Case No. 12838/6

Inventor: BURKE, Christopher John

Title: REMOTE ENTRY SYSTEM

POWER OF ATTORNEY

The specification of the above-identified patent application:

□ is attached hereto

☒ was filed on **February 13, 2006** as **U.S. Application Serial No. 10/568,207**.

I hereby revoke all previously granted powers of attorney in the above-identified patent application and appoint the following attorneys to prosecute said patent application and to transact all business in the Patent and Trademark Office connected therewith:

Michael E. Milz (Reg. No. 34,880)
Robert D. Summers, Jr. (Reg. No. 57,844)

Please address all correspondence and telephone calls to Michael E. Milz in care of:

Brinks Hofer Gilson & Lione
P.O. Box 10395
Chicago, Illinois 60610
(312)321-4200

The undersigned hereby authorizes the U.S. attorneys named herein to accept and follow instructions from Martin Friedgut as to any action to be taken in the Patent and Trademark Office regarding this application without direct communication between the U.S. attorney and the undersigned. In the event of a change in the persons from whom instructions may be taken, the U.S. attorneys named herein will be so notified by the undersigned.

As required by 37 CFR 3.73(b)(1) and shown below, the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

Securicom (NSW) Pty Ltd., an Australian company, certifies that it is the assignee of the entire right, title and interest in the patent application identified above by virtue of either:

☒ An assignment from the inventor(s) of the patent application identified above, which is being recorded concurrently herewith pursuant to 37 CFR 3.11, a copy of which is attached hereto.
OR

□ An assignment from the inventor(s) of the patent application identified above. The assignment was recorded in the Patent and Trademark Office at Reel _____, frame _____.
OR

□ A chain of title from the inventor(s) of the patent application identified above to the current assignee as shown below:

1. From _____ To: _____
   The document was recorded in the Patent and Trademark Office at
   Reel _____, frame _____, or a copy thereof is attached.
2. From _____ To: _____
   The document was recorded in the Patent and Trademark Office at
   Reel _____, frame _____, or a copy thereof is attached.

□ Additional documents in the chain of title are listed on a supplemental sheet.

The undersigned has reviewed the assignment or all the documents in the chain of title of the patent application identified above and, to the best of undersigned's knowledge and belief, title is in the assignee identified above.

The undersigned (whose title is supplied below) is empowered to act on behalf of the assignee.

I hereby declare that all statements made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true; and further, that these statements are made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001, Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature __________

Date: 19. 5 - 2008 (Day/month/year)

Name: CHRISTOPHER BURKE

Title: MANAGING DIRECTOR

Remote Entry System

Inventors: **Burke; John Christopher**; *(New South Wales, AU)*

Description

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation patent application of U.S. Non-Provisional Application No. 10/568,207 for REMOTE ENTRY SYSTEM, filed June 04, 2008, the disclosure of which is incorporated by reference in its entirety.

FIELD OF THE INVENTION

[0001] The present invention relates to secure access systems and, in particular, to systems using wireless transmission of security code information.

BACKGROUND

[0002] FIG. 1 shows a prior art arrangement for providing secure access. A user 401 makes a request, as depicted by an arrow 402, directed to a code entry module 403. The module 403 is typically mounted on the external jamb of a secure door. The request 402 is typically a secure code of some type which is compatible with the code entry module 403. Thus, for example, the request 402 can be a sequence of secret numbers directed to a keypad 403. Alternately, the request 402 can be a biometric signal from the user 401 directed to a corresponding biometric sensor 403. One example of a biometric signal is a fingerprint. Other physical attributes that can be used to provide biometric signals include voice, retinal or iris pattern, face pattern, palm configuration and so on.

[0003] The code entry module 403 conveys the request 402 by sending a corresponding signal, as depicted by an arrow 404, to a controller 405 which is typically situated in a remote or inaccessible place. The controller 405 authenticates the security information provided by the user 401 by interrogating a database 407 as depicted by an arrow 406. If the user 401 is authenticated, and has the appropriate access privileges, then the controller 405 sends an access signal, as depicted by an arrow 408, to a device 409 in order to provide the desired access. The device 409 can, for example, be the locking mechanism of a secure door, or can be an electronic lock on a personal computer (PC) which the user 401 desires to access.

[0004] A proximity card can also be used to emit the request 402, in which case the code entry module 403 has appropriate functionality.

[0005] Although the request 402 can be made secure, either by increasing the number of secret digits or by using a biometric system, the communication infrastructure in FIG. 1 is typically less secure. The infrastructure 400 is generally hardwired, with the code entry module 403 generally being mounted on the outside jamb of a secured door. In such a situation, the signal path 404 can be over a significant distance in order to reach the controller 405. The path 404 represents one weak point in the security system 400, providing an unauthorised person with relatively easy access to the information being transmitted between the code entry module 403 and the controller 405. Such an unauthorised person can, given this physical access, decipher the communicated information between the code entry module 403 and the controller 405. This captured information can be deciphered, replayed in order to gain the access which rightfully belongs to the user 401, or to enable modification for other subversive purposes.

[0006] Current systems as depicted in FIG. 1 utilise a communication protocol called "Wiegand" for communication between the code entry module 403 and the controller 405. The Wiegand protocol is a simple one-way data protocol that can be modified by increasing or decreasing the bit count to ensure uniqueness of the protocol among different security companies. The Wiegand protocol does not secure the information being sent between the code entry module 403 and the controller 405.

[0007] More advanced protocols such as RS 485 have been used in order to overcome the vulnerability of the Wiegand protocol over the long distance route 404. RS 485 is a duplex protocol offering encryption capabilities at both the transmitting and receiving ends, i.e. the code entry module 403 and the controller 405 respectively in the present case. The length of the path 404 nonetheless provides an attack point for the unauthorised person.

[0008] Due to the cost and complexity of re-wiring buildings and facilities, security companies often make use of existing communication cabling when installing and/or upgraded security systems, thereby maintaining the vulnerability described above.

SUMMARY

[0009] It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

[0010] According to a first aspect of the present invention, there is provided a system for providing secure access to a controlled item, the system comprising:

[0011] a database of biometric signatures;

[0012] a transmitter subsystem comprising: [0013] a biometric sensor for receiving a biometric signal; [0014] means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and [0015] means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth.TM. protocol, and a WiFi.TM. protocol; and

[0016] a receiver sub-system comprising; [0017] means for receiving the transmitted secure access signal; and [0018] means for providing conditional access to the controlled item dependent upon said information.

[0019] According to another aspect of the present invention, there is provided a transmitter sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for receiving a secure access signal transmitted by the transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal; wherein the transmitter subsystem comprises: [0020] a biometric sensor for receiving a biometric signal; [0021] means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and [0022] means for emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth.TM. protocol, and a WiFi.TM. protocol.

