(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년02월23일
(11) 등록번호 10-1831633
(24) 등록일자 2018년02월19일

(51) 국제특허분류(Int. Cl.)
G06F 21/44 (2013.01) *G06K 19/06* (2006.01)
G06K 7/14 (2006.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
G06F 21/445 (2013.01)
G06K 19/06009 (2013.01)
(21) 출원번호 10-2016-0131256
(22) 출원일자 2016년10월11일
심사청구일자 2016년10월11일
(56) 선행기술조사문헌
KR1020060027929 A*
JP2015001764 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
도인실
인천광역시 연수구 센트럴로 194, 201동 2705호 (더샵센트럴파크2단지아파트)
채기준
서울특별시 강남구 강남대로136길 34
양단아
서울특별시 은평구 수색로20길 5-5, 402호(수색동, 동진아트빌)
(74) 대리인
윤귀상

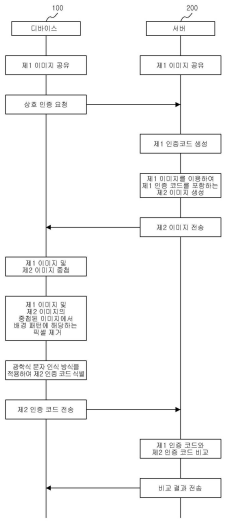
전체 청구항 수 : 총 8 항 심사관 : 문남두

(54) 발명의 명칭 **시각암호 기반의 상호 인증 방법 및 시각암호 기반의 상호 인증을 수행하는 디바이스의 제어 방법**

(57) 요 약

시각암호 기반의 상호 인증 방법에 있어서, 상호 인증을 수행할 디바이스와 서버 간에 제1 이미지를 공유하여 미리 저장하고, 상기 서버에서 상기 디바이스로부터 상호 인증 요청을 수신하는 경우, 제1 인증 코드를 생성하고, 상기 제1 이미지와 중첩되면 상기 제1 인증 코드가 식별되는 제2 이미지를 생성하여 상기 디바이스로 전송하고, 상기 디바이스에서 상기 제1 이미지 및 상기 제2 이미지를 중첩하고, 중첩된 이미지로부터 광학식 문자 인식 방식으로 인증 코드를 식별하고, 식별한 인증 코드인 제2 인증 코드를 상기 서버로 전송하며, 상기 서버에서 상기 제1 인증 코드 및 상기 제2 인증 코드를 비교하여 상기 디바이스와의 상호 인증 성공 여부를 판단한다.

대 표 도 - 도2



(52) CPC특허분류
G06K 7/1404 (2013.01)
H04L 63/0869 (2013.01)
G06F 2221/2133 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 2016R1A2B4015899
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 기초연구사업(학술진흥)-중견연구자지원사업
연구과제명 CPS환경에서의신뢰성있는서비스제공을위한보안기법및공격대응방안
기 여 율 1/1
주관기관 이화여자대학교 산학협력단
연구기간 2016.06.01 ~ 2019.05.31
공지예외적용 : 있음

명 세 서

청구범위

청구항 1

상호 인증을 수행할 디바이스와 서버 간에 검정 픽셀과 투명 픽셀들의 조합으로 이루어지는 제1 이미지를 공유하여 미리 저장하고,

상기 서버에서 상기 디바이스로부터 상호 인증 요청을 수신하는 경우, 제1 인증 코드를 생성하고, 상기 제1 이미지와 중첩되면 상기 제1 인증 코드에 해당하는 패턴이 검정색으로 식별되는 제2 이미지를 생성하여 상기 디바이스로 전송하고,

상기 디바이스에서 상기 제1 이미지 및 상기 제2 이미지를 중첩하여 검정 픽셀과 투명 픽셀들의 조합으로 이루어지는 중첩된 이미지를 생성하고, 상기 중첩된 이미지를 구성하는 복수의 픽셀을 소정의 픽셀 범위로 나누고, 상기 픽셀 범위에 적어도 하나의 투명 픽셀이 포함되는 경우, 해당 픽셀 범위에 포함되는 모든 픽셀을 투명 픽셀로 재정의하여 상기 중첩된 이미지에서 배경 패턴을 제거하고, 배경 패턴이 제거된 중첩된 이미지로부터 광학식 문자 인식 방식으로 인증 코드를 식별하고, 식별한 인증 코드인 제2 인증 코드를 상기 서버로 전송하며,

상기 서버에서 상기 제1 인증 코드 및 상기 제2 인증 코드를 비교하여 상기 디바이스와의 상호 인증 성공 여부를 판단하는 시각암호 기반의 상호 인증 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 소정의 픽셀 범위는 2X2로 나누어지는 시각암호 기반의 상호 인증 방법.

청구항 4

제1항에 있어서,

상기 디바이스에서 식별한 인증 코드인 제2 인증 코드를 상기 서버로 전송하는 것은,

상기 디바이스에서 상기 제2 인증 코드에 해쉬 함수를 적용하고, 상기 제2 인증 코드에 해쉬 함수를 적용한 값을 상기 서버로 전송하는 것인 시각암호 기반의 상호 인증 방법.

청구항 5

제4항에 있어서,

상기 서버에서 상기 제1 인증 코드 및 상기 제2 인증 코드를 비교하여 상기 디바이스와의 상호 인증 성공 여부를 판단하는 것은,

상기 서버에서 상기 제1 인증 코드에 해쉬 함수를 적용하고, 상기 제1 인증 코드에 해쉬 함수를 적용한 값과 상기 디바이스로부터 수신하는 상기 제2 인증 코드에 해쉬 함수를 적용한 값을 비교하여 상기 디바이스와의 상호 인증 성공 여부를 판단하는 것인 시각암호 기반의 상호 인증 방법.

청구항 6

제1항에 있어서,

상기 서버에서 상기 디바이스와의 상호 인증 성공 여부에 대한 판단 결과를 상기 디바이스로 알리는 것을 더 포함하는 시각암호 기반의 상호 인증 방법.

청구항 7

서버와 통신 시, 상기 서버와 시각암호 기반의 상호 인증을 수행하는 디바이스의 제어방법에 있어서,

상기 서버와 검정 픽셀과 투명 픽셀들의 조합으로 이루어지는 제1 이미지를 공유하여 미리 저장하고,

상기 서버와 통신을 시도하는 경우, 상기 서버로 상호 인증을 요청하여 상기 서버로부터 상기 제1 이미지를 이용하여 제1 인증 코드에 해당하는 패턴이 검정색으로 식별되도록 생성한 제2 이미지를 수신하고,

상기 제1 이미지 및 상기 제2 이미지를 중첩하여 검정 픽셀과 투명 픽셀들의 조합으로 이루어지는 중첩된 이미지를 생성하고,

상기 중첩된 이미지를 구성하는 복수의 픽셀을 소정의 픽셀 범위로 나누고, 상기 픽셀 범위에 적어도 하나의 투명 픽셀이 포함되는 경우, 해당 픽셀 범위에 포함되는 모든 픽셀을 투명 픽셀로 재정의하여 상기 중첩된 이미지에서 배경 패턴을 제거하고,

배경 패턴이 제거된 중첩된 이미지에 광학식 문자 인식 알고리즘을 적용하여 제2 인증 코드를 식별하고,

상기 제2 인증 코드를 상기 서버로 전송하여 상기 서버로부터 상기 제1 인증 코드와 상기 제2 인증 코드의 비교 결과에 따른 상호 인증 결과를 수신하는 시각암호 기반의 상호 인증을 수행하는 디바이스의 제어방법.

청구항 8

삭제

청구항 9

제7항에 있어서,

상기 소정의 픽셀 범위는 2X2로 나누어지는 시각암호 기반의 상호 인증을 수행하는 디바이스의 제어방법.

