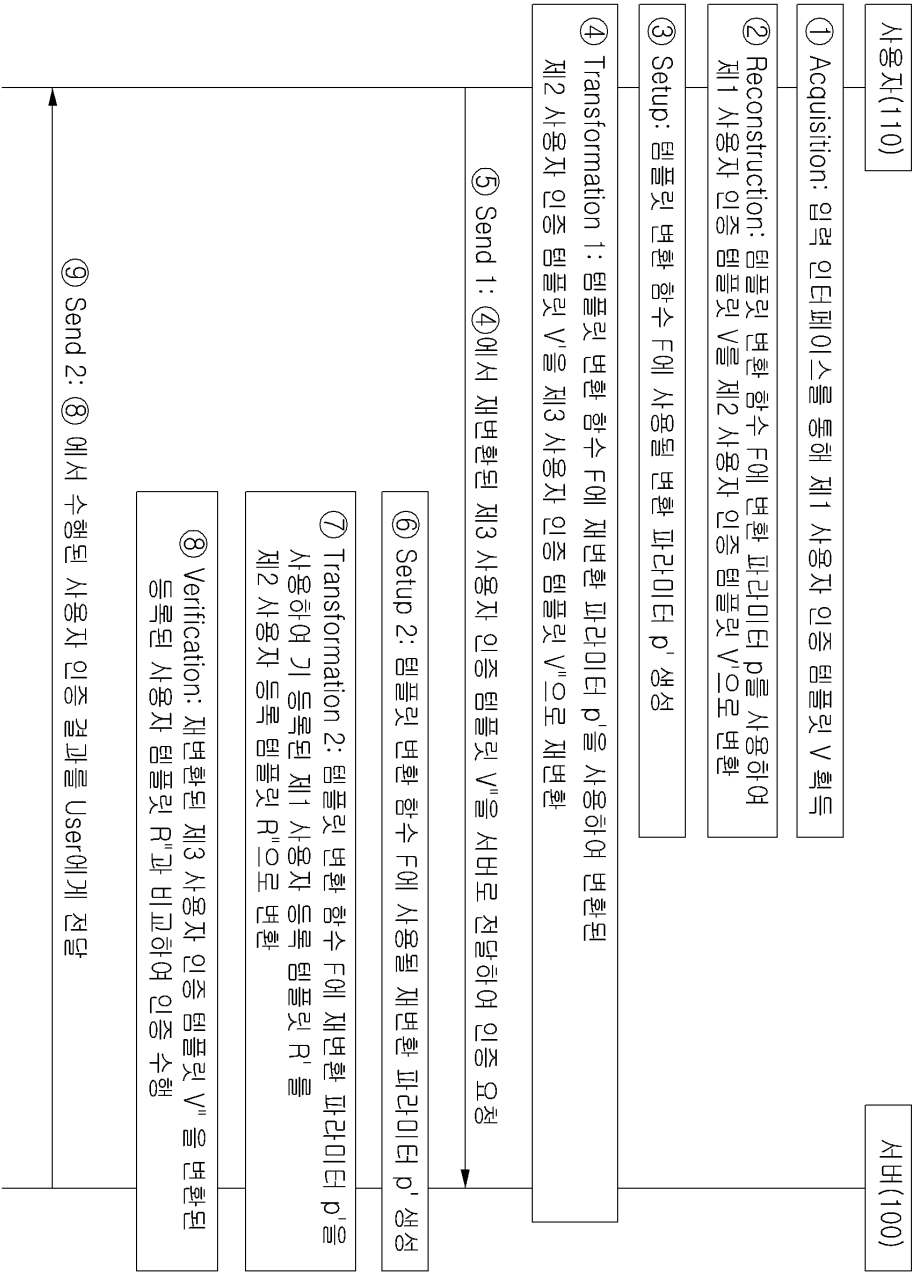
도면3

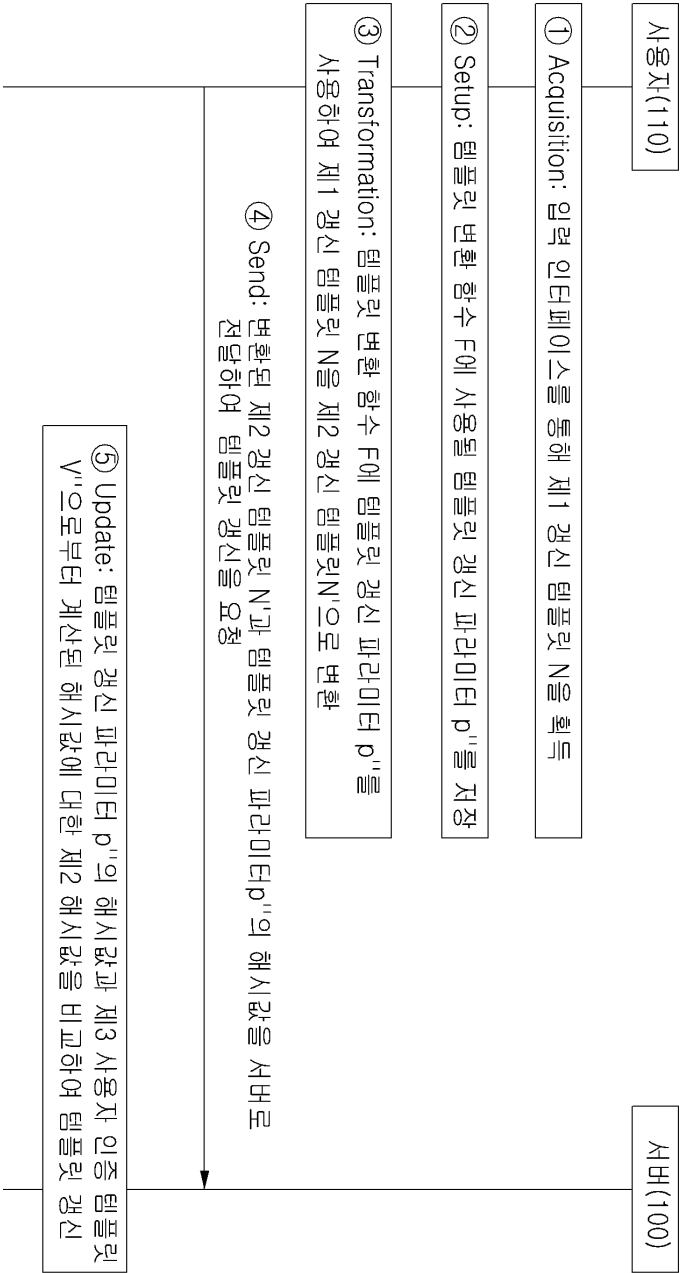


도면4



도면5





도면6