(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년12월12일
(11) 등록번호 10-1340746
(24) 등록일자 2013년12월05일

(51) 국제특허분류(Int. Cl.)
G06F 15/16 (2006.01)
(21) 출원번호 10-2011-0035869
(22) 출원일자 2011년04월18일
심사청구일자 2011년10월25일
(65) 공개번호 10-2012-0118357
(43) 공개일자 2012년10월26일
(56) 선행기술조사문헌
KR100825209 B1
KR100377464 B1
KR1020080044716 A
JP2002055772 A

(73) 특허권자
주식회사 팬택
서울특별시 마포구 성암로 179 (상암동,팬택계열 알앤디센터빌딩)
(72) 발명자
문지욱
서울특별시 마포구 성암로 179, DMC I- 2 팬택빌딩 (상암동)
김광백
서울특별시 마포구 성암로 179, DMC I- 2 팬택빌딩 (상암동)
(74) 대리인
특허법인무한

전체 청구항 수 : 총 22 항 심사관 : 이석형

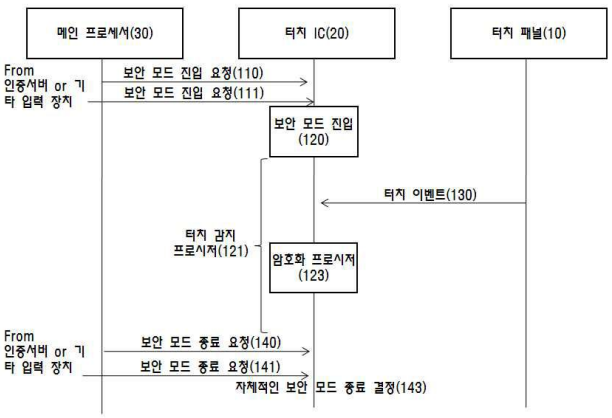
(54) 발명의 명칭 **전자 기기, 전자 기기의 사용자 입력 데이터의 보안 방법 및 장치**

(57) 요 약

전자 기기, 전자 기기의 사용자 입력 데이터의 보안 방법 및 장치, 사용자 입력 데이터의 보안 시스템이 개시된다.

전자 기기의 사용자 입력 데이터의 보안 장치는, 사용자의 데이터 입력을 위한 입력 인터페이스를 제공하는 터치 패널; 및 상기 터치 패널과 연결된 터치 IC를 포함하고, 상기 터치 IC는, "N(N은 1 이상의 정수)번의 터치 이벤트 각각의 발생 위치에 대한 N개의 좌표 데이터"를 저장하는 좌표 데이터 저장부; 및 사용자의 데이터 입력이 완료 되었음을 인지하면, 보안 키를 이용하여 상기 "N개의 좌표 데이터"를 암호화하는 암호화부를 포함한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

사용자의 데이터 입력을 위한 입력 인터페이스를 제공하는 터치 패널; 및

상기 터치 패널과 연결된 터치 IC를 포함하고,

상기 터치 IC는,

"N(N은 1 이상의 정수)번의 터치 이벤트 각각의 발생 위치에 대한 N개의 좌표 데이터"를 저장하는 좌표 데이터 저장부;

사용자의 데이터 입력이 완료 되었음을 인지하면, 보안 키를 이용하여 상기 "N개의 좌표 데이터"를 암호화하는 암호화부; 및

보안 모드의 진입을 요청하는 보안 모드 진입 요청 신호를 수신하여 보안 모드로 진입하면 상기 암호화부를 활성화시켜 암호화를 진행하고, 보안 모드가 아닌 경우 암호화부를 비활성화시켜 암호화를 진행하지 않도록 상기 암호화부를 제어하는 모드 제어부를 포함하는,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 2

제1항에 있어서,

상기 터치 IC는,

상기 보안 모드에서 발생되는 터치 이벤트, 또는 상기 좌표 데이터가 상기 전자기기의 메인 프로세서에 의해 감지되지 않도록 상기 터치 IC와 상기 메인 프로세서 사이의 전달 경로를 차단하는,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 3

제1항에 있어서,

상기 보안 모드 진입 요청 신호는,

보안이 필요한 어플리케이션이 실행되는 경우, "터치 패널을 통해 사용자의 특정 숫자의 입력, 특정 패턴의 입력"이 감지 경우, 또는 "터치 패널 이외의 기타 입력 장치를 통한 특정 숫자의 입력, 특정 입력 패턴"에 의해 발생되거나, 인증 서버로부터 수신되는,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 4

제1항에 있어서,

상기 모드 제어부는,

상기 보안 모드의 종료를 요청하는 보안 모드 종료 요청 신호를 수신하면, 좌표 데이터 저장부에 저장된 상기 "N개의 좌표 데이터"를 삭제하는,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 5

제2항에 있어서,

상기 모드 제어부는,

상기 보안 모드에서 "상기 터치 이벤트를 감지하는 터치 감지 프로시저" 및 "상기 N개의 좌표 데이터를 암호화

하는 암호화 프로시저" 각각에 대한 시스템 리소스 할당을 조정하는,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 6

제5항에 있어서,

상기 모드 제어부는,

상기 보안 모드에서 상기 터치 감지 프로시저 보다 상기 암호화 프로시저에 더 많은 시스템 리소스를 할당하는,

전자 기기의 사용자 입력 데이터의 보안 장치

청구항 7

제1항에 있어서,

상기 터치 IC는,

상기 암호화된 좌표 데이터를 상기 전자 기기의 통신 모듈을 통해 서버로 전송하는 송수신부를 더 포함하는,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 8

제7항에 있어서,

상기 송수신부는 상기 전자 기기의 메인 프로세서를 통하지 않고, 상기 암호화된 좌표 데이터를 직접(directly) 상기 통신 모듈에 전달하는,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 9

제7항에 있어서,

상기 송수신부는,

상기 터치 패널의 해상도, 상기 터치 패널의 크기, 상기 터치 패널에서 상기 입력 인터페이스의 위치에 대한 정보, 상기 터치 패널의 사양 정보, 또는 상기 전자기기의 사양 정보를 상기 통신 모듈을 통해 서버로 전송하는,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 10

제1항에 있어서,

상기 보안 키는 비 대칭 암호화 방식의 암호화를 위한 키 값인,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 11

제1항에 있어서,

상기 터치 IC는 "상기 N번의 터치 이벤트 각각에 대하여 터치가 감지 되었음을 나타내는 피드백 신호"를 생성하고, 상기 피드백 신호를 실행중인 어플리케이션 또는 디스플레이 제어부에 제공하는 피드백부를 더 포함하고,

여기서, 상기 피드백 신호는 랜덤한 값 또는 기 설정된 고유의 값인,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 12

사용자의 데이터 입력을 위한 입력 인터페이스를 제공하는 터치 패널; 및

상기 터치 패널과 연결된 터치 IC를 포함하고,

상기 터치 IC는,

상기 입력 인터페이스를 통해 터치 이벤트가 발생하면, 상기 터치 이벤트의 발생 위치에 대한 좌표 데이터를 획득하는 좌표 데이터 획득부;

상기 좌표 데이터를 사용자의 입력 데이터에 대응하는 사용자 입력 값으로 변환하고, 상기 사용자 입력 값을 저장부에 저장하는 변환부;

"N(N은 1 이상의 정수)번의 터치 이벤트 각각에 대한 N개의 사용자 입력 값"을 저장하는 저장부;

사용자의 데이터 입력이 완료 되었음을 인지하면, 보안키를 이용하여 상기 N개의 사용자 입력 값을 암호화하는 암호화부; 및

보안 모드의 진입을 요청하는 보안 모드 진입 요청 신호를 수신하여 보안 모드로 진입하면 상기 암호화부를 활성화시켜 암호화를 진행하고, 보안 모드가 아닌 경우 암호화부를 비활성화시켜 암호화를 진행하지 않도록 상기 암호화부를 제어하는 모드 제어부를 포함하는,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 13

제12항에 있어서,

상기 변환부는,

변환 기반 데이터에 기초하여 상기 좌표 데이터를 사용자의 입력 데이터에 대응하는 사용자 입력 값으로 변환하고,

상기 변환 기반 데이터는 "상기 입력 인터페이스를 통해 제공되는 숫자 키들, 문자 자판의 키들, 또는 기호 키들 각각에 할당된 좌표 정보"를 포함하는,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 14

제13항에 있어서,

상기 변환 기반 데이터는 상기 입력 인터페이스의 디스플레이 상태가 변경되면, 상기 입력 인터페이스의 디스플레이 상태에 따라 변경된 정보를 갖는,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 15

제13항에 있어서,

상기 변환 기반 데이터는 상기 터치 IC에 기 저장된 것, 또는 상기 전자 기기의 통신 모듈을 통해 서버로부터 직접 수신된 것인,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 16

사용자의 데이터 입력을 위한 입력 인터페이스를 제공하는 터치 패널; 및

상기 터치 패널과 연결된 터치 IC를 포함하고,

상기 터치 IC는,

"N(N은 1 이상의 정수)번의 터치 이벤트 각각의 발생 위치에 대한 N개의 좌표 데이터"를 저장하는 좌표 데이터 저장부;

사용자의 데이터 입력이 완료 되었음을 인지하면, 상기 N개의 좌표 데이터 각각을 사용자의 입력 데이

터에 대응하는 N개의 사용자 입력 값으로 변환하는 변환부;

보안키를 이용하여 상기 N개의 사용자 입력 값을 암호화하는 암호화부; 및

보안 모드의 진입을 요청하는 보안 모드 진입 요청 신호를 수신하여 보안 모드로 진입하면 상기 암호화부를 활성화시켜 암호화를 진행하고, 보안 모드가 아닌 경우 암호화부를 비활성화시켜 암호화를 진행하지 않도록 상기 암호화부를 제어하는 모드 제어부를 포함하는,

전자 기기의 사용자 입력 데이터의 보안 장치.

청구항 17

사용자의 데이터 입력을 위한 입력 인터페이스를 제공하는 터치 패널;

상기 입력 인터페이스를 통해 터치 이벤트가 발생하면, "보안모드에서 발생된 N(N은 1 이상의 정수)번의 터치 이벤트 각각의 발생 위치에 대한 N개의 좌표 데이터" 또는 "보안 모드에서 발생된 N번의 터치 이벤트 각각에 대응하는 N개의 사용자 입력 값"을 보안 키를 이용하여 암호화하는 터치 IC; 및

사용자의 데이터 입력이 완료 되면, 상기 암호화된 N개의 좌표 데이터 또는 상기 암호화된 N개의 사용자 입력 값을 서버로 전송하는 통신 모듈을 포함하고,

상기 터치 IC는 상기 보안 모드에서 발생되는 터치 이벤트, 상기 좌표 데이터, 또는 상기 사용자 입력 값이 전자기기의 메인 프로세서에 의해 감지되지 않도록 상기 터치 IC와 상기 메인 프로세서 사이의 전달 경로를 차단하는,

전자 기기.

청구항 18

제17항에 있어서,

정보의 보안이 필요한 어플리케이션이 실행되면, 보안 모드의 진입을 요청하는 보안 모드 진입 요청 신호를 상기 터치 IC로 전송하는 메인 프로세서를 더 포함하는,

전자 기기.

청구항 19

제18항에 있어서,

상기 메인 프로세서는 "상기 입력 인터페이스를 통해 제공되는 숫자 키들, 문자 자판의 키들, 또는 기호 키들 각각에 할당된 좌표 정보"를 포함하는 변환 기반 데이터를 상기 터치 IC로 제공하고,

상기 터치 IC는 상기 변환 기반 데이터에 기초하여 상기 N번의 터치 이벤트 각각에 대응하는 좌표 데이터를 사용자의 입력 데이터에 대응하는 사용자 입력 값으로 변환하는

전자 기기.

청구항 20

터치 패널을 통해 사용자의 데이터 입력을 위한 입력 인터페이스를 제공하는 단계;

상기 터치 패널과 연결된 터치 IC가 "N(N은 1 이상의 정수)번의 터치 이벤트 각각의 발생 위치에 대한 N개의 좌표 데이터"를 저장하는 단계; 및

보안 모드에서 사용자의 데이터 입력이 완료 되었음을 인지하면, 상기 터치 IC가 보안 키를 이용하여 상기 "N개의 좌표 데이터"를 암호화하는 단계를 포함하고,

상기 터치 IC는 상기 보안 모드에서 발생되는 터치 이벤트, 또는 상기 좌표 데이터가 전자기기의 메인 프로세서에 의해 감지되지 않도록 상기 터치 IC와 상기 메인 프로세서 사이의 전달 경로를 차단하는,

전자기기의 사용자 입력 데이터의 보안 방법.

