



(22) Date de dépôt/Filing Date: 2016/04/11

(41) Mise à la disp. pub./Open to Public Insp.: 2017/10/11

(51) Cl.Int./Int.Cl. *H04W 12/06* (2009.01),
H04L 9/32 (2006.01)

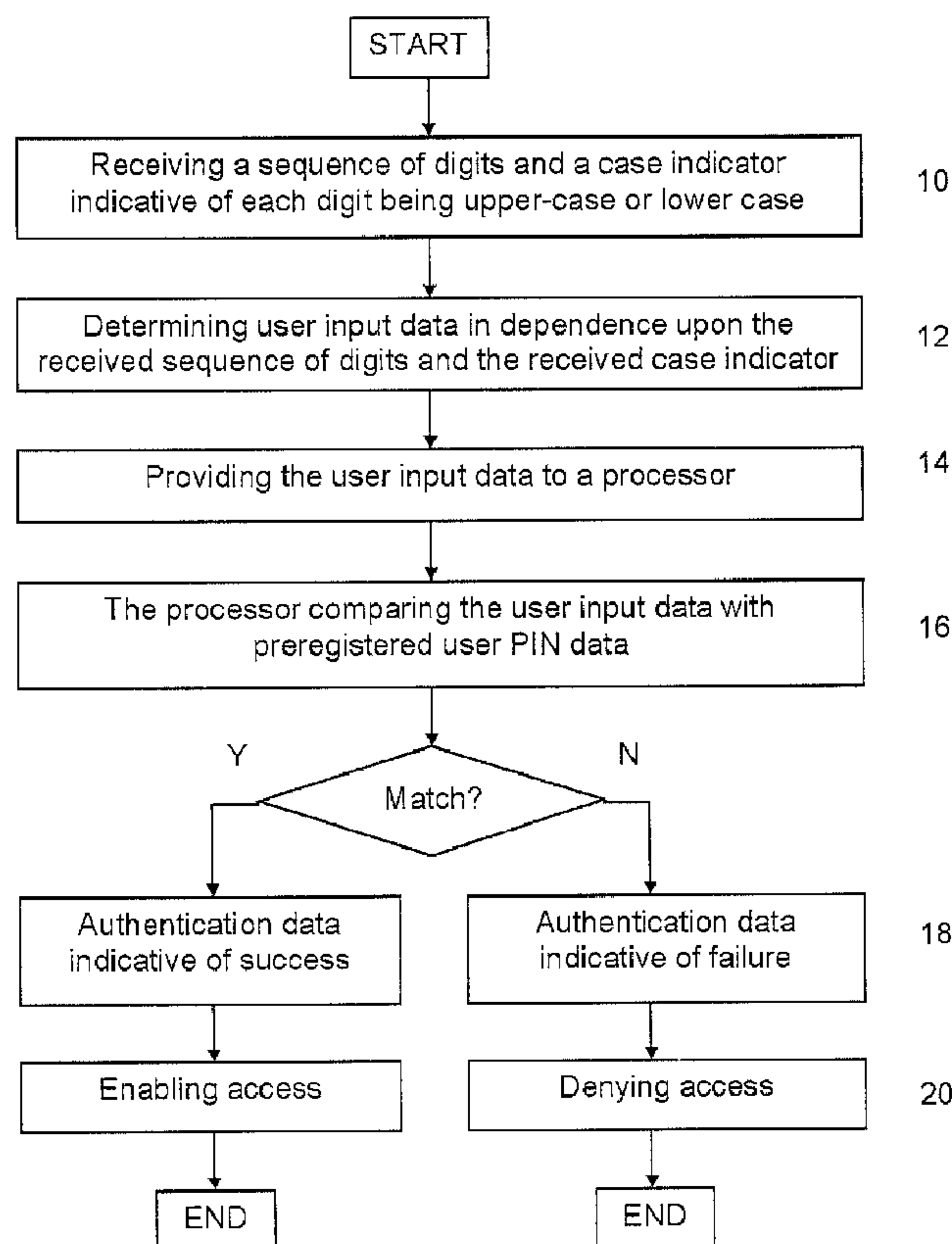
(71) Demandeur/Applicant:
YARNTON, DEVIN, CA

(72) Inventeur/Inventor:
YARNTON, DEVIN, CA

(74) Agent: FURMAN IP LAW & STRATEGY PC

(54) Titre : METHODE ET SYSTEME D~AUTHENTIFICATION D~UTILISATEUR DE DISPOSITIF MOBILE

(54) Title: METHOD AND SYSTEM FOR MOBILE DEVICE USER AUTHENTICATION



(57) Abrégé/Abstract:

A method and system for authenticating a personal identification number (PIN) of a user is provided. At a user interface a sequence of digits and a case indicator indicative of each digit being upper-case or lower case is received. A controller of the user interface

(57) **Abrégé(suite)/Abstract(continued):**

determines user input data in dependence upon the received sequence of digits and the received case indicator and provides the same to a processor. The processor compares the user input data with preregistered user PIN data and determines user authentication data. The user authentication data are: indicative of success in authenticating the user if the user input data match the preregistered user PIN data; and indicative of failure in authenticating the user if the user input data do not match the preregistered user PIN data.

ABSTRACT

A method and system for authenticating a personal identification number (PIN) of a user is provided. At a user interface a sequence of digits and a case indicator indicative of each digit
5 being upper-case or lower case is received. A controller of the user interface determines user input data in dependence upon the received sequence of digits and the received case indicator and provides the same to a processor. The processor compares the user input data with preregistered user PIN data and determines user authentication data. The user authentication data are: indicative of success in authenticating the user if the user input data match the
10 preregistered user PIN data; and indicative of failure in authenticating the user if the user input data do not match the preregistered user PIN data.