청구항 10

제7항에 있어서,

상기 제2 인증 코드를 상기 서버로 전송하여 상기 서버로부터 상기 제1 인증 코드와 상기 제2 인증 코드의 비교 결과에 따른 상호 인증 결과를 수신하는 것은,

상기 제2 인증 코드에 해쉬 함수를 적용하고, 상기 제2 인증 코드에 해쉬 함수를 적용한 값을 상기 서버로 전송하며, 상기 서버로부터 상기 제1 인증 코드에 해쉬 함수를 적용한 값과 상기 제2 인증 코드에 해쉬 함수를 적용한 값의 비교 결과에 따른 상호 인증 결과를 수신하는 것인 시각암호 기반의 상호 인증을 수행하는 디바이스의 제어방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 시각암호 기반의 상호 인증 방법 및 시각암호 기반의 상호 인증을 수행하기 위한 디바이스의 제어방법에 관한 것으로, 보다 상세하게는 IoT(Internet of Things) 서비스 환경에서 서버와 디바이스 간 통신 시 서버와 디바이스 간의 시각암호 기반의 상호 인증 방법 및 시각암호 기반의 상호 인증을 수행하기 위한 디바이스의 제어방법에 관한 것이다.

배 경 기 술

[0002] 디바이스들과 서버 간에 통신이 요구되는 IoT(Internet of Things) 서비스는 그 수요가 증가하고 있으며, 이러한 IoT 서비스가 발전함에 따라 인증과 관련된 보안 기술의 중요성 또한 부각되고 있다.

[0003] 사용자는 IoT 서비스의 일 예로, 서비스 서버로부터 외부에서의 스마트 보일러의 전원 온, 오프 제어 및 온도 제어가 가능한 원격 제어 서비스를 제공받을 수 있는데, 이러한 IoT 서비스를 제공받기 전에 사용자뿐만 아니라 스마트 보일러는 반드시 서버와의 상호 인증 절차를 수행하여야 한다. 이는 서비스 서버가 피싱 서버가 아니며

또는 위조된 스마트 디바이스가 아닌지 등을 증명하기 위함이다.

[0004] 한편, 디바이스 간 상호 인증을 위한 방법으로 시각암호를 이용한 상호 인증 방법이 제안된 바 있다. 구체적으로는, 시각암호는 두 개 이상의 이미지가 인증 숫자, 메시지 등의 코드를 포함하고 있으며, 두 개 이상의 이미지가 중첩되는 경우 사람의 시각에 의해 코드가 확인될 수 있다. 따라서, 시각암호를 이용한 상호 인증 방법은 암호화 및 복호화 하는데 수학적 계산을 할 필요가 없으며 기밀성이 보증된다는 장점을 갖는다.

[0005] 그러나, 시각암호를 이용한 상호 인증 방법은 사람의 시각에 의존할 뿐이므로, IoT 디바이스, GUI(Graphical User Interface)를 지원하지 않는 헤드리스 디바이스(Headless Device), 또는, 사람이 살 수 없는 악조건의 자연환경에서 생태계의 정보를 수집하는 디바이스 등을 인증하는 데에는 적용하기 어렵다는 문제점이 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 일측면은 시각암호 이미지에서 광학식 문자 인식(OCR: Optical Character Recognition) 방식으로 인증 코드를 인식하여 상호 인증을 수행하는 시각암호 기반의 상호 인증 방법 및 시각암호 기반의 상호 인증을 수행하는 디바이스의 제어방법을 제공한다.

과제의 해결 수단

[0007] 본 발명의 일측면은 상호 인증을 수행할 디바이스와 서버 간에 제1 이미지를 공유하여 미리 저장하고, 상기 서버에서 상기 디바이스로부터 상호 인증 요청을 수신하는 경우, 제1 인증 코드를 생성하고, 상기 제1 이미지와 중첩되면 상기 제1 인증 코드가 식별되는 제2 이미지를 생성하여 상기 디바이스로 전송하고, 상기 디바이스에서 상기 제1 이미지 및 상기 제2 이미지를 중첩하고, 중첩된 이미지로부터 광학식 문자 인식 방식으로 인증 코드를 식별하고, 식별한 인증 코드인 제2 인증 코드를 상기 서버로 전송하며, 상기 서버에서 상기 제1 인증 코드 및 상기 제2 인증 코드를 비교하여 상기 디바이스와의 상호 인증 성공 여부를 판단한다.

[0008] 한편, 상기 디바이스에서 상기 제1 이미지 및 상기 제2 이미지를 중첩하고, 중첩된 이미지로부터 광학식 문자 인식 방식으로 인증 코드를 식별하는 것은, 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지에서 배경 패턴을 제거한 뒤, 광학식 문자 인식 방식으로 인증 코드를 식별하는 것일 수 있다.

[0009] 또한, 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지에서 배경 패턴을 제거하는 것은, 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지를 구성하는 복수의 픽셀을 2X2의 픽셀 범위로 나누고, 상기 픽셀 범위에 적어도 하나의 투명 픽셀이 포함되는 경우, 해당 픽셀 범위에 포함되는 모든 픽셀을 투명 픽셀로 재정의하는 것일 수 있다.

[0010] 또한, 상기 디바이스에서 식별한 인증 코드인 제2 인증 코드를 상기 서버로 전송하는 것은, 상기 디바이스에서 상기 제2 인증 코드에 해쉬 함수를 적용하고, 상기 제2 인증 코드에 해쉬 함수를 적용한 값을 상기 서버로 전송하는 것일 수 있다.

[0011] 또한, 상기 서버에서 상기 제1 인증 코드 및 상기 제2 인증 코드를 비교하여 상기 디바이스와의 상호 인증 성공 여부를 판단하는 것은, 상기 서버에서 상기 제1 인증 코드에 해쉬 함수를 적용하고, 상기 제1 인증 코드에 해쉬 함수를 적용한 값과 상기 디바이스로부터 수신하는 상기 제2 인증 코드에 해쉬 함수를 적용한 값을 비교하여 상기 디바이스와의 상호 인증 성공 여부를 판단하는 것일 수 있다.

[0012] 또한, 상기 서버에서 상기 디바이스와의 상호 인증 성공 여부에 대한 판단 결과를 상기 디바이스로 알리는 것을 더 포함할 수 있다.

[0013] 한편, 본 발명의 다른 측면은 서버와 통신 시, 상기 서버와 시각암호 기반의 상호 인증을 수행하는 디바이스의 제어방법에 있어서, 상기 서버와 제1 이미지를 공유하여 미리 저장하고, 상기 서버와 통신을 시도하는 경우, 상기 서버로 상호 인증을 요청하여 상기 서버로부터 상기 제1 이미지를 이용하여 제1 인증 코드를 포함하도록 생성한 제2 이미지를 수신하고, 상기 제1 이미지 및 상기 제2 이미지를 중첩하고, 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지에 광학식 문자 인식 알고리즘을 적용하여 제2 인증 코드를 식별하고, 상기 제2 인증 코드를 상기 서버로 전송하여 상기 서버로부터 상기 제1 인증 코드와 상기 제2 인증 코드의 비교 결과에 따른 상호 인증 결과를 수신하는 시각암호 기반의 상호 인증을 수행한다.

[0014] 한편, 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지에 광학식 문자 인식 알고리즘을 적용하여 제2 인증

코드를 식별하는 것은, 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지에서 배경 패턴을 제거하는 것을 더 포함할 수 있다.

[0015] 또한, 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지에서 배경 패턴을 제거하는 것은, 상기 제1 이미지 및 상기 제2 이미지의 중첩된 이미지를 구성하는 복수의 픽셀을 2X2의 픽셀 범위로 나누고, 상기 픽셀 범위에 적어도 하나의 투명 픽셀이 포함되는 경우, 해당 픽셀 범위에 포함되는 모든 픽셀을 투명 픽셀로 재정의하는 것일 수 있다.

[0016] 또한, 상기 제2 인증 코드를 상기 서버로 전송하여 상기 서버로부터 상기 제1 인증 코드와 상기 제2 인증 코드의 비교 결과에 따른 상호 인증 결과를 수신하는 것은, 상기 제2 인증 코드에 해쉬 함수를 적용하고, 상기 제2 인증 코드에 해쉬 함수를 적용한 값을 상기 서버로 전송하며, 상기 서버로부터 상기 제1 인증 코드에 해쉬 함수를 적용한 값과 상기 제2 인증 코드에 해쉬 함수를 적용한 값의 비교 결과에 따른 상호 인증 결과를 수신하는 것일 수 있다.

발명의 효과

[0017] 상술한 본 발명의 일측면에 따르면 한 쌍의 이미지로 이루어지는 시각암호에 기기 간 상호 인증을 수행함으로써, 상호 인증에 필요한 연산을 최소화할 수 있으며, 광학식 문자 인식(OCR: Optical Character Recognition) 방식을 적용하여 사람의 개입이 없어도 시각암호 기반의 상호 인증을 수행할 수 있다.