청구항 21

터치 패널을 통해 사용자의 데이터 입력을 위한 입력 인터페이스를 제공하는 단계;

상기 입력 인터페이스를 통해 터치 이벤트가 발생하면, 상기 터치 패널과 연결된 터치 IC가 상기 터치 이벤트의 발생 위치에 대한 좌표 데이터를 획득하는 단계;

보안 모드에서 상기 좌표 데이터를 사용자의 입력 데이터에 대응하는 사용자 입력 값으로 변환하고, 상기 사용자 입력 값을 저장부에 저장하는 단계; 및

보안 모드에서 사용자의 데이터 입력이 완료 되었음을 인지하면, 상기 터치 IC가 보안키를 이용하여 상기 저장부에 저장된 N개의 사용자 입력 값을 암호화하는 단계를 포함하고,

상기 터치 IC는 상기 보안 모드에서 발생되는 터치 이벤트, 상기 좌표 데이터, 또는 상기 사용자 입력 값이 전자기기의 메인 프로세서에 의해 감지되지 않도록 상기 터치 IC와 상기 메인 프로세서 사이의 전달 경로를 차단하는,

전자기기의 사용자 입력 데이터의 보안 방법.

청구항 22

터치 패널을 통해 사용자의 데이터 입력을 위한 입력 인터페이스를 제공하는 단계;

상기 터치 패널과 연결된 터치 IC가 "N(N은 1 이상의 정수)번의 터치 이벤트 각각의 발생 위치에 대한 N개의 좌표 데이터"를 저장하는 단계;

보안 모드에서 사용자의 데이터 입력이 완료 되었음을 인지하면, 상기 N개의 좌표 데이터 각각을 사용자의 입력 데이터에 대응하는 N개의 사용자 입력 값으로 변환하는 단계; 및

상기 터치 IC가 보안키를 이용하여 상기 N개의 사용자 입력 값을 암호화하는 단계를 포함하고,

상기 터치 IC는 상기 보안 모드에서 발생되는 터치 이벤트, 또는 상기 좌표 데이터가 전자기기의 메인 프로세서에 의해 감지되지 않도록 상기 터치 IC와 상기 메인 프로세서 사이의 전달 경로를 차단하는,

전자기기의 사용자 입력 데이터의 보안 방법.

명 세 서

기 술 분 야

[0001] 기술분야는, 전자 기기의 사용자 입력 데이터의 보안 방법 및 장치, 전자 기기의 사용자 입력 데이터의 보안 방법 및 장치가 적용된 전자 기기, 및 사용자 입력 데이터의 보안을 적용한 통신 시스템에 관한 것이다. 여기서, 전자 기기는 스마트 폰, 태블릿 PC, 멀티미디어 기기 등의 휴대용 단말을 포함한다.

배 경 기 술

[0002] 최근 스마트 폰, 태블릿 PC 등에서 금융 프로그램과 같이 보안을 요구하는 어플리케이션의 사용이 빈번해 지고 있다. 그러나, 보안이 필요한 어플리케이션 또는 전자 기기의 해킹 등에 대한 대비는 취약하다. 예를 들어, 소스가 공개된(Open source) OS(Operating System)를 사용하는 전자 기기의 경우 해킹에 더욱 취약할 수 있다.

[0003] 한편, 웹 서버에서 제공되는 가상 키보드를 이용한 보안 방법이 있을 수 있다. 그러나, 가상 키보드를 이용한 보안 방법의 경우, 반드시 웹 서버에 접속해야 하는 문제가 있고, 전자 기기 자체에 대한 해킹에 취약한 문제가 있다.

발명의 내용

해결하려는 과제

[0004] 본 명세서에서는 사용자에 의해 입력되는 중요 정보를 보호하는 다양한 수단을 제공하고자 한다.

[0005] 또한, 본 발명은 터치 스크린 또는 터치 패널을 이용하는 다양한 전자 기기에서, 터치 스크린 또는 터치 패널을 통해 입력되는 정보를 터치 IC에서 암호화함으로써, 전자 기기의 보안을 강화할 수 있는 방법 및 장치를 제공한

다.

과제의 해결 수단

[0006] 일 측면에 있어서, 전자 기기의 사용자 입력 데이터의 보안 장치는, 사용자의 데이터 입력을 위한 입력 인터페이스를 제공하는 터치 패널; 및 상기 터치 패널과 연결된 터치 IC를 포함하고, 상기 터치 IC는, "N(N은 1 이상의 정수)번의 터치 이벤트 각각의 발생 위치에 대한 N개의 좌표 데이터"를 저장하는 좌표 데이터 저장부; 및 사용자의 데이터 입력이 완료 되었음을 인지하면, 보안 키를 이용하여 상기 "N개의 좌표 데이터"를 암호화하는 암호화부 및 보안 모드의 진입을 요청하는 보안 모드 진입 요청 신호를 수신하면 상기 암호화부를 활성화시키는 모드 제어부를 포함한다.

[0007] 다른 일 측면에 있어서, 상기 터치 IC는, 상기 입력 인터페이스를 통해 터치 이벤트가 발생하면, 상기 터치 이벤트의 발생 위치에 대한 좌표 데이터를 획득하는 좌표 데이터 획득부와, 상기 좌표 데이터를 사용자의 입력 데이터에 대응하는 사용자 입력 값으로 변환하고, 상기 사용자 입력 값을 저장부에 저장하는 변환부와, "N(N은 1 이상의 정수)번의 터치 이벤트 각각에 대한 N개의 사용자 입력 값"을 저장하는 저장부 및 사용자의 데이터 입력이 완료 되었음을 인지하면, 보안키를 이용하여 상기 N개의 사용자 입력 값을 암호화하는 암호화부 및 보안 모드의 진입을 요청하는 보안 모드 진입 요청 신호를 수신하여 보안 모드로 진입하면 상기 암호화부를 활성화시켜 암호화를 진행하고, 보안 모드가 아닌 경우 암호화부를 비활성화시켜 암호화를 진행하지 않도록 상기 암호화부를 제어하는 모드 제어부를 포함한다.

[0008] 다른 일 측면에 있어서, 상기 터치 IC는, "보안 모드에서 발생된 N(N은 1 이상의 정수)번의 터치 이벤트 각각의 발생 위치에 대한 N개의 좌표 데이터"를 저장하는 좌표 데이터 저장부와, 사용자의 데이터 입력이 완료 되었음을 인지하면, 상기 N개의 좌표 데이터 각각을 사용자의 입력 데이터에 대응하는 N개의 사용자 입력 값으로 변환하는 변환부와, 보안키를 이용하여 상기 N개의 사용자 입력 값을 암호화하는 암호화부 및 보안 모드의 진입을 요청하는 보안 모드 진입 요청 신호를 수신하면 상기 암호화부를 활성화시키는 모드 제어부를 포함한다.

[0009] 일 측면에 있어서, 전자 기기는, 사용자의 데이터 입력을 위한 입력 인터페이스를 제공하는 터치 패널과, 보안 모드에서 상기 입력 인터페이스를 통해 터치 이벤트가 발생하면, "보안 모드에서 발생된 N(N은 1 이상의 정수)번의 터치 이벤트 각각의 발생 위치에 대한 N개의 좌표 데이터" 또는 "N번의 터치 이벤트 각각에 대응하는 N개의 사용자 입력 값"을 보안 키를 이용하여 암호화하는 터치 IC 및 사용자의 데이터 입력이 완료 되면, 상기 암호화된 N개의 좌표 데이터 또는 상기 암호화된 N개의 사용자 입력 값을 서버로 전송하는 통신 모듈을 포함한다. 이때, 상기 터치 IC는 상기 보안 모드에서 발생되는 터치 이벤트, 또는 상기 좌표 데이터가 상기 전자기기의 메인 프로세서에 의해 감지되지 않도록 상기 터치 이벤트 또는 상기 좌표 데이터의 전달 경로를 차단한다.

[0010] 일 측면에 있어서, 전자기기의 사용자 입력 데이터의 보안 방법은, 터치 패널을 통해 사용자의 데이터 입력을 위한 입력 인터페이스를 제공하는 단계와, 상기 터치 패널과 연결된 터치 IC가 "보안 모드에서 발생된 N(N은 1 이상의 정수)번의 터치 이벤트 각각의 발생 위치에 대한 N개의 좌표 데이터"를 저장하는 단계 및 사용자의 데이터 입력이 완료 되었음을 인지하면, 상기 터치 IC가 보안 키를 이용하여 상기 "N개의 좌표 데이터"를 암호화하는 단계를 포함한다.

[0011] 다른 일 측면에 있어서, 전자기기의 사용자 입력 데이터의 보안 방법은, 터치 패널을 통해 사용자의 데이터 입력을 위한 입력 인터페이스를 제공하는 단계와, 보안 모드에서 상기 입력 인터페이스를 통해 터치 이벤트가 발생하면, 상기 터치 패널과 연결된 터치 IC가 상기 터치 이벤트의 발생 위치에 대한 좌표 데이터를 획득하는 단계와, 상기 좌표 데이터를 사용자의 입력 데이터에 대응하는 사용자 입력 값으로 변환하고, 상기 사용자 입력 값을 저장부에 저장하는 단계와, "N(N은 1 이상의 정수)번의 터치 이벤트 각각에 대한 N개의 사용자 입력 값"을 저장하는 단계 및 사용자의 데이터 입력이 완료 되었음을 인지하면, 상기 터치 IC가 보안키를 이용하여 상기 N개의 사용자 입력 값을 암호화하는 단계를 포함한다.

[0012] 다른 일 측면에 있어서, 전자기기의 사용자 입력 데이터의 보안 방법은, 터치 패널을 통해 사용자의 데이터 입력을 위한 입력 인터페이스를 제공하는 단계와, 상기 터치 패널과 연결된 터치 IC가 "보안 모드에서 발생된 N(N은 1 이상의 정수)번의 터치 이벤트 각각의 발생 위치에 대한 N개의 좌표 데이터"를 저장하는 단계와, 사용자의 데이터 입력이 완료 되었음을 인지하면, 상기 N개의 좌표 데이터 각각을 사용자의 입력 데이터에 대응하는 N개의 사용자 입력 값으로 변환하는 단계 및 상기 터치 IC가 보안키를 이용하여 상기 N개의 사용자 입력 값을 암호화하는 단계를 포함한다.

발명의 효과

[0013] 사용자에 의해 입력되는 중요 정보를 효과적으로 보호할 수 있다.

[0014] 터치 스크린 또는 터치 패널을 이용하는 다양한 전자 기기에서, 터치 스크린 또는 터치 패널을 통해 입력되는 정보를 터치 IC에서 암호화함으로써, 전자 기기의 보안을 강화할 수 있다.

[0015] 즉, 터치 스크린 또는 터치 패널을 통해 입력되는 정보를 터치 IC에서 암호화함으로써, 해킹 문제를 근본적으로 차단할 수 있다.

[0016] 또한, 본 발명의 실시 예들에 따르면, 메인 프로세서를 통하지 않고 터치 IC에서 직접 암호화하고 암호화된 정보를 통신 모듈을 통해 직접 외부 서버로 전송함으로써, 메인 프로세서가 해킹된다 하더라도 중요 정보를 보호할 수 있다.

도면의 간단한 설명

[0017] 도 1은 사용자 입력 데이터의 보안을 설명하기 위한 도면이다.

도 2는 일 실시 예에 따른 전자 기기의 구성을 나타내는 도면이다.

도 3은 일 실시 예에 따른 터치 IC의 구성을 나타내는 도면이다.

도 4는 일 실시 예에 따른 전자 기기의 사용자 입력 데이터의 보안 방법을 나타내는 도면이다.

도 5a는 다른 실시 예에 따른 전자 기기의 사용자 입력 데이터의 보안 방법을 나타내는 도면이다.

도 5b는 다른 실시 예에 따른 전자 기기의 사용자 입력 데이터의 보안 방법을 나타내는 도면이다.

도 6은 터치 패널에 입력 인터페이스가 디스플레이된 예를 나타낸다.

