A Portable Device Having Biometrics-Based Authentication Capabilities

The present invention relates to a portable device, and in particular, a portable data storage and access control device having biometrics-based authentication capabilities.

Portable data storage devices have become a class of indispensable peripherals that are widely utilized in business, educational and home computing. These devices are generally not permanently fitted to a particular host platform, such as a personal computer (PC). Rather, they can be conveniently removed from and attached to any computer having the appropriate connection port (e.g., a serial bus port like a USB port, an IEEE 1394 ("Firewire") port). Thus, these portable data storage devices enable a user to transfer data among different computers that are not otherwise connected. A popular type of portable storage device utilizes a non-volatile solid-state memory (e.g., flash memory) as the storage medium and so does not require moving parts or a mechanical drive mechanism for accessing the data. The absence of a drive mechanism enables these portable solid-state memory devices to be more compact than surface storage devices such as magnetic disks and CD-ROMs.

As portable storage devices become more widely used in various institutional and personal computing environments, preventing unauthorized users from accessing information stored on a portable or designated storage media is one of the most significant challenges in information technology today. For example, to secure confidential business information, personal information like medical and financial or other types of sensitive data, it is essential to have a reliable security measure that is simple to use, convenient and provides a level of protection appropriate for the type of information to be secured.

To date, most portable storage devices have resorted to user passwords as a security measure for protecting against unauthorized data access. While the use of passwords as an authentication mechanism provides some level of protection against unauthorized access, it is often regarded by users as cumbersome and inconvenient due to the need to remember the password and to key it in every time the user requests access. In many systems, a user is also

required to periodically change his/her password as an added level of security. This further adds to the inconvenience. Moreover, since a typical user generally needs access to several computer systems and/or networks requiring access control, the user may have to memorize numerous different passwords because they are not necessarily identical on the different systems. Thus, it would be advantageous to provide a reliable authentication mechanism for preventing unauthorized access to information stored on a portable or designated storage media that is not cumbersome or inconvenient for the user.

In addition, passwords are not unique among different users and are also subject to hacking by many skilled hackers. Once a password has been compromised, whether by inadvertent disclosure by a bona fide user to an unauthorized party or by malicious hacking, confidential data that is supposed to be password-protected are no longer guarded. Indeed, unauthorized access to such information may go unnoticed for extended periods of time. Ongoing intrusions usually remains undeterred until the victimized user finally realizes that the data has been accessed and/or destroyed, or until the system administrator detects a pattern of suspicious activities. Therefore, it would also be advantageous to provide a secured access control mechanism for protection against unauthorized access to data stored in portable storage media and various computer systems which is not easily compromised by hacking and preferably provides a unique "access key" for each individual user.

Accordingly, the present invention provides a method and system which delivers a highly reliable and user-friendly authentication mechanism for preventing unauthorized access to information stored on a portable or designated storage media. Furthermore, embodiments of the present invention also provide a highly secure access control mechanism for protection against unauthorized access to stored data and computer resources as well as guarding against unauthorized entry to premises. Aspects of the present invention, which utilizes a unique biometrics marker as a basis for identity authentication and as an "access key" for each individual user, are described in detail herein.

Specifically, a preferred embodiment of the present invention provides a portable device which includes a microprocessor, a non-volatile memory coupled

thereto, and a biometrics-based authentication module controlled by the microprocessor. Preferably, the biometrics technology used is fingerprint authentication technology, and flash memory is used as the non-volatile memory. In this embodiment, the fingerprint authentication module automatically prompts the user to register his/her fingerprint with the portable device upon its first use. In a currently preferred embodiment, a compact and encrypted version of the fingerprint is stored in the portable device's flash memory when the registration process is completed. Upon a subsequent use, the fingerprint authentication module reads the user's fingerprint, compares it with the registered fingerprint stored in the flash memory and reliably determines whether there is a match between the two. If a match is identified, authentication of the user's identity is successful, and the authenticated user is granted access to the restricted resource, the access to which is being safeguarded using the present access control system. On the other hand, if a match cannot be found between the user's fingerprint and the registered fingerprint, access to the restricted resource is denied. As such, this embodiment of the present invention delivers a highly convenient, secured and reliable system for user authentication and access control which is superior to password-based authentication approaches in prior art. The present invention appreciates that fingerprints, being unique signatures for an individual, have been legally and universally accepted for verifying identity for over a century, that they cannot be forgotten by a user, as passwords could, and further that they are almost impossible to alter, duplicate, or crack by hacking. As such, fingerprints and other biometrics-based techniques are well-suited for use as an authentication and/or access control solution, as embodied in the present invention.

Advantages of the invention will be set forth, in part, in the description that follows and, in part, will be understood by those skilled in the art from the description herein.

The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate several embodiments of the invention and, together with the description, serves to explain the principles of the invention.

Figure 1A is a block diagram illustrating functional blocks of one embodiment of the portable device of the present invention and an illustrative operational configuration thereof.

Figure 1B is a block diagram illustrating functional blocks of another embodiment of the portable device of the present invention.