도면의 간단한 설명

[0018] 도 1은 상호 인증을 수행하는 IoT(Internet of Things) 서비스 시스템을 개략적으로 도시한 도면이다.

도 2는 도 1에 도시된 IoT 서비스 시스템에서의 시각암호 기반의 상호 인증 단계를 도시한 플로우차트이다.

도 3은 도 1에 도시된 디바이스의 제어 블록도이다.

도 4는 시각암호를 생성하는 방법을 설명하기 위한 도면이다.

도 5는 시각암호의 이미지에서 배경 패턴을 제거하는 방법을 설명하기 위한 도면이다.

도 6은 도 3에 도시된 디바이스에서 인증 코드를 식별한 일 예를 도시한 도면이다.

도 7 및 도 8은 도 3에 도시된 디바이스의 제어방법을 설명하기 위한 순서도이다.

도 9는 도 1에 도시된 서버의 제어 블록도이다.

도 10은 도 9에 도시된 서버의 제어방법을 설명하기 위한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[0020] 이하, 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.

[0021] 도 1은 상호 인증을 수행하는 IoT(Internet of Things) 서비스 시스템을 개략적으로 도시한 도면이다.

[0022] 도 1을 참조하면, IoT 서비스 시스템은 홈 네트워크에 접속되는 디바이스(100) 및 사용자에게 디바이스(100)에 대한 제어 서비스를 제공하는 서버(200)로 구성될 수 있다. 이러한 IoT 서비스 시스템에서 디바이스(100) 및 서버(200) 간에 통신이 이루어지는데, 통신을 수행하기 전, 보안을 위해 디바이스(100) 및 서버(200) 간에 상호 인증이 이루어지는 것이 바람직하다.

[0023] 한편, 본 발명의 일 실시예에 따른 시각암호 기반의 상호 인증 방법은 시각암호에 기반하여 기기 간 상호 인증을 지원할 수 있으며, 아울러, 사람의 시각에 의존하여 시각암호를 인식하는 종래의 기술과는 달리 광학식 문자 인식(OCR) 알고리즘을 적용하여 기기 자체적으로 시각암호의 인식이 가능하다.

[0024] 따라서, 본 발명의 일 실시예에 따른 시각암호 기반의 상호 인증 방법은 도 1에 도시된 IoT 서비스 시스템과 같이 디바이스(100)와 서버(200)간의 통신 시 상호 인증 방법으로 적합하다. 이외에도, 본 발명의 일 실시예에 따른 시각암호 기반의 상호 인증 방법은 GUI(Graphical User Interface)를 지원하지 않는 헤드리스 디바이스(Headless Device), 또는, 사람이 살 수 없는 악조건의 자연환경에서 생태계의 정보를 수집하는 디바이스 간의 상호 인증 시 적용될 수 있다.

[0025] 이하에서는, 본 발명의 일 실시예에 따른 시각암호 기반의 상호 인증 방법에 대하여, 도 1과 같은 디바이스(100)와 서버(200) 간의 상호 인증을 수행하는 시스템에 적용된 경우를 예로 들어 설명하기로 한다.

[0026] 도 2는 도 1에 도시된 IoT 서비스 시스템에서의 시각암호 기반의 상호 인증 단계를 도시한 플로우차트이다.

[0027] 도 2를 참조하면, 먼저 디바이스(100)와 서버(200)는 제1 이미지를 공유할 수 있다. 이때, 제1 이미지는 예를 들면, 디바이스(100) 및 서버(200) 이외의 제3의 보안 관련 장치로부터 생성되어 디바이스(100) 및 서버(200)로 배포될 수 있으며, 디바이스(100) 및 서버(200)는 각각 제1 이미지를 저장할 수 있다. 이러한 제1 이미지는 소정의 규칙에 따른 검정 픽셀과 투명 픽셀들의 조합으로 이루어져 전체적으로는 회색으로 식별될 수 있다.

[0028] 한편, 디바이스(100)에서 서버(200)와의 통신을 수행하기 위해서는, 서버(200)로 상호 인증을 요청할 수 있다.

[0029] 서버(200)는 이러한 디바이스(100)로부터의 상호 인증 요청에 응답하여 제1 인증 코드를 생성할 수 있다. 이때, 제1 인증 코드는 일예로 4자리의 숫자일 수 있다. 그리고, 서버(200)는 제1 이미지를 이용하여 제1 인증 코드를 포함하는 제2 이미지를 생성하고, 생성한 제2 이미지를 디바이스(100)로 전송할 수 있다. 즉, 서버(200)는 제1 이미지와 중첩되는 경우 제1 인증 코드에 해당하는 패턴이 검정색으로 식별되는 제2 이미지를 생성할 수 있다. 이러한 제1 이미지 및 제2 이미지 한 쌍을 시각암호라 할 수 있다. 이와 관련하여 구체적인 설명은 후술하기로 한다.

[0030] 디바이스(100)는 서버(200)로부터 제2 이미지를 수신하면, 제1 이미지와 제2 이미지를 중첩하고, 제1 이미지와 제2 이미지의 중첩된 이미지에서 배경 패턴에 해당하는 픽셀을 제거한 뒤, 광학식 문자 인식 방식을 적용하여 제1 이미지와 제2 이미지의 중첩된 이미지로부터 제2 인증 코드를 식별할 수 있다. 즉, 제1 이미지와 제2 이미지의 중첩된 이미지에 광학식 문자 인식 방식을 적용하여 제2 인증 코드에 해당하는 텍스트 형태의 정보를 획득할 수 있다. 이때, 광학식 문자 인식 방식은 이미지 형태의 정보로부터 텍스트 형태의 정보를 추출할 수 있는 방식으로, 일예로, 구글 사에 의해 무료로 배포되어 널리 사용되고 있는 Tesseract 알고리즘 기반의 광학식 문자 인식 방식이 적용 가능하다.

[0031] 이후, 디바이스(100)는 제2 인증 코드를 서버(200)로 전송할 수 있다.

[0032] 서버(200)는 제1 인증 코드와 디바이스(100)로부터 수신한 제2 인증 코드를 비교하고, 그 결과에 따라 상호 인증 성공 여부를 결정할 수 있으며, 그 결과를 디바이스(100)로 알릴 수 있다. 즉, 서버(200)는 제1 인증 코드와 제2 인증 코드가 일치하는 경우 디바이스(100)와 서버(200) 간에 상호 인증에 성공한 것으로 결정할 수 있다.

[0033] 여기에서, 디바이스(100)는 제2 인증 코드를 서버(200)로 전송 시, 제2 인증 코드에 해쉬 함수를 적용한 뒤 그 값을 전송할 수 있으며, 이와 같은 경우, 서버(200)는 제1 인증 코드에 해쉬 함수를 적용하고, 제1 인증 코드에 해쉬 함수를 적용한 값과, 디바이스(100)로부터 수신하는 제2 인증 코드에 해쉬 함수를 적용한 값을 비교하여 디바이스(100)와 서버(200) 간의 상호 인증을 수행할 수 있다.

[0034] 이와 같은, 도 1에 도시된 IoT 서비스 시스템에서의 시각암호 기반의 상호 인증 단계에 따르면, 서버(200)에서 생성하는 시각암호 기반의 상호 인증이 이루어지므로 상호 인증을 위한 암호화 또는 복호화 시 필요한 연산량을 최소화할 수 있다. 아울러, 디바이스(100)에서는 광학식 문자 인식 방식으로 텍스트 형태의 인증 코드 식별이 가능하여 사람의 개입이 없어도 시각암호 기반의 상호 인증을 수행할 수 있다.

[0035] 이하에서는, 도 3 내지 도 10을 참조하여, 본 발명의 일 실시예에 따른 시각암호 기반의 상호 인증 방법에 따른 상호 인증을 수행하는 IoT 서비스 시스템에 포함되는 각 구성요소에 대하여 구체적으로 설명하기로 한다.

[0036] 먼저, 도 3은 도 1에 도시된 디바이스의 제어 블록도이다.

