



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년04월05일
(11) 등록번호 10-1133544
(24) 등록일자 2012년03월29일

(51) 국제특허분류(Int. Cl.)
G06F 3/023 (2006.01) H03M 11/00 (2006.01)
(21) 출원번호 10-2009-0060610
(22) 출원일자 2009년07월03일
심사청구일자 2009년07월03일
(65) 공개번호 10-2011-0003027
(43) 공개일자 2011년01월11일
(56) 선행기술조사문헌
KR1020020008962 A
KR100755934 B1
KR1020070010557 A

(73) 특허권자
한국인터넷진흥원
서울특별시 송파구 중대로 135 (가락동)
(72) 발명자
원유재
경기도 성남시 분당구 미금로 215, 809동 302호
(금곡동, 청솔마을)
정현철
서울특별시 송파구 동남로23가길 8-7, 멀티파트
B-201호 (오금동)
(뒷면에 계속)
(74) 대리인
특허법인다울

전체 청구항 수 : 총 12 항

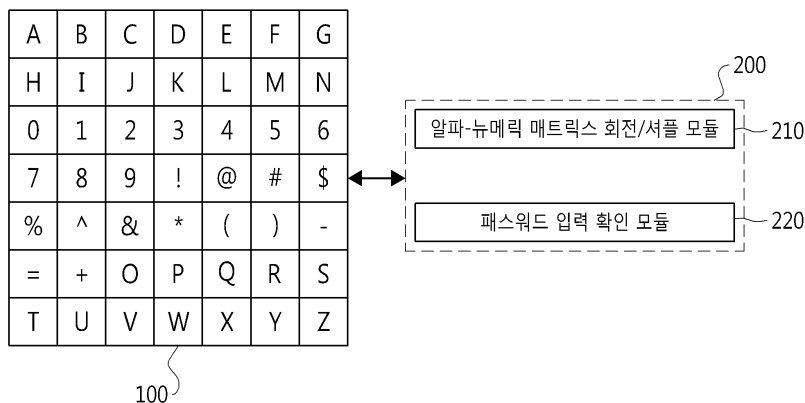
심사관 : 이정호

(54) 발명의 명칭 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템 및 방법

(57) 요약

본 발명은 패스워드 입력 알고리즘에 대한 것으로서, 특히 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템 및 그 방법에 관한 것이다. 본 발명은 알파-뉴메릭 매트릭스에서 패스워드를 구성하는 문자와 기설정된 간격 이격된 알파-뉴메릭 매트릭스 문자를 최종 패스워드로 입력하여 키로깅 공격과 숄더 서핑 공격을 방어할 수 있는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템 및 방법을 제공할 수 있다. 또한, 본 발명은 알파-뉴메릭 매트릭스에서 패스워드를 구성하는 문자와 기설정된 간격 이격된 알파-뉴메릭 매트릭스 문자를 최종 패스워드로 입력하되, 하나의 문자를 입력할 때마다 알파-뉴메릭 매트릭스를 회전시켜 키로깅 공격과 숄더 서핑 공격의 방어 확률을 더욱 증가시킬 수 있는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템 및 방법을 제공할 수 있다. 또한, 본 발명은 패스워드를 구성하는 문자를 앞의 한자리 문자가 연관되도록 두 자리씩 기억하고, 이에 대한 알파-뉴메릭 매트릭스에서의 교차점을 최종 패스워드로 입력하여 키로깅 공격과 숄더 서핑 공격을 방어할 수 있는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템 및 방법을 제공할 수 있다.

대표도 - 도1



(72) 발명자

전인경

경기도 성남시 분당구 수내동 푸른마을신성아파트
403동 701호

한병진

경기도 안산시 상록구 이화6길 10, 삼성아트빌 40
2호 (사동)

양대현

서울특별시 서초구 서초동 삼풍아파트 3동 405호

강전일

충청남도 공주시 무령로 300 (옥룡동)

맹영재

서울특별시 광진구 아차산로 295-12 (자양동)

이환진

서울특별시 송파구 중대로 109, 대동빌딩 (가락동)

특허청구의 범위

청구항 1

삭제

청구항 2

문자가 매트릭스 형태로 배열되어 n자릿수의 패스워드를 입력받는 알파-뉴메릭 매트릭스와,

상기 알파-뉴메릭 매트릭스에 입력된 패스워드를 확인하는 패스워드 입력 확인 모듈을 포함하여 이루어진 패스워드 입력 시스템으로서,

상기 패스워드 입력 확인 모듈은 상기 알파-뉴메릭 매트릭스에서 상기 패스워드를 구성하는 문자에서 두 자릿수의 패스워드 문자군의 첫 번째 문자가 위치한 행과 두 번째 문자가 위치한 열의 교차점인 상기 패스워드를 구성하는 문자(제1문자)로부터 기설정된 간격 이격된 문자(제2문자)의 입력을 통하여 상기 패스워드를 구성하는 문자(제1문자)를 확인함으로써 이루어지는 것을 특징으로 하는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템.

청구항 3

청구항 2에 있어서,

상기 두 자릿수의 패스워드 문자군은 n자리의 패스워드의 {[1자리, 2자리], [2자리, 3자리], ..., [n자리, 1자리]}의 패스워드 문자군을 포함하는 것을 특징으로 하는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템.

청구항 4

문자가 매트릭스 형태로 배열되어 n자릿수의 패스워드를 입력받는 알파-뉴메릭 매트릭스와,

상기 알파-뉴메릭 매트릭스에 입력된 패스워드를 확인하는 패스워드 입력 확인 모듈을 포함하여 이루어진 패스워드 입력 시스템으로서,

상기 패스워드 입력 확인 모듈은 상기 알파-뉴메릭 매트릭스에서 상기 패스워드를 구성하는 문자에서 두 자릿수의 패스워드 문자군의 첫 번째 문자가 위치한 행과 두 번째 문자가 위치한 열의 교차점의 입력을 통하여 상기 패스워드를 구성하는 문자를 확인함으로써 이루어지는 것을 특징으로 하는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템.