METHOD AND SYSTEM FOR MOBILE DEVICE USER AUTHENTICATION

FIELD OF THE INVENTION

5

The present invention relates to user authentication for mobile devices, and more particularly, to a method and system for passcode based mobile device user authentication having enhanced security.

10

BACKGROUND OF THE INVENTION

15

With the widespread use of mobile devices such as, for example, smartphones, personal digital assistants, and tablet computers, an increasing number of applications for use with mobile devices are provided. Applications such as, for example, enabling remote access, making payments, and banking, use the mobile devices for transmission and storage of sensitive information, requiring implementation of security measures to prevent unauthorized access in case a mobile device is lost or stolen.

20

Typically, user authorization on mobile devices is provided using a 4 digit passcode or Personal Identification Number (PIN). Current 4 digit PINs – with each digit being an integer number 0-9 – offer 10^4 or 10,000 unique combinations a user can select. In order to increase security, users can add multiple layers to the authentication process, requiring several steps and multiple fields of information to be entered.

However, adding multiple layers of to the authentication process results in a cumbersome and time consuming process requiring the user to memorize multiple pieces of information to be entered in the correct order.

5

It is desirable to provide a method and system for mobile device user authentication that uses a simple process and provides increased security.

10

It is also desirable to provide a method and system for mobile device user authentication that uses a single layer process and provides increased security.

15

It is also desirable to provide a method and system for mobile device user authentication that uses a single layer PIN based process and provides increased security.

SUMMARY OF THE INVENTION

20

Accordingly, one object of the present invention is to provide a method and system for mobile device user authentication that uses a simple process and provides increased security.

Another object of the present invention is to provide a method and system for mobile device user authentication that uses a single layer process and provides increased security.

Another object of the present invention is to provide a method and system for mobile device

user authentication that uses a single layer PIN based process and provides increased security.

According to one aspect of the present invention, there is provided a method for authenticating a personal identification number (PIN) of a user. At a user interface a sequence of digits and a case indicator indicative of each digit being upper-case or lower case is received. A controller of the user interface determines user input data in dependence upon the received sequence of digits and the received case indicator and provides the same to a processor. The processor compares the user input data with preregistered user PIN data and determines user authentication data.

The user authentication data are: indicative of success in authenticating the user if the user input data match the preregistered user PIN data; and indicative of failure in authenticating the user if the user input data do not match the preregistered user PIN data. The process of preregistering user PIN data to a user profile of a user will be understood to those skilled in the art of ecommerce system design and security/authentication and database design. The specifics of any method of preregistering the preregistered user PIN data are intended to be within the scope hereof.

According to the aspect of the present invention, there is provided a system for authenticating a personal identification number (PIN) of a user. The system comprises a user interface, which is adapted for receiving from the user a sequence of digits and a case indicator indicative of each digit being upper-case or lower case and for providing user input data in dependence thereupon. a storage device having stored therein preregistered user PIN data. A processor is connected to the user interface and the storage device. The processor receives the user input data, compares the user input data with the preregistered user PIN data, and determines user authentication data. The user authentication data are: indicative of success in authenticating the user if the user input

data match the preregistered user PIN data; and indicative of failure in authenticating the user if the user input data do not match the preregistered user PIN data.

The advantage of the present invention is that it provides a method and system for mobile device user authentication that uses a simple process and provides increased security.

A further advantage of the present invention is that it provides a method and system for mobile device user authentication that uses a single layer process and provides increased security.

A further advantage of the present invention is that it provides a method and system for mobile device user authentication that uses a single layer PIN based process and provides increased security.

BRIEF DESCRIPTION OF THE DRAWINGS

A preferred embodiment of the present invention is described below with reference to the accompanying drawings, in which:

Figure 1a is a simplified block diagram illustrating a system for authenticating a PIN of a user according to a preferred embodiment of the invention;

Figures 1b and 1c are simplified block diagrams illustrating user interfaces of the system for authenticating a PIN of a user according to the preferred embodiment of the

invention;

Figures 2a and 2b are simplified block diagrams illustrating processes for entering a PIN
in the system for authenticating a PIN of a user according to the preferred embodiment
of the invention;

Figures 3a and 3b are simplified block diagrams illustrating bit sequences of a PIN
entered in the system for authenticating a PIN of a user according to the preferred
embodiment of the invention; and,

Figure 4 is a simplified flow diagram illustrating a method for authenticating a personal
identification number (PIN) of a user according to the preferred embodiment of the
invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Unless defined otherwise, all technical and scientific terms used herein have the same meaning
as commonly understood by one of ordinary skill in the art to which the invention belongs.

Although any methods and materials similar or equivalent to those described herein can be used
in the practice or testing of the present invention, the preferred methods and materials are now
described.

While the description of the preferred embodiments hereinbelow is with reference to mobile
device user authentication, it will become evident to those skilled in the art that the

embodiments of the invention are not limited thereto, but that the embodiments of the invention may also be employed for user authentication in other applications such as, for example, Automated Teller Machines (ATMs), and debit/credit card payments using Point Of Sale (POS) terminals.

5

Referring to Figures 1a to 1c, a system 100 for authenticating a PIN of a user according to a preferred embodiment of the invention is provided. The system comprises a mobile device 102 having user interface 104 adapted for receiving from the user a sequence of digits and a case indicator indicative of each digit being 'upper-case' or 'lower case', as will be described
10 hereinbelow. Controller 106 of the user interface 104 generates user input data in dependence upon the received sequence of digits and the case indicator and provides the same to processor/storage device 108 connected thereto. The processor/storage device 108 compares the user input data with preregistered user PIN data stored in storage device 110 such as, for example, non-volatile flash memory, and enables/denies access to the mobile device in
15 dependence upon the comparison. For example, the processor receives the user input data, compares the user input data with the preregistered user PIN data, and determines user authentication data for enabling/denying access when executing executable commands stored in the storage device 110. The process of preregistering user PIN data to a user profile of a user will be understood to those skilled in the art of ecommerce system design and
20 security/authentication and database design. The specifics of any method of preregistering the preregistered user PIN data are intended to be within the scope hereof.