[0037] 도 3을 참조하면, 디바이스(100)는 디바이스 통신부(110), 디바이스 제어부(120) 및 디바이스 메모리부(130)를

포함하여, 서버(200)와의 상호 인증을 수행할 수 있으며, 특히, 상호 인증 시 시각암호 이미지로부터 문자 형태의 인증 코드를 식별할 수 있다. 이러한 디바이스(100)는 도 3에 도시된 구성요소보다 많은 구성요소에 의해 구현되거나, 보다 적은 구성요소에 의해 구현될 수 있다. 이하, 상술한 구성요소들에 대해 구체적으로 설명하기로 한다.

[0038] 디바이스 통신부(110)는 디바이스(100)와 서버(200) 간의 통신을 가능하게 하며, 이를 위해, 무선 통신 또는 근거리 무선 통신을 수행하게 하는 하나 이상의 구성요소를 포함하여 구현될 수 있다. 예를 들면, 디바이스 통신부(110)는 서버(200)로 상호 인증 요청과 관련된 신호를 송신하거나, 후술하는 디바이스 제어부(120)에서 획득하는 인증 코드 정보를 송신할 수 있다. 또한, 디바이스 통신부(110)는 서버(200)로부터 인증 코드를 포함하는 이미지를 수신하거나, 상호 인증 결과를 수신할 수 있다. 또한, 디바이스 통신부(110)는 서버(200) 이외의 제3의 장치로부터 시각암호와 관련된 이미지를 수신할 수 있다.

[0039] 디바이스 제어부(120)는 디바이스(100)의 전반적인 동작을 제어할 수 있다. 특히, 디바이스 제어부(120)는 서버(200)로부터 수신하는 정보에 기반하여 서버(200)와의 상호 인증을 위한 정보를 생성할 수 있다. 이를 위해, 디바이스 제어부(120)는 이미지 중첩부(121), 배경 패턴 제거부(122), 인증 코드 식별부(123) 및 인증 코드 암호화부(124)를 포함할 수 있다.

[0040] 이미지 중첩부(121)는 시각암호를 구성하는 한 쌍의 이미지를 중첩할 수 있다. 이때, 시각암호를 구성하는 한 쌍의 이미지는 제1 이미지 및 제2 이미지일 수 있다. 제1 이미지는 디바이스(100) 및 서버(200) 이외의 제3의 보안 관련 장치에서 생성되고 배포되어 디바이스(100)와 서버(200) 간에 공유되는 이미지일 수 있으며, 디바이스 메모리부(130)에 이러한 제1 이미지가 미리 저장된 상태일 수 있다. 또는, 제1 이미지는 서버(200)에서 생성되고 배포될 수 있다. 제2 이미지는 서버(200)로부터 수신할 수 있는데, 서버(200)와의 통신이 요구되는 경우, 디바이스(100)로부터 서버(200)로 통신 요청 신호가 전송되고, 이러한 통신 요청 신호에 응답한 서버(200)로부터 수신할 수 있다. 이미지 중첩부(121)는 서버(200)와의 상호 인증을 수행하기 위한 인증 코드를 획득할 수 있도록 이러한 제1 이미지 및 제2 이미지를 중첩할 수 있다. 이와 관련하여, 도 4 및 도 5를 참조하여 설명하기로 한다.

[0041] 도 4 및 도 5는 시각암호를 구성하는 한 쌍의 이미지의 일 예를 도시한 도면이다.

[0042] 도 4를 참조하면, 제1 이미지(Shared Image 1)는 소정의 규칙에 따른 검정 픽셀과 투명 픽셀들의 조합으로 이루어져 육안으로는 회색으로 보여질 수 있다. 구체적으로는, 제1 이미지를 구성하는 복수의 픽셀을 2X2 픽셀 범위로 나눌 수 있으며, 제1 이미지의 각 열(column)은 도 5의 배경 픽셀(Background Pixel)의 복수의 패턴 중 랜덤으로 선택되는 하나의 패턴을 갖는 2X2 픽셀 범위가 나열될 수 있다. 예를 들면, 도 4에 도시된 제1 이미지의 첫 번째 열은 도 5의 배경 픽셀의 4번째 패턴(shape no 4)을 갖는 2X2 픽셀 범위가 나열될 수 있다. 이와 같은 방식으로 생성 가능한 제1 이미지는 디바이스(100) 및 서버(200) 이외의 제3의 보안 관련 장치에서 생성되거나, 서버(200)에서 생성되고 디바이스(100) 및 서버(200)로 배포되어 공유될 수 있다.

[0043] 한편, 제2 이미지(shared Image 2)는 서버(200)에 의해 제1 이미지로부터 생성될 수 있다. 구체적으로는, 서버(200)는 디바이스(100)로부터 통신 요청 신호를 수신하면 제2 이미지를 생성하는데, 먼저 4자리 숫자의 인증 코드를 생성할 수 있으며, 이러한 인증 코드에 대응하는 패턴을 포함하는 이미지(Original Image)를 생성할 수 있다. 이때, 인증 코드에 대응하는 패턴을 포함하는 이미지는 제1 이미지와 동일한 크기일 수 있다. 서버(200)는 인증 코드에 대응하는 패턴을 포함하는 이미지를 참조하여, 제1 이미지에서 인증 코드에 대응하는 패턴에 해당하는 2X2 픽셀 범위를 반전시켜 제2 이미지를 생성할 수 있다. 즉, 제1 이미지에서 인증 코드에 대응하는 패턴에 해당하는 2X2 픽셀 범위에 포함되는 픽셀이 투명 픽셀인 경우 검정 픽셀로 재정의하고, 검정 픽셀인 경우 투명 픽셀로 재정의할 수 있다. 예를 들면, 도 4를 참조하면, 제1 이미지에서 인증 코드 "9"에 대응하는 패턴에 해당하는 2X2 픽셀 범위가 도 5의 배경 픽셀의 5번째 패턴(shape no 5)을 갖는 2X2 픽셀 범위라면, 해당 2X2 픽셀 범위를 도 5의 레터 픽셀의 5번째 패턴(shape no 5)을 갖는 2X2 픽셀 범위로 재정의할 수 있다.

[0044] 따라서, 이미지 중첩부(121)에 의해 제1 이미지와 제2 이미지가 중첩되는 경우, 동일한 패턴을 갖는 2X2 픽셀 범위에 해당하는 영역은 회색으로 식별되나, 서로 반전되는 패턴을 갖는 2X2 픽셀 범위에 해당하는 영역은 검정색으로 식별될 수 있다. 이때, 제1 이미지와 제2 이미지의 중첩된 이미지에서 회색으로 식별되는 영역은 배경 패턴일 수 있으며, 검정색으로 식별되는 영역은 인증 코드를 나타낼 수 있다.

[0045] 배경 패턴 제거부(122)는 제1 이미지와 제2 이미지의 중첩되는 이미지에서 배경 패턴을 제거할 수 있다. 배경 패턴 제거부(122)는 제1 이미지와 제2 이미지의 중첩되는 이미지에서 회색으로 식별되는 패턴을 갖는 2X2 픽셀

범위에 포함되는 픽셀을 투명 픽셀로 재정의하는 방식으로 회색의 배경을 제거할 수 있다. 배경 패턴 제거부(122)에서 제1 이미지와 제2 이미지의 중첩되는 이미지의 회색의 배경 패턴을 제거하는 것은 후술하는 인증 코드 식별부(123)에서 광학식 문자 인식 알고리즘의 적용을 가능하게 하기 위함이다.