도 7은 일 실시 예에 따라서 사용자에게 디스플레이되는 화면의 예시도이다.

도 8은 일 실시 예에 따른 보안 키 획득 방법을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0019] 도 1은 일 실시 예에 따른 사용자 입력 데이터의 보안을 설명하기 위한 도면이다.

[0020] 도 1을 참조하면, 본 발명의 일 실시 예에 따른 사용자 입력 데이터의 보안은, 보안이 필요한 사용자의 입력 데이터를 터치 패널(10)로부터 수신하는 단계에서 터치 IC(20)가 사용자의 입력 데이터를 암호화함으로써, 전자기기의 메인 프로세서가(30) 사용자의 입력 데이터가 무엇인지를 알지 못하도록 하는 것이다.

[0021] 한편, 종래 기술에 따른 터치 IC는 보안 모드에서도 터치 패널을 통해 입력되는 사용자의 입력을 암호화하지 않았다. 또한, 종래기술에 따르면, 사용자의 데이터 입력은 전자기기의 메인 프로세서에 의해 바로 감지되고, 메인 프로세서에서 암호화를 제어하였다. 따라서, 종래 기술에 따르면, 전자기기의 메인 프로세서가 해킹되는 경우 사용자의 중요 정보가 노출될 수 있었다. 본 발명의 실시 예에 따른 터치 IC는 보안 모드에서 터치 패널을 통해 입력되는 데이터를 암호화하고, 보안 모드가 아닌 경우에는 암호화를 수행하지 않을 수 있다.

[0022] 보안 모드에서, 전자기기의 메인 프로세서(30)가 사용자의 입력 데이터가 무엇인지를 알지 못하도록 하는 방법은 아래의 3가지가 있을 수 있다.

[0023] 1) 방법 1: 보안 모드에서, 터치 이벤트의 발생 유무 자체를 전자 기기의 메인 프로세서(30)가 인식하지 못하도록 하는 방법. 예를 들어, 보안 모드에서 터치 IC는(20)는 터치 IC(20)와 메인 프로세서(30) 사이 또는 터치 패널(10)과 메인 프로세서(30)의 물리적인 또는 소프트웨어 적인 연결 경로를 차단함으로써, 메인 프로세서(30)가 터치 이벤트의 발생 자체를 감지하지 못하도록 할 수 있다.

[0024] 2) 방법 2: 보안 모드에서, 터치 이벤트의 발생은 전자 기기의 메인 프로세서(30)에 의해 감지되지만, 터치 이벤트의 발생 후 암호화된 사용자의 입력 데이터를 전자 기기의 메인 프로세서(30)로 전달하지 않는 방법. 방법 2에서, 터치 IC(20)는 메인 프로세서(30)를 거치지 않고 전자 기기의 통신 모듈을 통해 암호화된 사용자의 입력 데이터를 서버로 직접 전송할 수 있다.

[0025] 3) 방법 3: 보안 모드에서, 터치 이벤트의 발생은 전자 기기의 메인 프로세서에 의해 감지되고, 터치 이벤트의 발생 후 암호화된 사용자의 입력 데이터를 전자 기기의 메인 프로세서로 전달하는 방법. 방법 3에서 사용자의 입력 데이터는 터치 IC에 의해 암호화되어 있기 때문에 메인 프로세서는 사용자의 입력 데이터가 무엇인지 알 수 없다.

[0026] 상기 방법 1 내지 방법 3은 도 2 내지 도 3을 통해 더욱 구체적으로 설명될 것이다. 상기 방법 1 내지 방법 3은 전자기기의 메인 프로세서가(30) 사용자의 입력 데이터가 무엇인지를 알지 못하도록 하는 예시들일 뿐이다. 따라서, 전자기기의 메인 프로세서가(30) 사용자의 입력 데이터가 무엇인지를 알지 못하도록 하는 다양한 구현 예들이 가능하다.

[0027] 다시 도 1을 참조하면, 110단계 또는 111단계에서 터치 IC(20)는 보안 모드의 진입을 요청하는 보안 모드 진입 요청 신호를 수신할 수 있다. 이때, 보안 모드의 진입은, 보안이 필요한 어플리케이션이 실행되는 경우 필요할 수 있다. 보안이 필요한 어플리케이션은, 예를 들어 금융에 관련된 어플리케이션이 있다. 물론, 보안 모드의 진입은 전자 기기가 외부의 서버에 접속하여 로그인 하는 경우, 또는 앱 스토어에서 어플리케이션을 구매하는 경우와 같이, 패스 워드의 입력이 필요한 경우에도 필요할 수 있다. 도 1의 110 단계는 보안 모드 진입 요청 신호가 전자기기이 메인 프로세서(30)를 통해 수신되는 경우이고, 111 단계는 보안 모드 진입 요청 신호가 전자기기이 메인 프로세서(30)를 통하지 않고 터치 IC(20)로 직접 수신되는 경우를 나타낸다.

[0028] 도 1의 110 단계 또는 111단계에서 보안 모드 진입 요청 신호는, "터치 패널(10)을 통해 사용자의 특정 숫자의 입력, 특정 패턴의 입력"이 감지되거나, "센서를 통해 사용자의 특정 모션, 전자 기기의 특정 움직임"이 감지되거나, "터치 패널(10) 이외의 기타 입력 장치를 통한 특정 숫자의 입력, 특정 입력 패턴" 등에 의해서도 발생될 수 있다. 또한, 사용자는 입력 인터페이스에서 특정 숫자 또는 버튼을 터치함으로써, 보안 모드가 실행되도록 전자 기기를 조작할 수 도 있다.

[0029] 도 1의 111단계에서 보안 모드 진입 요청 신호는, 인증 서버로부터 네트워크를 통해 수신될 수 도 있다. 이때, 인증 서버는 객체를 암호화하여 보내 줄 것을 요청하는 서버를 의미한다. 예를 들어, 금융사의 서버는 인증 서버일 수 있다. 또한, 인증 서버는 사용자를 인증하기 위한 별도의 서버일 수도 있다. 보안 모드 진입 요청 신호가 인증 서버로부터 수신되는 경우, 서버로부터 수신되는 보안 모드 진입 요청 신호는 메인 프로세서(30)의 개입 없이, 통신 모듈로부터 터치 IC(20)로 직접 전달되도록 구현될 수 있다.

[0030] 110단계 또는 111단계에서 메인 프로세서(30)는 보안 키, 터치 패널에서 입력 인터페이스가 차지하는 영역에 대한 정보, 또는 변환 기반 데이터를 터치 IC(20)로 전송할 수 도 있다. 이때, 보안 키는 터치 IC(20)에서 사용자의 입력 데이터를 암호화하는데 필요한 키 값을 의미한다. 본 명세서에서 "보안 키"라는 용어는 터치 IC에서 사용자의 입력 데이터를 암호화하는데 사용되는 키 값을 의미한다. 이때, 보안 키는 대칭 키일 수도 있고, 비대칭키 일 수도 있다. 이와 같이, 보안 키는 메인 프로세서(30)로부터 터치 IC(20)에 전달될 수 도 있지만, 터치 IC(20)에 내장되어 있을 수도 있다. 터치 IC(20)에 내장된 보안 키는 외부에서 접근하지 못하는 보안 메모리 영역에 저장되고, 터치 IC(20)의 제작 시에 할당된 키 값일 수 있다. 또한, 보안 키는 예를 들어, 도 8에 도시된 방법에 따라 인증 서버로부터 수신될 수도 있다. 한편, 터치 IC(20)의 보안 메모리 영역은 터치 패널(10)에서 입력 인터페이스가 차지하는 영역에 대한 정보, 또는 변환 기반 데이터를 저장하고 있을 수 있다. 이때, 보안 메모리 영역은 특정 키를 통해서만 접근 가능한 메모리 영역으로 구현될 수도 있다.

[0031] 터치 IC(20)는 보안 모드 진입 요청 신호를 수신하면, 120 단계에서 보안 모드로 진입한다. 보안 모드는, 사용자가 입력하는 데이터를 암호화하는 모드로 정의할 수 있다. 보안 모드에서 터치 IC(20)는 암호화 알고리즘을 수행하는 암호화부를 활성화시킨다.

[0032] 보안 모드에서 터치 이벤트(130)가 발생되면, 123 단계에서 터치 IC(20)는 암호화 프로시저(123)를 수행한다. 이때, 암호화 프로시저(123)는, 사용자의 입력 데이터를 암호화하는 일련의 절차들을 의미한다. 예를 들어, 암호화 프로시저(123)는 좌표 데이터를 암호화하는 절차를 포함할 수 있다. 또한, 암호화 프로시저(123)는 N개의 좌표 데이터를 암호화하는 절차를 포함할 수 있다. 또한, 암호화 프로시저(123)는 터치 IC(20)가 사용자 입력 값을 암호화하는 절차를 포함할 수 있다. 한편, 터치 IC(20)는 보안 모드에서 주기적으로 터치 감지 프로시저(121)를 수행할 수 있다. 터치 감지 프로시저(121)는, 터치 이벤트를 감지하는 일련의 절차들을 의미한다. 즉, 터치 감지 프로시저(121)는 "기 설정된 주기로 터치 패널을 스캔함으로써, 터치 이벤트의 발생을 감지하는 절차"를 포함할 수 있다.

[0033] 한편, 보안 모드에서 터치 IC(20)는 데이터의 암호화 수행을 위한 최적화를 수행할 수 있다. 즉, 보안 모드에

서 터치 IC(20)는 "상기 터치 이벤트를 감지하는 터치 감지 프로시저(121)" 및 "상기 좌표 데이터를 암호화하는 암호화 프로시저(123)" 각각에 대한 시스템 리소스 할당을 조정할 수 있다. 즉, 보안 모드에서 터치 IC는 상기 터치 감지 프로시저(121) 보다 상기 암호화 프로시저(123)에 더 많은 시스템 리소스를 할당할 수 있다. 예를 들어, 터치 IC는 터치 패널을 스캔하는 주기를 늘려서, 터치 감지 프로시저(121)에 할당된 시스템 리소스를 줄일 수 있다. 또한, 터치 IC는 보안 모드에서 사용자의 입력이 완료된 후에 암호화를 수행하기 때문에, 사용자의 입력이 완료된 시점, 즉 터치 이벤트의 좌표 데이터가 획득된 후에 암호화 프로시저에 더 많은 시스템 리소스를 할당할 수 있다.

[0034] 보안 모드에서 사용자의 데이터 입력이 완료되거나, 보안 모드를 종료할 필요가 있는 경우, 140단계 또는 141단계에서 터치 IC(20)는 보안 모드 종료 요청 신호를 수신한다. 보안 모드 종료 요청 신호는 보안 모드의 종료를 요청하는 신호이다. 이때, 사용자의 데이터 입력이 완료되었는지 여부는, 다양한 방식으로 인지될 수 있다. 예를 들어, 패스 워드를 입력하는 경우 기 설정된 자릿수가 입력되거나, 완료 키가 터치되거나, "Log-in 키"가 터치되거나, 일정 시간 동안 터치 이벤트가 발생되지 않는 경우 사용자의 데이터 입력이 완료된 것으로 결정될 수 있다. 또한, 보안 모드 종료 신호는 "보안 모드 진입 요청 신호"와 마찬가지로, "터치 패널(10)을 통해 사용자의 특정 숫자의 입력, 특정 패턴의 입력"이 감지되거나, "센서를 통해 사용자의 특정 모션, 전자 기기의 특정 움직임"이 감지되거나, "터치 패널(10) 이외의 기타 입력 장치를 통한 특정 숫자의 입력, 특정 입력 패턴" 등에 의해서도 발생될 수 있다. 또한, 보안 모드 종료 신호는 "보안 모드 진입 요청 신호"와 마찬가지로, 인증 서버로부터 수신될 수도 있다.

[0035] 한편, 터치 IC(20)는 143단계에서 보안 모드의 종료를 자체적으로 판단할 수도 있다. 즉, 터치 IC(20)는 보안 모드에서 사용자의 데이터 입력이 완료된 것으로 판단되면, 보안 모드를 종료할 수 있다. 터치 IC(20)는 보안 모드가 종료되거나, 보안 모드 종료 요청 신호를 수신하면, 암호화부를 비활성화 시킬 수 있다.