[0023] According to another aspect of the present invention, there is provided receiver sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth.TM. protocol, and a WiFi.TM. protocol; wherein the receiver sub-system comprises; [0024] means for receiving the transmitted secure access signal; and [0025] means for providing conditional access to the controlled item dependent upon said information.

[0026] According to another aspect of the present invention, there is provided a method for providing secure access to a controlled item, the method comprising the steps of:

[0027] receiving a biometric signal;

[0028] matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute;

[0029] emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth.TM. protocol, and a WiFi.TM. protocol; and

[0030] providing conditional access to the controlled item dependent upon said information.

[0031] According to another aspect of the present invention, there is provided a method for populating a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon information in said secure access signal, said method comprising the steps of:

[0032] receiving a series of entries of the biometric signal;

[0033] determining at least one of the number of said entries and a duration of each said entry;

[0034] mapping said series into an instruction; and

[0035] populating the database according to the instruction.

[0036] According to another aspect of the present invention, there is provided a method for transmitting a secure access signal in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for receiving the secure access signal transmitted by a transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal, said method comprising the steps of: [0037] receiving a biometric sensor by biometric signal; [0038] matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and [0039] emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth.TM. protocol, and a WiFi.TM. protocol.

[0040] According to another aspect of the present invention, there is provided a method for receiving a secure access signal in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth.TM. protocol, and a WiFi.TM. protocol, said method comprising the steps of: [0041] receiving the transmitted secure access signal; and [0042] providing conditional access to the controlled item dependent upon said information.

[0043] According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to provide secure access to a controlled item, said computer program product comprising:

[0044] code for receiving a biometric signal;

[0045] code for matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute;

[0046] code for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth.TM. protocol, and a WiFi.TM. protocol; and

[0047] code for providing conditional access to the controlled item dependent upon said information.

[0048] According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to populate a database of biometric signatures in a system for providing secure access to a controlled item, said computer program product comprising:

[0049] code for receiving a series of entries of the biometric signal;

[0050] code for determining at least one of the number of said entries and a duration of each said entry;

[0051] code for mapping said series into an instruction; and

[0052] code for populating the database according to the instruction.

[0053] According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to transmit a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

[0054] code for receiving a biometric sensor by biometric signal;

[0055] code for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

[0056] code for emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth.TM. protocol, and a WiFi.TM. protocol.

[0057] According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to receive a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

[0058] code for receiving the transmitted secure access signal; and

[0059] code for providing conditional access to the controlled item dependent upon said information.

[0060] According to another aspect of the present invention, there is provided a system for providing secure access, the system comprising:

[0061] a biometric sensor for authenticating the identity of a user;

[0062] a transmitter for transmitting information using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and

[0063] a control panel for receiving the information and for providing the secure access requested.

[0064] Other aspects of the invention are also disclosed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0065] Some aspects of the prior art and one or more embodiments of the present invention are described with reference to the drawings, in which:

[0066] FIG. 1 shows a prior art arrangement for providing secure access;

[0067] FIG. 2 is a functional block diagram of an arrangement for providing secure access according to the present disclosure;

[0068] FIG. 3 shows an example of a method of operation of the remote control module of FIG. 2;

[0069] FIG. 4 shows an example of a method of operation of the (fixed) control device of FIG. 2;

[0070] FIG. 5 shows incorporation of a protocol converter into the arrangement of FIG. 2; and

[0071] FIG. 6 shows another example of how the remote access system operates;

[0072] FIG. 7 shows an access process relating to the example of FIG. 6;

[0073] FIG. 8 shows one enrolment process relating to the example of FIG. 6;

[0074] FIG. 9 shows another enrolment process relating to the example of FIG. 6; and

[0075] FIG. 10 is a schematic block diagram of the system in FIG. 2.

DETAILED DESCRIPTION INCLUDING BEST MODE

[0076] It is to be noted that the discussions contained in the "Background" section relating to prior art arrangements relate to discussions of documents or devices which form public knowledge through their respective publication and/or use. Such should not be interpreted as a representation by the present inventor(s) or patent applicant that such documents or devices in any way form part of the common general knowledge in the art.

[0077] Where reference is made in any one or more of the accompanying drawings to steps and/or features, which have the same reference numerals, those steps and/or features have for the purposes of this description the same function(s) or operation(s), unless the contrary intention appears.

[0078] FIG. 2 is a functional block diagram of an arrangement for providing secure access according to the present disclosure. A user 101 makes a request, as depicted by an arrow 102, to a code entry module 103. The code entry module 103 includes a biometric sensor 121 and the request 102 takes a form which corresponds to the nature of the sensor 121 in the module 103. Thus, for example, if the biometric sensor 121 in the code entry module 103 is a fingerprint sensor, then the request 102 typically takes the form of a thumb press on a sensor panel (not shown) on the code entry module 103.

[0079] The code entry module 103 interrogates, as depicted by an arrow 104, a user identity database 105. Thus for example if the request 102 is the thumb press on the biometric sensor panel 121 then the user database 105 contains biometric signatures for authorised users against which the request 102 can be authenticated. If the identity of the user 101 is authenticated successfully, then the code entry module 103 sends a signal 106 to a controller/transmitter 107. The controller/transmitter 107 checks, as depicted by an arrow 112, the current rolling code in a database 113. The controller 107 then updates the code and sends the updated code, this being referred to as an access signal, as depicted by an arrow 108 to a controller 109. The rolling code protocol offers non-replay encrypted communication.

[0080] The controller 109 tests the rolling code received in the access signal 108 against the most recent rolling code which has been stored in a database 115, this testing being depicted by an arrow 114. If the incoming rolling code forming the access signal 108 is found to be legitimate, then the controller 109 sends a command, as depicted by an arrow 110, to a controlled item 111. The controlled item 111 can be a door locking mechanism on a secure door, or an electronic key circuit in a personal computer (PC) that is to be accessed by the user 101. It is noted that the controller 109 contains a receiver 118 that receives the transmitted access signal 108 and converts it into a form that is provided, as depicted by an arrow 120, into a form that the controller 109 can use.

[0081] The code entry module 103 also incorporates at least one mechanism for providing feedback to the user 101. This mechanism can, for example, take the form or one or more Light Emitting Diodes (LEDs) 122 which can provide visual feedback, depicted by an arrow 123 to the user 101. Alternately or in addition the mechanism can take the form of an audio signal provided by an audio transducer 124 providing audio feedback 125.

[0082] The arrangement in FIG. 2 has been described for the case in which the secure code in the access signal 108 used between the sub-systems 116 and 117 is based upon the rolling code. It is noted that this is merely one arrangement, and other secure codes can equally be used. Thus, for example, either of the Bluetooth.TM. protocol, or the Wi Fi.TM. protocols can be used.