[0046] 구체적으로는, 배경 패턴 제거부(122)는 아래의 알고리즘에 따라 제1 이미지와 제2 이미지의 중첩되는 이미지에서 배경 패턴을 제거할 수 있다.

```
//두 Share이미지를 Overlap하여 생성한 이미지의 픽셀을 배열에 담는다.
int[][] src_colors = new int[bitmap.getPixels.getWidth()][bitmap.getPixels.getHeight()];

//픽셀을 하나씩 꺼내온다.
    for(int y= 0; y < src_width; y += 1)
    {
      for(int x=0; x < src_height; x += 1)
      {
//2X2픽셀 범위를 정한다.
//이 중 하나의 픽셀이라도 투명색이라면
        if( src_colors[bitmap.getWidth()][bitmap.getHeight()] == Color.TRANSPARENT || src_colors[bitmap.getWidth()][bitmap.getHeight()+1] == Color.TRANSPARENT
            || src_colors[bitmap.getWidth()+1][bitmap.getHeight()] == Color.TRANSPARENT || src_colors[bitmap.getWidth()+1][bitmap.getHeight()+1] == Color.TRANSPARENT ){

//그 범위에 있는 모든 픽셀을 투명색으로 재정의한다.
                    src_colors[bitmap.getWidth()][bitmap.getHeight()] = Color.TRANSPARENT;
src_colors[bitmap.getWidth()][bitmap.getHeight()+1] = Color.TRANSPARENT;
src_colors[bitmap.getWidth()+1][bitmap.getHeight()] = Color.TRANSPARENT;
src_colors[bitmap.getWidth()+1][bitmap.getHeight()+1] = Color.TRANSPARENT;
        }
      }
    }
```

[0047]

[0048] 배경 패턴 제거부(122)는 제1 이미지와 제2 이미지의 중첩된 이미지를 구성하는 복수의 픽셀을 2X2 픽셀 범위로 나누고, 2X2 픽셀 범위를 각각 확인하는데, 2X2 픽셀 범위에 적어도 하나의 투명 픽셀이 포함되는 경우, 해당 픽셀 범위에 포함되는 모든 픽셀을 투명 픽셀로 재정의할 수 있다. 예를 들면, 제1 이미지와 제2 이미지의 중첩된 이미지의 2X2 픽셀 범위 중 어느 하나가 도 5의 배경 픽셀의 5번째 패턴(shape no 5)을 갖는 경우, 해당 픽셀 범위에는 투명 픽셀이 포함되므로, 해당 픽셀 범위에 포함되는 모든 픽셀을 투명 픽셀로 재정의할 수 있다.

[0049] 이와 같은 방식으로 배경 패턴 제거부(122)는 제1 이미지와 제2 이미지의 중첩된 이미지에서 배경 패턴에 해당하는 픽셀을 모두 투명색으로 재정의함으로써 배경 패턴을 제거할 수 있다. 할 수 있다. 이에 따라, 제1 이미지와 제2 이미지의 중첩된 이미지에서 배경 패턴이 제거되어 인증 코드를 나타내는 패턴이 보다 명확하게 식별될 수 있다.

[0050] 인증 코드 식별부(123)는 제1 이미지와 제2 이미지의 중첩된 이미지에서 배경 패턴이 제거되면, 해당 이미지에 광학식 문자 인식 방식을 적용하여 인증 코드를 식별할 수 있다. 즉, 인증 코드 식별부(123)는 광학식 문자 인식 방식을 통해 이미지로부터 문자 형태의 정보를 획득할 수 있다. 이와 관련하여 도 6을 참조하여 설명하기로 한다.

[0051] 도 6은 도 3에 도시된 디바이스에서 인증 코드를 식별한 일 예를 도시한 도면이다.

[0052] 광학식 문자 인식 방식이란 이미지를 읽고, 이미지 형태의 정보를 텍스트 형태의 정보로 변환할 수 있는 방식으로, 다양한 오픈 소스가 무료로 배포된 상태로, 일예로, 구글 사에 의해 배포된 Tesseract algorithm 알고리즘을 채용한 광학식 문자 인식 방식이 있다.

[0053] 도 6의 왼쪽은 제1 이미지와 제2 이미지의 중첩된 이미지에서 배경 패턴이 제거된 이미지로, 사람의 시각으로는 검정색의 인증 코드 "7968"이 식별 가능하나, 디바이스(100) 자체적으로는 이를 확인할 수 없다. 인증 코드 식별부(123)는 이러한 이미지에 광학식 문자 인식 방식을 적용할 수 있으며, 이와 같은 경우 도 6에 도시된 바와 같이 "7968"의 문자 형태의 데이터를 획득할 수 있다. 이때, 배경 패턴 제거부(122)에 의해 인증 코드에 해당하는 패턴을 포함하는 이미지의 배경 패턴이 제거되었으므로, 광학식 문자 인식 방식으로부터의 문자 형태의 데이

터 획득에 있어서 정확도를 높일 수 있다.

[0054] 인증 코드 암호화부(124)는 인증 코드 식별부(123)에 의해 식별된 인증 코드를 암호화할 수 있다. 이때, 인증 코드는 문자, 일예로 4자리 숫자일 수 있으며, 인증 코드 암호화부(124)는 이러한 인증 코드에 해쉬 함수를 적용하여 해쉬 값을 획득할 수 있다. 그리고, 인증 코드 암호화부(124)는 해쉬 값을 서버(200)로 전송할 수 있다. 이와 같은 경우, 서버(200)에서는 디바이스(100)로부터 수신한 해쉬 값과, 서버(200)에서 생성한 인증 코드에 해쉬 함수를 적용하여 획득한 해쉬 값을 비교함으로써 디바이스(100)와의 상호 인증을 수행할 수 있다.

[0055] 디바이스 메모리부(130)는 디바이스(100)의 처리 및 제어를 위한 프로그램이 저장될 수 있으며, 입출력되는 데이터들의 임시 저장을 위한 기능을 수행할 수 있다. 예를 들면, 디바이스 메모리부(130)는 서버(200)와 공유하는 제1 이미지를 저장할 수 있다.

[0056] 이하, 도 7 및 도 8을 참조하여, 도 3에 도시된 디바이스(100)의 제어방법에 대하여 설명하기로 한다.

[0057] 도 7 및 도 8은 도 2에 도시된 디바이스의 제어방법을 설명하기 위한 순서도이다.

[0058] 먼저, 도 7을 참조하면, 디바이스(100)는 서버(200)와 공유하는 제1 이미지를 배포받아 저장할 수 있다(700). 이때, 제1 이미지는 디바이스(100) 및 서버(200) 이외의 보안 관련 장치로부터 생성되어 배포되거나, 서버(200)에서 생성되어 배포될 수 있다.

[0059] 그리고, 디바이스(100)는 서버(200)와의 상호 인증을 요청할 수 있다(710). 디바이스(100)는 서버(200)와 통신을 수행하여야 하는 경우, 통신을 시작하기 전 서버(200)로 상호 인증을 요청할 수 있다.

[0060] 이와 같은 경우, 디바이스(100)는 서버(200)로부터 제2 이미지를 수신할 수 있다(720). 서버(200)는 디바이스(100)로부터 상호 인증을 요청 받는 경우, 이에 응답하여 인증 코드를 생성하고, 제1 이미지를 이용하여 인증 코드를 포함하는 제2 이미지를 생성할 수 있으며, 이러한 제2 이미지를 디바이스(100)로 송신할 수 있다.

[0061] 이후, 디바이스(100)는 제1 이미지 및 제2 이미지를 중첩하고(730), 제1 이미지 및 제2 이미지의 중첩된 이미지에서 배경 패턴에 해당하는 픽셀을 제거할 수 있다(740).

[0062] 이와 관련하여 도 8을 참조하여 구체적으로 설명하면, 디바이스(100)는 제1 이미지 및 제2 이미지의 중첩된 이미지를 구성하는 복수의 픽셀을 2X2 픽셀 범위로 나눌 수 있다(800). 그리고, 디바이스(100)는 2X2 픽셀 범위를 각각 확인하는데, 각 픽셀 범위에 투명 픽셀이 포함되는지를 확인할 수 있다(810).

[0063] 디바이스(100)는 픽셀 범위에 투명 픽셀이 포함되는 것으로 확인되면(810), 해당 픽셀 범위에 포함되는 픽셀을 모두 투명 픽셀로 재정의할 수 있다(820).

[0064] 이와 같은 방식으로 디바이스(100)는 모든 픽셀 범위를 확인할 수 있으며(830), 그 결과 제1 이미지 및 제2 이미지의 중첩된 이미지에서 배경 패턴에 해당하는 픽셀은 모두 투명 픽셀로 재정의되어 결과적으로는 배경이 제거될 수 있다.

[0065] 다시 도 7을 참조하면, 디바이스(100)는 배경 패턴이 제거된 제1 이미지 및 제2 이미지의 중첩된 이미지에 광학식 문자 인식 알고리즘을 적용하여 인증 코드를 식별할 수 있다(750). 즉, 디바이스(100)는 광학식 문자 인식 방식으로 제1 이미지 및 제2 이미지의 중첩된 이미지로부터 인증 코드를 인식할 수 있다.