청구항 5

청구항 4에 있어서,

상기 두 자릿수의 패스워드 문자군은 n자리의 패스워드의 {[1자리, 2자리], [2자리, 3자리], ..., [n자리, 1자리]}로 이루어지는 것을 특징으로 하는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템.

청구항 6

청구항 4 내지 청구항 5 중 어느 한 항에 있어서,

상기 알파-뉴메릭 매트릭스를 전체 회전시키거나, 열 또는 행 단위로 셔플시키는 알파-뉴메릭 매트릭스 회전/셔플 모듈을 더 포함하는 것을 특징으로 하는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템.

청구항 7

청구항 2에 있어서,

상기 알파-뉴메릭 매트릭스에 패스워드 문자를 입력하는 입력도구를 포함하고,

상기 입력도구는 키보드, 키패드, 마우스, 터치스크린 중 선택된 하나인 것을 특징으로 하는 알파-뉴메릭 매트

릭스를 이용한 패스워드 입력 시스템.

청구항 8

삭제

청구항 9

문자가 매트릭스 형태로 배열된 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법으로서,

상기 알파-뉴메릭 매트릭스에서 패스워드를 구성하는 n 개의 문자에서 두 자릿수의 패스워드 문자군을 선택하는 단계;

상기 알파-뉴메릭 매트릭스에서 상기 두 자릿수의 패스워드 문자군 각각의 첫 번째 문자가 위치한 행과 두 번째 문자가 위치한 열의 교차점에 위치한 상기 패스워드 문자를 인지하는 단계; 및

상기 알파-뉴메릭 매트릭스에서 패스워드 문자와 기설정된 거리에 위치한 알파-뉴메릭 매트릭스 문자를 선택하여 입력하는 단계를 포함하는 것을 특징으로 하는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법.

청구항 10

청구항 9에 있어서,

상기 두 자릿수의 패스워드 문자군은 n 자리의 패스워드의 {[1자리, 2자리], [2자리, 3자리], ..., [n자리, 1자리]}로 이루어진 것인, 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법.

청구항 11

청구항 9 내지 청구항 10 중 어느 하나에 있어서,

상기 알파-뉴메릭 매트릭스에서 패스워드 문자와 기설정된 거리에 위치한 알파-뉴메릭 매트릭스 문자를 선택하여 입력하는 단계는,

상기 알파-뉴메릭 매트릭스에서 패스워드 문자와 일정한 거리에 위치한 하나의 알파-뉴메릭 매트릭스 문자의 선택을 완료할 때마다,

상기 알파-뉴메릭 매트릭스를 전체 회전시키거나, 열 또는 행 단위로 셔플시키는 단계를 더 포함하는 것을 특징으로 하는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법.

청구항 12

문자가 매트릭스 형태로 배열된 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법으로서,

상기 패스워드를 구성하는 n 개의 문자에서 두 자릿수의 패스워드 문자군을 선택하는 단계와,

상기 알파-뉴메릭 매트릭스에서 상기 두 자릿수의 패스워드 문자군 각각의 첫 번째 문자가 위치한 행과 두 번째 문자가 위치한 열의 교차점에 위치한 상기 패스워드 문자를 순차적으로 입력하는 단계를 포함하는 것을 특징으로 하는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법.

청구항 13

청구항 12에 있어서,

상기 두 자릿수의 패스워드 문자군은 n 자리의 패스워드의 {[1자리, 2자리], [2자리, 3자리], ..., [n자리, 1자리]}로 이루어진 것인, 특징으로 하는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법.

청구항 14

청구항 12 또는 청구항 13에 있어서,

상기 알파-뉴메릭 매트릭스에서 상기 두 자릿수의 패스워드 문자군 각각의 첫 번째 문자가 위치한 행과 두 번째 문자가 위치한 열의 교차점에 위치한 상기 패스워드 문자를 순차적으로 입력하는 단계는,

상기 알파-뉴메릭 매트릭스에서 상기 패스워드 문자 n 개 중 하나의 입력을 완료할 때마다,

상기 알파-뉴메릭 매트릭스를 전체 회전시키거나, 열 또는 행 단위로 서플시키는 단계를 더 포함하는 것을 특징으로 하는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법.

명세서

발명의 상세한 설명

기술 분야

[0001] 본 발명은 패스워드 입력 알고리즘에 대한 것으로서, 특히 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템 및 그 방법에 관한 것이다.

배경 기술

[0002] 일반적으로 인터넷으로 웹사이트와, 인터넷 뱅킹 등을 이용하기 위해서는 본인확인을 위해 아이디와 패스워드 등을 입력하게 된다. 하지만 기존의 키보드를 이용한 패스워드 입력방식은 사용자가 입력하는 키 정보를 기록하여 아이디와 패스워드 등을 알아내는 키로깅 공격이나 사용자의 어깨 뒤에서 사용자가 입력하는 아이디와 패스워드 등을 보고 알아내는 숄더 서핑(Shoulder Surfing, 개인의 통제 하에 있지 않는 공간에서 발생하는 공격으로 단순한 훑쳐보기를 넘어 CCTV 등 영상물을 이용한 공격도 포함) 공격에 매우 취약한 단점이 지적되어 왔다.

[0003] 지난해 시만텍사가 월평균 탐지해 막은 악성코드 2억 4500만개 중 90%는 기밀정보를 노렸으며, 그 중 76%는 사용자의 키보드 입력정보를 빼내 인터넷 은행계좌 인증정보 등을 훔칠 수 있는 키로깅과 관련된 위협이었다. 이러한 문제점, 즉, 키보드 입력 패스워드 입력방식을 보완하기 위한 수많은 기법들이 연구 되었으며, 현재 연구된 기법은 크게 그래픽을 이용한 패스워드 입력 기법과 사람의 연산능력을 요구하는 패스워드 입력 기법으로 나눌 수 있다.