Typical user interfaces for enabling a user to 'log-on' to a mobile device are display 114 and keypad 116, as illustrated in Figure 1b, and touchscreens 104, as illustrated in Figure 1c. The

keypad 116 typically comprises number keys 0-9, a STAR key and a POUND key, while using the touchscreen 104, typically, only 0-9 number buttons 118 are displayed. In field 112 the user is prompted to enter the PIN and is provided with an indicator showing which digits of the PIN have been entered.

5

Current 4digit PINs using a number 0-9 for each digit offer 10^4 or 10,000 unique combinations a user can select. Employing 'upper-case' and 'lower case' numbers 0-9 expands the number of unique combinations available to 20^4 or 160,000. For example, if a user chooses the PIN to be '1234' there is only one combination to enter the PIN when using only a number 0-9 for each digit. Employing 'upper-case' and 'lower case' numbers 0-9, 16 possible combinations are available when using the same numbers in the same order '1234' such as, for example, 'upper case' 1; 'lower case' 2; 'upper case' 3; and, 'lower case' 4.

10

15

The case indicator comprises, for example, pressing/tapping a number 0-9 for the respective digit or pressing/tapping one of a STAR key/button and a POUND key/button followed by pressing/tapping a number 0-9 for the respective digit. For example, PIN 1234 with 1 and 3 being 'upper case' while 2 and 4 being 'lower case' is provided, as illustrated in Figure 2a. Here, 'upper case' is provided by pressing/tapping a 'shift' key, i.e. STAR key or POUND key, once, indicating the following number as 'upper case' number. The sequence of key presses for entering the above PIN is:

20

1. Press the STAR key once;
2. Press the number 1 key (the 'shift' function automatically resets after a number key is pressed);
3. Press the number 2 key;

4. Press the STAR key once;
5. Press the number 3 key; and,
6. Press the number 4 key.

5 The PIN: 'upper case' 1; 'lower case' 2; 'upper case' 3; 'lower case' 4 has now been entered.

'Upper-case' and 'lower case' numbers 0-9 can also be entered using only number buttons 0-9 displayed, for example, on the touch screen 104. For example, a 'lower case' number is indicated by tapping the respective number and an 'upper case' number is indicated by tapping and holding the respective number, with, for example, a 'tapping' event being registered when the respective button 118 on the touch screen 104 is touched for a brief amount of time (for example only, 0.1 – 0.5 seconds) and a 'tapping and holding' event being registered when the touch screen is touched for longer than a "tap event" (for example only, longer than 0.5 seconds).

15

As illustrated in Figure 2b, the sequence of key presses for entering the above PIN is:

1. Tap and hold on number button 1;
2. Tap on number button 2;
3. Tap and hold on number button 3; and
- 20 4. Tap on number button 4.

The PIN: 'upper case' 1; 'lower case' 2; 'upper case' 3; 'lower case' 4 has now been entered.

Alternatively, other case indicators such as, for example, a SHIFT key, may be employed when

available. For example, when implemented on mobile devices having a physical keyboard.

As is evident, employment of 'upper-case' and 'lower case' numbers 0-9 substantially increases security by providing a substantially increased number of possible combinations while enabling
5 users to provide the PIN using a simple familiar procedure and existing user interfaces.

Furthermore, using the combination of the number keys 0-9 with other keys or using tapping/tapping and holding when entering the PIN substantially inhibits recognition of the entered PIN by an un-authorized person visually observing the user entering the PIN.

10 Figures 3a and 3b, illustrate example user input data generated by the controller 106 using four-bit binary values for the digits D1-D4 of the above PIN and a one-bit case indicator with '0' indicating 'lower case' and '1' indicating 'upper case'. In the bit sequence illustrated in Figure 3a each of the case indicators I1-I4 is placed together with the respective digit D1-D4, while in the bit sequence illustrated in Figure 3b the case indicators I1-I4 are placed together followed by
15 the digits D1-D4. As is evident to those skilled in the art, there are numerous other possibilities for generating and processing the user input data as a bit sequence having a case indicator.

Referring to Figure 4, a method for authenticating a personal identification number (PIN) of a user according to a preferred embodiment of the invention is provided. At the user interface 104
20 a sequence of digits and a case indicator indicative of each digit being 'upper-case' or 'lower case' is received - 10. The controller 106 of the user interface 104 determines user input data in dependence upon the received sequence of digits and the received case indicator - 12 - and provides - 14 - the same to the processor/storage device 108. The processor/storage device 108 compares - 16 - the user input data with preregistered user PIN data stored in the storage device

110. The processor/storage device 108 then determines user authentication data – 18 – in dependence upon the comparison. The user authentication data are: indicative of success in authenticating the user if the user input data match the preregistered user PIN data; and indicative of failure in authenticating the user if the user input data do not match the preregistered user PIN data. At 20, the processor/storage device 108 enables/denies access to the mobile device in dependence upon the user authentication data.

The method and system for authenticating a personal identification number (PIN) of a user according to a preferred embodiment of the invention is implementable by adapting existing hardware/software technology for mobile devices.

The present invention has been described herein with regard to preferred embodiments. However, it will be obvious to persons skilled in the art that a number of variations and modifications can be made without departing from the scope of the invention as described herein.

**THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE
PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:**

1. A method for authenticating a personal identification number (PIN) of a user comprising:

5 providing a user interface for entering the PIN;

receiving at the user interface a sequence of digits and a case indicator indicative of each digit
being upper-case or lower case;

determining user input data in dependence upon the received sequence of digits and the received
case indicator;

10 providing the user input data to a processor;

the processor comparing the user input data with preregistered user PIN data; and

the processor determining user authentication data, the user authentication data being:

indicative of success in authenticating the user if the user input data match the
preregistered user PIN data; and

15 indicative of failure in authenticating the user if the user input data do not match the
preregistered user PIN data.

2. The method according to claim 1 wherein the case indicator comprises pressing/tapping the
respective digit or pressing/tapping one of a STAR button and a POUND button followed by
20 pressing/tapping the respective digit.

3. The method according to claim 1 wherein the case indicator comprises tapping the respective
digit or tapping and holding the respective digit.

4. The method according to claim 1 comprising:

enabling access to a mobile device if the user authentication data are indicative of success, the

mobile device comprising the user interface and the processor; and

denying access to the mobile device if the user authentication data are indicative of failure.

5

5. A system for authenticating a personal identification number (PIN) of a user comprising:

a user interface, the user interface being adapted for receiving from the user a sequence of digits

and a case indicator indicative of each digit being upper-case or lower case and for providing

user input data in dependence thereupon;

10

a storage device having stored therein preregistered user PIN data; and

a processor connected to the user interface and the storage device, the processor for performing:

receiving the user input data;

comparing the user input data with the preregistered user PIN data; and

determining user authentication data, the user authentication data being:

15

indicative of success in authenticating the user if the user input data match the

preregistered user PIN data; and

indicative of failure in authenticating the user if the user input data do not match

the preregistered user PIN data.