[0083] Rolling codes provide a substantially non-replayable non-repeatable and encrypted radio frequency data communications scheme for secure messaging. These codes use inherently secure protocols and serial number ciphering techniques which in the present disclosure hide the clear text values required for authentication between the key fob (transmitter) sub-system 116 and the receiver/controller 118/109.

[0084] Rolling codes use a different code variant each time the transmission of the access signal 108 occurs. This is achieved by encrypting the data from the controller 107 with a mathematical algorithm, and ensuring that successive transmissions of the access signal 108 are modified using a code and/or a look-up table known to both the transmitter sub-system 116 and the receiver sub-system 117. Using this approach successive transmissions are modified, resulting in a non-repeatable data transfer, even if the information from the controller 107 remains the same. The modification of the code in the access signal 108 for each transmission significantly reduces the likelihood that an intruder can access the information replay the information to thereby gain entry at some later time.

[0085] The sub-system in FIG. 2 falling to the left hand side, as depicted by an arrow 116, of a dashed line 119 can be implemented in a number of different forms. The sub-system 116 can for example be incorporated into a remote fob (which is a small portable device carried by the user 101), or alternately can be mounted in a protected enclosure on the outside jamb of a secured door. The sub-system 116 communicates with the sub-system 117 on the right hand side of the dashed line 119 via the wireless communication channel used by the access signal 108. The sub-system 117 is typically located in an inaccessible area such as a hidden roof space or alternately in a suitable protected area such as an armoured cupboard. The location of the sub-system 117 must of course be consistent with reliable reception of the wireless access signal 108.

[0086] Although typically the communication channel uses a wireless transmission medium, there are instances where the channel used by the access signal 108 can use a wired medium. This is particularly the case when the transmitter sub-system 116 is mounted in an enclosure on the door jamb rather than in a portable key fob.

[0087] The biometric signature database 105 is shown in FIG. 2 to be part of the transmitter sub-system 116. However, in an alternate arrangement, the biometric signature database 105 can be located in the receiver sub-system 117, in which case the communication 104 between the code entry module 103 and the signature database 105 can also be performed over a secure wireless communication channel such as the one used by the access signal 108. In the event that the secure access system is being applied to providing secure access to a PC, then the secured PC can store the biometric signature of the authorised user in internal memory, and the PC can be integrated into the receiver sub-system 117 of FIG. 1.

[0088] In the event that the sub-system 116 is implemented as a remote fob, the combination of the biometric verification and the strongly encrypted wireless communication provides a particularly significant advantage over current systems. The remote key fob arrangement allows easy installation, since the wired communication path 404 (see FIG. 1) is avoided. Other existing wiring elements of the present systems 400 can be used where appropriate. When the sub-system 116 is implemented as a remote fob, the fob incorporates the biometric (eg fingerprint) authentication arrangement, in which case only one biometric signature is stored in the fob. This arrangement reduces the requirements on the central database 115. Once the key fob authenticates the user through biometric signature (eg fingerprint) verification, the rolling code in the access signal 108 is transmitted to the controller 109 for authorisation of the user for that location at that time.

[0089] In addition to authenticating the user 101 the biometric sensor 121 in the code entry module 103 in conjunction with the controller 107 can also check other access privileges of the user 101. These access privileges can be contained in the database 105 which can be located either locally in the remote key fob, or in the receiver sub-system 117 as previously described. In one example, Tom Smith can firstly be authenticated as Tom Smith using the thumb press by Tom on the biometric sensor panel (not shown). After Tom's personal biometric identity is authenticated, the transmitter sub-system 116 can check if Tom Smith is in fact allowed to use the particular door secured by the device 111 on weekends. Thus the security screening offered by the described arrangement can range from simple authentication of the user's identity, to more comprehensive access privilege screening.

[0090] The incorporation of the biometric sensor 121 into the code entry module 103 in the form of a remote key fob also means that if the user 101 loses the remote key fob, the user need not be concerned that someone else can use it. Since the finder of the lost key fob will not be able to have his or her biometric signal authenticated by the biometric sensor 121 in the code entry module 103, the lost key fob is useless to anyone apart from the rightful user 101.

[0091] The transmitter sub-system 116 is preferably fabricated in the form of a single integrated circuit (IC) to reduce the possibility of an authorised person bypassing the biometric sensor 121 in the code entry module 103 and directly forcing the controller 107 to emit the rolling code access signal 108.

[0092] FIG. 3 shows the method of operation of the remote control module (i.e. the sub-system 116) of FIG. 2. The method 200 commences with a testing step 201 in which the biometric sensor 121 in the code entry module 103 checks whether a biometric signal 102 is being received. If this is not the case, then the method 200 is directed in accordance with an NO arrow back to the step 201 in a loop. If, on the other hand, the biometric signal 102 has been received, then the method 200 is directed in accordance with a YES arrow to a step 202. The step 202 compares the received biometric signal 102 with information in the biometric signature database 105 in order to ensure that the biometric signal received 102 is that of the rightful user 101 of the sub-system 116.

[0093] A subsequent testing step 203 checks whether the comparison in the step 202 yields the desired authentication. If the biometric signature matching is authenticated, then the process 200 is directed in accordance with a YES arrow to a step 204. The authentication of the biometric signature matching produces an accessibility attribute for the biometric signal 102 in question. The accessibility attribute establishes whether and under which conditions access to the controlled item 111 should be granted to a user. Thus, for example, the accessibility attribute may comprise one or more of an access attribute (granting unconditional access), a duress attribute (granting access but with activation of an alert tone to advise authorities of the duress situation), an alert attribute (sounding a chime indicating that an unauthorised, but not necessarily hostile, person is seeking access, and a telemetry attribute, which represents a communication channel for communicating state information for the transmitter sub-system to the receiver sub-system such as a "low battery" condition. The step 204 enables the user 101 to select a control option by providing one or more additional signals (not shown) to the controller 107. Thus for example the control option could enable the user 101 to access one of a number of secure doors after his or her identity has been authenticated in the step 203. In the subsequent step 205 the controller 107 sends the appropriate access signal 108 to the controller 109. The process 200 is then directed in accordance with an arrow 206 back to the step 201.

[0094] Thus for example the sub-system 116 can be provided with a single biometric sensor 121 in the code entry module 103 which enables the user 101 to select one of four door entry control signals by means of separate buttons on the controller 107 (not shown). This would enable the user 101, after authentication by the biometric sensor 121 in the code entry module 103 and the controller 107 to obtain access to any one of the aforementioned for secure doors.