[0004] 최근의 몇몇 인터넷 뱅킹사이트에서 마우스를 이용하여 비밀번호(숫자)를 입력하게 하는 그래픽을 이용한 패스워드 입력 기법이 도입되어 사용 중이지만, 대부분 6 내지 8자리의 알파벳과 숫자를 혼합한 패스워드가 아닌 4 내지 6자리의 숫자인 비밀번호의 입력을 위한 패스워드 입력 기법을 도입 중이다. 이러한 인터넷 뱅킹사이트에서 도입된 마우스를 이용하여 비밀번호(숫자)를 입력하게 하는 기법은 화면상에 입력 시마다 랜덤하게 생성된 숫자판 때문에 키로깅 공격은 큰 효력을 발휘하지 못한다. 하지만, 입력 시에 숫자 자체를 입력하기 때문에 숄더 서핑 공격에는 취약한 면모를 보인다. 이러한 패스워드 입력방법의 취약성으로 인해 사용자에게 PC방과 공용 PC 등의 공공환경에서의 인터넷뱅킹 사용이나 로그인 후 사용하는 웹사이트, 온라인 게임 등의 사용을 자제할 것을 권장하고 있다. 하지만, 부득이하게 공공환경에서 키보드를 이용한 패스워드를 사용한 경우나 숄더 서핑이 가능한 경우, 사용자의 피해로 이어지거나 정보 유출에 대한 불안감에 시달리는 일이 발생되고 있다.

[0005] 따라서, 이러한 현상을 막기 위해서는 키로깅 공격뿐만 아니라 숄더 서핑 공격에도 강한 패스워드 입력 방법을 개발하여 피치 못할 사정으로 공공환경에서 패스워드를 사용하는 경우에도 안심하고 사용할 수 있는 방안이 요구되고 있다.

발명의 내용

해결 하고자하는 과제

[0006] 본 발명의 목적은 키로깅 공격과 숄더 서핑 공격을 방지할 수 있는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템 및 그 방법을 제공하는 것이다.

과제 해결수단

[0007] 상술한 목적을 달성하기 위해 본 발명은 문자가 매트릭스 형태로 배열되어 n 자릿수의 패스워드를 입력받는 알파-뉴메릭 매트릭스와, 상기 알파-뉴메릭 매트릭스에 입력된 패스워드를 확인하는 패스워드 입력 확인 모듈을 포함하여 이루어진 패스워드 입력 시스템으로서, 상기 패스워드 입력 확인 모듈의 패스워드 확인은, 상기 알파-뉴메릭 매트릭스에서 상기 패스워드를 구성하는 문자에서 두 자릿수의 패스워드 문자군의 첫 번째 문자가 위치한 행과 두 번째 문자가 위치한 열의 교차점인 상기 패스워드를 구성하는 문자(제1문자)로부터 기설정된 간격 이격된 문자(제2문자)의 입력을 통하여 상기 패스워드를 구성하는 문자(제1문자)를 확인함으로써 이루어진다. 상기

두 자릿수의 패스워드 문자군은 n 자리의 패스워드의 {[1자리, 2자리], [2자리, 3자리], ..., [n자리, 1자리]}의 패스워드 문자군을 포함할 수 있다.

[0008] 또한, 본 발명은 문자가 매트릭스 형태로 배열되어 n 자릿수의 패스워드를 입력받는 알파-뉴메릭 매트릭스와, 상기 알파-뉴메릭 매트릭스에 입력된 패스워드를 확인하는 패스워드 입력 확인 모듈을 포함하여 이루어진 패스워드 입력 시스템으로서, 상기 패스워드 입력 확인 모듈은 상기 알파-뉴메릭 매트릭스에서 상기 패스워드를 구성하는 문자에서 두 자릿수의 패스워드 문자군의 첫 번째 문자가 위치한 행과 두 번째 문자가 위치한 열의 교차점의 입력을 통하여 상기 패스워드를 구성하는 문자를 확인함으로써 이루어지는 것을 특징으로 하는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템을 제공한다. 상기 두 자릿수의 패스워드 문자군은 n 자리의 패스워드의 {[1자리, 2자리], [2자리, 3자리], ..., [n자리, 1자리]}로 이루어질 수 있다. 상기 알파-뉴메릭 매트릭스를 전체 회전시키거나, 열 또는 행 단위로 셔플시키는 알파-뉴메릭 매트릭스 회전/셔플 모듈을 더 포함할 수 있다. 상기 알파-뉴메릭 매트릭스에 패스워드 문자를 입력하는 입력도구를 포함하고, 상기 입력도구는 키보드, 키패드, 마우스, 터치스크린 중 선택된 하나일 수 있다.

[0009] 또한, 본 발명은 문자가 매트릭스 형태로 배열된 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법으로서, 상기 알파-뉴메릭 매트릭스에서 패스워드를 구성하는 n 개의 문자에서 두 자릿수의 패스워드 문자군을 선택하는 단계; 상기 알파-뉴메릭 매트릭스에서 상기 두 자릿수의 패스워드 문자군 각각의 첫 번째 문자가 위치한 행과 두 번째 문자가 위치한 열의 교차점에 위치한 상기 패스워드 문자를 인지하는 단계; 및 상기 알파-뉴메릭 매트릭스에서 패스워드 문자와 기설정된 거리에 위치한 알파-뉴메릭 매트릭스 문자를 선택하여 입력하는 단계를 포함하는 것을 특징으로 하는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법을 제공한다.

상기 두 자릿수의 패스워드 문자군은 n 자리의 패스워드의 {[1자리, 2자리], [2자리, 3자리], ..., [n자리, 1자리]}로 이루어질 수 있다. 상기 알파-뉴메릭 매트릭스에서 패스워드 문자와 일정한 거리에 위치한 알파-뉴메릭 매트릭스 문자를 선택하는 단계는, 상기 알파-뉴메릭 매트릭스에서 패스워드 문자와 기설정된 거리에 위치한 하나의 알파-뉴메릭 매트릭스 문자의 선택을 완료할 때마다, 상기 알파-뉴메릭 매트릭스를 전체 회전시키거나, 열 또는 행 단위로 셔플시키는 단계를 더 포함할 수 있다.