Figure 2 is a front perspective view of a portable device with an integrated fingerprint module in accordance with one embodiment of the present invention.

Figure 3 is a rear perspective view of the portable device with an integrated fingerprint module as shown in Figure 2.

Figure 4 is a bottom plan view of the portable device with an integrated fingerprint module as shown in Figure 2.

Figure 5 is a top plan view of the portable device with an integrated fingerprint module as shown in Figure 2.

Figure 6 is a left side elevation view of the portable device with an integrated fingerprint module as shown in Figure 2.

Figure 7 is a right side elevation view of the portable device with an integrated fingerprint module as shown in Figure 2.

Figure 8 is a front elevation view of the portable device with an integrated fingerprint module as shown in Figure 2.

Figure 9 is a rear elevation view of the portable device with an integrated fingerprint module as shown in Figure 2.

Figure 10 is a flow diagram illustrating steps of a user registration/authentication process using a portable device in accordance with one embodiment of the present invention.

Figures 11(a) and 11(b) are rear perspective views of a second portable device according to an embodiment of the invention;

Figure 12 is a top plan view of the second portable device with an integrated fingerprint module as shown in Figures 11(a) and 11(b);

Figure 13 is a bottom plan view of the second portable device with an integrated fingerprint module as shown in Figures 11(a) and 11(b);

Figure 14 is a left side view of the second portable device with an integrated fingerprint module as shown in Figures 11(a) and 11(b);

Figure 15 is a right side view of the second portable device with an integrated fingerprint module as shown in Figures 11(a) and 11(b);

Figure 16 is a front elevation view of the second portable device with an integrated fingerprint module as shown in Figures 11(a) and 11(b);

Figure 17 is a rear elevation view of the second portable device with an integrated fingerprint module as shown in Figures 11(a) and 11(b).

The present invention now will be described more fully with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. The present invention may, however, be embodied in many different forms and should not be construed as being limited to the embodiments set forth herein; rather these embodiments are provided so that this disclosure will be thorough and complete and will fully convey the invention to those skilled in the art. Indeed, the invention is intended to cover alternatives, modifications and equivalents of these embodiments, which will be included within the scope and spirit of the invention as defined by the appended claims. Furthermore, in the following detailed description of the present invention, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be clear to those of ordinary skill in the art that the present invention may be practiced without such specific details. In other instances, well known methods, procedures, components, and circuits have not been described in detail as not to unnecessarily obscure aspects of the present invention.

Figure 1A is a block diagram illustrating functional blocks of one embodiment of the portable device of the present invention and an illustrative operational configuration thereof. Figure 1A shows a portable device 70 coupled to a host platform 90. In this embodiment, host platform 90 is coupled to a power supply circuit 80 located in portable device 70. Power supply circuit 80 draws power from host platform 90 and serves as a power source for various components of portable device 70.

Referring still to Figure 1A, portable device 70 further includes an integrated circuit 10, a flash memory 20, a volatile memory 30 and a fingerprint module 50. Integrated circuit 10 can be conveniently implemented as an

application-specific integrated circuit (ASIC). In a currently preferred embodiment, flash memory 20 can have a storage capacity between 8 MB and 512 MB, a portion of which can be used to store one or more templates generated in accordance with the present invention as described below. Moreover, in a preferred embodiment, the template(s) are stored in a reserved area of flash memory 20 which is specifically designated for this purpose and which is not otherwise accessible to the user. Additionally, as described in detail further below, a template is encrypted before it is stored in flash memory 20 in a currently preferred embodiment, thereby providing added security against hacking. In one embodiment, volatile memory 30 is external to integrated circuit 10 and can comprise either a dynamic random access memory (DRAM) or a static random access memory (SRAM). Among other uses, volatile memory 30 can serve as an initial storage and staging area for a fingerprint image captured in accordance with the present invention.

Integrated circuit 10 comprises a microprocessor 11 which, in one embodiment, is a RISC processor. In a currently preferred embodiment, an authentication engine 12 is included in integrated circuit 10. Authentication engine 12 in turns comprises a template generator 12a and a verification module 12b. Template generator 12a is used to generate an encoded version of an image of a fingerprint. Within the scope of the present invention, such an encoded fingerprint image is referred to as a template. It should be appreciated that according to current biometrics technology, a fingerprint can be uniquely identified using between 8 and 13 distinct points in the raw image of the fingerprint. Fingerprint information can thus be conveniently stored in a condensed fashion as data pertaining to the 8 to 13 relevant data points. A preferred embodiment of the present invention advantageously stores a fingerprint in a compact format as a template referred to above. In this embodiment, a template has a size of 512 bytes. Other embodiments can use templates of different sizes. The other component of authentication engine 12, verification module 12b, is used to compare a newly generated template against a stored template to validate the authenticity of a fingerprint provided by someone purporting to be an authorized user. Thus, authentication engine 12 works in conjunction with fingerprint module

50, described in greater detail below, to implement user authentication in accordance with the present invention.