20

6. The system according to claim 5 wherein the user interface comprises a keypad.

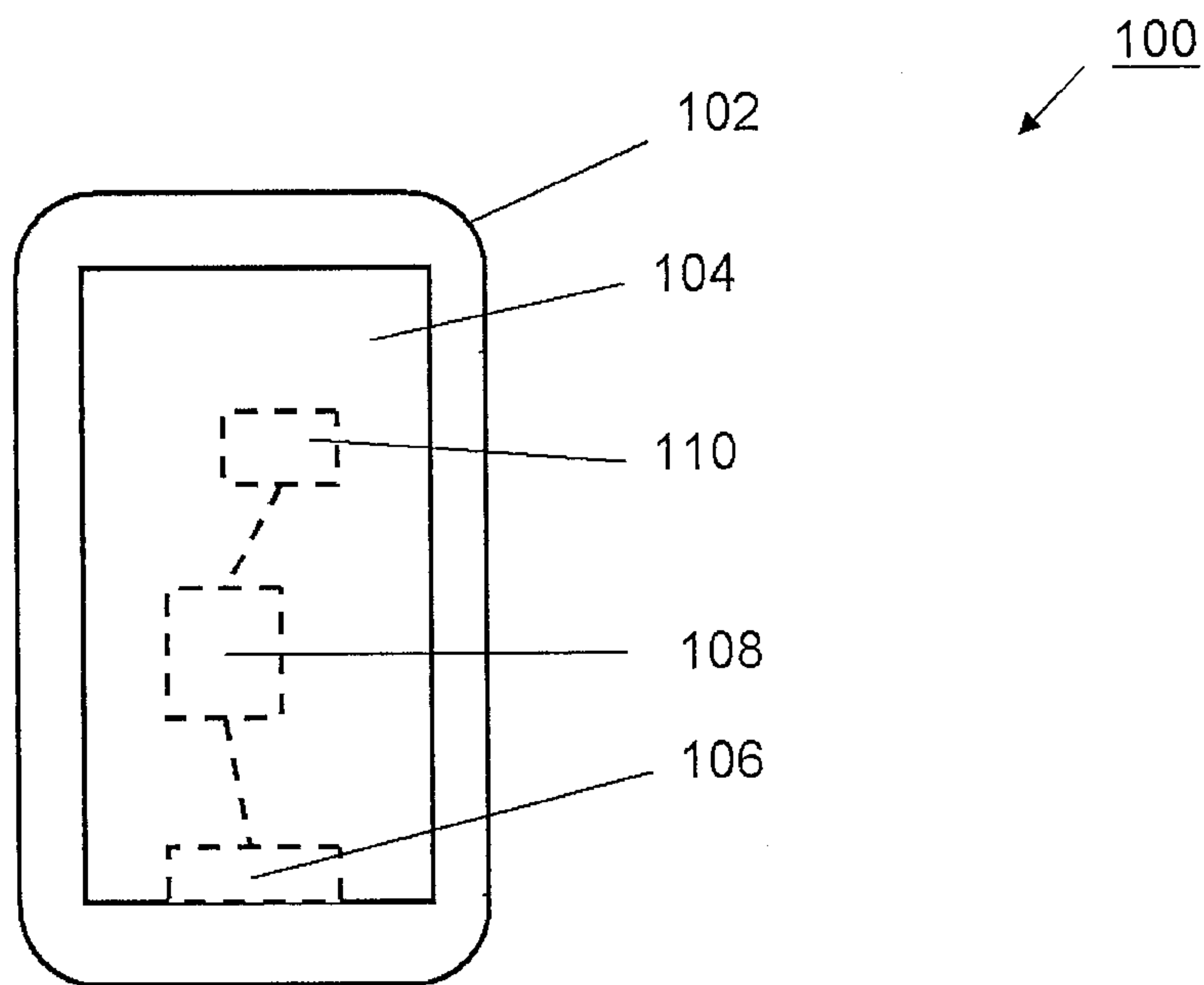
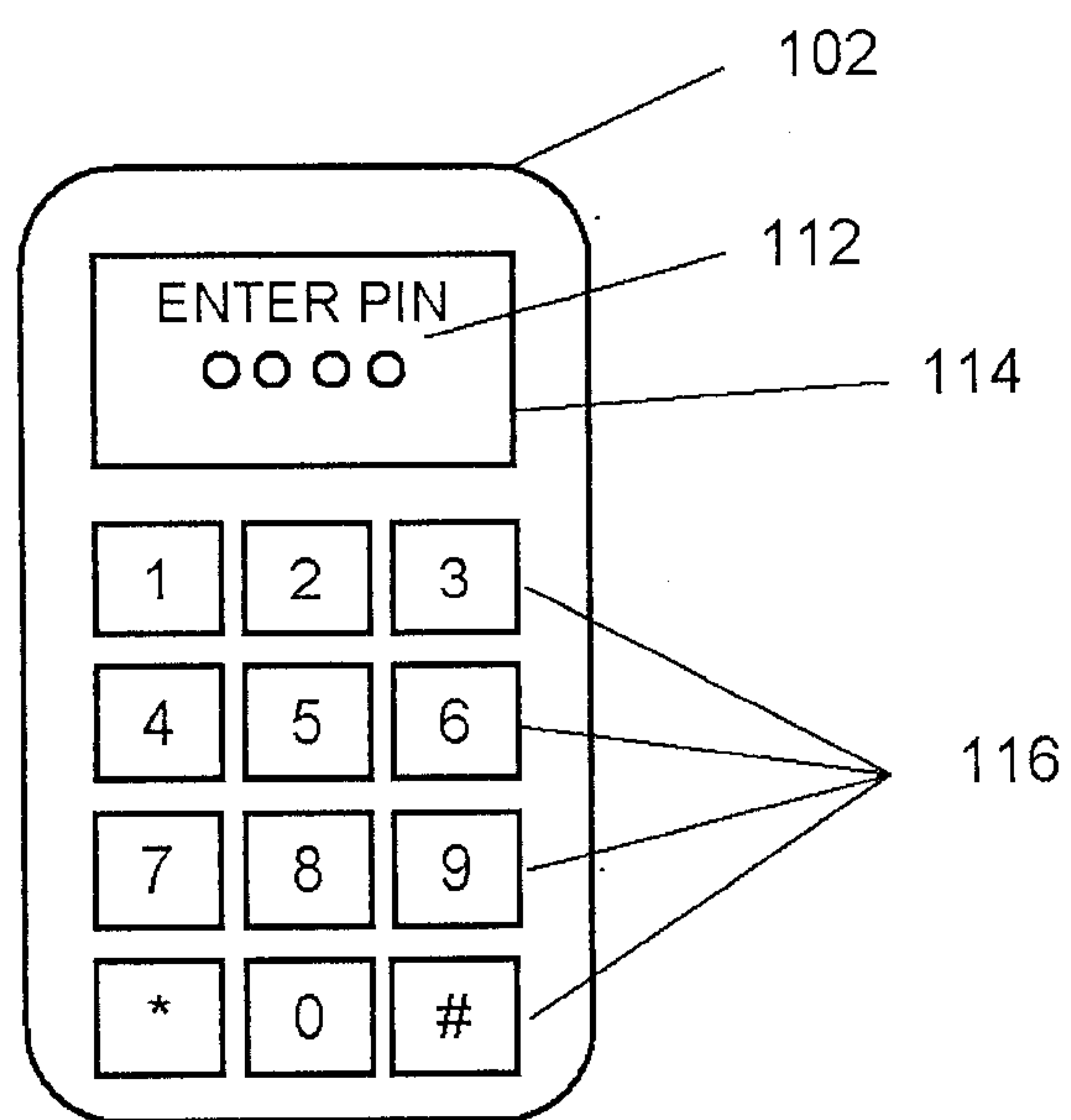
7. The system according to claim 5 wherein the user interface comprises a touchscreen.

8. The system according to claim 5 wherein the user interface, the storage device, and the

processor are adapted for:

enabling access to a mobile device if the user authentication data are indicative of success; and

denying access to the mobile device if the user authentication data are indicative of failure.