[0010] 또한, 본 발명은 문자가 매트릭스 형태로 배열된 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법으로서, 상기 패스워드를 구성하는 n 개의 문자에서 두 자릿수의 패스워드 문자군을 선택하는 단계와, 상기 알파-뉴메릭 매트릭스에서 상기 두 자릿수의 패스워드 문자군 각각의 첫 번째 문자가 위치한 행과 두 번째 문자가 위치한 열의 교차점에 위치한 상기 패스워드 문자를 순차적으로 입력하는 단계를 포함하는 것을 특징으로 하는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법을 제공한다. 상기 두 자릿수의 패스워드 문자군은 n 자리의 패스워드의 {[1자리, 2자리], [2자리, 3자리], ..., [n자리, 1자리]}로 이루어질 수 있다. 상기 알파-뉴메릭 매트릭스에서 상기 두 자릿수의 패스워드 문자군 각각의 첫 번째 문자가 위치한 행과 두 번째 문자가 위치한 열의 교차점에 위치한 상기 패스워드 문자를 순차적으로 입력하는 단계는, 상기 알파-뉴메릭 매트릭스에서 상기 패스워드 문자 n 개 중 하나의 입력을 완료할 때마다, 상기 알파-뉴메릭 매트릭스를 전체 회전시키거나, 열 또는 행 단위로 셔플시키는 단계를 더 포함할 수 있다.

효 과

[0011] 본 발명은 알파-뉴메릭 매트릭스에서 패스워드를 구성하는 문자와 일정한 간격 이격된 알파-뉴메릭 매트릭스 문자를 최종 패스워드로 입력하여 키로깅 공격과 솔더 서핑 공격을 방어할 수 있는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템 및 방법을 제공할 수 있다.

[0012] 또한, 본 발명은 알파-뉴메릭 매트릭스에서 패스워드를 구성하는 문자와 일정한 간격 이격된 알파-뉴메릭 매트릭스 문자를 최종 패스워드로 입력하되, 하나의 문자를 입력할 때마다 알파-뉴메릭 매트릭스를 회전시켜 키로깅 공격과 솔더 서핑 공격의 방어 확률을 더욱 증가시킬 수 있는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템 및 방법을 제공할 수 있다.

[0013] 또한, 본 발명은 패스워드를 구성하는 문자를 앞의 한자리 문자가 연관되도록 두 자리씩 선택하여 기억하고, 이에 대한 알파-뉴메릭 매트릭스에서의 교차점을 최종 패스워드로 입력하여 키로깅 공격과 솔더 서핑 공격을 방어할 수 있는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템 및 방법을 제공할 수 있다.

발명의 실시를 위한 구체적인 내용

[0014] 이하, 도면을 참조하여 본 발명의 실시예를 상세히 설명하기로 한다.