[0095] Returning to the testing step 203, if the signature comparison indicates that the biometric signal 102 is not authentic, and has thus not been received from the proper user, then the process 200 is directed in accordance with a NO arrow back to the step 201. In an alternate arrangement, the NO arrow from the step 203 could lead to a disabling step which would disable further operation of the sub-system 116, either immediately upon receipt of the incorrect biometric signal 102, or after a number of attempts to provide the correct biometric signal 102.

[0096] FIG. 4 shows the method of operation of the control sub-system 117 of FIG. 2. The method 300 commences with a testing step 301 which continuously checks whether the access signal 108 has been received from 107. The step 301 is performed by the controller 109. As long as the access signal 108 is not received the process 300 is directed in accordance with a NO arrow in a looping manner back to the step 301. When the access signal 108 is received, the process 300 is directed from the step 301 by means of a YES arrow to a step 302. In the step 302, the controller 109 compares the rolling code received by means of the access signal 108 with a reference code in the database 115. A subsequent testing step 303 is performed by the controller 109. In the step 303 if the code received on the access signal 108 is successfully matched against the reference code in the database 115 then the process 300 is directed in accordance with a YES arrow to a step 304.

[0097] In the step 304 the controller 109 sends the control signal 110 to the controlled item 111 (for example opening the secured door). The process 300 is then directed from the step 304 as depicted by an arrow 305 back to the step 301. Returning to the testing step 303 if the code received on the access signal 108 is not successfully matched against the reference code in the database 115 by the controller 109 then the process 300 is directed from the step 303 in accordance with a NO arrow back to the step 301.

[0098] As was described in regard to FIG. 3, in an alternate arrangement, the process 300 could be directed, if the code match is negative, from the step 303 to a disabling step which would disable the sub-system 117 if the incorrect code where received once or a number of times.

[0099] FIG. 5 shows incorporation of a protocol converter into the arrangement of FIG. 2. In the arrangement of FIG. 2 the receiver 118 in the controller 109 is able to directly receive and process the rolling code in the access signal 108 in a manner as to provide, as depicted by the arrow 120, the necessary information to the controller 109. FIG. 5 shows how an existing controller depicted by a reference numeral 109' that uses Wiegand input signalling can be used in the disclosed arrangement when alarm systems are upgraded. FIG. 5 shows how the incoming access signal 108 is received by a receiver 118' as is the case in FIG. 2. In FIG. 5 however the receiver 118' provides, as depicted by an arrow 503, the received rolling code from the access signal 108 to a rolling code/Wiegand protocol converter 501. The converter 501 converts, as depicted by an arrow 504, the incoming rolling code 503 to a form that can be used by the controller 109' that is designed to handle Wiegand protocol incoming signals. Therefore, the converted incoming signal 504 is in the Wiegand format.

[0100] The converter 501 uses a microprocessor-based arrangement running software code to process the incoming rolling code information 503 and decode this information 503 to clear text form. The converter 501 converts this clear text to a Wiegand variable bit-length data stream. In FIG. 2, the receiver 118 performs the conversion of the incoming rolling code access signal 108 to clear text which enables the controller 109 to identify the serial number of the originating key fob sub-system 116 to enable the access rights of the user to be verified.

[0101] Further to the Wiegand conversion arrangement, the protocol converter 501 approach can be adapted to convert between the incoming rolling code 503 (or any other appropriate secure code) to any other convenient protocol used by the controller 169'.

[0102] The advantage of the rolling code/Wiegand converter 501 is that security system upgrades can be made without replacing Wiegand compatible controller 109'. Accordingly, existing systems as are described in FIG. 1 can be upgraded by replacing the code entry module 403 and the transmission path 404, leaving the other components of the system 400 (i.e., the controller 405, the code database 407, and the controlled item 409, together with existing wiring 408 and 406), largely intact. Minor modifications might however be necessary. When upgrading systems in this manner, the sub-system 116 can either be used in a remote fob configuration, or can be placed in a secure housing on an external door jamb.

[0103] From a practical perspective, incorporating the protocol converter 501 into an existing controller 109' would require direct wiring of the converter 501 into the housing of the secure controller 109'.

[0104] FIG. 6 shows another process 700 of operation of the remote access system. The process 700 commences with a step 701 that determines if a biometric signal has been received by the biometric sensor 121 in the code entry module in FIG. 2. If not, then the process 700 follows a NO arrow back to the step 701. If however a biometric signal has been received, then the process 700 follows a YES arrow to a step 702 that determines if the user ID database 105 in FIG. 2 is empty. This would be the case, for example, if the code entry module is new and has never been used, or if the user 101 has erased all the information in the database 105.

[0105] If the database 105 is empty, then the process 700 is directed by an arrow 703 to 706 in FIG. 8 which depicts a process 800 dealing with the enrolment or the administration function for loading relevant signatures into the database 105. If on the other hand the database 105 is not empty, then the process 700 is directed to a step 704 that determines if the biometric signal that has been received is an administrator's biometric signal.

[0106] The disclosed remote entry system can accommodate at least three classes of user, namely administrators, (ordinary) users, and duress users. The administrators have the ability to amend data stored, for example, in the database 105, while the ordinary users do not have this capability. The first user of the code entry module 103, whether this is the user who purchases the module, or the user who programs the module 103 after all data has been erased from the database 105, is automatically categorised as an administrator. This first administrator can direct the system 100 to either accept further administrators, or alternately to only accept further ordinary users.

[0107] Although the present description refers to "Users", in fact it is "fingers" which are the operative entities in system operation when the biometric sensor 121 (see FIG. 2) is a fingerprint sensor. In this event, a single user can enrol two or more of his or her own fingers as separate administrators or (ordinary) users of the system, by storing corresponding fingerprints for corresponding fingers in the database 105 via the enrolment process 800 (see FIG. 8).

[0108] Some class overlap is possible. Thus a stored signature can belong to an administrator in the duress class.

[0109] The first administrator can provide control information to the code entry module by providing a succession of finger presses to the biometric sensor 121, providing that these successive presses are of the appropriate duration, the appropriate quantity, and are input within a predetermined time. In one arrangement, the control information is encoded by either or both (a) the number of finger presses and (b) the relative duration of the finger presses. If the successive finger presses are provided within this predetermined time, then the controller 107 accepts the presses as potential control information and checks the input information against a stored set of legal control signals.

[0110] One example of a legal control signal can be expressed as follows:

[0111] "Enrol an ordinary user"->dit, dit, dit, dah

where "dit" is a finger press of one second's duration (provided by the user 101 in response to the feedback provided by the Amber LED as described below), and "dah" is a finger press of two second's duration.

[0112] In the event that a legitimate sequence of finger presses are not delivered within the predetermined time, then the presses are considered not to be control information and merely to be presses intended to provide access to the controlled item 111. Legitimate control sequences are defined in Read Only Memory (ROM) in the controller 107.