**Figure 1a****Figure 1b**

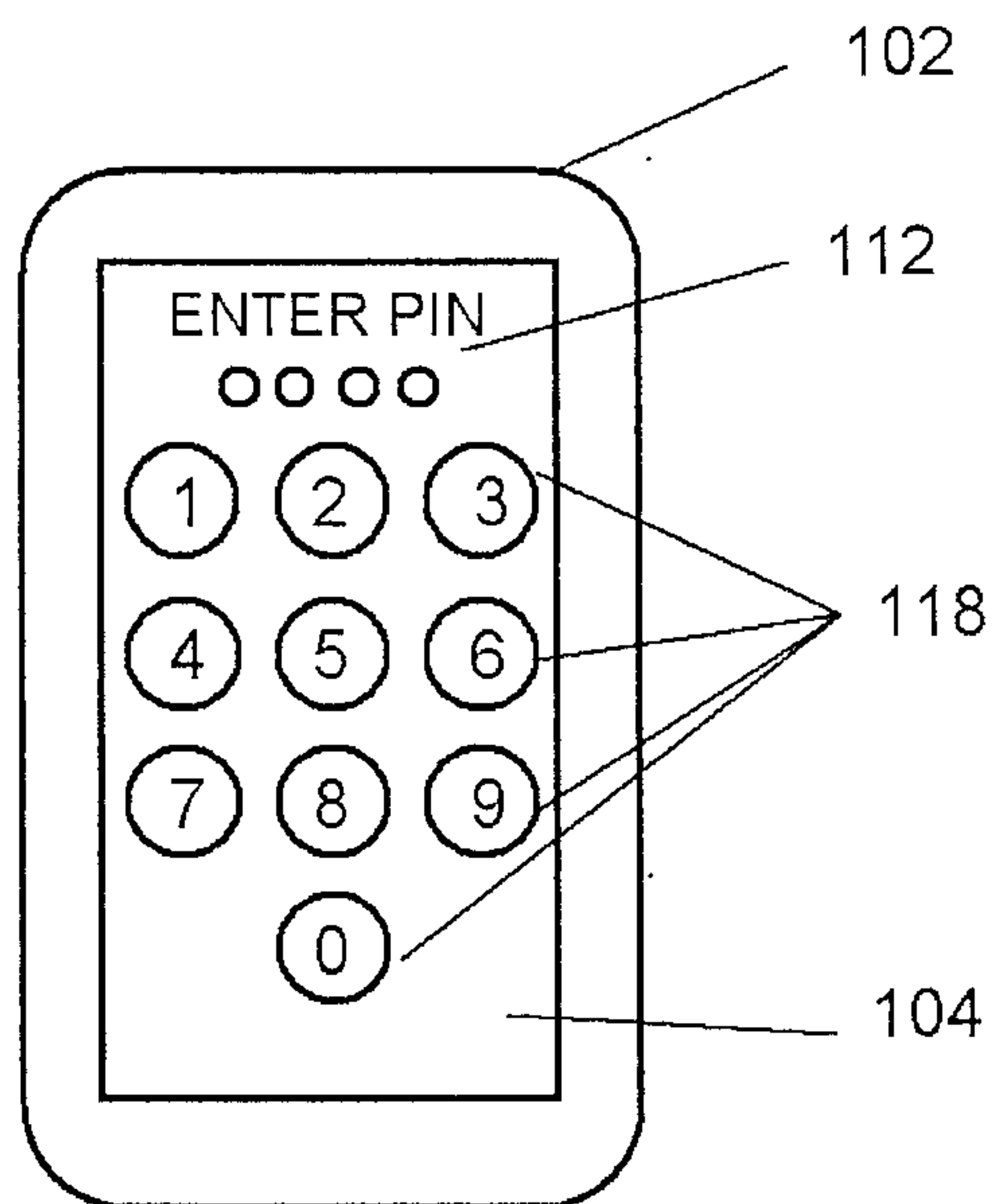


Figure 1c

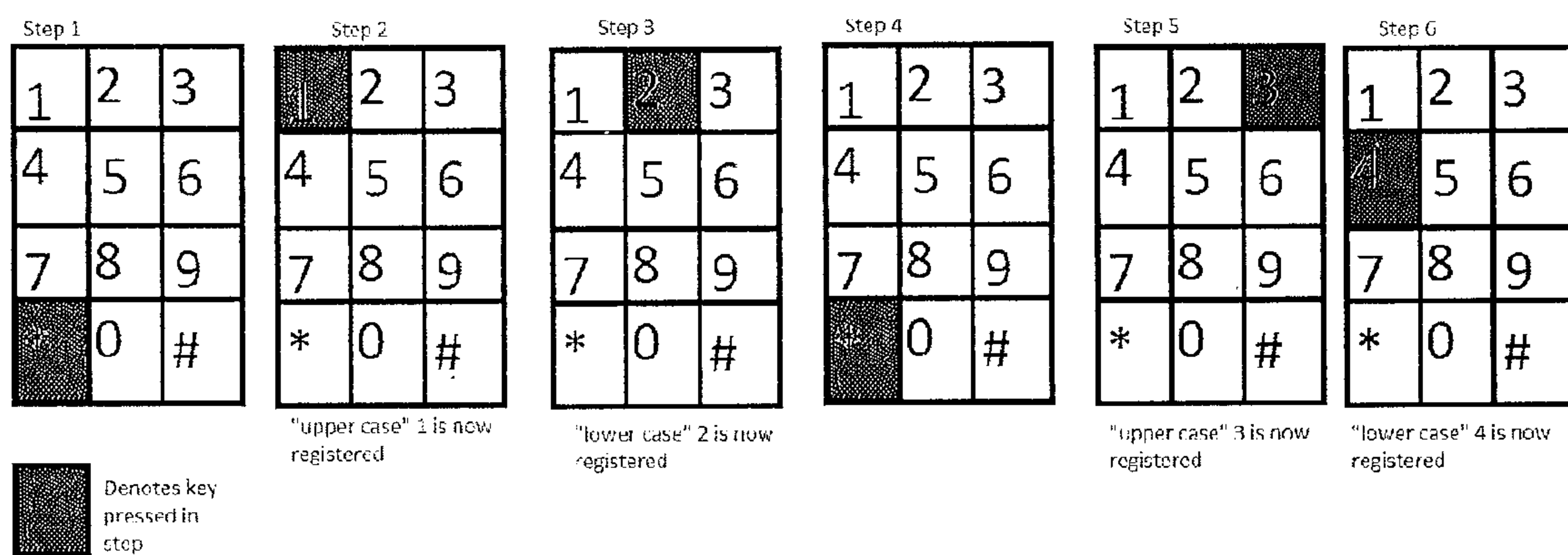