- [0015] 그러나 본 발명은 이하에서 개시되는 실시예에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이다. 도면상의 동일 부호는 동일한 요소를 지칭한다.
- [0016] 도 1은 본 발명에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템의 개념도이다.
- [0017] 본 발명에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 알고리즘은 도 1에 도시된 바와 같이, 알파-뉴메릭 매트릭스(100)와, 알파-뉴메릭 매트릭스 구동 모듈(200)을 포함한다.
- [0018] 알파-뉴메릭 매트릭스(100, Alpha-Numeric Matrix)는 사용자가 패스워드를 직접 입력하기 위한 것으로서, 행과 열을 포함하는 매트릭스 형태의 표에 문자가 매트릭스 형태로 배치된다. 이때, 상기 문자는 'A' 내지 'Z'를 포함하는 알파벳 26자와, '0' 내지 '9'를 포함하는 숫자 10자와, '!' 내지 '='를 포함하는 특수문자 13자 등의 문자를 포함할 수 있다. 하지만, 알파-뉴메릭 매트릭스의 문자는 알파벳, 즉, 영문뿐만 아니라 한글의 자음 또는 모음, 한문, 일어 등 세계에서 통용되는 언어를 포함할 수 있다. 알파-뉴메릭 매트릭스의 문자는 영문 또는 본 발명이 적용되는 국가의 언어에 대응되는 것이 바람직하다. 예를 들어, 대한민국에서 본 발명이 적용될 경우, 알파-뉴메릭 매트릭스의 문자는 영문과 숫자 및 특수문자 또는 한글의 자음 또는 모음과 숫자 및 특수문자를 포함할 수 있다. 이때, 특수문자는 상기에서 나열된 특수문자, 즉, 키보드에서 지원되는 특수문자를 포함하는 것이 바람직하다. 물론, 본 실시예의 특수문자 이외에 키보드에서 지원되는 '[', ']', '{', '}', '"', ';' 등의 특수문자 또는 키보드에서 지원되지 않는 무늬 등을 포함하는 특수문자를 사용할 수도 있다. 또한, 알파-뉴메릭 매트릭스는 문자열 지원을 위해 도 1에 도시된 바와 같은 7×7의 알파-뉴메릭 매트릭스를 이용할 수 있다. 하지만, 본 발명은 이에 한정되는 것은 아니며, 6×6 또는 8×8 등과 같이 필요로 하는 문자의 개수에 따라 알파-뉴메릭 매트릭스(100)를 조절할 수 있다. 물론, 알파-뉴메릭 매트릭스(100)의 크기를 조절함에 따라 알파-뉴메릭 매트릭스(100)에 포함되는 문자는 조절되어야 한다.
- [0019] 알파-뉴메릭 매트릭스 구동 모듈(200)은 알파-뉴메릭 매트릭스(100)의 이동과 회전 등과 같은 매트릭스의 구동 및 패스워드 입력 확인 등을 수행하기 위한 것으로서, 알파-뉴메릭 매트릭스 회전/서플 모듈(210)과, 패스워드 입력 확인 모듈(220)을 포함한다.
- [0020] 알파-뉴메릭 매트릭스 회전/서플 모듈(210)은 알파-뉴메릭 매트릭스(100)를 일방향으로 회전 또는 서플시킨다. 이때, 알파-뉴메릭 매트릭스(100)의 회전은 왼쪽 또는 오른쪽 방향으로 90도 또는 180도 또는 270도 회전시킴으로써 수행할 수 있다. 또한, 알파-뉴메릭 매트릭스(100)의 서플은 알파-뉴메릭 매트릭스(100)의 행 및/또는 열을 적어도 한칸 이상 이동, 즉, 서플시켜 수행할 수 있다. 이러한 알파-뉴메릭 매트릭스의 회전 및/또는 서플은 알파-뉴메릭 매트릭스를 이용하여 패스워드를 구성하는 문자 하나를 순차적으로 입력할 때마다 수행되는 것이 효과적이다. 하지만, 본 발명은 이에 한정되는 것은 아니며, 패스워드를 구성하는 문자의 적어도 하나 이상, 예를 들어, 두 개 또는 세 개의 입력이 순차적으로 완료된 후 수행될 수도 있다. 더욱이, 본 발명은 패스워드를 구성하는 문자 모두를 입력한 후, 추후에 진행될 본인확인을 위해 알파-뉴메릭 매트릭스의 회전 및/또는 서플을 수행할 수도 있다.
- [0021] 패스워드 입력 확인 모듈(220)은 사용자가 입력한 패스워드가 제대로 입력되었는지 확인한다. 사용자가 입력한 패스워드가 제대로 입력되지 않았을 경우 패스워드 입력 확인 모듈(220)은 사용자에게 오류 메시지를 보내며, 사용자가 입력한 패스워드가 제대로 입력되었을 경우, 패스워드 입력 확인 모듈(220)은 시스템에 패스워드 확인 메시지를 보낸다.
- [0022] 본 발명의 패스워드 입력은 사용자가 패스워드를 구성하는 문자와 일정한 간격을 갖는 알파-뉴메릭 매트릭스 문자를 선택하여 수행될 수 있다. 또한, 사용자가 패스워드를 구성하는 문자를, 앞의 두 자리 문자의 마지막 문자가 다음 두 자리 문자의 첫 번째 문자가 되도록 두 자리씩 선택하여 기억하고, 상기 두 자리 문자에 대한 교차점을 알파-뉴메릭 매트릭스(100)에서 찾아서 선택하여 패스워드를 입력할 수 있다. 이때, 상기 두 자리 문자에 대한 교차점은 상기 두 자리 문자 각각을 알파-뉴메릭 매트릭스(100)에서 찾고, 각각의 행과 열이 교차하는 지점을 의미한다. 물론, 두 자리 문자 중 첫 번째 문자의 행과 두 번째 문자의 열이 교차하는 지점을 교차점으로 하거나, 두 자리 문자 중 첫 번째 문자의 열과 두 번째 문자의 행이 교차하는 지점을 교차점으로 할 수 있다. 이때, 상기 두 가지의 교차점을 구하는 방법을 일관 되게 유지하는 것이 중요하다. 또한, 전술된 두 가지 방법에 대해 패스워드를 구성하는 하나의 문자를 입력할 때마다 알파-뉴메릭 매트릭스(100)를 회전 및/또는 서플시켜 키로깅 공격 및 숄더 서핑 공격의 방어 확률을 증가시킬 수 있다. 물론, 전술된 바와 같이, 패스워드의 교차

점을 구하고, 교차점과 일정한 간격을 갖는 알파-뉴메릭 매트릭스 문자를 선택하여 패스워드를 입력할 수도 있다. 또한, 이에 더해 패스워드를 구성하는 하나의 문자를 입력할 때마다 알파-뉴메릭 매트릭스(100)를 회전 및/또는 서플시킬 수도 있다.

[0023] 즉, 패스워드 입력 확인 모듈(220)은 이와 같은 방법의 패스워드 입력 방식을 인식하여 사용자가 입력한 패스워드를 판단하여 사용자 본인을 확인한다. 또한, 시스템은 패스워드 확인 메시지를 수신함으로써, 사용자 본인확인을 완료할 수 있다.

[0024] 한편, 본 발명에 따른 알파-뉴메릭 매트릭스(100)를 이용한 패스워드 입력 시스템은 알파-뉴메릭 매트릭스(100)에서 패스워드를 입력하기 위한 입력도구(미도시)를 구비한다. 이때, 이러한 입력도구로 키보드를 이용할 경우, 키보드의 자판을 이용하여 패스워드를 직접 입력할 수 있다. 또한, 입력도구로 키패드를 이용할 경우, 알파-뉴메릭 매트릭스 문자에 나타난 음영과 같은 표시를 키패드로 조정하여 패스워드를 입력할 수 있다. 물론, 마우스와 터치스크린으로 패스워드를 입력할 경우, 알파-뉴메릭 매트릭스(100)의 특정 문자를 마우스로 클릭하거나 터치스크린에 터치하여 패스워드를 입력할 수 있다.

[0025] 다음은 본 발명에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템을 이용한 본 발명의 제 1 실시예에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법에 대해 도면을 참조하여 설명하고자 한다. 후술할 내용 중 전술된 본 발명에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 알고리즘의 설명과 중복되는 내용은 생략하거나 간략히 설명하기로 한다.

[0026] 도 2는 본 발명의 제 1 실시예에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법의 순서도이고, 도 3 내지 도 5는 본 발명의 제 1 실시예에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법을 설명하기 위한 알파-뉴메릭 매트릭스이다.

[0027] 본 발명의 제 1 실시예에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법은 도 2에 도시된 바와 같이, 알파-뉴메릭 매트릭스에서 패스워드의 각 문자를 인지하는 단계(S_1)와, 알파-뉴메릭 매트릭스에서 패스워드 문자와 일정한 거리에 위치한 문자를 선택하는 단계(S_2)와, 알파-뉴메릭 매트릭스를 회전시키는 단계(S_3)를 포함한다.