[0113] The code entry module 103 has feedback signalling mechanisms 122, implemented for example by a number of LEDs, and 124, implemented by an audio transducer. The LEDs 122 and the audio transducer 124 are used by the controller to signal the state of the code entry module 103 to the user 101, and to direct the administration process. Thus, in one example, three LEDs, being Red, Amber and Green are provided.

[0114] When the Amber LED is flashing, it means "Press the sensor". When the Amber

LED is steady ON, it means "Maintain finger pressure". When the Amber LED is OFF, it means "Remove finger pressure". When the system enters the enrolment state (depicted by the process 800 in FIG. 8), then the audio transducer 124 emits the "begin enrolment" signal (dit dit dit dit) and the Red LED flashes. Enrolment of a normal user (according to the step 807 in FIG. 8) is signalled by the OK audio signal (dit dit) and a single blink of the Green LED.

[0115] Returning to the step 704, if the step determines that the biometric signal received is an administrator's signal, then the process 700 is directed by a YES arrow to 706 in FIG. 8 as depicted by the arrow 703. If on the other hand, the step 704 indicates that the received biometric signal does not belong to an administrator then the process 700 is directed by a NO arrow to 707 in FIG. 7.

[0116] FIG. 7 shows the access process 600 by which a biometric signal 102 (see FIG. 2) is processed in order to provide access to the controlled item 111, or to take other action. Entering the process at 707 from FIG. 6, the process 600 proceeds to a step 602 that compares the received biometric signature to signatures stored in the database 105. A following step 603 determines if the received signal falls into the "duress" category. Signatures in this category indicate that the user 101 is in a coercive situation where, for example, an armed criminal is forcing the user 101 to access the secure facility (such as a bank door). If the step 603 determines that the signature is in the duress class, then a following step 604 prepares a "duress" bit for incorporation into the code access signal 108. The aforementioned duress bit is an access attribute of the biometric signal 102. Thereafter the process 600 proceeds to a step 605.

[0117] Modules used in the code entry module for producing the rolling code enable a number of user defined bits to be inserted into the access signal 108, and these bits can be used to effect desired control functions in the receiver sub-system 117. The disclosed system 100 utilises four such user bits, namely (a) to indicate that the user belongs to the duress category, (b) to indicate a "battery low" condition, or other desired system state or "telemetry" variable, for the code entry module 103, (c) to indicate that the biometric signal represents a legitimate user in which case the secure access to the controlled item 111 is to be granted, or (d) to indicate that the biometric signal is unknown, in which case the controller 109 in the receiver sub-system 117 sounds an alert tone using a bell (not shown) or the like.

[0118] Returning to FIG. 7, if the step 603 determines that the biometric signal is not in the duress class, then the process 600 proceeds according to a NO arrow to the step 605. The step 605 determines if the code entry module 103 has a low battery condition, in which event the process 600 proceeds according to a YES arrow to a step 606 that prepares a telemetry bit for insertion into the access signal 108. The aforementioned telemetry bit is an access attribute of the biometric signal 102. Thereafter, the process proceeds to a step 607.

[0119] If the step 605 determines that telemetry signalling is not required, then the process 600 proceeds according to a NO arrow to the step 607. The step 607 checks the biometric signal against the signatures in the database 105. If the received biometric signal matches a legitimate signature in the database 105, then the process is directed to a step 608 that prepares an "access" bit for insertion into the access signal 108. This access bit directs the controller 109 in the receiver sub-system 117 to provide access to the controlled item 111. The aforementioned access bit is an access attribute of the biometric signal 102. The process 600 then proceeds to a step 610.

[0120] If the step 607 determines that the biometric input signal does not match any legitimate signatures in the database 105, then the process 600 proceeds according to a NO arrow to a step 609 that prepares an "alert" bit for insertion into the access signal 108. The aforementioned alert bit is an access attribute of the biometric signal 102. This alert bit directs the controller 109 (a) not to provide access to the controlled item 111, and (b) to provide an alert tone, like ringing a chime or a bell (not shown), to alert personnel in the vicinity of the receiver sub-system 117 that an unauthorised user is attempting to gain access to the controlled item 111. The alert bit can also cause a camera mounted near the controlled item 111 to photograph the unauthorised user for later identification of that person. The camera can be activated if the person attempting to gain access is unauthorised, and also if the person attempting to gain access is authorised but uses a duress signature.

[0121] An optional additional step (not shown) can prepare an identification field for insertion into the access signal 108. This sends, to the receiver sub-system 117, ID information that the receiver sub-system can use to construct an audit trail listing which users, having signatures in the database 105, have been provided with access to the controlled item 111.

[0122] The process 600 is then directed to the step 610 which inserts the various user defined bits into the access signal 108 and sends the signal 108 to the receiver sub-system 117. Thereafter, the process 600 is directed by an arrow 611 to 705 in FIG. 6.

[0123] FIG. 8 shows a process 800 for implementing various enrolment procedures. The process 800 commences at 706 from FIG. 6 after which a step 801 determines if the biometric signal is a first administrators input (which is the case if the database 105 is empty). If this is the case, then the process 800 is directed to a step 802 that stores the administrator's signature in the database 105. From a terminology perspective, this first administrator, or rather the first administrator's first finger (in the event that the biometric sensor 121 in FIG. 2 is a fingerprint sensor), is referred to as the "superfinger". Further administrator's fingers are referred to as admin-fingers, and ordinary users fingers are referred to merely as "fingers". The reason that someone would enrol more than one of their own fingers into the system is to ensure that even in the event that one of their enrolled fingers is injured, the person can still operate the system using another enrolled finger.

[0124] It is noted that the step 802, as well as the steps 805, 807 and 809 involve sequences of finger presses on the biometric sensor 121 in conjunction with feedback signals from the LEDs 122 and/or the audio speaker 124. The process 800 then proceeds to a step 810 that determines if further enrolment procedures are required. If this is the case, then the process 800 proceeds by a YES arrow back to the step 801. If no further enrolment procedures are required, then the process 800 proceeds by a NO arrow to 705 in FIG. 6.

[0125] Returning to the step 801, if the biometric signal is not a first administrator's signal, then the process 800 proceeds by a NO arrow to a step 803. The step 803 determines if a further administrator signature is to be stored. It is noted that all signatures stored in the database are tagged as belonging to one or more of the classes of administrator, ordinary user, and duress users. If a further administrator signature is to be stored, then the process 800 proceeds by a YES arrow to the step 802 that stores the biometric signal as a further administrator's signature.