It should be appreciated that authentication engine 12 is well-adapted to numerous implementations within the scope of the present invention. In one embodiment, authentication engine 12 is implemented as firmware stored in a non-volatile memory within portable device 70. In another embodiment, authentication engine 12 is implemented as part of microprocessor 11. In still another embodiment, authentication engine 12 is implemented as a processor separate from microprocessor 11. In yet another embodiment, authentication engine 12 includes the same components and serves the same functions as described herein, but is located in host platform 90 rather than in portable device 70. In other words, within the scope of the present invention, authentication engine 12 is not required to reside in portable device 70. Instead, where authentication engine 12 is to be placed is a design choice, thus affording design flexibility to suit different applications in which the present invention can be utilized.

Referring still to Figure 1A, in a preferred embodiment, integrated circuit 10 also comprises a bus interface 13 which facilitates communication between integrated circuit 10 and other components, such as volatile memory 30. Integrated circuit 10 further includes a flash controller 14 for controlling access to flash memory 20. In one embodiment, upon the successful generation of a template during user registration, flash controller 14 communicates with template generator 12a to store the newly generated template into flash memory 20 for use in subsequent user authentication. Moreover, in a currently preferred embodiment, portable device 70 is compatible with the universal serial bus (USB) standard and includes a USB connector (not shown). In this embodiment, integrated circuit 10 also includes a USB device controller 15, which serves to control the communication between portable device 70 and host platform 90, such as a USB-compatible personal computer (PC) having a USB host controller 93 therein.

With reference still to Figure 1A, integrated circuit 10 also includes a volatile memory 16 and a non-volatile memory 17. In a preferred embodiment, volatile

memory 16 is a random access memory (RAM) that serves as a working memory for microprocessor 11 during its operation. Non-volatile memory 17 is a read-only memory (ROM) in this embodiment and can be used to store firmware that perform various functions of portable device 70. Additionally, integrated circuit 10 includes an optional error checking (ECC) engine 19 for performing various error checking tasks during the operation of portable device 70. It should be appreciated that ECC engine 19, like authentication engine 12, is well-suited to numerous implementations within the scope of the present invention. For example, ECC engine 19 can be implemented by software (e.g., firmware stored in a non-volatile memory), as part of microprocessor 11, or as a processor unit separate from microprocessor 11.

Referring again to Figure 1A, fingerprint module 50 comprises a sensor 52 which is used to capture the fingerprint image of a finger being placed thereon. Fingerprint module 50 also comprises a converter 54, which serves to convert a captured fingerprint image into electrical signals representing the image. In a currently preferred embodiment, a fingerprint print image is converted into 64 KB of data by converter 54 and sent to volatile memory 30 of portable device 70 for temporary storage. In other embodiments, converter 54 can produce image data of different sizes. Fingerprint module 50 further includes an optional control unit 56 which, in a currently preferred embodiment, is controlled via microprocessor 11 in portable device 70 and is used for checking the quality of fingerprint images captured by sensor 52 to determine whether a given image is acceptable or not. As described in more detail below, if it is determined that the quality of a captured image is unacceptable, the user will be prompted to place his/her finger on sensor 52 again so that a new image can be captured.

Reference is now made to Figure 1B, which is a block diagram illustrating functional blocks of another embodiment of the portable device of the present invention. In this embodiment, portable device 170 is compatible with the USB standard and includes a USB plug 118 which, as Figure 1B shows, is coupled to a USB host controller 193 of a host platform. Optionally, portable device 170 further includes an additional USB port 162 that is coupled to USB plug 118. USB port 162 is provided as a convenient feature that can be used to couple other USB-

compatible device(s) to the USB via portable device 170. In this embodiment, portable device 170 also includes a USB device controller 115 for controlling the communication between portable device 170 and the host platform via USB host controller 193. In one embodiment, a driver software 177 and an application programming interface (API) 197, which in turn includes monitoring software 199, reside in the host platform and communicate with USB host controller 193 to facilitate the operation of portable device 170.

Portable device 170 further comprises an integrated circuit 110, a flash memory 120 and a volatile memory 130. Integrated circuit 110 can be conveniently implemented as an ASIC. In a preferred embodiment, a reserved area 122 of flash memory 120 is used to store one or more templates generated in accordance with the present invention. Furthermore, in this embodiment, reserved flash memory area 122 includes a status flag 121 which indicates whether or not portable device 170 has been previously registered in accordance with the present invention. Status flag 121 thus enables portable device 170 to automatically invoke a registration process upon its initial use, as described in detail further below. In one embodiment, volatile memory 130 comprises either a DRAM or a SRAM, which serves as an initial storage area for a fingerprint image captured in accordance with the present invention.