[0066] 그리고, 디바이스(100)는 식별한 인증 코드를 암호화하고(760), 암호화된 인증 코드를 서버(200)로 전송할 수 있다(770).

[0067] 여기에서, 디바이스(100)는 인증 코드에 해쉬 함수를 적용하고, 그 결과 산출되는 값을 서버(200)로 전송할 수 있다. 이와 같은 경우, 서버(200)에서는 디바이스(100)로부터 수신하는 값과, 서버(200)에서 생성한 인증 코드에 해쉬 함수를 적용한 값을 비교하고, 그 결과 두 값이 일치하면 디바이스(100)와의 상호 인증에 성공한 것으로 판단할 수 있다.

[0068] 한편, 도 9는 도 1에 도시된 서버의 제어 블록도이다.

[0069] 도 9를 참조하면, 서버(200)는 서버 통신부(210), 서버 제어부(220) 및 서버 메모리부(230)를 포함하여, 디바이스(100)와의 상호 인증을 수행할 수 있으며, 특히, 상호 인증을 위한 시각암호 이미지를 생성할 수 있다. 이러한 서버(200)는 도 9에 도시된 구성요소보다 많은 구성요소에 의해 구현되거나, 보다 적은 구성요소에 의해 구현될 수 있다. 이하, 상술한 구성요소들에 대해 구체적으로 설명하기로 한다.

[0070] 서버 통신부(210)는 서버(200)와 디바이스(100) 간의 통신을 가능하게 하며, 이를 위해, 무선 통신 또는 근거리

통신을 수행하게 하는 하나 이상의 구성요소를 포함하여 구현될 수 있다. 예를 들면, 서버 통신부(210)는 디바이스(100)로부터 성호 인증 요청과 관련된 신호를 수신하거나, 디바이스(100)에서 획득한 인증 코드와 관련된 정보를 수신할 수 있다. 또한, 서버 통신부(210)는 디바이스(100)로 후술하는 서버 제어부(220)에서 생성한 상호 인증을 위한 이미지를 송신할 수 있다. 또한, 서버 통신부(210)는 디바이스(100) 이외의 제3의 장치로부터 시가암호와 관련된 이미지를 수신할 수 있다.

[0071] 서버 제어부(220)는 서버(200)의 전반적인 동작을 제어할 수 있다. 특히, 서버 제어부(220)는 디바이스(100)와 상호 인증을 위한 정보를 생성하며, 디바이스(100)로부터 수신하는 정보에 기반하여 디바이스(100)와의 상호 인증을 수행할 수 있다. 이를 위해, 서버 제어부(220)는 인증 코드 생성부(221), 이미지 생성부(222) 및 인증 코드 비교부(223)를 포함할 수 있다.

[0072] 인증 코드 생성부(221)는 디바이스(100)로부터 상호 인증 요청 신호, 또는 통신 요청 신호를 수신하는 경우, 이에 응답하여 인증 코드를 생성할 수 있다. 이때, 인증 코드는 일예로, 4자리의 숫자일 수 있다.

[0073] 이미지 생성부(222)는 인증 코드를 포함하는 이미지를 생성할 수 있다. 이때, 이미지 생성부(222)는 제1 이미지를 이용하여 인증 코드를 포함하는 제2 이미지를 생성할 수 있다. 즉, 제1 이미지 및 제2 이미지는 시각암호를 구성할 수 있으며, 제1 이미지와 제2 이미지가 중첩되는 경우, 인증 코드가 육안으로 식별 가능하다.

[0074] 구체적으로는, 제1 이미지는 디바이스(100) 및 서버(200) 이외의 제3의 보안 관련 장치에서 생성되고 배포되어 디바이스(100)와 서버(200) 간에 공유되는 이미지일 수 있다. 이와 같은 경우, 서버 메모리부(230)에 제1 이미지가 미리 저장된 상태일 수 있다. 또는, 이미지 생성부(222)에서 제1 이미지를 생성하고, 이를 디바이스(100)와 공유할 수 있다. 이러한, 제1 이미지는 상술한 바와 같이 소정의 규칙에 따른 검정 픽셀과 투명 픽셀들의 조합으로 이루어져 육안으로는 회색으로 보여질 수 있다. 제1 이미지의 생성 방법과 관련하여 구체적은 설명은 상술하였으므로 생략하기로 한다.

[0075] 이미지 생성부(222)는 제1 이미지로부터 제2 이미지를 생성할 수 있는데, 이를 위해 먼저 인증 코드에 대응하는 패턴을 포함하는 이미지를 생성할 수 있다. 이때, 인증 코드에 대응하는 패턴을 포함하는 이미지는 제1 이미지와 동일한 크기일 수 있다.

[0076] 그리고, 이미지 생성부(222)는 인증 코드에 대응하는 패턴에 해당하는 이미지를 참조하여, 제1 이미지에서 인증 코드에 대응하는 패턴에 해당하는 2X2 픽셀 범위를 반전시켜 제2 이미지를 생성할 수 있다. 즉, 제1 이미지에서 인증 코드에 대응하는 패턴에 해당하는 2X2 픽셀 범위에 포함되는 픽셀이 투명 픽셀인 경우 검정 픽셀로 재정의하고, 검정 픽셀인 경우 투명 픽셀로 재정의할 수 있다. 예를 들면, 도 4를 참조하면, 제1 이미지에서 인증 코드 "9"에 대응하는 패턴에 해당하는 2X2 픽셀 범위가 도 5의 배경 픽셀의 5번째 패턴(shape no 5)을 갖는 2X2 픽셀 범위라면, 해당 2X2 픽셀 범위를 도 5의 레터 픽셀의 5번째 패턴(shape no 5)을 갖는 2X2 픽셀 범위로 재정의할 수 있다. 따라서, 제1 이미지와 제2 이미지가 중첩되는 경우, 동일한 패턴을 갖는 2X2 픽셀 범위에 해당하는 영역은 회색으로 식별되나, 서로 반전되는 패턴을 갖는 2X2 픽셀 범위에 해당하는 영역은 검정색으로 식별될 수 있다. 이때, 제1 이미지와 제2 이미지의 중첩된 이미지에서 회색으로 식별되는 영역은 배경 패턴일 수 있으며, 검정색으로 식별되는 영역은 인증 코드를 나타낼 수 있다.

[0077] 이미지 생성부(222)는 이와 같은 방식으로 서버(200)와 디바이스(100) 간에 공유하는 제1 이미지와 중첩되는 경우, 제1 이미지가 식별되는 제2 이미지를 생성하여 디바이스(100)로 전송할 수 있다.

[0078] 인증 코드 비교부(223)는 디바이스(100)로부터 수신하는 인증 코드인 제2 인증 코드와 인증 코드 생성부(221)에서 생성한 인증 코드인 제1 인증 코드를 비교하고, 그 결과에 따라 디바이스(100)와의 상호 인증 성공 여부를 결정할 수 있다. 즉, 인증 코드 비교부(223)는 제1 인증 코드와 제2 인증 코드가 동일하면 서버(200)와 디바이스(100)간에 상호 인증에 성공한 것으로 판단하고, 그 결과를 디바이스(100)로 알릴 수 있다. 이와 같은 경우, 서버(200)와 디바이스(100) 간에 통신이 수행될 수 있다.

[0079] 한편, 디바이스(100)는 상술한 바와 같이 제2 인증 코드를 획득하면, 제2 인증 코드에 해쉬 함수를 적용하고, 제2 인증 코드에 해쉬 함수를 적용한 값을 서버(200)로 전송할 수 있다. 이에 따라, 인증 코드 비교부(223) 또한 제1 인증 코드에 해쉬 함수를 적용하여 그 값을 획득할 수 있다. 그리고, 인증 코드 비교부(223)는 제1 인증 코드에 해쉬 함수를 적용한 값과, 디바이스(100)로부터 수신하는 제2 인증 코드에 해쉬 함수를 적용한 값을 비교하여 디바이스(100)와의 상호 인증을 수행할 수 있다.

[0080] 서버 메모리부(230)는 서버(200)의 처리 및 제어를 위한 프로그램이 저장될 수 있으며, 입출력되는 데이터들의 임시 저장을 위한 기능을 수행할 수 있다. 예를 들면, 서버 메모리부(230)는 디바이스(100)와 공유하는 제1 이

미지를 저장할 수 있다.