[0126] If a further administrator's signature is not required, then the process 800 proceeds according to a NO arrow to a step 804 that determines if a duress signature is to be stored. If this is the case then the process 800 follows a YES arrow to a step 805 that stores a duress signature. The process 800 then proceeds to the step 810. If however the step 804 determines that a duress signature is not required, then the process 800 proceeds by a NO arrow to s step 806.

[0127] The step 806 determines if a further simple signature (i.e. belonging to an ordinary user) is to be stored. If a further simple signature is to be stored, then the process 800 proceeds by a YES arrow to the step 807 that stores the biometric signal as a further ordinary signature.

[0128] If a further simple signature is not required, then the process 800 proceeds according to a NO arrow to a step 808 that determines if any or all signatures are to be erased from the database 105. If this is the case then the process 800 follows a YES arrow to a step 809 that erases the desired signatures. The process 800 then proceeds to the step 810. If however the step 804 determines that no signatures are to be erased, then the process 800 proceeds by a NO arrow to the step 810.

[0129] FIG. 9 shows another enrolment process relating to the example of FIG. 6. The process 900 commences at 706 from FIG. 6 after which a step 901 determines if the received biometric signal comes from the first administrator. If this is the case, then the process 900 proceeds according to a YES arrow to a step 902. The step 902 emits an "Enrolment" tone and flashes the green LED once only. Thereafter, a step 905 reads the incoming biometric signal which is provided by the user as directed by the Amber LED. When the Amber LED flashes continuously, this directs the user to "Apply Finger". When the Amber LED is in a steady illuminated state, this directs the user to "Maintain Finger Pressure". Finally, when the amber LED is off, this directs the user to "Remove Finger".

[0130] Returning to the step 901, if the incoming biometric signal does not belong to the first administrator, then the process 900 proceeds according to a NO arrow to a step 903. The step 903 emits an "Enrolment" tone, and flashes the Red LED in an on-going fashion. Thereafter, the process 900 proceeds according to an arrow 904 to the step 905.

[0131] Following the step 905, a step 906 determines whether the incoming biometric signal is legible. If this is not the case, then the process 900 proceeds according to a NO arrow to a step 907. The step 907 emits a "Rejection" tone, after which the process 900 is directed, according to an arrow 908 to 705 in FIG. 6. Returning to the step 906, if the incoming biometric signal is legible, then the process 900 follows a YES arrow to a step 909. The step 909 determines whether the finger press exceeds a predetermined time. If this is not the case, then the process 900 follows a NO arrow to a step 910 which stores the biometric signal, which in the present case is a fingerprint signature. Thereafter the process 900 follows an arrow 911 to 705 in FIG. 6.

[0132] Returning to the step 909 if the finger press does exceed the predetermined period, then the process follows a YES arrow to a step 912. The step 912 erases relevant signatures depending upon the attributes of the incoming biometric signal. Thus, for example, if the incoming biometric signal belongs to an ordinary user, then the ordinary user's signature in the database 105 is erased by the step 912. If, on the other hand, the incoming biometric signal belongs to the first administrator, then all the signatures in the database 105 are erased. Administrators who are not the first administrator can be granted either the same powers as the first administrator in regard to erasure of signatures, or can be granted the same powers as ordinary user in this respect.

[0133] Once the step 912 has completed erasure of the relevant signatures, then the process 900 follows an arrow 913 to 705 in FIG. 6.

[0134] FIG. 10 is a schematic block diagram of the system in. FIG. 2. The disclosed secure access methods are preferably practiced using a computer system arrangement 100', such as that shown in FIG. 10 wherein the processes of FIGS. 3-4, and 6-9 may be implemented as software, such as application program modules executing within the computer system 100'. In particular, the method steps for providing secure access are effected by instructions in the software that are carried out under direction of the respective processor modules 107 and 109 in the transmitter and receiver sub-systems 116 and 117. The instructions may be formed as one or more code modules, each for performing one or more particular tasks. The software may also be divided into two separate parts, in which a first part performs the provision of secure access methods and a second part manages a user interface between the first part and the user. The software may be stored in a computer readable medium, including the storage devices described below, for example. The software is loaded into the transmitter and receiver sub-systems 116 and 117 from the computer readable medium, and then executed under direction of the respective processor modules 107 and 109. A computer readable medium having such software or computer program recorded on it is a computer program product. The use of the computer program product in the computer preferably effects an advantageous apparatus for provision of secure access.

[0135] The following description is directed primarily to the transmitter sub-system 116, however the description applies in general to the operation of the receiver sub-system 117. The computer system 100' is formed, having regard to the transmitter sub-system 116, by the controller module 107, input devices such as the bio sensor 121, output devices including the LED display 122 and the audio device 124. A communication interface/transceiver 1008 is used by the controller module 107 for communicating to and from a communications network 1020. Although FIG. 2 shows the transmitter sub-system 116 communicating with the receiver sub-system 117 using a direct wireless link for the access signal 108, this link used by the access signal 108 can be effected over the network 1020 forming a tandem link comprising 108-1020-108'. The aforementioned communications capability can be used to effect communications between the transmitter sub-system 116 and the receiver sub-system 117 either directly or via the Internet, and other network systems, such as a Local Area Network (LAN) or a Wide Area Network (WAN).

[0136] The controller module 107 typically includes at least one processor unit 1005, and a memory unit 1006, for example formed from semiconductor random access memory (RAM) and read only memory (ROM). The controller module 107 also includes an number of input/output (I/O) interfaces including an audio-video interface 1007 that couples to the LED display 122 and audio speaker 124, an I/O interface 1013 for the bio-sensor 121, and the interface 1008 for communications. The components 1007, 1008, 1005, 1013 and 1006 the controller module 107 typically communicate via an interconnected bus 1004 and in a manner which results in a conventional mode of operation of the controller 107 known to those in the relevant art.

[0137] Typically, the application program modules for the transmitter sub-system 116 are resident in the memory 1006 iROM, and are read and controlled in their execution by the processor 1005. Intermediate storage of the program and any data fetched from the bio sensor 121 and the network 1020 may be accomplished using the RAM in the semiconductor memory 1006. In some instances, the application program modules may be supplied to the user encoded into the ROM in the memory 1006. Still further, the software modules can also be loaded into the transmitter sub-system 116 from other computer readable media, say over the network 1020. The term "computer readable medium" as used herein refers to any storage or transmission medium that participates in providing instructions and/or data to the transmitter sub-system 116 for execution and/or processing. Examples of storage media include floppy disks, magnetic tape, CD-ROM, a hard disk drive, a ROM or integrated circuit, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the transmitter sub-system 116. Examples of transmission media include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

INDUSTRIAL APPLICABILITY

[0138] It is apparent from the above that the arrangements described are applicable to the security industry.

[0139] The foregoing describes only some embodiments of the present invention, and modifications and/or changes can be made thereto without departing from the scope and spirit of the invention, the embodiments being illustrative and not restrictive.