Referring still to Figure 1B, integrated circuit 110 comprises a microprocessor 111 which preferably is a RISC processor. Integrated circuit 110 further includes a flash controller 114 for controlling access to flash memory 120 and a memory controller 133 for controlling access to volatile memory 130. Integrated circuit 110 also includes a volatile memory 116 and a non-volatile memory 117. Preferably, volatile memory 116 comprises a RAM for use as a working memory for microprocessor 111 during its operation, while non-volatile memory 117 comprises a ROM for storing firmware that perform various functions of portable device 170. Specifically, in one embodiment, ROM 117 stores the following firmware code: firmware 117a for reading fingerprint sensor 152, firmware 117b for processing fingerprint images, firmware 117c for generating templates, firmware 117d for encrypting fingerprint images and/or templates, and firmware 117e for verifying fingerprint authenticity. Nevertheless, it should be

appreciated that in an alternative embodiment of the present invention, such firmware can be stored in a non-volatile memory within the host platform rather than in portable device 170.

Additionally, integrated circuit 110 includes an optional error checking (ECC) engine 119 for performing various error checking tasks during the operation of portable device 170. It should be appreciated that ECC engine 119 can be implemented as software (e.g., firmware) or hardware (e.g., processor/processor module) within the scope of the present invention.

Referring still to Figure 1B, fingerprint module 150 comprises a sensor 152, a converter 154 and an optional controller 156. In this embodiment, sensor 152 is used to capture the fingerprint image of a finger being placed thereon, converter 154 serves to convert a captured fingerprint image into electrical signals representing the image, and optional controller 156 is used to check the quality of fingerprint images captured by sensor 152 to determine whether a given image is acceptable or not. It should be appreciated that such image processing capabilities can be implemented using software (e.g., firmware) or hardware (e.g., processor/processor module) within the scope of the present invention.

In a currently preferred embodiment as illustrated in Figure 1B, microprocessor 111 controls various components of portable device 170, including flash controller 114, USB device controller 115, RAM 116, ROM 117 (and execution of firmware code stored therein), ECC engine 119, memory controller 133, and controller 156 of fingerprint module 150. In this embodiment, portable device 170 also includes a write-protection switch 140 which, when activated, triggers microprocessor 111 to disable write-access to flash memory 120.

With reference next to Figure 2, a front perspective view of a first form of a portable device with an integrated fingerprint module in accordance with one embodiment of the present invention is shown. In Figure 2, portable device 70 is shown with USB connector 18 protruding from its front end. Fingerprint module 50 is shown as being structurally integrated with portable device 70 in a unitary construction, with sensor 52 disposed on the top side of portable device 70. A light emitting diode (LED) 73 is also shown disposed near the edge of the top side of portable device 70. In one embodiment, LED 73 flashes when data in portable

device is being accessed, thus serving as an activity indicator. In another embodiment, LED 73 lights up to indicate that an authentication process is underway.

Referring next to Figure 3, a rear perspective view of the portable device with an integrated fingerprint module as depicted in Figure 2 is shown. Again, portable device 70 is shown with USB connector 18 protruding from its front end, and fingerprint module 50 is shown as being structurally integrated with portable device 70 in a unitary construction, with sensor 52 disposed on the top side thereof. LED 73 is again shown disposed near the edge of the top side of portable device 70. Optional write protection switch 40 is also shown as being located at the rear end of portable device 70.

Reference is now made to Figure 4, which shows a bottom plan view of the portable device with an integrated fingerprint module as illustrated in Figure 2. A substantially semicircular indentation 77, an optional feature which allows a user to hold portable device 70 firmly while coupling or decoupling portable device 70 to/from host platform 90 (Figure 1A), is shown on the bottom side of portable device 70 in Figure 4. USB connector 18 is also shown.

Referring next to Figure 5, a top plan view of the portable device with an integrated fingerprint module as shown in Figure 2 is depicted. Portable device 70 is shown with USB connector 18 protruding from its front end, and fingerprint module 50 is shown as being structurally integrated with portable device 70 in a unitary construction, with sensor 52 disposed on the top side thereof. LED 73 is again shown disposed near the edge of the top side of portable device 70.

Reference is now made to Figure 6, which is a left side elevation view of the portable device with an integrated fingerprint module as shown in Figure 2. USB connector 18 is shown protruding from the front of portable device 70, and the periphery of sensor 52 is shown slightly raised from the top side of portable device 70.

Next, Figure 7 is a right side elevation view of the portable device with an integrated fingerprint module as shown in Figure 2. Once again, USB connector 18 is shown protruding from the front of portable device 70, and the periphery of sensor 52 is shown slightly raised from the top side of portable device 70.

Referring next to Figure 8, a front elevation view of the portable device with an integrated fingerprint module as shown in Figure 2 is depicted. The insertion end of USB connector 18 is centrally depicted, and the periphery of sensor 52 is shown slightly raised from the top side of portable device 70.

Reference is now made to Figure 9, which is a rear elevation view of the portable device with an integrated fingerprint module as shown in Figure 2. The periphery of sensor 52 is shown slightly raised from the top side of portable device 70, and optional indentation 77 on the bottom side of portable device 70 is also visible. Optional write protection switch 40 is also shown as being located at the rear end of portable device 70.