[0081] 이하, 도 10을 참조하여, 도 9에 도시된 서버(200)의 제어방법에 대하여 설명하기로 한다.

[0082] 도 10은 도 9에 도시된 서버의 제어방법을 설명하기 위한 순서도이다.

[0083] 도 9를 참조하면, 서버(200)는 디바이스(100)와 공유하는 제1 이미지를 배포 받아 저장할 수 있다(1000). 이때, 제1 이미지는 서버(200) 및 디바이스(100) 이외의 보안 관련 장치로부터 생성되어 배포되거나, 서버(200)에서 생성하여 디바이스(100)와 공유할 수 있다.

[0084] 그리고, 서버(200)는 디바이스(100)로부터 상호 인증 요청을 수신하면(1100), 인증 코드를 생성할 수 있다(1200).

[0085] 그리고, 서버(200)는 제1 이미지를 이용하여 인증 코드를 포함하는 제2 이미지를 생성하고(1300), 제2 이미지를 디바이스(100)로 전송할 수 있다(1400).

[0086] 이와 같은 경우, 디바이스(100)는 제1 이미지 및 제2 이미지를 중첩하고, 제1 이미지 및 제2 이미지의 중첩된 이미지에 광학식 문자 인식 알고리즘을 적용하여 인증 코드를 식별할 수 있다. 그리고, 디바이스(100)는 식별한 인증 코드를 암호화하고, 암호화된 인증 코드를 서버(200)로 전송할 수 있다.

[0087] 서버(200)는 디바이스(100)로부터 암호화된 인증 코드를 수신하고(1500), 생성한 인증 코드를 암호화한 뒤 디바이스(100)로부터 수신한 암호화된 인증 코드와 비교할 수 있다(1600). 이때, 서버(200) 및 디바이스(100)는 모두 해쉬 함수를 적용하여 인증 코드를 암호화할 수 있다.

[0088] 서버(200)는 비교 결과 인증 코드가 일치하면(1700), 디바이스(100)와의 상호 인증에 성공한 것으로 판단할 수 있으며(1750), 반면, 비교 결과 인증 코드가 일치하지 않으면(1700), 디바이스(100)와의 상호 인증에 실패한 것으로 판단하고(1800), 이러한 상호 인증 결과를 디바이스(100)로 알릴 수 있다(1900).

[0089] 이와 같은, 본 발명의 일 실시예에 따른 시각암호 기반의 상호 인증 방법, 상호 인증을 수행하기 위한 디바이스(100) 및 서버(200)의 제어방법은 애플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.

[0090] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거니와 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[0091] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD 와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.

[0092] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드 뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0093] 이상에서는 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

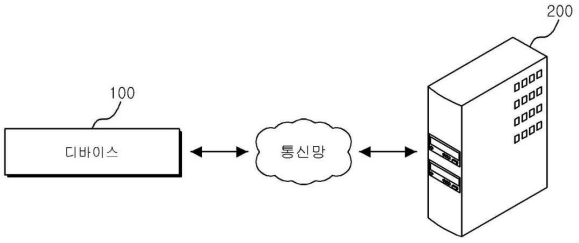
부호의 설명

[0094] 100: 서버

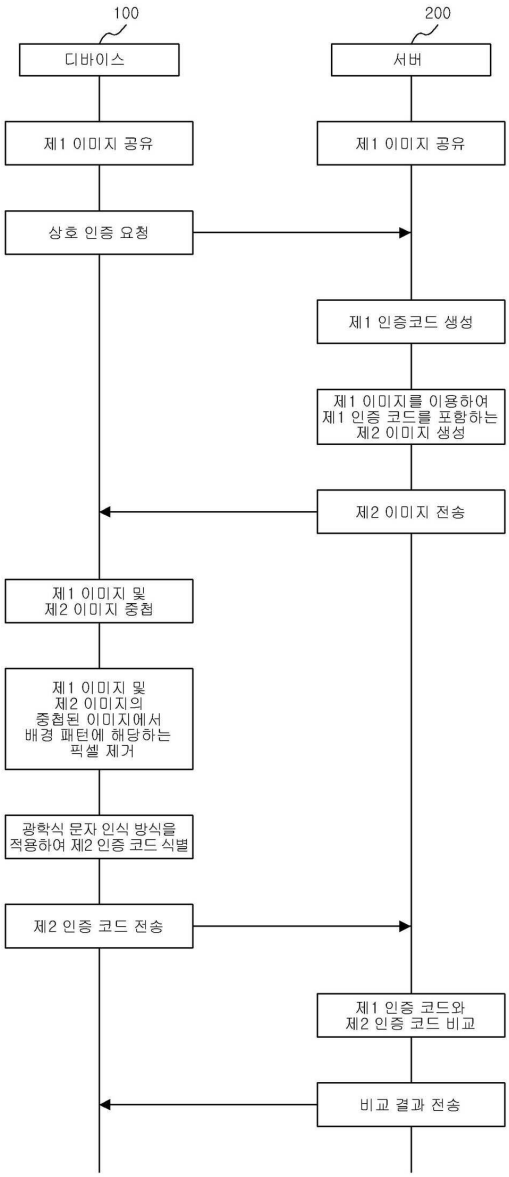
200: 디바이스

도면

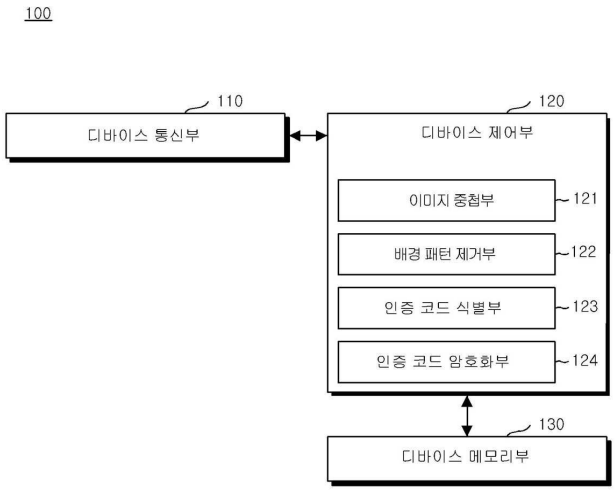
도면1


200
100
디바이스
통신망

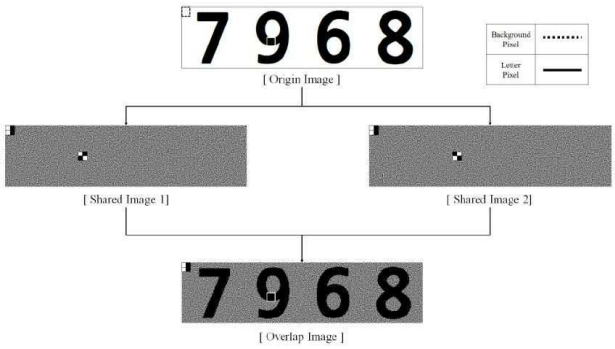
도면2


100
디바이스
200
서버
제1 이미지 공유
제1 이미지 공유
상호 인증 요청
제1 인증코드 생성
제1 이미지를 이용하여
제1 인증 코드를 포함하는
제2 이미지 생성
제2 이미지 전송
제1 이미지 및
제2 이미지 중첩
제1 이미지 및
제2 이미지의
중첩된 이미지에서
배경 패턴에 해당하는
픽셀 제거
광학식 문자 인식 방식을
적용하여 제2 인증 코드 식별
제2 인증 코드 전송
제1 인증 코드와
제2 인증 코드 비교
비교 결과 전송