[0140] The system 100 can also be used to provide authorised access to lighting systems, building control devices, exterior or remote devices such as air compressors and so on. The concept of "secure access" is thus extendible beyond mere access to restricted physical areas.

Claims

Claims

1. A system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a transmitter subsystem comprising:

a biometric sensor for receiving a biometric signal;

means for enrolling relevant signatures into the database using the biometric sensor; wherein the means for enrolling relevant signatures into the database of biometric signatures comprises:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for enrolling relevant signatures into the database according to the instruction;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute; said system further comprising:

a receiver sub-system comprising;

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information.

2. A system according to claim 1, wherein the biometric sensor and the transmitter are located in a remote portable key fob.

3. A system according to claim 1 further comprising:

means for providing a signal for directing input of the series of entries of the biometric signal;

means for incorporating into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database; and

means for constructing an audit trail of biometric signals provided to the biometric sensor for the purpose of accessing the controlled item.

4. A system according to claim 3, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class.

5. A system according to claim 4, wherein the accessibility attribute comprises:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

6. A system according to claim 5, wherein the controlled item is one of:

a locking mechanism of a door; and

an electronic lock on a Personal Computer (PC).

7. A system according to claim 5, wherein the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

8. A system according to claim 5, wherein said conditional access comprises one of:

provision of access to the controlled item if the accessibility attribute comprises an access attribute;

provision of access to the controlled item and sounding of an alert if the accessibility attribute comprises a duress attribute; and

denial of access to the controlled item and sounding of an alert if the accessibility attribute comprises an alert attribute.

9. A system according to claim 1, further comprising a control panel for receiving the information and for providing the secure access requested.

10. A system according to claim 9 wherein the control panel includes a converter for receiving the secure wireless signal and for outputting the information.

11. A system according to claim 9, wherein the biometric sensor authenticates the identity of the user by comparing a biometric input from the user with a biometric signature for the user in the biometric database.

12. A system according to claim 9, wherein the secure wireless signal comprises an RF carrier and a rolling code.

13. A system according to claim 10, wherein the secure wireless signal comprises an RF carrier and a rolling code, and the converter converts the rolling code to the Wiegand protocol.

14. A transmitter sub-system for operating in a system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a receiver sub-system comprising means for receiving a secure access signal transmitted by the transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal; wherein the transmitter subsystem comprises:

a biometric sensor for receiving a biometric signal;

means for enrolling relevant signatures into the database using the biometric sensor; wherein the means for enrolling relevant signatures into the database of biometric signatures comprises:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for enrolling relevant signatures into the database according to the instruction;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and

means for emitting the secure access signal conveying said information dependent upon said accessibility attribute.

15. A transmitter sub-system according to claim 14, wherein the biometric sensor and the transmitter are located in a remote portable key fob.

16. A transmitter sub-system according to claim 14 further comprising:

means for providing a signal for directing input of the series of entries of the biometric signal; and

means for incorporating into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database, said identification field for use in constructing an audit trail of biometric signals provided to the biometric sensor for the purpose of accessing the controlled item.

17. A transmitter sub-system according to claim 16, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class.

18. A transmitter sub-system according to claim 17, wherein the accessibility attribute comprises:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

19. A transmitter sub-system according to claim 18, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class and a system user class.

20. A transmitter sub-system according to claim 18, wherein the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

21. A receiver sub-system for operating in a system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a transmitter subsystem comprising:

a biometric sensor for receiving a biometric signal;

means for enrolling relevant signatures into the database using the biometric sensor; wherein the means for enrolling relevant signatures into the database of biometric signatures comprises:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for enrolling relevant signatures into the database according to the instruction, the transmitter sub-system further comprising:

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute;

wherein the receiver sub-system comprises;

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information.

22. A receiver sub-system according to claim 21 wherein the biometric sensor and the transmitter are located in a remote portable key fob.

23. A receiver sub-system according to claim 21, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class and a system user class.

24. A receiver sub-system according to claim 23, wherein the accessibility attribute comprises:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

25. A receiver sub-system according to claim 24, wherein said conditional access comprises one of:

provision of access to the controlled item if the accessibility attribute comprises an access attribute;

provision of access to the controlled item and sounding of an alert if the accessibility attribute comprises a duress attribute; and

denial of access to the controlled item and sounding of an alert if the accessibility attribute comprises an alert attribute.

26. A receiver sub-system according to claim 25, wherein the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

27. A method for providing secure access to a controlled item, the method comprising the steps of:

enrolling, by a transmitter sub-system, relevant signatures into a database using a biometric sensor, by receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry, mapping said series into an instruction, and enrolling relevant signatures into the database according to the instruction;

receiving, by the transmitter sub-system, a biometric signal;

matching, by the transmitter sub-system, the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated;

emitting, by the transmitter sub-system, a secure access signal conveying information dependent upon said accessibility attribute; and

providing conditional access to the controlled item dependent upon said information.

28. A method according to claim 27, wherein the transmitter sub-system and the biometric sensor are located in a remote portable key fob.

29. A method according to claim 27, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class.

30. A method according to claim 29, wherein the accessibility attribute comprises:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures, and wherein the step of providing said conditional access comprises the steps of:

providing access to the controlled item if the accessibility attribute comprises an access attribute;

providing access to the controlled item and sounding an alert if the accessibility attribute comprises a duress attribute; and

denying access to the controlled item and sounding an alert if the accessibility attribute comprises an alert attribute.

31. A method for enrolling, by a transmitter subsystem, relevant signatures into a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising:

said database of biometric signatures;

the transmitter sub-system comprising:

a biometric sensor configured for receiving a biometric signal;

means for enrolling relevant signatures into the database using the biometric sensor;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute; and

a receiver sub-system comprising:

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon information in said secure access signal; said method comprising the steps of:

receiving, by the transmitter sub-system, a series of entries of the biometric signal characterised according to at least one of the number of said entries and a duration of each said entry;

determining, by the transmitter sub-system, at least one of the number of said entries and a duration of each said entry;

mapping, by the transmitter sub-system, said series into an instruction; and

enrolling, by the transmitter sub-system, said relevant signatures into the database according to the instruction.

32. A method according to claim 31, wherein the transmitter subsystem is located in a remote portable key fob.

33. A method for transmitting a secure access signal in a system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a receiver sub-system comprising:

means for receiving the secure access signal transmitted by a transmitter sub-system, the transmitter sub-system comprising a biometric sensor and being configured for enrolling relevant signatures into the database using the biometric sensor by receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry, mapping said series into an instruction, and enrolling relevant signatures into the database according to the instruction;

means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal; said method comprising the steps of:

receiving, by the transmitter sub-system, a biometric signal by the biometric sensor;

matching, by the transmitter sub-system, the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and

emitting, by the transmitter sub-system, the secure access signal conveying said information dependent upon said accessibility attribute.