With reference next to Figure 11(a), a first rear perspective view of a second portable device 370 with an integrated fingerprint module in accordance with one embodiment of the present invention is shown. The electronic construction of the device 370 is identical with that of the device 70 (and hence many of the reference numerals used in Fig. 11(a) are similar to those used in Figure 2 but higher by 300), but, apart from an different external shape, it has two additional features. Firstly, there is a cover 300 which slidably covers a sensor 352. The cover 300 is shown in the closed position in Figure 11(a), and Figure 11(b) is a second rear perspective view of the portable device 370 shown in Figure 11(a), but with the cover 300 in an open configuration. Secondly, the sensor 352 is rotatable during the operation of sensing a fingerprint, so as to make a rolling contact with the finger. The second form of the second portable device 370 is described in more detail as follows.

In Figures 11(a) and 11(b), the portable device 370 is shown with USB connector 318 protruding from its front end. Fingerprint module 350 is shown as being structurally integrated with portable device 370 in a unitary construction, with sensor 352 (shown in Figure 11(b)) disposed on the top side of portable device 370. A light emitting diode (LED) 373 is also shown disposed on the rear side of portable device 370. In one embodiment, LED 373 flashes when data in portable device is being accessed, thus serving as an activity indicator. In another embodiment, LED 373 lights up to indicate that an authentication process is underway.

The cover 300 is provided as a plate supported for sliding in the plane of the top surface of the portable device 372 by L-shaped guides 400 projecting from the upper surface of the portable device 370. The cover 300 is provided with finger engagement means (e.g. grooves) 450 so that a user can slide it between a first position (Figure 11(a)) in which the cover 300 covers and protects the sensor 352, and a second position (Figure 11(b)) in which it does not.

Optional write protection switch 340 is also shown as being located at the rear end of portable device 370.

Referring next to Figure 12, a top plan view of the portable device with an integrated fingerprint module as shown in Figures 11(a) and 11(b) is depicted. Portable device 370 is shown with USB connector 318 protruding from its front end, and fingerprint module 350 is shown as being structurally integrated with portable device 370 in a unitary construction, with sensor 52 disposed on the top side thereof. The cover 300 is the open configuration of Figure 11(b).

Reference is now made to Figure 13, which shows a bottom plan view of the portable device with an integrated fingerprint module as illustrated in Figures 11(a) and11(b). A substantially semicircular indentation 377, an optional feature which allows a user to hold portable device 370 firmly while coupling or decoupling portable device 370 to/from host platform 90 (Figure 1A), is shown on the bottom side of portable device 370 in Figure 13. USB connector 318 is also shown.

Reference is now made to Figure 14, which is a left side elevation view of the portable device with an integrated fingerprint module as shown in Figures 11(a) and11(b). USB connector 318 is shown protruding from the front of portable device 370, and the cover 300 and guides 400 are shown slightly raised from the top side of portable device 370.

Next, Figure 15 is a right side elevation view of the portable device with an integrated fingerprint module as shown in Figures 11(a) and 11(b). Once again, USB connector 318 is shown protruding from the front of portable device 370, and the cover 300 and guides 400 are shown slightly raised from the top side of portable device 370.

Referring next to Figure 16, a front elevation view of the portable device 370 with an integrated fingerprint module as shown in Figures 11(a) and 11(b) is

depicted. The insertion end of USB connector 318 is centrally depicted, and the cover 300 and guides 400 are shown slightly raised from the top side of portable device 370.

Reference is now made to Figure 17, which is a rear elevation view of the portable device with an integrated fingerprint module as shown in Figures 11(a) and 11(b). The cover 300 and guides 400 are shown slightly raised from the top side of portable device 370. Optional write protection switch 340 is also shown as being located at the rear end of portable device 370.

As mentioned above, a significant difference between the first form of the portable device 70 and the second form of the portable device 370, is that the sensor 352 of the second form of the portable device 370 is provided as a cylinder having its axis lying parallel to both the top surface and the rear surface of the device 370. In other words, this axis extends through the device 370, sandwiched between its bottom and top surfaces, from left to right.

The sensor 352 is designed to be rotatable around its axis (either fully rotatable, or rotatable within a defined angular range). At times when the cover 300 is open, a portion of the cylindrical surface sensor 352 is uppermost, and is exposed through an opening in the housing of the portable device 370, but this portion varies as the sensor 352 is rotated. When the user comes to use the device, he first opens the cover 300 (thereby exposing a portion of the cylindrical surface of the sensor 352) and then rolls his finger (or thumb) on the cylindrical surface of the sensor 352, causing it to rotate and to bring successively new portions of the cylindrical surface into the exposed region. In this way the user is able to contact the sensor 352 with a larger area of his finger in total than the area of the cylindrical surface which is exposed at any one moment.

An advantage of this feature is that, even though the proportion of the top surface of the portable device 370 which is occupied by the sensor 352 remains approximately as in the device 70 of Figure 2, the sensor 352 is capable (in a single sensing operation) of sensing larger areas on fingers than the sensor 52. The present inventors have found that this is a useful feature, meaning that a single device can be operated by individuals whose fingerprints are of greatly differing sizes, e.g. individuals of different races.