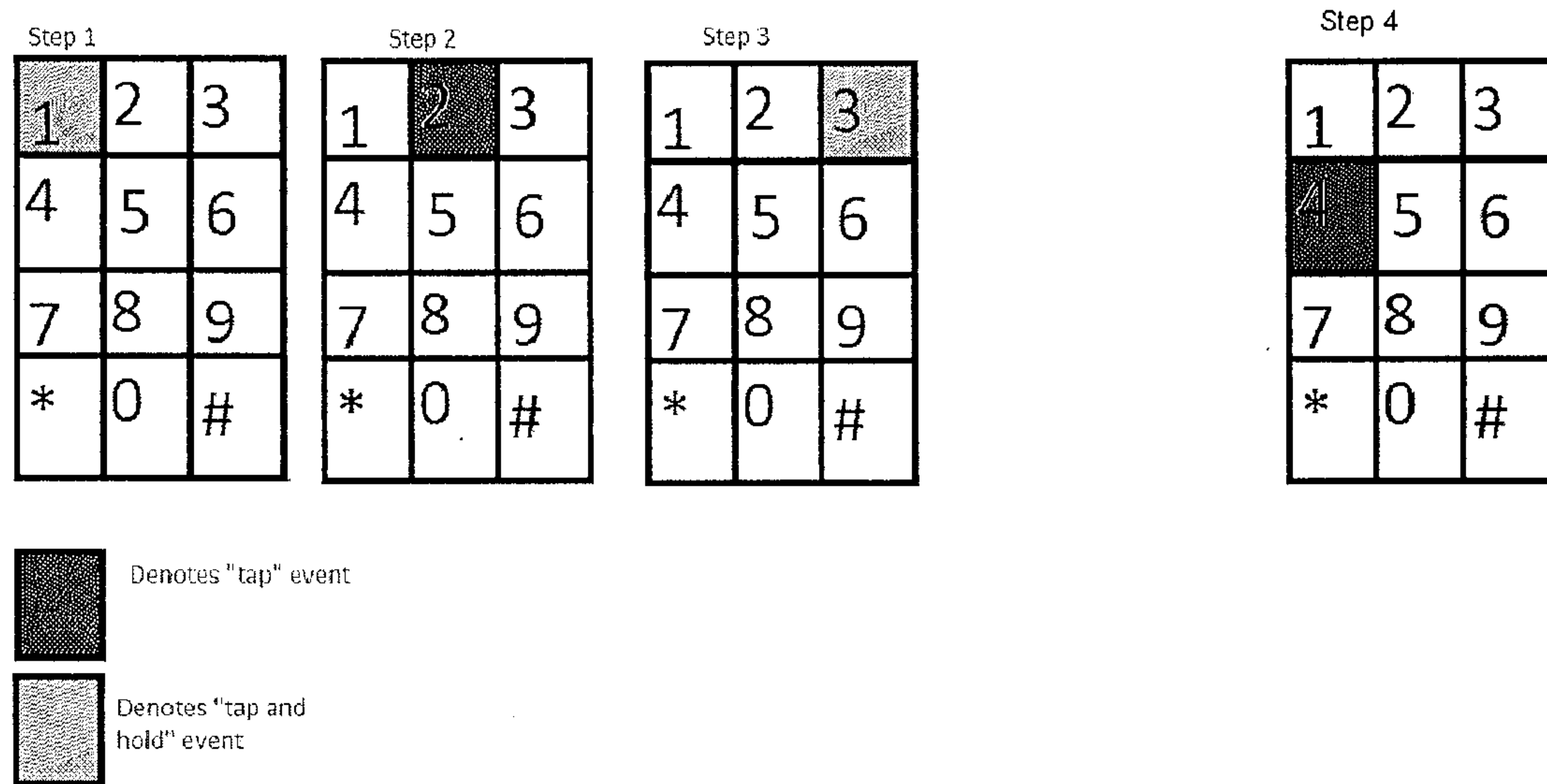
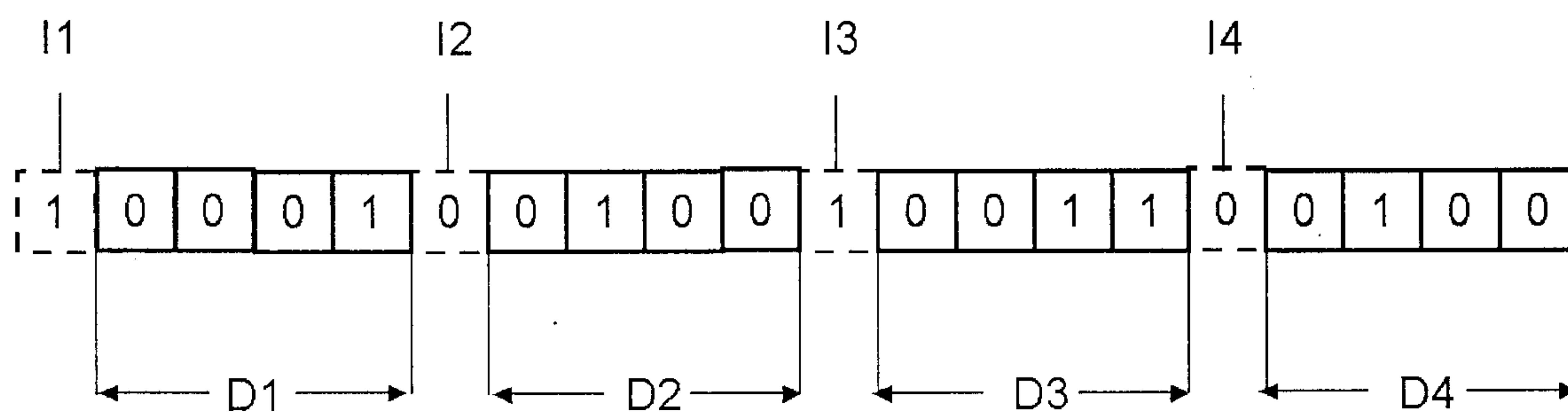
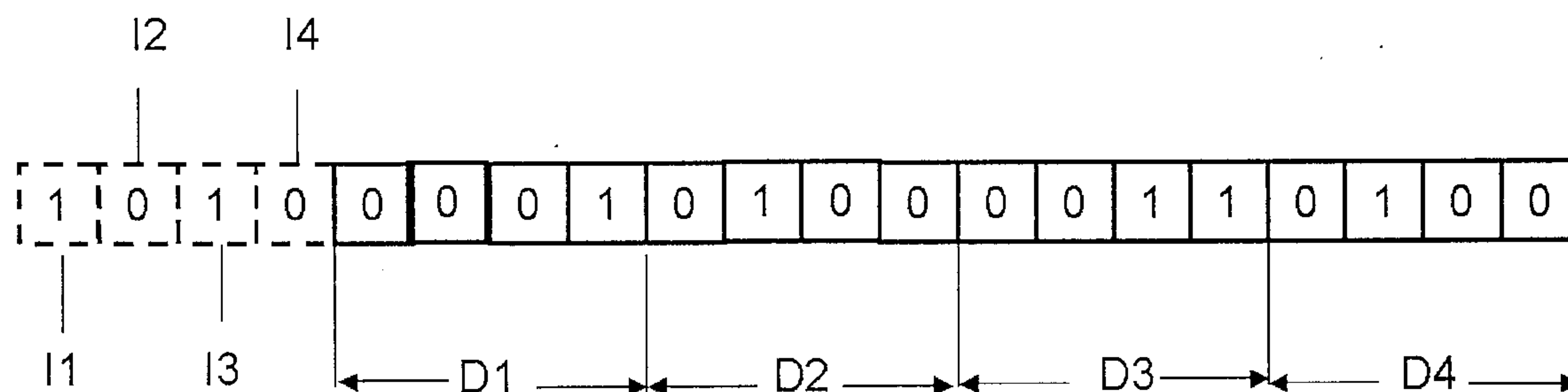