[0028] 알파-뉴메릭 매트릭스에서 패스워드의 각 문자를 인지하는 단계(S_1)는 사용자가 알파-뉴메릭 매트릭스에서 패스워드를 구성하는 각 문자를 찾아서 인지한다. 예를 들어, 패스워드가 'DRAGON'일 때, 도 2에 도시된 바와 같이, 사용자는 알파-뉴메릭 매트릭스에서 'D'를 찾아서 인식한다.

[0029] 알파-뉴메릭 매트릭스에서 패스워드 문자와 일정한 거리에 위치한 문자를 선택하는 단계(S_2)는 패스워드를 구성하는 각각의 문자와 일정한 거리에 있는 문자를 순차적으로 선택하여 패스워드를 입력한다. 예를 들어, 패스워드가 'DRAGON'일 때, 사용자는 알파-뉴메릭 매트릭스에서 패스워드의 각 문자를 인지하는 단계(S_1)에서 패스워드를 구성하는 첫 문자인 'D'를 찾아서 인식하였다. 이에 따라, 사용자는 알파-뉴메릭 매트릭스에서 패스워드를 구성하는 첫 문자인 'D'에서 일정한 거리에 있는 문자를 선택하여 패스워드를 입력한다. 예를 들어, 도 3에 도시된 바와 같이, 상기 일정한 거리를 패스워드를 구성하는 첫 문자인 'D'에서 아래로 두 칸 오른쪽으로 두 칸에 위치한 문자인 'T'를 암호화된 첫 문자로 선택할 수 있다. 물론, 이를 응용하여, 패스워드를 구성하는 나머지 문자인 'R', 'A', 'G', 'O', 'N' 역시 이와 같은 방법으로 각각 입력할 수 있다. 이때, 패스워드를 구성하는 문자의 선택은 키보드, 키패드, 마우스, 터치패드 등의 입력도구 중 선택된 하나를 사용할 수 있다.

[0030] 한편, 본 실시예는 키로깅 공격과 숄더 서핑 공격을 방어 확률을 증가시키기 위해 패스워드를 구성하는 문자를 각각 입력할 때마다 알파-뉴메릭 매트릭스를 회전시키는 단계를 더 포함할 수 있다.

[0031] 알파-뉴메릭 매트릭스를 회전시키는 단계(S_3)는 패스워드를 구성하는 문자 각각의 입력을 완료할 때마다 알파-뉴메릭 매트릭스를 회전시킨다. 이러한 알파-뉴메릭 매트릭스의 회전은 알파-뉴메릭 매트릭스를 왼쪽 또는 오른쪽으로 90도 또는 180도 또는 270도 회전시킬 수 있다. 물론, 본 발명은 알파-뉴메릭 매트릭스를 회전 시키는 것뿐만 아니라, 알파-뉴메릭 매트릭스의 행 및/또는 열을 적어도 한칸 이상 이동시키는 서플을 수행할 수도 있다.

[0032] 예를 들어, 알파-뉴메릭 매트릭스를 오른쪽으로 90도 회전시킬 경우 도 5에 도시된 바와 같이 나타낼 수 있으며, 사용자는 다시 전술된 알파-뉴메릭 매트릭스에서 패스워드의 각 문자를 인지하는 단계(S_1)와, 알파-뉴메

릭 매트릭스에서 패스워드 문자와 일정한 거리에 위치한 문자를 선택하는 단계(S_2)를 수행하여 패스워드를 구성하는 문자를 입력할 수 있다. 즉, 도 5에 도시된 바와 같이, 패스워드가 'DRAGON'일 때, 패스워드를 구성하는 두 번째 문자인 'R'의 아래쪽 2칸 및 오른쪽 2칸에 위치한 'T'를 두 번째 암호화된 문자로 선택할 수 있다.

[0033] 물론, 이러한 알파-뉴메릭 매트릭스를 회전시키는 단계(S_3)는 생략될 수 있으며, 이 경우, 본 실시예는 전술된 알파-뉴메릭 매트릭스에서 패스워드의 각 문자를 인지하는 단계(S_1)와, 알파-뉴메릭 매트릭스에서 패스워드 문자와 일정한 거리에 위치한 문자를 선택하는 단계(S_2)만을 수행하여 패스워드를 입력할 수 있다.

[0034] 상술한 바와 같이 본 실시예는 알파-뉴메릭 매트릭스에서 패스워드를 구성하는 문자와 일정한 간격 이격된 알파-뉴메릭 매트릭스 문자를 최종 패스워드로 입력하여 키로깅 공격과 숄더 서핑 공격을 방어할 수 있는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법을 제공할 수 있다. 또한, 본 실시예는 알파-뉴메릭 매트릭스에서 패스워드를 구성하는 문자와 일정한 간격 이격된 알파-뉴메릭 매트릭스 문자를 최종 패스워드로 입력하되, 하나의 문자를 입력할 때마다 알파-뉴메릭 매트릭스를 회전시켜 키로깅 공격과 숄더 서핑 공격의 방어 확률을 더욱 증가시킬 수 있는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법을 제공할 수 있다.

[0035] 다음은 알파-뉴메릭 매트릭스에서 패스워드의 각 문자를 인지하는 단계에서 패스워드 문자의 교차점을 구하는 본 발명의 제 2 실시예에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법에 대해 도면을 참조하여 설명하고자 한다. 후술할 내용 중 전술된 본 발명의 제 1 실시예에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 알고리즘의 설명과 중복되는 내용은 생략하거나 간략히 설명하기로 한다.

[0036] 도 6은 본 발명의 제 2 실시예에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법의 순서도이고, 도 7은 본 발명의 제 2 실시예에 따른 패스워드의 예시이다. 또한, 도 8 및 도 9는 본 발명의 제 2 실시예에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법을 설명하기 위한 알파-뉴메릭 매트릭스이다.