[0036] 사용자의 데이터 입력이 완료되거나, 보안 모드가 종료되면, 터치 IC는 암호화된 데이터를 제외한 모든 데이터를 삭제할 수 있다.

[0037] 보안 키로 암호화된 데이터는 보안 키에 대응하는 복호화 키를 가진 서버에서 복호화(decryption)될 수 있다. 이때, 보안 키에 대응하는 복호화 키는 사용자의 입력 데이터를 암호화하는 데 사용된 보안 키와 동일하거나, 사용자의 입력 데이터를 암호화하는 데 사용된 보안 키와 페어(pair) 관계에 있는 암호화 키를 의미한다.

[0038] 도 2는 일 실시 예에 따른 전자 기기의 구성을 나타내는 도면이다.

[0039] 도 2를 참조하면, 전자 기기(200)는 터치 패널(210), 터치 IC(220) 및 시스템(230)을 포함한다. 도 1에 도시된 예에서, 터치 패널(210) 및 터치 IC(Integrated Circuit)(220)는 일 실시 예에 따른 전자 기기의 사용자 입력 데이터의 보안 장치에 해당된다. 전자 기기(200)는 센서(241), 기타 입/출력 장치(243) 및 외부 포트(245)를 더 포함할 수 있다.

[0040] 터치 패널(210)은 사용자의 데이터 입력을 위한 입력 인터페이스를 제공한다. 즉, 터치 패널(210)은 사용자가 터치에 의하여 숫자, 문자, 기호 등을 입력할 수 있는 자판배열을 디스플레이 할 수 있다. 이때, 터치 패널(210)에 디스플레이 되는 자판 배열은 입력 인터페이스의 예시 일 뿐 입력 인터페이스는 다양한 형태로 제공될 수 있다. 본 명세서에서 터치 패널(210)은 터치 스크린을 포함하는 개념으로 이해되어야 한다. 따라서, 터치 패널(210)은 터치 감지 영역 및 디스플레이 영역을 포함할 수 있다.

[0041] 터치 IC(220)는 터치 패널(210)과 연결되고, 터치 패널(210)로부터 수신되는 전기적인 신호를 감지할 수 있다. 터치 IC(220)는 보안 모드에서 터치 패널(210)을 통해 입력되는 데이터를 암호화한다. 특히, 터치 IC(220)는 보안 모드에서만 암호화를 수행하고, 보안 모드가 아닌 경우에는 암호화를 수행하지 않을 수 있다. 터치 IC(220)에 다양한 방식의 암호화 알고리즘을 수행하는 프로그램이 내장되어 있을 수 있다. 터치 IC(220)는 터치 패널(210)로부터 수신되는 전기적인 신호를 기 설정된 의미를 갖는 데이터로 변환하고, 변환된 데이터를 암호화할 수 있다. 이때, 터치 IC(220)는 암호화 키를 이용하여 데이터를 암호화 할 수 있다. 일 측면에 있어서, 터치 IC(220)는 터치 이벤트가 발생된 위치에 대한 좌표 데이터를 암호화 할 수 있다. 또한, 터치 IC(220)는 좌표 데이터를 숫자 또는 문자로 변환하고, 숫자 또는 문자를 암호화할 수 있다. 이와 같이, 보안 모드에서 터치 IC(220)는 사용자의 입력을 수신하는 과정에서 암호화를 수행할 수 있다. 보안 모드에서 터치 IC(220)에 의해 수행되는 암호화는 시스템(230)의 개입 없이 독립적으로 수행될 수 있다.

[0042] 터치 IC(220)는 "상기 방법 1"에 따라, 보안 모드에서 발생되는 터치 이벤트가 상기 전자기기의 메인 프로세서

에 의해 감지되지 않도록 상기 터치 이벤트의 전달 경로(201)를 차단할 수 있다. 이와 같이, "상기 방법 1"에 따르면, 전자 기기의 메인 프로세서(231)가 터치 이벤트가 발생되는 것 자체를 감지하지 못하도록 구현할 수 있다. 상기 방법 1에 따르면, 보안 모드에서 시스템(230)은 터치 이벤트의 발생 자체를 감지할 수 없다.

[0043] 또한, 터치 IC(220)는 "상기 방법 2"에 따라, 상기 보안 모드에서 발생되는 터치 이벤트의 발생 여부를 시스템(230) 또는 메인 프로세서(231)로 전달하되, 상기 좌표 데이터, 또는 상기 사용자 입력 값이 상기 전자기기의 메인 프로세서에 의해 감지되지 않도록 상기 좌표 데이터, 또는 상기 사용자 입력 값의 전달 경로(201)를 차단할 수 있다.

[0044] 또한, 터치 IC(220)는 "상기 방법 3"에 따라, 보안 모드에서 발생되는 터치 이벤트의 발생 여부를 시스템(230) 또는 메인 프로세서(231)로 전달하고, 암호화된 좌표 데이터, 또는 암호화된 사용자 입력 값을 시스템(230) 또는 메인 프로세서(231)로 전달할 수 있다.

[0045] "상기 방법 2" 또는 "상기 방법 3"에서, 터치 이벤트의 발생 여부는 사용자의 입력 데이터와 상관 없는 일종의 피드백 신호의 형태로 시스템(230) 또는 메인 프로세서(231)에 전달될 수 있다. 피드백 신호에 대해서는 도 3을 통해 더욱 상세히 설명하기로 한다. 상기 방법 2 또는 상기 방법 3에 따르면, 보안 모드에서 시스템(230)은 터치 이벤트가 발생되었다는 것은 알 수 있지만, 암호화된 데이터를 수신하기 때문에사용자의 입력 값이 무엇인지 알 수 없다.

[0046] 터치 IC(220)는 터치 패널(210)로부터 수신되는 전기적인 신호를 감지함으로써, 입력 인터페이스를 통해 터치 이벤트가 발생되었음을 알 수 있다. 이때, 터치 이벤트는 사용자의 손가락에 의해 발생될 수 있다. 또한, 터치 이벤트는 스타일러스와 같은 도구를 통해 발생될 수 도 있다. 터치 이벤트의 종류는, 예를 들어, 제스춰, 드래그, 탭(tap), 멀티-탭(multi-tap), 플릭(flick) 등이 있을 수 있다. 터치 IC(220)는 입력 인터페이스를 통해 터치 이벤트가 발생하면, "상기 터치 이벤트의 발생 위치에 대한 좌표 데이터" 또는 "상기 좌표 데이터를 사용자의 입력 데이터에 대응하는 값으로 변환한 사용자 입력 값"을 보안 키를 이용하여 암호화한다.

[0047] 시스템(230)은 메인 프로세서(231), 메모리(232), 주변 장치 인터페이스(233), 디스플레이 컨트롤러(234), 센서 컨트롤러(235), 기타 입/출력 컨트롤러(236), 통신 모듈(237) 및 오디오 회로(238)를 포함할 수 있다. 한편, 본 명세서에서 "시스템(230)" 또는 "시스템"이라는 용어는, 전자 기기(200)에 포함된 컴포넌트들 중, 터치 패널(210) 및 터치 IC(220)를 제외한 컴포넌트들을 가리키는 것으로 사용될 수 도 있다. 시스템(230)에 포함되는 컴포넌트들 각각은 하나 이상의 통신 버스 또는 신호선을 통해 통신할 수 있다. 전자 기기(200)에 포함되는 컴포넌트들 각각은, 하드웨어, 소프트웨어, 또는 하드웨어 및 소프트웨어 양자의 조합으로 구현될 수 있다.

[0048] 메인 프로세서(231)는 터치 IC(220)의 동작 모드를 변경하기 위한 시그널링을 수행할 수 있다. 즉, 메인 프로세서(231)는 도 1의 110 단계에서 설명된, 보안 모드의 진입을 요청하는 보안 모드 진입 요청 신호를 상기 터치 IC(220)로 전송할 수 있다. 또한, 메인 프로세서(231)는 입력 인터페이스를 통해 제공되는 숫자 키들, 문자 자판의 키들, 또는 기호 키들 각각에 할당된 좌표 정보"를 포함하는 변환 기반 데이터를 터치 IC(220)로 제공할 수 있다. 변환 기반 데이터에 대한 상세한 설명은 후술하기로 한다.

[0049] 한편, 메인 프로세서(231)는 복수의 프로세서들을 포함하여 구성될 수 도 있다. 즉, 메인 프로세서(231)는 복수의 기능들 각각을 수행하도록 구성된(configured) 복수의 프로세서들을 포함할 수 있다.

[0050] 메모리(232)는 예를 들어 고속 랜덤 액세스 메모리(high-speed random access memory), 자기 디스크, 에스램(SRAM), 디램(DRAM), 롬(ROM), 플래시 메모리 또는 비휘발성 메모리를 포함할 수 있다. 메모리(232)는 전자 기기(200)의 동작에 필요한 소프트웨어 모듈, 명령어 집합 또는 그밖에 다양한 데이터를 저장할 수 있다.

[0051] 주변 장치 인터페이스(233)는 전자 기기(200)의 입력 및/또는 출력 주변장치를 메인 프로세서(231) 및 메모리(232)에 결합시킬 수 있다.

[0052] 디스플레이 컨트롤러(234)는 터치 패널(210)을 제어함으로써, 사용자에 대한 시각적 출력을 디스플레이 할 수 있다. 예를 들어, 디스플레이 컨트롤러(234)는 터치 IC(220)로부터 피드백 신호를 수신하고, 기 설정된 기호를 디스플레이 할 수 있다. 피드백 신호에 대한 상세한 설명은 후술하기로 한다. 여기서, 디스플레이 컨트롤러(234)는 메인 프로세서(231)의 개입 없이, 피드백 신호를 바로 디스플레이 할 수 있다.

[0053] 센서 컨트롤러(235)는 전자 기기(200)에 구비되는 각종 센서(241)를 제어하고, 센서(241)로부터 센싱 데이터를 수신할 수 있다. 예를 들어, 센서 컨트롤러(235) 자이로 센서 또는 지자기 센서 등을 활성화 시키거나, 비활성화 시킬 수 있다. 센서(241)는 복수의 센서들을 포함할 수 있다. 예를 들어, 센서(241)는 움직임 감지 센서,

모션 감지 센서, 자이로 센서, 지자기 센서 등을 포함할 수 있다.

[0054] 기타 입/출력 컨트롤러(236)는 기타 입/출력 장치(243)로 신호를 보내거나, 기타 입/출력 장치(243)로부터 신호를 수신할 수 있다. 이때, 기타 입/출력 장치(243)의 예는 물리적인 버튼, LED, 물리적인 키보드, 진동 모터 등이 있을 수 있다.

[0055] 통신 모듈(237)은 터치 IC(220)로부터 수신되는 데이터를 서버로 전송할 수 있다. 이때, 통신 모듈(237)은 메인 프로세서(231)의 개입 없이, 터치 IC(220)로부터 수신되는 데이터를 서버로 전송할 수 있다. 또한, 통신 모듈(237)은 터치 이벤트가 발생할 때 마다, 터치 IC(220)에 의해 암호화된 좌표 데이터 또는 터치 IC(220)에 의해 암호화된 사용자 입력 값을 서버로 전송할 수 있다. 이때, "사용자 입력 값"에 대한 구체적인 설명은 도 6을 통해 상세히 설명하기로 한다.

[0056] 통신 모듈(237)은 도 8에 도시된 바와 같이, 고유 키(unique key) 저장부(801), 파싱부(803) 및 암호화부(805)를 포함할 수 있다. 즉, 통신 모듈(237)은 IC로 구현될 수 있다. 고유 키(unique key) 저장부(801), 파싱부(803) 및 암호화부(805)에 대한 설명은 도 8을 통해 설명하기로 한다.

[0057] 한편, 통신 모듈(237)은 전기 신호를 전자기 신호로 변환하거나 전자기 신호로부터 전기 신호를 변환하고, 전자기 신호를 통해 통신 네트워크 및 다른 통신 장치와 통신하기 위한 RF(Radio Frequency) 회로를 포함할 수 있다. 또한, 통신 모듈(237)은 GSM(Global System for Mobile Communications), EDGE(Enhanced Data GSM Environment), W-CDMA(wideband code division multiple access), CDMA(code division multiple access), TDMA(time division multiple access), 블루투스(Bluetooth), (IEEE 802.11a, IEEE 802.11b, IEEE 802.11g 및/또는 IEEE 802.11n 등의) Wi-Fi(Wireless Fidelity), VoIP(voice over Internet Protocol), Wi-MAX, LTE(Long Term Evolution), RFID, NFC(Near Field Communication) 등의 통신을 수행하기 위한 적어도 하나의 회로 소자를 포함할 수 있다.