Referring next to Figure 10, a flow diagram 200 illustrating steps of a user registration/authentication process using either a device 70 of the first form or device 370 of the second form with an integrated fingerprint module in accordance with one embodiment of the present invention is shown. In the following description, various modules and components referred to have been described above with reference to Figure 1A using the same reference numerals. In step 210, upon being coupled to a host platform, portable device 70, 370 undergoes an initialization procedure. In a currently preferred embodiment, the initialization procedure involves establishing communication with the host platform and ensuring the host platform is aware that portable device 70, 370 has been coupled thereto.

In step 220, portable device 70, 370 determines whether a user registration is necessary. For example, if portable device 70, 370 is being used for the first time and no template has yet been stored in flash memory 20, portable device 70, 370 will guide the user to complete a registration process (steps 225, 235, 245 and 255 as described below) via a user interface (e.g., pop-up message windows) through the host platform. Thus, upon the first use of portable device 70, 370 (e.g., immediately after purchase), a preferred embodiment automatically initiate the registration process to generate the first ("master") template. This is preferably accomplished by checking a status flag (e.g., flag 121 in flash memory 120 of Figure 1B). Subsequent registration(s), as described below, can be activated by individual users via software on the host platform.

In one embodiment, portable device 70, 370 supports more than one user. In another embodiment, the same user may register multiple fingerprints as separate templates. In yet another embodiment, the same user fingerprint may be registered multiple times as different templates. Thus, portable device 70, 370 can facilitate the registration of additional user(s) and/or additional template(s) either by periodically (e.g., upon startup) inquiring whether a new user/template needs to be added or upon the user's request in step 220. If an additional user/template is to be registered, the registration process will be invoked. If it is determined that no new registration is necessary, process 200 proceeds with an authentication process (steps 230, 240 and 260 as described below).

It should be appreciated that within the scope of the present invention, software (e.g., a software driver) may need to be installed on the host platform prior to the first use of portable device 70, 370 to enable its utilization of the host platform's user interface to communicate with the user. It should also be appreciated that if the operating system of the host platform has built-in support for such functionality, no additional software needs to be installed thereon.

Referring still to Figure 10, the registration process is now described. In step 225, the registration process is initiated. In one embodiment, this involves informing the user that a registration process will commence and prompting the user to place his/her finger on sensor 52.

In step 235, sensor 52 is read to capture an image of the fingerprint of the user's finger that has been placed thereon. In a currently preferred embodiment, step 235 also includes verifying that the captured image is of sufficient quality for further processing (e.g., template generation). This is preferably performed by control unit 56 as directed by microprocessor 11. In one embodiment, step 235 will be repeated if the quality of the captured fingerprint image is unacceptable. Under such circumstances, the user will be prompted to place his/her finger on sensor 52 again so that a new image can be captured. Preferably, the number of retry is user-configurable.

Once an acceptable fingerprint image has been captured in step 235, process 200 proceeds to step 245, wherein a template is generated based on the captured fingerprint image. As described above, in a preferred embodiment, the captured image is converted into 64 KB of data, which is then used as input to template generator 12a for generating a 512-byte template.

In step 248, the template generated in step 245 is encrypted. In one embodiment, the encryption is performed by firmware (e.g., encryption firmware 117d of Figure 1B), thereby providing an added level of security against hacking.

In step 255, the encrypted template is stored into flash memory 20. In one embodiment, upon successful generation and encryption of a template, flash controller 14 is prompted by template generator 12a to store the newly generated and encrypted template into flash memory 20 for use in subsequent user authentication. Moreover, as described above, in a preferred embodiment, the

template is stored in a reserved area of flash memory 20 which is specifically designated for storing template(s) and which is not otherwise accessible to the user.

In step 280, a signal or message indicating the successful completion of the registration process is generated. In an embodiment where portable device 70, 370 is used as a secure storage device, step 280 can also entail enabling portable device, i.e., granting the newly registered user access (e.g., read data therefrom and write data thereto) to portable device 70, 370 and mapping portable device 70, 370 to a valid drive letter on host platform 90.

With reference still to Figure 10, the authentication process using the portable device 70, 370 is now described. In step 230, sensor 52, 352 is read to capture an image of the fingerprint of the user's finger that has been placed thereon. In a currently preferred embodiment, step 230 also includes a quality check of the captured image by control unit 56, so that the image capture will be repeated if the quality of the captured fingerprint image is unacceptable for template generation. If a repeat capture is needed, the user will be so prompted. Preferably, the number of retry is user-configurable. In a currently preferred embodiment, step 230 also includes generating a template based on the captured fingerprint image and storing the resulting template into volatile memory 16.

In step 240, the stored template(s) are read from flash memory 20 for use as the basis of authenticating the identity of the user whose fingerprint image has been captured in step 230. In a currently preferred embodiment, microprocessor 11 directs flash controller 14 to retrieve the registered template(s) from flash memory 20.

In step 250, the registered template(s) read from flash memory 20, which are stored in encrypted form in a preferred embodiment, are decrypted. The decrypted template(s) are loaded into volatile memory 16 in one embodiment.