[0037] 본 발명의 제 2 실시예에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법은 도 6에 도시된 바와 같이, 패스워드의 문자를 두 자리씩 선택하는 단계(S_1)와, 두 자리씩 선택된 패스워드 문자의 교차점을 구하는 단계(S_2)와, 알파-뉴메릭 매트릭스에서 패스워드 문자의 교차점과 일정한 거리에 위치한 문자를 선택하는 단계(S_3)와, 알파-뉴메릭 매트릭스를 회전시키는 단계(S_4)를 포함한다.

[0038] 패스워드의 문자를 두 자리씩 선택하는 단계(S_1)는 사용자가 패스워드의 앞자리부터 두 자리씩 선택한다. 예를 들어, 도 7에 도시된 바와 같이, 패스워드가 'DRAGON'일 경우, 사용자는 'DRAGON'을 'DR' (①)과, 'RA' (②)와, 'AG' (③)와, 'GO' (④)와, 'ON' (⑤)과, 'ND' (⑥) 즉, 앞자리의 문자가 연관되도록 두 자리씩 끊어서 선택하여 기억한다. 물론, 본 발명은 이에 한정되는 것은 아니며, 단순히 패스워드를 두 자리씩 선택할 수도 있다. 즉, 패스워드가 'DRAGON'일 경우, 사용자는 'DRAGON'을 'DR'과, 'AG'와, 'ON'으로 끊어서 선택하여 기억할 수도 있다. 또한, 특정 위치의 문자를 기준으로 패스워드를 두 자리씩 선택할 수도 있다. 예를 들어, 'DRAGON'에서 'D'를 기준으로 하고 'D'와 'R', 'A', 'G', 'O', 'N' 각각을 두 자리씩 묶어 'DR' 'DA' 'DG' 'DO' 'DN'와 같이 선택할 수도 있다.

[0039] 두 자리씩 선택된 패스워드 문자의 교차점을 구하는 단계(S_2)는 두 자리씩 선택된 패스워드 문자를 알파-뉴메릭 매트릭스를 이용하여 교차점을 구한다. 이때, 패스워드의 첫 번째 두자리 문자를 x,y 라고 할 때, $f(x,y)=z$ 연산은 문자 x,y 가 알파-뉴메릭 매트릭스에서 위치한 행과 열에 의해서 결정된다. 예를 들어, 패스워드가 'DRAGON'일 경우, 'DR'은 도 8에 도시된 바와 같이, 알파-뉴메릭 매트릭스에서 'D'와 'R'의 교차점에 위치한 'D'가 제 1 패스워드 문자 교차점이 된다. 즉, $f(x,y)$ 를 구하기 위해서 사용자는 알파-뉴메릭 매트릭스에서 각각의 문자 열의 위치에 따라 행과 열을 선택한다. 이와 같이 선택된 행과 열은 반드시 하나의 교차점이 존재하게 되며, 이를 연산의 결과로 한다. 전술된 'D'와 'R'의 경우 $f(D,R)=C*Z=D$ 가 된다. 이를 응용하면, 도 8에서 'RA'는 알파-뉴메릭 매트릭스에서 'R'과 'A'의 교차점에 위치한 'O'가 제 2 패스워드 문자 교차점이 된다. 또한, 'AG'는 알파-뉴메릭 매트릭스에서 'A'와 'G'의 교차점에 위치한 'G'가 제 3 패스워드 문자 교차점이 되며, 'GO'는 알파-뉴메릭 매트릭스에서 'G'와 'O'의 교차점에 위치한 'A'가 제 4 패스워드 문자 교차점이 된다. 또한, 'ON'은 알파-뉴메릭 매트릭스에서 'O'와 'N'의 교차점에 위치한 'U'가 제 5 패스워드 문자 교차점이 되며, 'ND'는 알파-뉴메릭 매트릭스에서 'N'과 'D'의 교차점에 위치한 'K'가 제 6 패스워드 문자 교차점이 된다. 즉, 제 1 내지 제 6 패스워드 문자 교차점인 'D'와, 'O'와, 'G'와, 'A'와, 'U' 및 'K'가 패스워드 'DRAGON'에 대한 패스워드

드 문자 교차점이 된다. 이러한 정의에 있어서 사용자가 교차점을 선택하였다 하더라도 원래의 연산의 입력인 두 개의 문자를 확정하기는 어렵다. 즉, 공격자는 단지 두 개의 문자가 들어 있는 행과 열에 대한 정보만을 얻을 수 있을 뿐이다.

[0040] 알파-뉴메릭 매트릭스에서 패스워드 문자의 교차점과 일정한 거리에 위치한 문자를 선택하는 단계(S_3)는 전술된 본 발명의 제 1 실시예와 같이, 패스워드를 구성하는 각각의 문자, 즉, 패스워드 문자 교차점과 일정한 거리에 있는 알파-뉴메릭 매트릭스 문자를 선택하여 패스워드를 입력한다. 예를 들어, 도 9에 도시된 바와 같이, 패스워드 문자 교차점이 'D'일 경우, 'D'와 일정한 거리, 예를 들어, 아래로 1칸 및 오른쪽으로 1칸에 위치한 'L'을 최종 패스워드로 입력할 수 있다. 물론, 이를 응용하여 모든 패스워드 문자 교차점에 대해서 전술된 방법으로 입력을 수행한다.

[0041] 알파-뉴메릭 매트릭스를 회전시키는 단계(S_4)는 전술된 본 발명의 제 1 실시예와 같이, 패스워드를 구성하는 문자, 즉, 패스워드 문자 교차점 각각의 입력을 완료할 때마다 알파-뉴메릭 매트릭스를 회전 및/또는 셔플시킨다.