[0058] 오디오 회로(238)는 스피커 및/또는 마이크로폰을 이용하여 사용자와 장치(200) 사이의 오디오 인터페이스를 제공할 수 있다.

[0059] 외부 포트(245)는 외부 장치와 연결되는 인터페이스일 수 있다. 예를 들어, 외부 포트(245)는 USB 포트, 외부 모니터 연결 포트 등을 포함할 수 있다.

[0060] 도 3은 일 실시 예에 따른 터치 IC의 구성을 나타내는 도면이다.

[0061] 도 3을 참조하면, 터치 IC(300)는 좌표 데이터 획득부(310) 및 암호화부(320)를 포함한다. 또한, 터치 IC(300)는 모드 제어부(330), 고유 키 저장부(340), 송수신부(350), 좌표 데이터 저장부(370), 피드백부(380)를 더 포함할 수 있다.

[0062] 좌표 데이터 획득부(310)는 입력 인터페이스를 통해 터치 이벤트가 발생하면, 상기 터치 이벤트의 발생 위치에 대한 좌표 데이터를 획득한다. 이때, 좌표 데이터는 터치 패널 상의 특정 위치를 나타내는 X축 좌표 및 Y축 좌표 일 수 있다.

[0063] 암호화부(320)는 터치 이벤트의 발생할 시 마다, 보안 키를 이용하여 상기 터치 이벤트의 발생 위치에 대한 좌표 데이터를 암호화한다. 또한, 암호화부(320)는 터치 이벤트가 발생할 때 마다, 보안키를 이용하여 상기 사용자 입력 값을 암호화할 수 있다. 또한, 암호화부(320)는 사용자의 데이터 입력이 완료 되었음을 인지하면, 보안 키를 이용하여 상기 좌표 데이터 저장부(370)에 저장되어 있는 "N개의 좌표 데이터"를 암호화할 수 있다. 또한, 암호화부(320)는 사용자의 데이터 입력이 완료 되었음을 인지하면, 저장부(390)에 저장되어 있는 "N번의 터치 이벤트 각각에 대한 N개의 사용자 입력 값"을 암호화할 수 있다. 이때, 암호화부(320)는 "N개의 좌표 데이터" 또는 "N개의 사용자 입력 값"을 하나의 암호화 대상으로 취급하여 한번에 암호화하거나, "N개의 좌표 데이터들" 또는 "N개의 사용자 입력 값들" 각각을 암호화 대상으로 취급하여 N번의 암호화를 수행할 수 도 있다. 예를 들어, N이 4이고, 보안 키가 "PKey"이고, 사용자 입력 값이 "1, 2, 3, 4"인 경우, 암호화부(320)는 "(1, 2, 3, 4)**PKey"로 암호화 하거나, "1** PKey", "2** PKey", "3** PKey", "4** PKey"로 암호화할 수 도 있다. 이때, "**"는 암호화 연산자를 의미한다. 한편, 암호화부(320)는 보안 키를 이용한 암호화 방식 이외에, 데이터를 암호화할 수 있는 다양한 암호화 알고리즘을 이용하여 좌표 데이터를 암호화 할 수 있다.

[0064] 모드 제어부(330)는 보안 모드의 진입을 요청하는 보안 모드 진입 요청 신호를 수신하면 상기 암호화부(320)를 활성화시키고, 상기 보안 모드의 종료를 요청하는 보안 모드 종료 요청 신호를 수신하면 상기 암호화부(320)를

비활성화 시킬 수 있다.

[0065] 모드 제어부(330)는 "상기 방법 1"에 따라, 보안 모드에서 발생되는 터치 이벤트가 상기 전자기기의 메인 프로세서에 의해 감지되지 않도록 터치 IC(300)를 제어할 수 있다. 또한, 모드 제어부(330)는 "상기 방법 2"에 따라, 상기 보안 모드에서 발생되는 터치 이벤트의 발생 여부를 시스템(230) 또는 메인 프로세서(231)로 전달하되, 상기 좌표 데이터, 또는 상기 사용자 입력 값이 상기 전자기기의 메인 프로세서에 의해 감지되지 않도록 터치 IC(300)를 제어할 수 있다. 또한, 모드 제어부(330)는 "상기 방법 3"에 따라, 보안 모드에서 발생되는 터치 이벤트의 발생 여부를 시스템(230) 또는 메인 프로세서(231)로 전달하고, 암호화된 좌표 데이터, 또는 암호화된 사용자 입력 값을 시스템(230) 또는 메인 프로세서(231)로 전달하도록 터치 IC(300)를 제어할 수 있다.

[0066] 모드 제어부(330)는 상기 보안 모드에서 "상기 터치 이벤트를 감지하는 터치 감지 프로시저" 및 "상기 좌표 데이터를 암호화하는 암호화 프로시저" 각각에 대한 시스템 리소스 할당을 조정할 수 있다. 이때, 모드 제어부(330)는 상기 보안 모드에서 상기 터치 감지 프로시저 보다 상기 암호화 프로시저에 더 많은 시스템 리소스를 할당할 수 있다.

[0067] 모드 제어부(330)는 보안 모드의 종료를 요청하는 보안 모드 종료 요청 신호를 수신하면, 좌표 데이터 저장부(370)에 저장된 "N개의 좌표 데이터"를 삭제한다.

[0068] 고유 키 저장부(340)는 터치 IC(300) 및 상기 전자기기의 통신 모듈(237)에 할당된 고유의 키(unique key)를 저장한다.

[0069] 피드백부(380)는 터치 이벤트 각각에 대하여 터치가 감지 되었음을 나타내는 피드백 신호"를 생성하고, 상기 피드백 신호를 실행중인 어플리케이션 또는 디스플레이 제어부에 제공한다. 이때, 피드백 신호는 랜덤한 값 또는 기 설정된 고유의 값일 수 있다. 즉, 피드백 신호는 실제 좌표 데이터가 아닌, 미리 설정된 영역의 X, Y 좌표일 수 있다. 시스템은 피드백 신호를 수신하면, 진동, LED 점등, 또는 특정 기호의 디스플레이를 통해, 사용자에게 터치가 감지 되었음을 알려 줄 수 있다. 이때, 피드백 신호는 랜덤한 값 또는 기 설정된 고유의 값일 수 있다. 즉, 피드백 신호는 사용자 입력값과는 무관하게 기 설정된 신호 등을 사용함으로써 피드백 신호를 통해서는 사용자 입력데이터를 알 수 없다.

[0070] 이하, 도 4 내지 도 8을 통해 터치 IC(300)의 구성 요소들을 상세히 설명하기로 한다.

[0071] 도 4는 일 실시 예에 따른 전자 기기의 사용자 입력 데이터의 보안 방법을 나타내는 도면이다.

[0072] 도 4를 참조하면, 410단계에서 N번째 터치 이벤트가 발생하면, 좌표 데이터 획득부(310)는 420단계에서, 터치 이벤트의 발생 위치에 대한 좌표 데이터를 획득한다. 물론, 도 4의 N번째 터치이벤트는 보안 모드 진입 후에 발생되는 터치 이벤트들을 의미한다. 즉, N번째 터치 이벤트가 입력되면, 보안 모드 진입 후 N개의 터치 이벤트가 발생된 것이다. 이때, 좌표 데이터는 터치 패널의 X축 좌표 및 Y축 좌표 일 수 있다. 즉, 좌표 데이터 획득부(310)는 터치 감지 센서의 정전 용량 변화 또는 전류량 변화 등을 이용하여 좌표 데이터를 계산할 수 있다. 한편, 좌표 데이터 획득부(310)는 터치 감지 센서의 전기적인 저항의 변화 등을 이용하여 좌표 데이터를 계산할 수 있다. 즉, 터치 감지 센서는 정전식 또는 감압식 등 다양한 방식으로 구현될 수 있다.

[0073] 430단계에서 좌표 데이터 저장부(370)는 "N(N은 1 이상의 정수)번의 터치 이벤트 각각의 발생 위치에 대한 N개의 좌표 데이터"를 저장한다. "N개의 좌표 데이터"를 저장하는 이유는, 사용자의 데이터 입력이 완료된 후 전체 사용자의 입력 데이터를 암호화하기 위한 것이다.

[0074] 440단계에서 피드백부(380)는 터치 이벤트 각각에 대하여 터치가 감지 되었음을 나타내는 피드백 신호"를 생성하고, 상기 피드백 신호를 실행중인 어플리케이션 또는 디스플레이 제어부에 제공할 수 있다.

[0075] 450 단계에서 암호화부(320)는 사용자의 데이터 입력이 완료 되었는지를 판단한다. 사용자의 데이터 입력이 완료되지 않았으면, 터치 IC(300)는 새로운 터치 이벤트 발생에 따라 420단계를 수행한다.

[0076] 사용자의 데이터 입력이 완료되면, 460단계에서 암호화부(320)는 보안 키를 이용하여 좌표 데이터 저장부(370)에 저장된 "N개의 좌표 데이터"를 암호화한다. 이때, 보안 키는 비 대칭 방식의 암호화를 위한 키 값일 수 있다. . 이때, 도 3에서 설명된 바와 같이, 암호화부(320)는 N개의 좌표 데이터를 하나의 암호화 대상으로 취급하여 한번에 암호화하거나, N개의 좌표 데이터들 각각을 암호화 대상으로 취급하여 N번의 암호화를 수행할 수

도 있다.

[0077] 470단계에서 송수신부(350) 는 암호화된 좌표 데이터를 전자 기기(200)의 통신 모듈(237)을 통해 서버로 전송할 수 있다. 이때, 송수신부(350)는 "상기 방법 1"또는 "상기 방법 2"에 따라, 전자 기기의 메인 프로세서(231)를 통하지 않고, 상기 암호화된 좌표 데이터를 직접(directly) 상기 통신 모듈(237)에 전달할 수 있다. 또한, 송수신부(350)는 상기 "상기 방법 3"에 따라, 암호화된 데이터를 전자 기기의 메인 프로세서(231)를 통해 통신 모듈(237)에 전달할 수 도 있다. 송수신부(350)는 터치 패널의 해상도, 상기 터치 패널의 크기, 상기 터치 패널에서 상기 입력 인터페이스의 위치에 대한 정보, 상기 터치 패널의 사양 정보, 또는 상기 전자기기의 사양 정보를 상기 통신 모듈을 통해 서버로 전송할 수도 있다. 전자 기기 또는 터치 패널의 사양 정보 등을 서버에 전송하는 이유는, 서버에서 암호화된 좌표 데이터를 복호화한 후, 좌표 데이터를 이용하여 사용자의 입력 값을 알 수 있도록 하기 위한 것이다. 터치 패널의 크기에 따라서 동일한 사용자 입력에 대한 좌표 데이터가 달라 질 수 있기 때문에, 송수신부(350)는 전자 기기 또는 터치 패널의 사양 정보를 서버에 전송한다. 서버는 좌표 데이터와 사용자 입력 값이 매핑되어 있는 룩업테이블을 이용하여 좌표 데이터로부터 사용자 입력 값을 알 수 있다.

[0078] 도 5a는 다른 실시 예에 따른 전자 기기의 사용자 입력 데이터의 보안 방법을 나타내는 도면이다.

[0079] 510단계에서 N번째 터치 이벤트가 발생하면, 좌표 데이터 획득부(310)는 520단계에서, 터치 이벤트의 발생 위치에 대한 좌표 데이터를 획득한다. 물론, 도 5의 N번째 터치이벤트는 보안 모드 진입 후에 발생되는 터치 이벤트들을 의미한다. 즉, N번째 터치 이벤트가 입력되면, 보안 모드 진입 후 N개의 터치 이벤트가 발생된 것이다.