In step 260, it is determined whether the user's fingerprint can be authenticated against the registered fingerprint template on record. In a currently preferred embodiment, verification module 12b compares the template pending verification against the registered template(s). If a match is detected, the user is authenticated; otherwise, authentication fails. In one embodiment, the user is

allowed to reattempt the authentication process if an initial attempt fails (e.g., steps 230, 240 and 250 are repeated) Preferably, the number of repeated attempts is user-configurable and can be set once an authorized user has been authenticated and granted access.

In one embodiment, when a user has failed to authenticated his/her identity as an authorized user, access to flash memory 20 will be blocked (e.g., in an embodiment where a software driver resides in host platform 90, the software driver can forbid such access). In another embodiment, microprocessor 11 in portable device 70 will shut down or otherwise disable flash controller 14 upon such authentication failure. These actions serve as added security measures against potential hacking and other forms of unauthorized access to the data stored in flash memory 20 and are triggered by repeated failed authentication attempts.

In one embodiment, optional step 270 is provided. In this embodiment, should verification module 12b malfunction and refuse to authenticate an authorized user whose fingerprint has been previously registered, the user is provided with an option to bypass the fingerprint authentication and provide a password to gain access instead. This embodiment affords the user the ability to avoid a helpless situation where access to contents of flash memory 20 cannot be had unless and until verification module 12b is fixed. If the bypass password is correctly entered, user authentication is deemed to be successful; otherwise, user authentication remains a failure. It should also be appreciated that if added security is desired, a password requirement can be implemented in addition to the fingerprint authentication even for normal routine authentication within the scope of the present invention.

In step 280, a signal or message indicating the successful authentication is generated. In an embodiment where portable device 70, 370 is used as a secure storage device, step 280 can also entail enabling portable device, i.e., granting the newly registered user access (e.g., read data therefrom and write data thereto) to portable device 70, 370 and mapping portable device 70, 370 to a valid drive letter on host platform 90.

It should be appreciated that in an embodiment where authentication engine 12 is located in host platform 90, appropriate modifications to the authentication process described above are needed. In particular, once a satisfactory fingerprint image has been obtained in step 230, the image data is first encrypted and then transmitted to host platform 90, wherein the steps to be performed by authentication engine 12 will be carried out. Thus, depending on the particular implementation or application, the information being transmitted from portable device 70, 370 to host platform 90 can either be a simple notification of success upon successful authentication, or image data representing a user fingerprint that is pending authentication.

In a currently preferred embodiment, performance of various steps of process 200 are controlled by microprocessor 11 executing firmware code, which is preferably stored in non-volatile memory 17 of portable device 70, 370.

Significantly, it should be appreciated that the present invention not only contemplates using portable device 70, 370 as a secure data storage device but also as an access control device. In particular, within the scope of the present invention, portable device 70, 370 can act as an "access key" to host platform 90 to which portable device 70, 370 is coupled. More specifically, in one embodiment, in order to access any resource on host platform 90 (e.g., data, files, application programs, peripherals) and/or any resource attached thereto (e.g., network access, network printers and storage devices, electronic mail) a user is required to first successfully authenticate his/her identity as an authorized user using portable device 70, 370 with integrated fingerprint module 50. In accordance with this embodiment, such fingerprint authentication is used preferably in lieu of (or alternatively in addition to) conventional password-based authentication. Thus, the user inconvenience and less stringent security that is inherent in the prior art password-based authentication approach is advantageously eliminated in accordance with the present invention.

Beyond access control to various computer resources, the present invention can also be advantageously utilized in numerous other applications that require security clearance, such as entry into private homes, offices, hotel rooms, bank vaults and security deposit boxes, and so on. The present invention can

also be beneficially applied to restrict the operation of machinery, such as factory machines and vehicles, to those who have been properly trained. In one embodiment, access control device 70, 370 can be used as a house key to a private home or room key to a hotel room in place of conventional keys. In the first example, the home owner first registers his/her fingerprint when the biometrics-based lock is installed at the house. In the latter example, a hotel guest first registers his/her fingerprint upon check-in at a hotel. Thereafter, access to the house or hotel room is securely restricted to the respective key holder (home owner or hotel guest). These and other wide-ranging applications of the biometrics-based access device technology disclosed herein are all intended to be within the scope and spirit of the present invention.

Although embodiments of the present invention have been described herein as using fingerprint authentication technology to implement access control, it should be appreciated that the present invention is not limited thereto but rather encompasses the use of other biometrics-based authentication techniques. One such technique is iris scan technology. While such other biometrics-based techniques are not expressly described herein, their applicability to access control implementations using a portable device is within the scope and spirit of the present invention disclosed.

Moreover, while preferred embodiments of the present invention have been described herein as using flash memory as a storage media, it should be appreciated that other types of non-volatile memory, such as ferroelectric random access memory (FRAM) or magnetic random access memory (MRAM), can also be used within the scope of the present invention. In addition, while such preferred embodiments have been described herein as being compatible with the USB standard, the portable device of the present invention is not intended to be restricted thereto. Rather, the present invention is intended to encompass portable devices that support other communication protocols and/or bus standards, such as the IEEE 1394 ("Firewire") standard.