[0042] 물론, 이러한 알파-뉴메릭 매트릭스에서 패스워드 문자의 교차점과 일정한 거리에 위치한 문자를 선택하는 단계(S_3)와 알파-뉴메릭 매트릭스를 회전시키는 단계(S_4) 중 적어도 어느 하나는 생략될 수 있으며, 이 경우, 본 실시예는 전술된 패스워드의 문자를 두 자리씩 선택하는 단계(S_1)와 두 자리씩 선택된 패스워드 문자의 교차점을 구하는 단계(S_2)와 알파-뉴메릭 매트릭스에서 패스워드 문자의 교차점과 일정한 거리에 위치한 문자를 선택하는 단계(S_3), 또는 패스워드의 문자를 두 자리씩 선택하는 단계(S_1)와 두 자리씩 선택된 패스워드 문자의 교차점을 구하는 단계(S_2) 후 상기 패스워드 문자의 교차점을 입력하는 단계만을 수행하여 패스워드를 입력할 수 있다.

[0043] 상술한 바와 같이 본 실시예는 패스워드를 구성하는 문자를 앞의 한자리 문자가 연관되도록 두 자리씩 선택하여 기억하고, 이에 대한 알파-뉴메릭 매트릭스에서의 교차점을 최종 패스워드로 입력하여 키로깅 공격과 솔더 서핑 공격을 방어할 수 있는 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법을 제공할 수 있다.

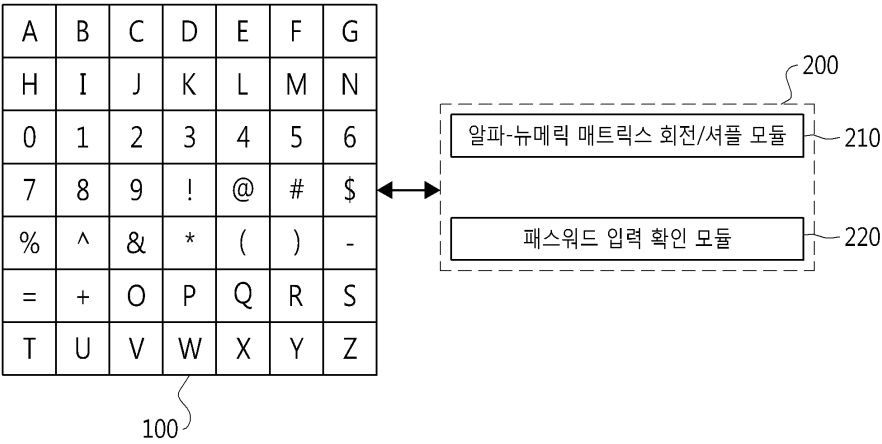
[0044] 이상에서는 도면 및 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허청구범위에 기재된 본 발명의 기술적 사상으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면의 간단한 설명

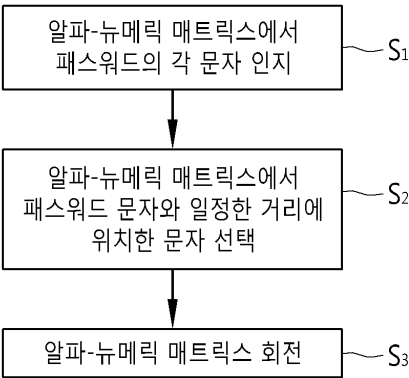
- [0045] 도 1은 본 발명에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 시스템의 개념도.
- [0046] 도 2는 본 발명의 제 1 실시예에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법의 순서도.
- [0047] 도 3 내지 도 5는 본 발명의 제 1 실시예에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법을 설명하기 위한 알파-뉴메릭 매트릭스.
- [0048] 도 6은 본 발명의 제 2 실시예에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법의 순서도.
- [0049] 도 7은 본 발명의 제 2 실시예에 따른 패스워드의 예시.
- [0050] 도 8 및 도 9는 본 발명의 제 2 실시예에 따른 알파-뉴메릭 매트릭스를 이용한 패스워드 입력 방법을 설명하기 위한 알파-뉴메릭 매트릭스.
- [0051] <도면의 주요 부분에 대한 부호의 설명>
- [0052] 100: 알파-뉴메릭 매트릭스
- [0053] 200: 알파-뉴메릭 매트릭스 구동 모듈
- [0054] 210: 알파-뉴메릭 매트릭스 회전/셔플 모듈
- [0055] 220: 패스워드 입력 확인 모듈

도면

도면1



도면2



도면3

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	0	1
2	3	4	5	6	7	8
9	!	@	#	\$	%	^
&	*	(	)	-	+	=

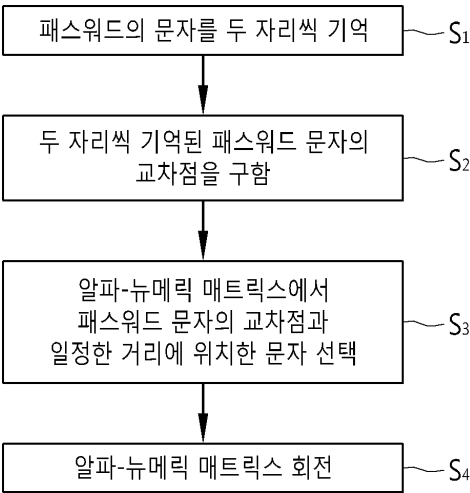
도면4

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	0	1
2	3	4	5	6	7	8
9	!	@	#	\$	%	^
&	*	(	)	-	+	=

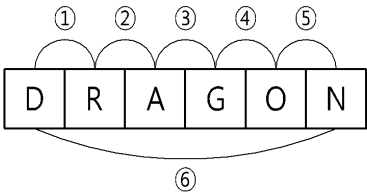
도면5

&	9	2	V	O	H	A
*	!	3	W	P	I	B
(	@	4	X	Q	J	C
)	#	5	Y	R	K	D
-	\$	6	Z	S	L	E
+	%	7	0	T	M	F
=	^	8	1	U	N	G

도면6



도면7



도면8

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	0	1
2	3	4	5	6	7	8
9	!	@	#	\$	%	^
&	*	(	)	-	+	=

도면9

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	0	1
2	3	4	5	6	7	8
9	!	@	#	\$	%	^
&	*	(	)	-	+	=