[0080] 530단계에서 변환부(350)는 좌표 데이터를 사용자의 입력 데이터에 대응하는 사용자 입력 값으로 변환한다. 이때, 변환부(350)는 사용자 입력 값을 저장부(390)에 저장할 수 있다. 따라서, 터치 이벤트가 N번 발생한 경우, 저장부(390)는 "N번의 터치 이벤트 각각에 대한 N개의 사용자 입력 값"을 저장할 수 있다. 이때, 변환부(350)는 변환 기반 데이터에 기초하여 상기 좌표 데이터를 사용자의 입력 데이터에 대응하는 사용자 입력 값으로 변환한다. 상기 변환 기반 데이터는 "상기 입력 인터페이스를 통해 제공되는 숫자 키들, 문자 자판의 키들, 또는 기호 키들 각각에 할당된 좌표 정보"를 포함한다. 예를 들어, 숫자 키 "1"은 X축 좌표 0.1~1.0 및 Y축 좌표 2.5~3.0이 할당되고, 숫자 키 "2"에는 X축 좌표 1.01~2.0 및 Y축 좌표 2.5~3.0가 할당될 수 도 있다. 만일 좌표 데이터가 (0.8, 2.6)이면 사용자 입력 값은 1이고, 좌표 데이터가 (1.5, 2.6)이면 사용자 입력 값은 "2"일 수 있다. 물론, 변환부(350)는 실제 사용자 입력 값에 미리 설정된 연산을 적용한 연산된 값을 암호화부(320)로 제공할 수도 있다. 한편, 입력 인터페이스의 타입이 변경되거나, 입력 인터페이스가 계속 바뀌는 경우에는, 변환 기반 데이터는 입력 인터페이스의 타입에 따라 변경된 정보를 갖게 된다. 예를 들어, 입력 인터페이스에 디스플레이 되는 숫자의 배열이 소정 주기로 변경되는 경우에는 변환 기반 데이터 역시 변경되어야 한다. 따라서, 시스템은 변경된 변환 기반 데이터를 터치 IC에 제공할 수 있다.

[0081] 한편, 변환 기반 데이터는 상기 터치 IC에 기 저장된 것, 또는 상기 전자 기기의 통신 모듈을 통해 서버로부터 직접 수신된 것일 수 있다.

[0082] 540단계에서 피드백부(380)는 터치 이벤트 각각에 대하여 터치가 감지 되었음을 나타내는 피드백 신호"를 생성하고, 상기 피드백 신호를 실행중인 어플리케이션 또는 디스플레이 제어부에 제공할 수 있다.

[0083] 550 단계에서 암호화부(320)는 사용자의 데이터 입력이 완료 되었는지를 판단한다. 사용자의 데이터 입력이 완료되지 않았으면, 터치 IC(300)는 새로운 터치 이벤트 발생에 따라 520단계를 수행한다.

[0084] 사용자의 데이터 입력이 완료되면, 560단계에서 암호화부(320)는 저장부(390)에 저장된 "N(N은 1 이상의 정수)번의 터치 이벤트 각각에 대한 N개의 사용자 입력 값"을 암호화한다. 즉, 560 단계에서 암호화부(320)는 사용자의 데이터 입력이 완료 되었음을 인지하면, 보안키를 이용하여 상기 N개의 사용자 입력 값을 암호화한다. 이때, 도 3에서 설명된 바와 같이, 암호화부(320)는 N개의 사용자 입력 값을 하나의 암호화 대상으로 취급하여 한번에 암호화하거나, N개의 사용자 입력 값들 각각을 암호화 대상으로 취급하여 N번의 암호화를 수행할 수 도 있다.

[0085] 570단계에서, 송수신부(350)는 암호화된 데이터를 서버에 전송할 수 있다.

[0086] 한편, 도 5에 도시된 바와 달리, 520단계 내지 560단계는, 도 5b의 520b단계 내지 560b단계와 같이 수행될 수도 있다.

[0087] 즉, 도 5b를 참조하면, 510단계에서 N번째 터치 이벤트가 발생하면, 좌표 데이터 획득부(310)는 520b단계에서,

터치 이벤트의 발생 위치에 대한 좌표 데이터를 획득하고, 획득된 좌표 데이터를 좌표 데이터 저장부(370)에 저장한다. 즉, 좌표 데이터 저장부(370)는 "N(N은 1 이상의 정수)번의 터치 이벤트 각각의 발생 위치에 대한 N개의 좌표 데이터"를 저장한다.

[0088] 530b단계에서 피드백부(380)는 터치 이벤트 각각에 대하여 터치가 감지 되었음을 나타내는 피드백 신호"를 생성하고, 상기 피드백 신호를 실행중인 어플리케이션 또는 디스플레이 제어부에 제공할 수 있다.

[0089] 540b단계에서 암호화부(320) 또는 변환부(350)는 사용자의 데이터 입력이 완료 되었는지를 판단한다. 사용자의 데이터 입력이 완료되지 않았으면, 터치 IC(300)는 새로운 터치 이벤트 발생에 따라 520b단계를 수행한다.

[0090] 사용자의 데이터 입력이 완료되면, 변환부(350)는 좌표 데이터 저장부(370)에 저장된 N개의 좌표 데이터 각각을 사용자의 입력 데이터에 대응하는 N개의 사용자 입력 값으로 변환한다. 즉, 변환부(350)는 사용자의 데이터 입력이 완료 되었음을 인지하면, 550b단계에서 상기 N개의 좌표 데이터 각각을 사용자의 입력 데이터에 대응하는 N개의 사용자 입력 값으로 변환한다.

[0091] 560단계에서, 암호화부(320)는 보안키를 이용하여 상기 N개의 사용자 입력 값을 암호화한다.

[0092] 도 6은 터치 패널에 입력 인터페이스가 디스플레이 된 예를 나타낸다.

[0093] 도 6을 참조하면, 입력 인터페이스는 숫자 자판이며 터치 패널(600)의 일부 영역(620)에 디스플레이 된다. 입력 인터페이스가 디스플레이되지 않은 영역(610)은 피드백 신호에 따라서 "*" 등의 기호가 디스플레이 될 수 있다. 또한, 변환 기반 데이터는 영역(610)과 영역(620)의 좌표 데이터를 포함할 수 있다. 도 6에 도시된 예에서, 사용자가 "1"을 터치한 경우, 사용자의 입력 값은 "1"이고, 좌표 데이터는 영역(620)에서 터치가 발생된 X/Y축 좌표 값이다.

[0094] 도 7은 일 실시 예에 따라서 사용자에게 디스플레이되는 화면의 예시도이다.

[0095] 도 7에서 710은 암호화 모드에서, 터치 이벤트가 한번 발생된 예를 나타낸다. 도 7에서 720은 암호화 모드에서, 터치 이벤트가 6번 발생된 예를 나타낸다. 720에서 디스플레이 영역(721)에 6개의 "*" 표시는 일종의 피드백 신호에 해당된다. 도 7에 도시된 예에서, 터치 IC(300)는 완료 버튼(723)이 터치 되는 것이 감지하면, 사용자의 데이터 입력이 완료된 것으로 판단할 수 할 수 있다. 또한, 6개의 숫자가 입력되면 자동으로 사용자 입력이 완료된 것으로 설정된 경우, 터치 IC(300)는 완료 버튼(723)이 터치 되는 것을 감지할 필요 없이, 사용자의 데이터 입력이 완료된 것으로 결정할 수 있다.

[0096] 도 8은 일 실시 예에 따른 보안 키 획득 방법을 설명하기 위한 도면이다.

[0097] 도 8을 참조하면, 고유 키(unique key) 저장부(801)는 터치 IC(300)에 저장된 고유의 키(unique key)와 동일한 고유의 키를 저장하고 있다. 이때, 고유의 키(unique key)는 터치 IC(300) 및 상기 전자기기의 통신 모듈(237)의 양산 시에 할당된 것이다. 따라서, 고유의 키는 외부에서 접근하지 못하는 보안 메모리 영역에 저장되어 있는 키 값일 수 있다.

[0098] 한편, 시스템 또는 터치 IC는 각각 811단계 또는 813 단계에서 보안 키를 요청하는 보안 키 요청 메시지를 통신 모듈(237)에 전송할 수 있다.

[0099] 820단계에서 통신 모듈(237)은 보안 키 요청 패킷을 생성하고, 보안 키 요청 패킷을 인증 서버에 전송한다.

[0100] 830단계에서 통신 모듈(237)은 인증 서버로부터 수신되는 패킷의 캡춰를 시작한다. 여기서, "패킷의 캡춰"는 수신 패킷의 헤더 만을 디코딩하여 "상기 보안 키를 포함하는 패킷"이 수신되는 지를 확인하는 것일 수 있다. 또한, "패킷의 캡춰"는 보안 키 요청 패킷을 인증 서버에 전송한 후, 소정 시간이 지난 다음에 수행될 수 있다.

[0101] 840 단계에서 인증 서버는 새로운 보안 키를 생성하거나, 기 저장되어 있는 보안 키를 통신 모듈(237)로 전송한다.

[0102] 850단계에서 통신 모듈(237)의 파싱부(803)는 인증 서버로부터 수신되는 패킷들 중, "보안 키를 포함하는 패킷"으로부터 보안 키를 파싱하고, 파싱된 보안 키를 암호화부(805)로 전달한다.

[0103] 860단계에서 암호화부(805)는 파싱된 보안 키를 상기 고유키 저장부(801)에 저장된 고유 키를 이용하여 암호화

한다.

[0104] 873 단계에서 암호화부(805)는 "상기 고유의 키에 의해 암호화된 보안 키"를 상기 터치 IC(300)로 전달한다. 도 8에서 871단계는 "상기 고유의 키에 의해 암호화된 보안 키"를 시스템을 거쳐 터치 IC(300)로 전달되는 경우를 나타낸다.

[0105] 880 단계에서 터치 IC(300)의 암호화부(320)는 통신 모듈로부터 "상기 고유의 키에 의해 암호화된 보안 키"를 수신하고, 고유 키 저장부(340)에 저장된 고유 키를 이용하여 "상기 고유의 키에 의해 암호화된 보안 키"를 복호화(decryption)한다.

[0106] <본 발명의 변형 예들>

[0107] - 보안 모드에서 터치 IC는, 사용자의 입력 데이터를 랜덤하게 변경한 서버로 전송할 수 도 있다.

[0108] - 본 명세서에서는 터치 패널과 터치 IC를 예를 들어 설명하였으나, 본 발명의 실시 예들은 다른 입력 장치에도 적용될 수 있다. 예를 들어, 자이로 센서, 음성 입력 등을 통해 사용자로 입력 명령을 수신하고, IC를 포함하는 센서 컨트롤러는 센싱 값을 암호화할 수 있다. 즉, 센서 컨트롤로는 센싱 값 자체를 암호화하고, 암호화된 센싱 값을 메인 프로세서의 개입 없이, 외부로 전송할 수 도 있다.

[0109] 입력 인터페이스에서 멀티 터치를 입력 받는 방법이 가능하다. 예를 들어, 전자 기기는 터치 패널에 동일한 숫자를 복수로 배열하고, 사용자가 동일한 숫자를 동시에 터치하는 경우에만 사용자의 입력이 있는 것으로 결정할 수 있다. 이때, 숫자의 배열은 랜덤하게 배열 될 수 있다. 예를 들어, 하기 표 1과 같이 배열된 숫자 자판이 입력 인터페이스로 디스플레이 될 수 있다.

[0110] [표 1]

[0111]

3	6	1	7	6
8	2	4	2	8
5	5	3	9	0
9	1	4	7	0

[0112] 이때, 좌표 데이터 획득부(310)는 상기 복수의 동일한 숫자가 동시에 터치되는 경우에만 상기 터치 이벤트의 발생 위치에 대한 좌표 데이터를 획득하도록 설정될 수 있다. 예를 들어, [표 1]에서 두 개의 "6"이 동시에 터치되면, 좌표 데이터 획득부(310)는 표 1의 1행 2열의 "6"에 대한 좌표데이터 또는 표 1의 1행 5열의 "6"에 대한 좌표데이터를 획득할 수 있다. 이에 따라, 보다 정확하게 사용자의 입력 값을 획득하는 것이 가능하다.