While preferred embodiments of the present invention, a method and system for implementing access control using biometrics-based technology, have been described, it is understood that those skilled in the art, both now and in the

future, may make various improvements and enhancements which fall within the scope of the claims that follow. These claims should be construed to maintain the proper protection for the invention first disclosed herein.

CLAIMS

1. A portable device comprising:

a microprocessor, and

a biometrics-based authentication module coupled to and controlled by the microprocessor, wherein access to a restricted resource, the restricted resource having a communication port communicatively coupled to the portable device, is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the restricted resource is denied to the user otherwise.

2. The portable device according to claim 1, wherein the biometrics-based authentication module is a fingerprint authentication module.

3. The portable device according to claim 2, wherein the fingerprint authentication module comprises a fingerprint sensor element.

4. The portable device according to claim 3 in which the sensor element is rotatable during a sensing operation, to bring successive portions of a user's finger into rolling contact with the sensor, and thereby sense successive portions of a user's fingerprint.

5. The portable device according to claim 3 or claim 4, wherein the fingerprint authentication module comprises a cover mounted for motion between a first position covering the sensor element and a second position revealing the sensor element.

6. The portable device according to claim 1 or claim 2, which is communicatively coupled to the communication port of the restricted resource via a universal serial bus (USB).

7. The portable device according to any of the preceding claims, wherein the biometrics-based authentication module comprises a biometrics sensor fitted on one surface of the portable device.

8. The portable device according to any of claims 1 to 7, further comprising a non-volatile memory capable or storing biometrics information usable for authentication.

9. The portable device according to any of claims 1 to 8, wherein the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.

10. The portable device according to any of claims 1 to 9, wherein the restricted resource comprises a host computer.

11. The portable device according to any of claims 1 to 10, wherein the restricted resource comprises a communication network.

12. The portable device according to any of claims 1 to 11, wherein the restricted resource is a real estate premises that imposes access restrictions.

13. The portable device according to any of claims 1 to 12, wherein the restricted resource is an operable machinery, the safe operation of which requires training.

14. A biometrics-based access control system for controlling access to a restricted resource, comprising:

a portable device which includes a non-volatile memory and a biometrics-based authentication module coupled thereto, wherein the biometrics-based authentication module is configured to (1) capture a first biometrics marker; (2) store the first biometrics marker in the non-volatile memory; (3) capture a second

biometrics marker; and (4) determine whether the second biometrics marker can be authenticated against the first biometrics marker, and wherein access to the restricted resource is granted upon a determination of successful authentication and wherein access to the restricted resource is denied otherwise.

15. The biometrics-based access control system as recited in Claim 14 wherein the biometrics-based authentication module is a fingerprint authentication module.

16. The biometrics-based access control system according to claim 14 or claim 15, wherein the portable device is communicatively coupled to a communication port of the restricted resource via a universal serial bus (USB).

17. The biometrics-based access control system according to any of claims 14 to 16, wherein the biometrics-based authentication module comprises a biometrics sensor which is structurally integrated with the portable device in a unitary construction, the biometrics sensor being disposed on one surface of the portable device.

18. The portable device according to claim 17 in which the sensor is a fingerprint sensor and includes a element which is rotatable during a sensing operation, to bring successive portions of a user's finger into rolling contact with the sensor, and thereby sense successive portions of a user's fingerprint.

19. The portable device according to claim 17 or claim 18, wherein the biometrics-based authentication module comprises a cover mounted for motion between a first position covering the element and a second position revealing the sensor.

20. The biometrics-based access control system according to any of claims 14 to 19, wherein the non-volatile memory of the portable device comprises flash memory.

21. The biometrics-based access control system according to any of claims 14 to 19, wherein a bypass mechanism for authentication is provided upon a determination of authentication failure by the biometrics-based authentication module.

22. A biometrics-based access control method for controlling access to a restricted resource and implemented using a portable device, the method comprising the steps of:

(a) obtaining a first biometrics marker from a user with a biometrics sensor installed on the portable device;

(b) retrieving a registered biometrics marker from a memory of the portable device, the registered biometrics marker having been stored therein during a registration process;

(c) comparing the first biometrics marker against the registered biometrics marker; and

(d) granting the user access to the restricted resource provided that a match is identified in said step (c).

23. The biometrics-based access control method as recited in Claim 22 wherein the registered biometrics marker is a fingerprint.

24. The biometrics-based access control method according to claim 22 or claim 23, wherein the registered biometrics marker is stored in an encrypted format.

25. The biometrics-based access control method according to any of claims 22 to 24, further comprising the step of denying the user access to the restricted resource provided that a match is not identified in said step (c).

26. The biometrics-based access control method according to any of claims 22 to 25, further comprising the step of providing the user with a bypass authentication procedure provided that a match is not identified in said step (c).