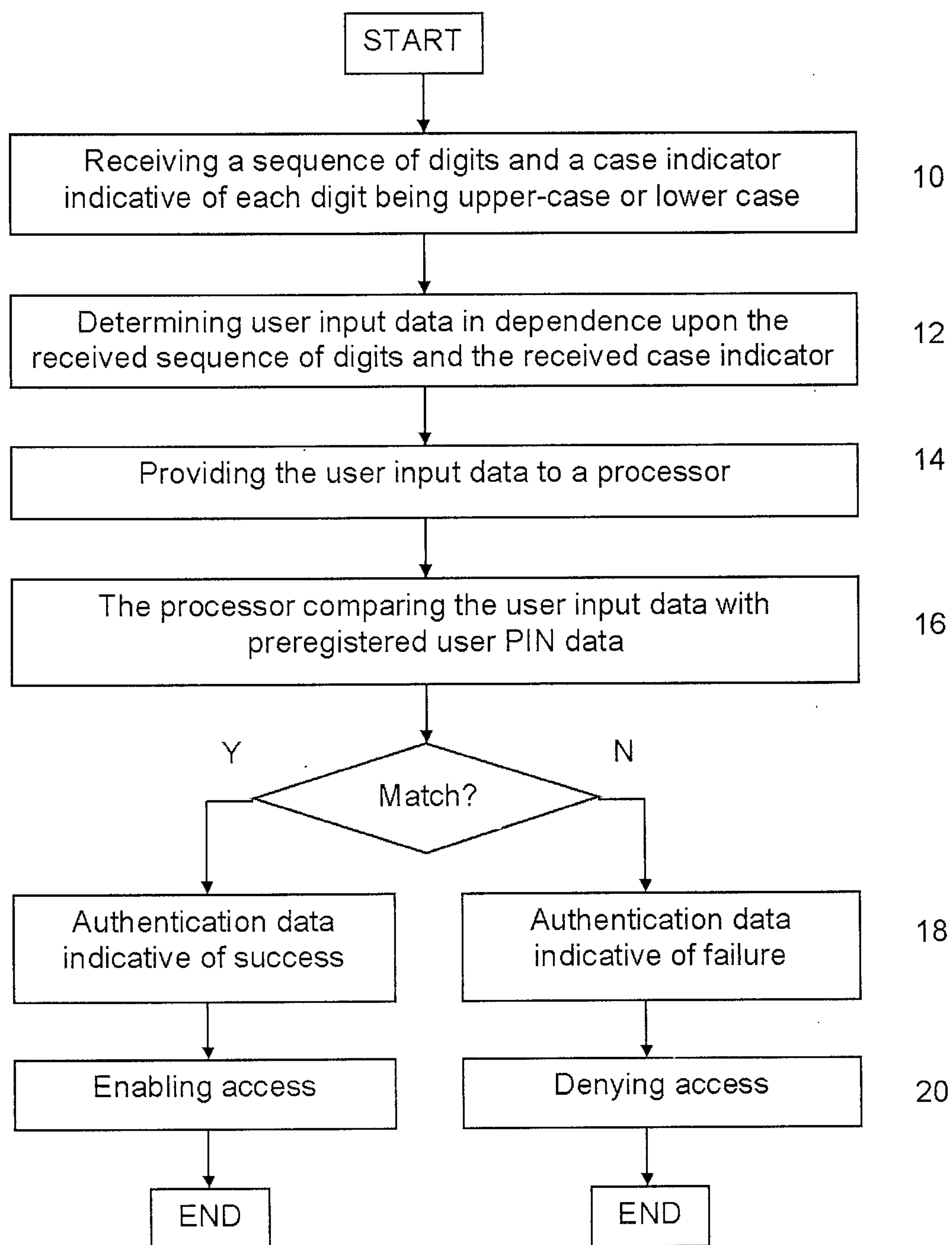


Figure 2a

**Figure 2b****Figure 3a****Figure 3b**

**Figure 4**