도면3



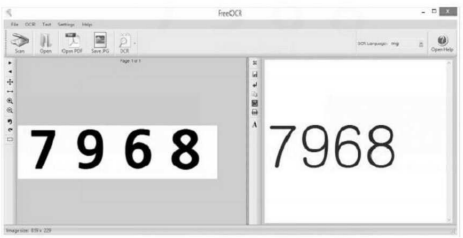
도면4



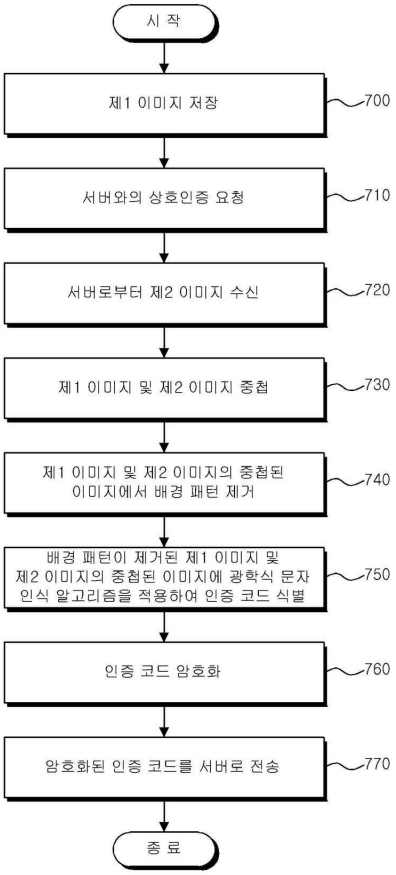
도면5

shape no	Background Pixel □					Letter Pixel ■				
	Share1		Share2		overlap	Share1		Share2		overlap
1		+		=			+		=	
2		+		=			+		=	
3		+		=			+		=	
4		+		=			+		=	
5		+		=			+		=	
6		+		=			+		=	

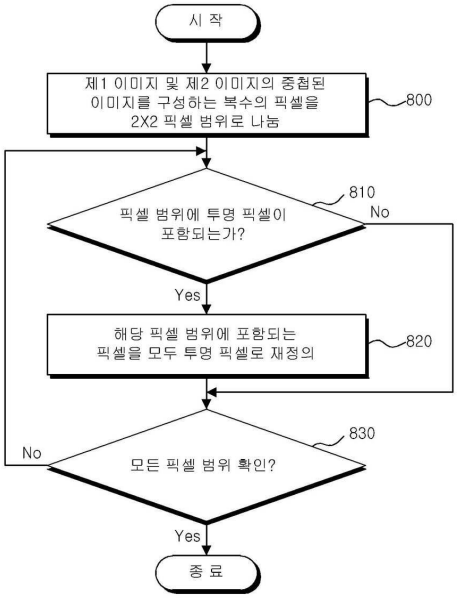
도면6



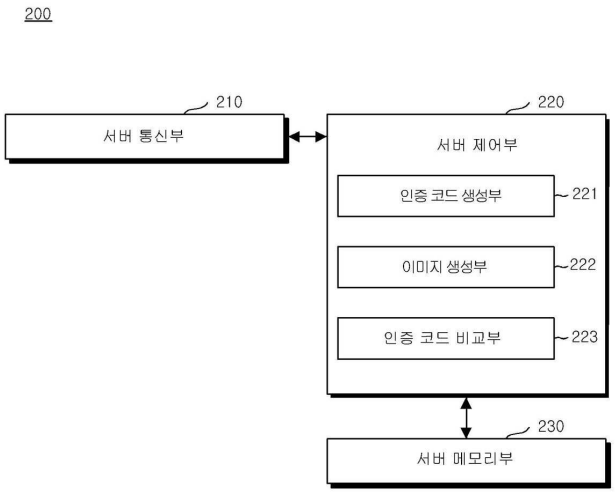
도면7


시 작
제1 이미지 저장
700
서버와의 상호인증 요청
710
서버로부터 제2 이미지 수신
720
제1 이미지 및 제2 이미지 중첩
730
제1 이미지 및 제2 이미지의 중첩된 이미지에서 배경 패턴 제거
740
배경 패턴이 제거된 제1 이미지 및 제2 이미지의 중첩된 이미지에 광학식 문자 인식 알고리즘을 적용하여 인증 코드 식별
750
인증 코드 암호화
760
암호화된 인증 코드를 서버로 전송
770
종 료

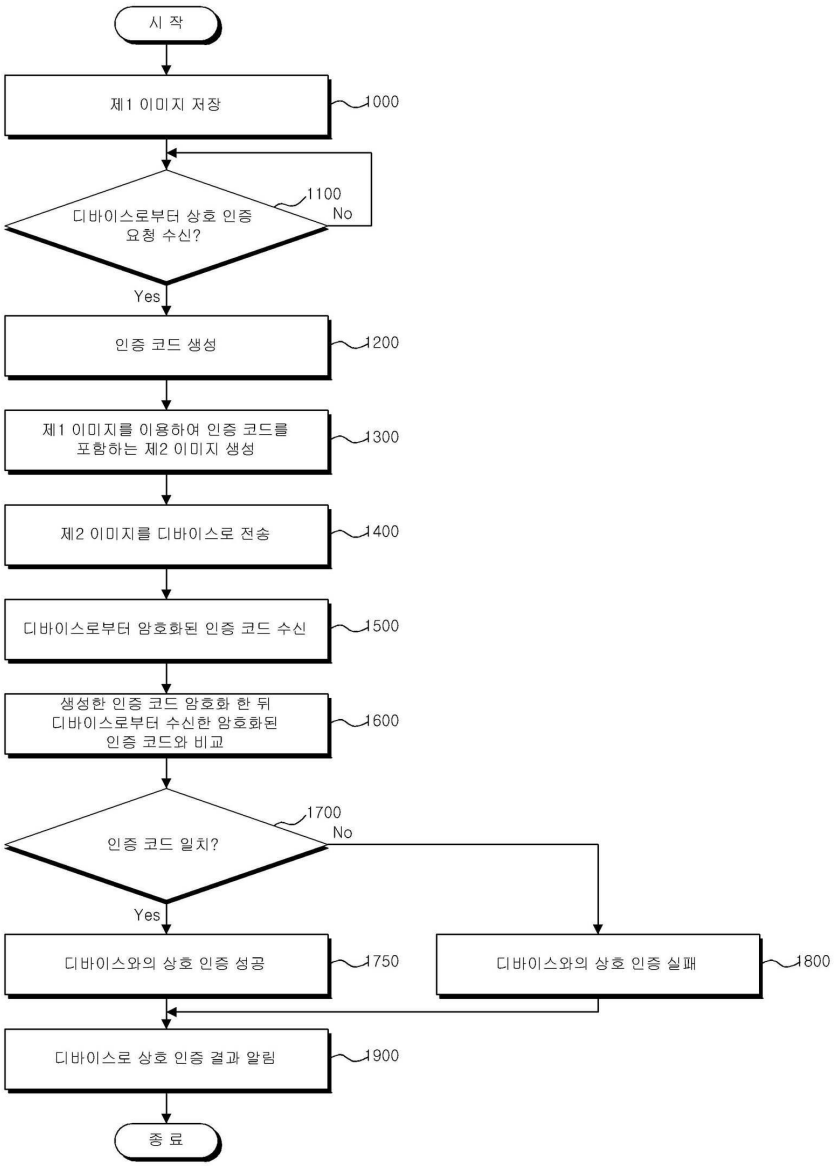
도면8


시 작
제1 이미지 및 제2 이미지의 중첩된 이미지를 구성하는 복수의 픽셀을 2X2 픽셀 범위로 나눔
800
픽셀 범위에 투명 픽셀이 포함되는가?
810
No
Yes
해당 픽셀 범위에 포함되는 픽셀을 모두 투명 픽셀로 재정의
820
모든 픽셀 범위 확인?
830
No
Yes
종 료

도면9


200
210
서버 통신부
220
서버 제어부
인증 코드 생성부
221
이미지 생성부
222
인증 코드 비교부
223
230
서버 메모리부

도면10


시 작
제1 이미지 저장
1000
디바이스로부터 상호 인증 요청 수신?
1100
No
Yes
인증 코드 생성
1200
제1 이미지를 이용하여 인증 코드를 포함하는 제2 이미지 생성
1300
제2 이미지를 디바이스로 전송
1400
디바이스로부터 암호화된 인증 코드 수신
1500
생성한 인증 코드 암호화 한 뒤 디바이스로부터 수신한 암호화된 인증 코드와 비교
1600
인증 코드 일치?
1700
No
Yes
디바이스와의 상호 인증 성공
1750
디바이스와의 상호 인증 실패
1800
디바이스로 상호 인증 결과 알림
1900
종 료