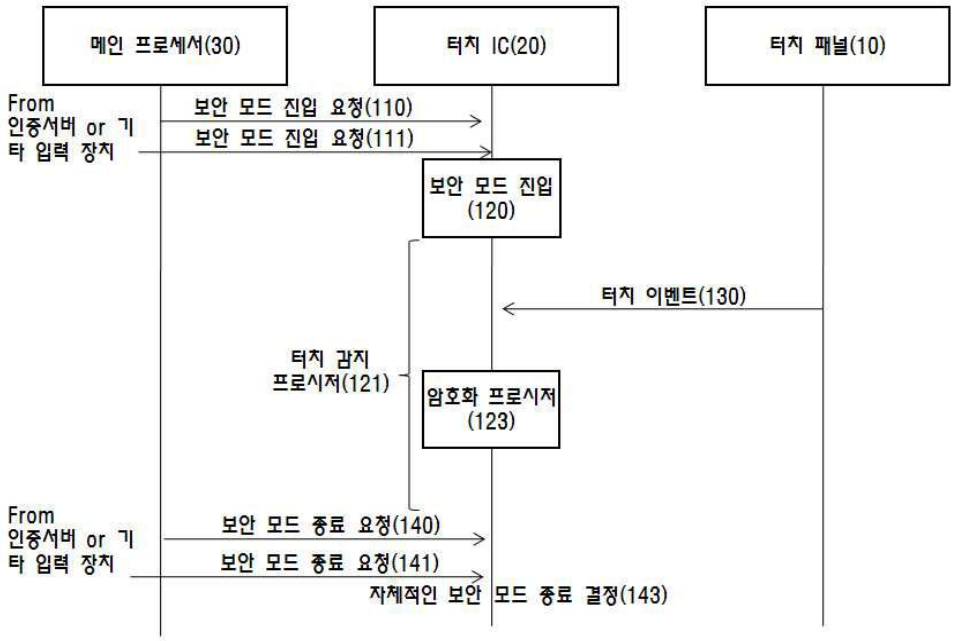
[0113] 본 발명의 실시 예에 따른 방법들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[0114] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

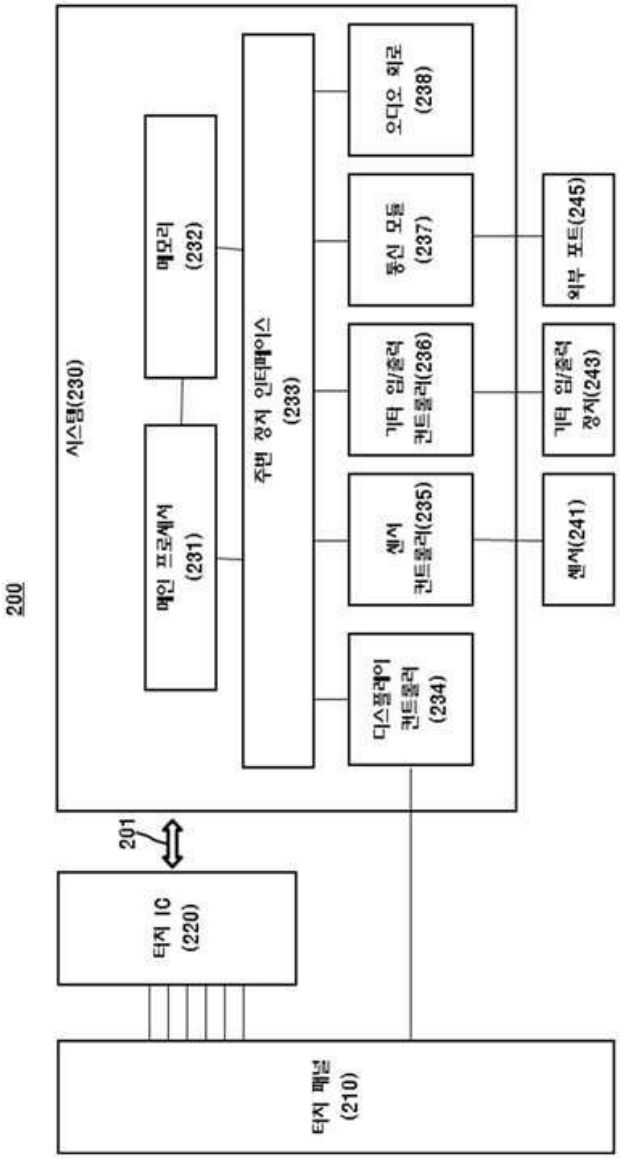
[0115] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

도면

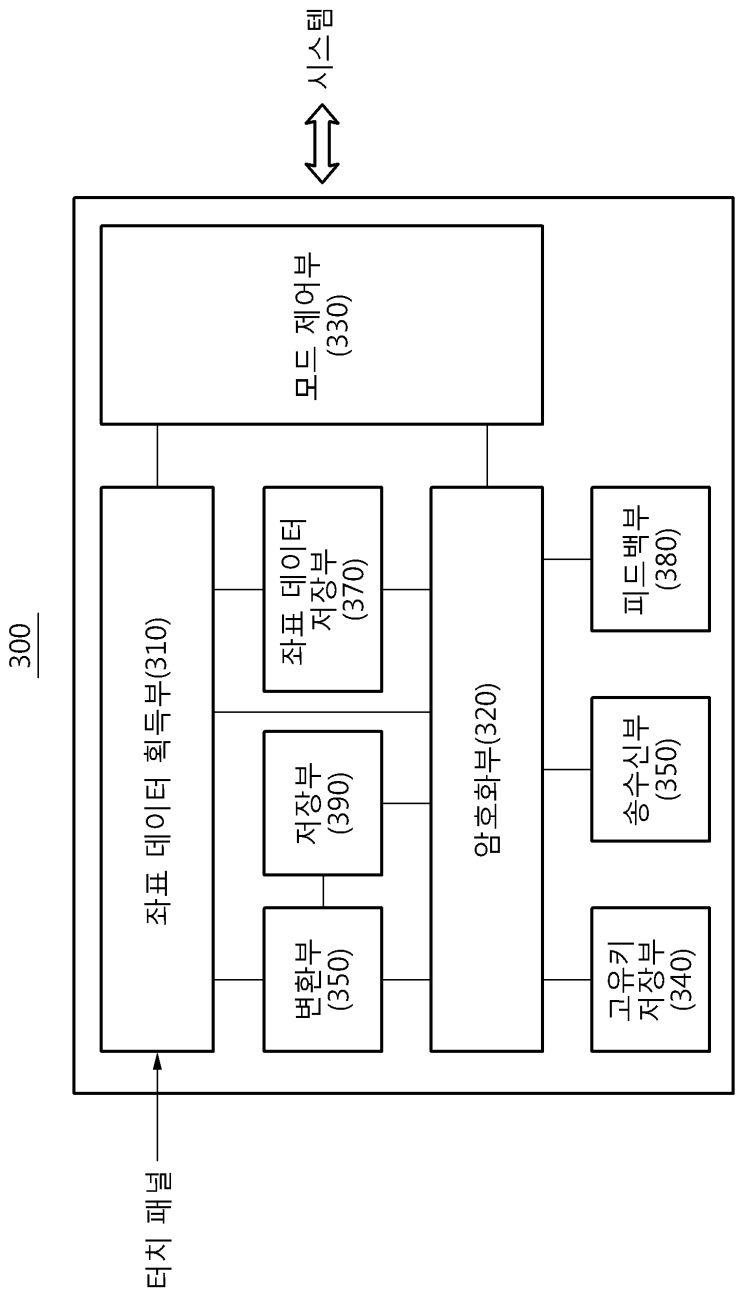
도면1


메인 프로세서(30)
터치 IC(20)
터치 패널(10)
From
인증서버 or 기타 입력 장치
보안 모드 진입 요청(110)
보안 모드 진입 요청(111)
보안 모드 진입 (120)
터치 이벤트(130)
터치 감지 프로시저(121)
암호화 프로시저 (123)
From
인증서버 or 기타 입력 장치
보안 모드 종료 요청(140)
보안 모드 종료 요청(141)
자체적인 보안 모드 종료 결정(143)

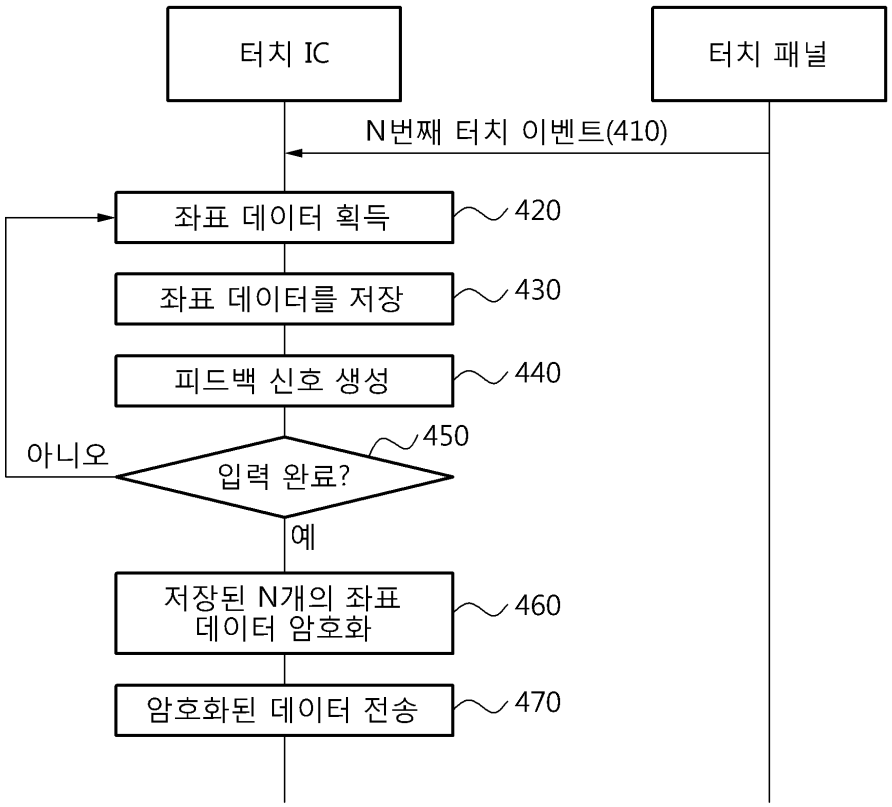
도면2


200
시스템(230)
메모리 (232)
메인 프로세서 (231)
주변 장치 인터페이스 (233)
오디오 회로 (238)
통신 모듈 (237)
기타 입/출력 컨트롤러(236)
센서 컨트롤러(235)
디스플레이 컨트롤러 (234)
외부 포트(245)
기타 입/출력 장치(243)
센서(241)
201
터치 IC (220)
터치 패널 (210)

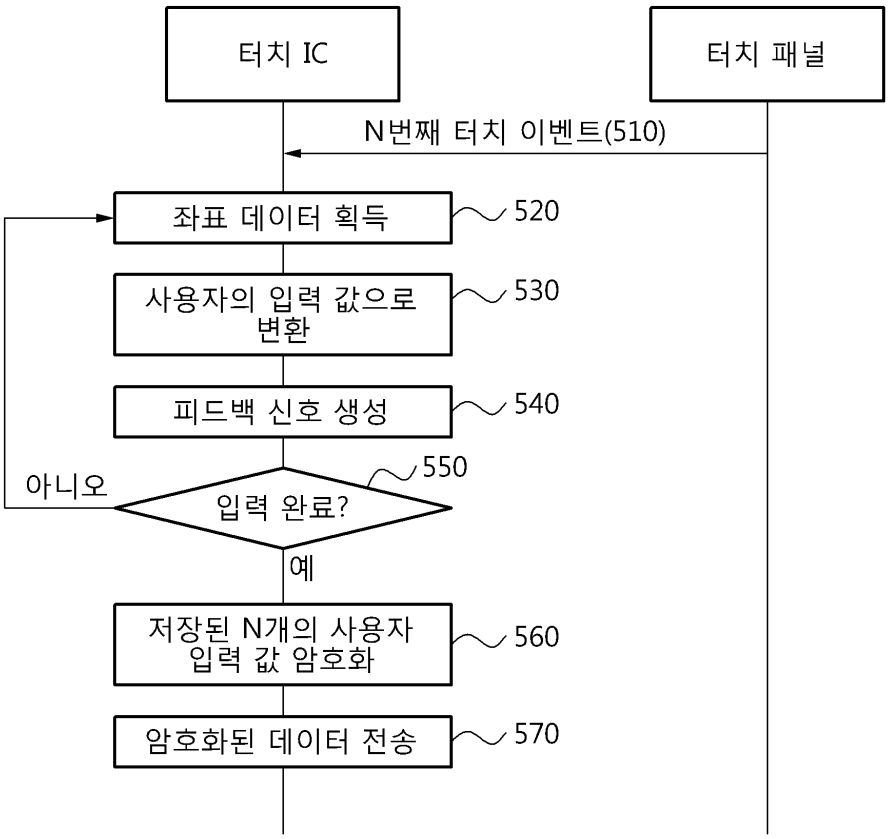
도면3


시스템
300
모드 제어부 (330)
좌표 데이터 획득부(310)
좌표 데이터 저장부 (370)
저장부 (390)
변환부 (350)
암호화부(320)
피드백부 (380)
송수신부 (350)
고유키 저장부 (340)
터치 패널

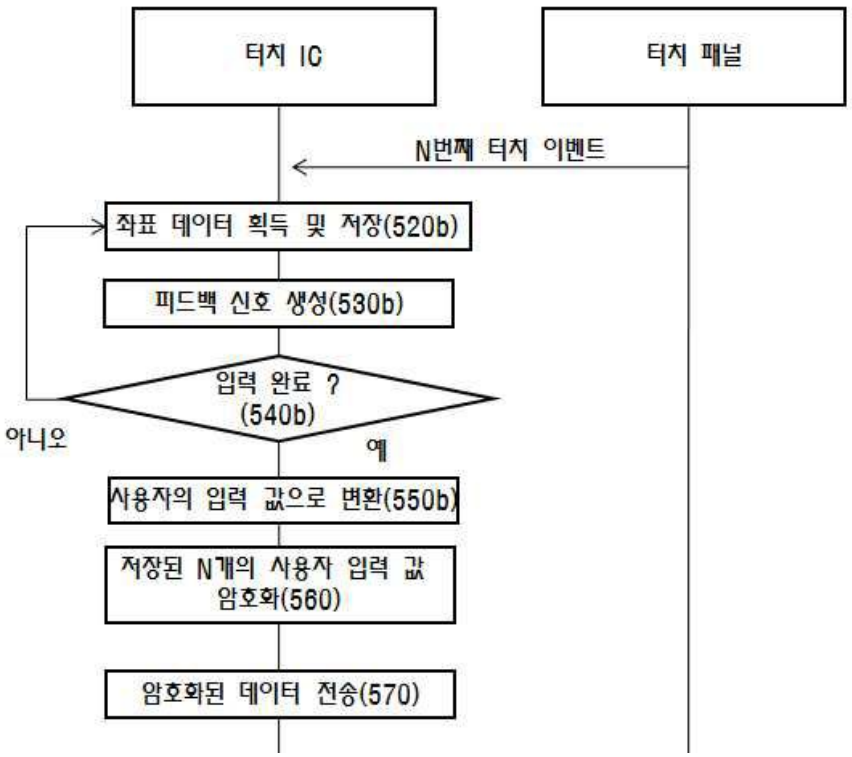
도면4


터치 IC
터치 패널
N번째 터치 이벤트(410)
좌표 데이터 획득
420
좌표 데이터를 저장
430
피드백 신호 생성
440
450
아니오
입력 완료?
예
저장된 N개의 좌표 데이터 암호화
460
암호화된 데이터 전송
470

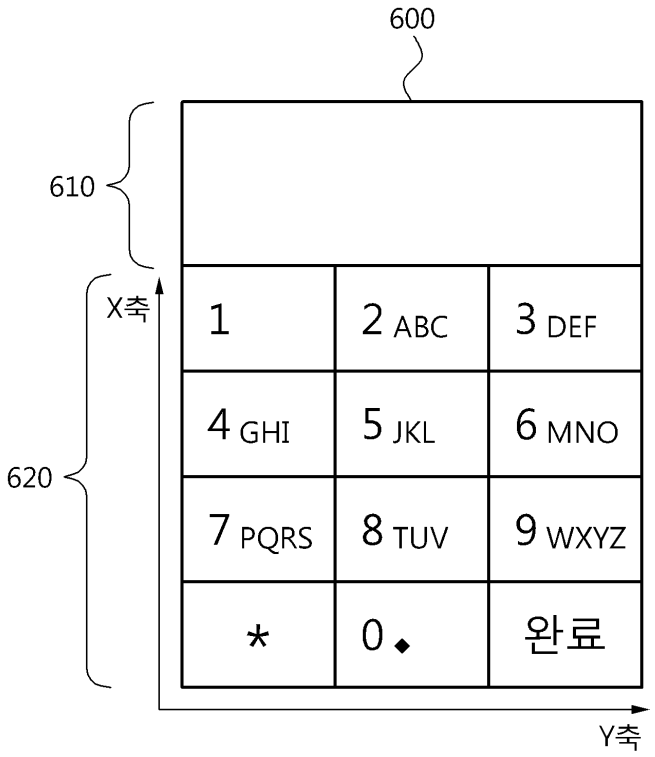
도면5a


터치 IC
터치 패널
N번째 터치 이벤트(510)
좌표 데이터 획득
520
사용자의 입력 값으로 변환
530
피드백 신호 생성
540
550
아니오
입력 완료?
예
저장된 N개의 사용자 입력 값 암호화
560
암호화된 데이터 전송
570

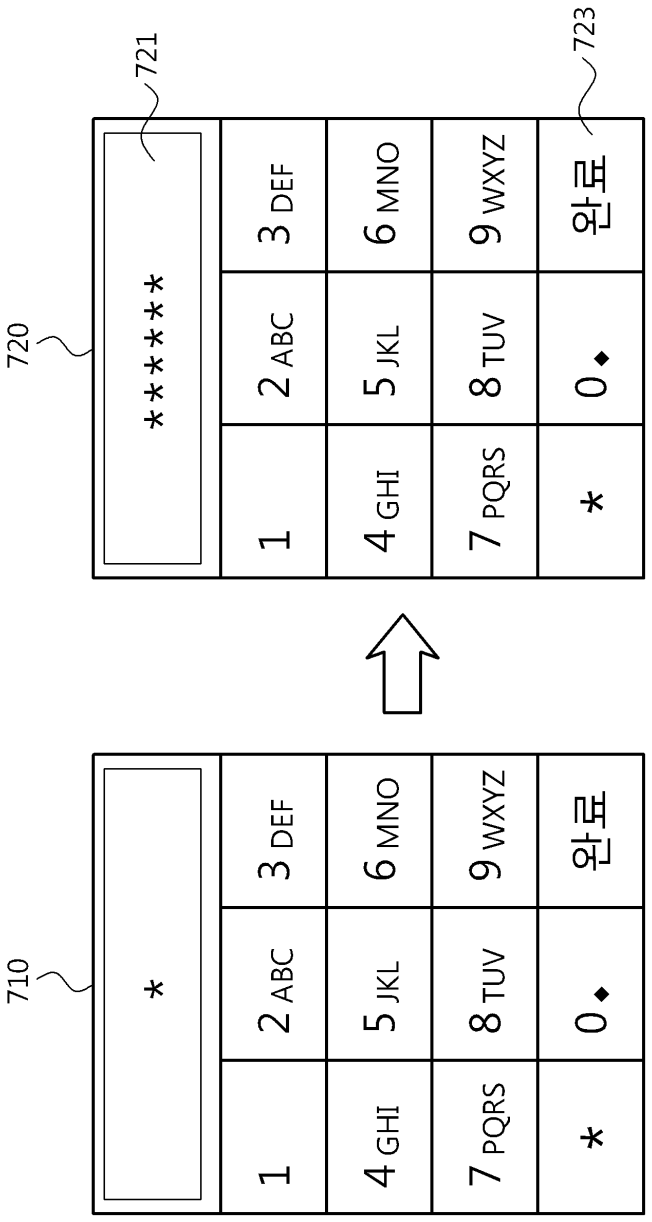
도면5b


터치 IC
터치 패널
N번째 터치 이벤트
좌표 데이터 획득 및 저장(520b)
피드백 신호 생성(530b)
입력 완료 ?
(540b)
아니오
예
사용자의 입력 값으로 변환(550b)
저장된 N개의 사용자 입력 값
암호화(560)
암호화된 데이터 전송(570)

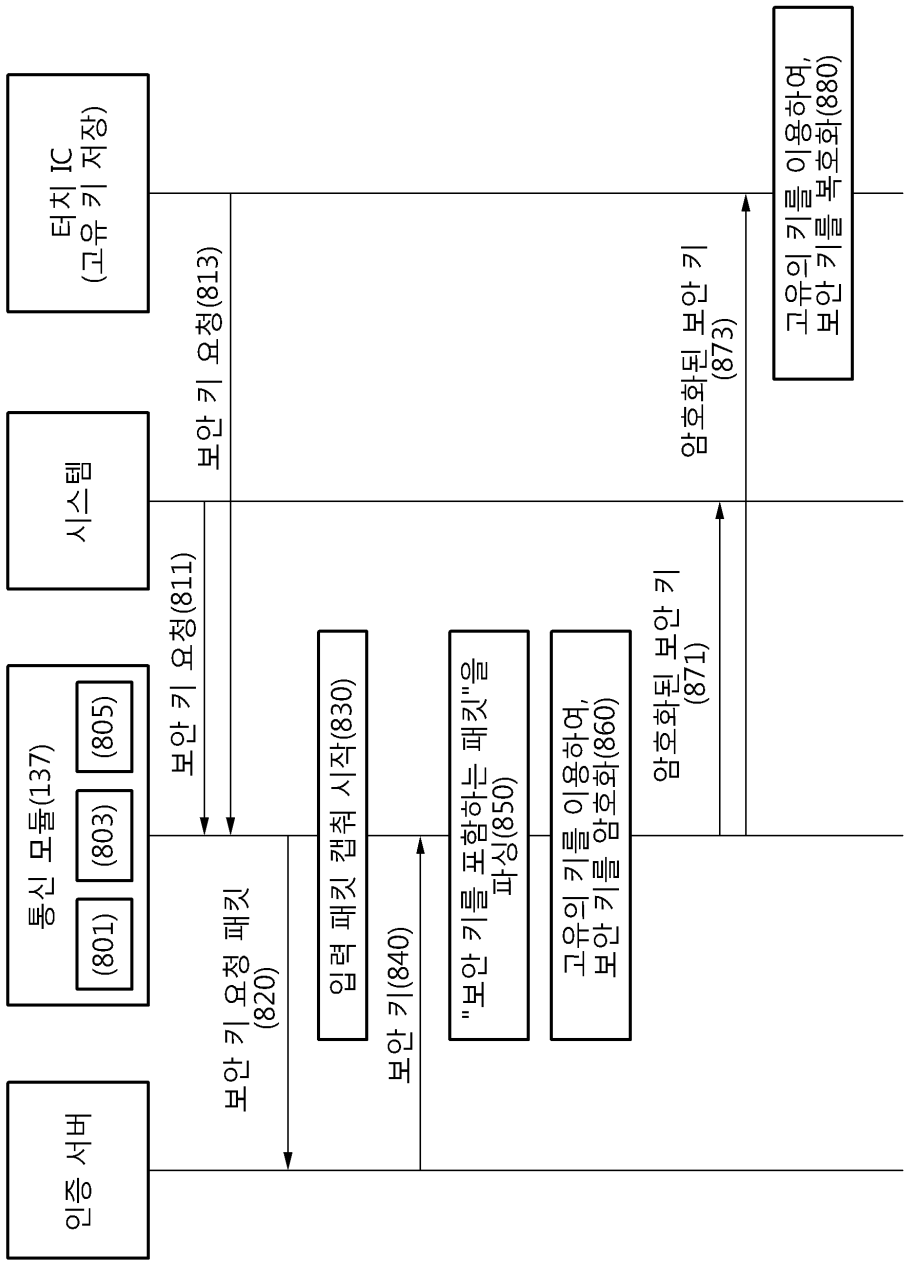
도면6


600
610
620
X축
Y축
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
*
0
완료

도면7


710
*
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
*
0
완료
720
721
****
723

도면8


터치 IC
(고유 키 저장)
시스템
통신 모듈(137)
(801)
(803)
(805)
인증 서버
보안 키 요청(811)
보안 키 요청(813)
보안 키 요청 패킷
(820)
입력 패킷 캡쳐 시작(830)
보안 키(840)
"보안 키를 포함하는 패킷"을
파싱(850)
고유의 키를 이용하여,
보안 키를 암호화(860)
암호화된 보안 키
(871)
암호화된 보안 키
(873)
고유의 키를 이용하여,
보안 키를 복호화(880)