34. A method according to claim 33, wherein the transmitter sub-system is located in a remote portable key fob.

35. A method for receiving a secure access signal in a system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a transmitter subsystem, comprising:

a biometric sensor for receiving a biometric signal;

means for enrolling relevant signatures into the database using the biometric sensor by receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry, mapping said series into an instruction, and enrolling relevant signatures into the database according to the instruction;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute, said method comprising the steps of:

receiving the transmitted secure access signal; and

providing conditional access to the controlled item dependent upon said information.

36. A method according to claim 35, wherein the transmitter sub-system is located in a remote portable key fob.

37. An apparatus for providing secure access to a controlled item, said apparatus comprising:

a transmitter sub-system comprising:

a biometric sensor for receiving a biometric signal;

means for enrolling relevant signatures into a database using the biometric sensor; wherein the means for enrolling relevant signatures into the database of biometric signatures comprises:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for enrolling relevant signatures into the database according to the instruction; the transmitter sub-system further comprising:

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute; and wherein conditional access is provided to the controlled item dependent upon said information.

38. A method according to claim 37, wherein the transmitter sub-system is located in a remote portable key fob.

39. An apparatus, in a transmitter sub-system, for enrolling relevant signatures into a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising:

said database of biometric signatures;

the transmitter subsystem, comprising:

a biometric sensor for receiving a biometric signal;

means for enrolling relevant signatures into the database using the biometric sensor;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute; the system further comprising:

a receiver sub-system comprising:

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon information in said secure access signal; said apparatus comprising:

means for receiving a series of entries of the biometric signal;

means for determining at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for enrolling relevant signatures into the database according to the instruction.

40. An apparatus according to claim 39, wherein the transmitter sub-system is located in a remote portable key fob.

41. A method of enrolling a biometric signature into a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising:

said database of biometric signatures;

a transmitter subsystem for receiving a biometric signal, the transmitter sub-system comprising:

a biometric sensor;

means for enrolling relevant signatures into the database using the biometric sensor; wherein the means for enrolling relevant signatures into the database of biometric signatures comprises:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for enrolling relevant signatures into the database according to the instruction;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute; the system further comprising:

a receiver sub-system comprising:

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon information in said secure access signal; said method comprising the steps of:

receiving a biometric signal; and

enrolling the relevant signatures into the database using the biometric sensor as an administrator if the database of biometric signatures is empty.

42. A method according to claim 41, wherein the transmitter sub-system is located in a remote key fob.

43. A method according to claim 41 wherein the enrolling step comprises receiving another biometric signal to confirm the enrolling of the biometric as an administrator.

44. A method according to claim 43 wherein the enrolling step is performed dependent upon generation of a feedback signal adapted to direct provision of at least one of the biometric signal and the other biometric signal.

Abstract

A system is disclosed for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth.TM. protocol, and a WiFi.TM. protocol, and a receiver sub-system comprising means for receiving the transmitted secure access signal and means for providing conditional access to the controlled item dependent upon said information.

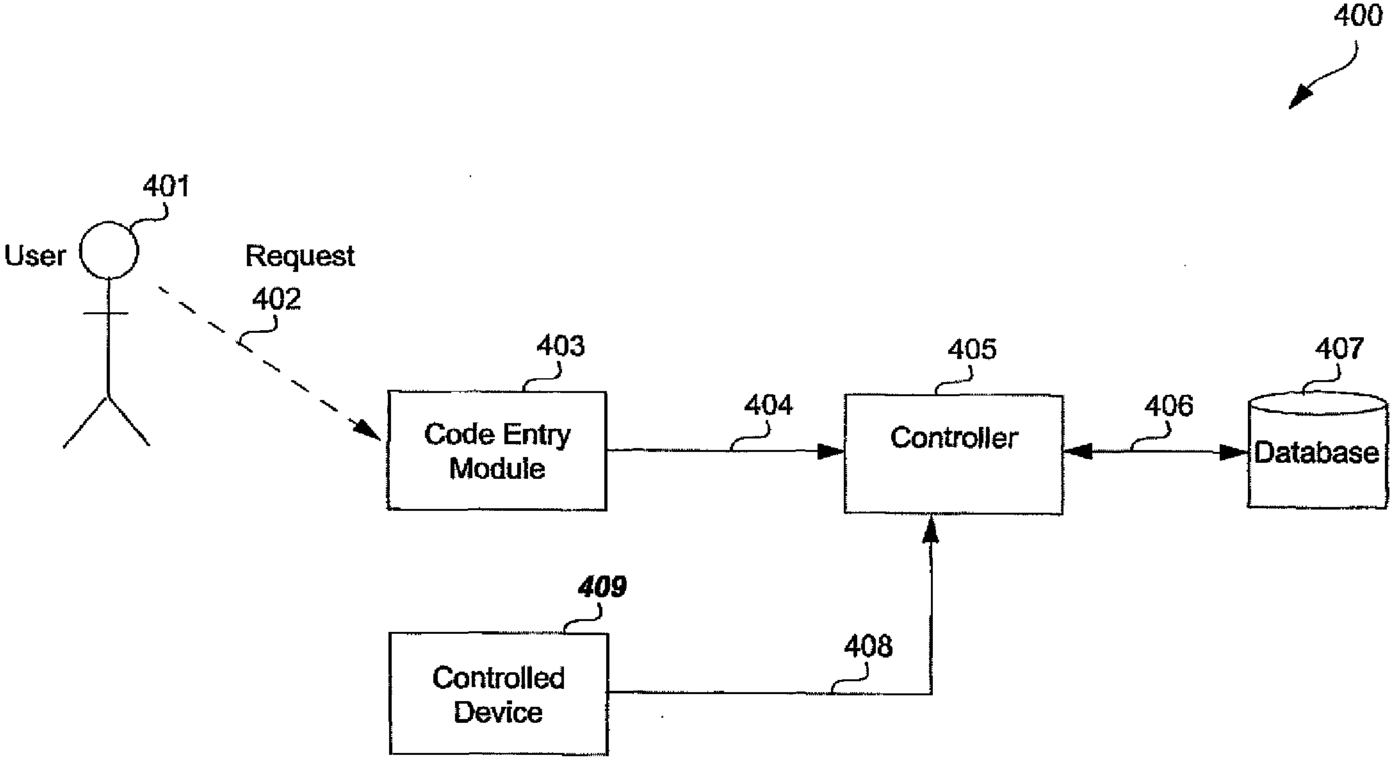


Fig. 1
(prior art)

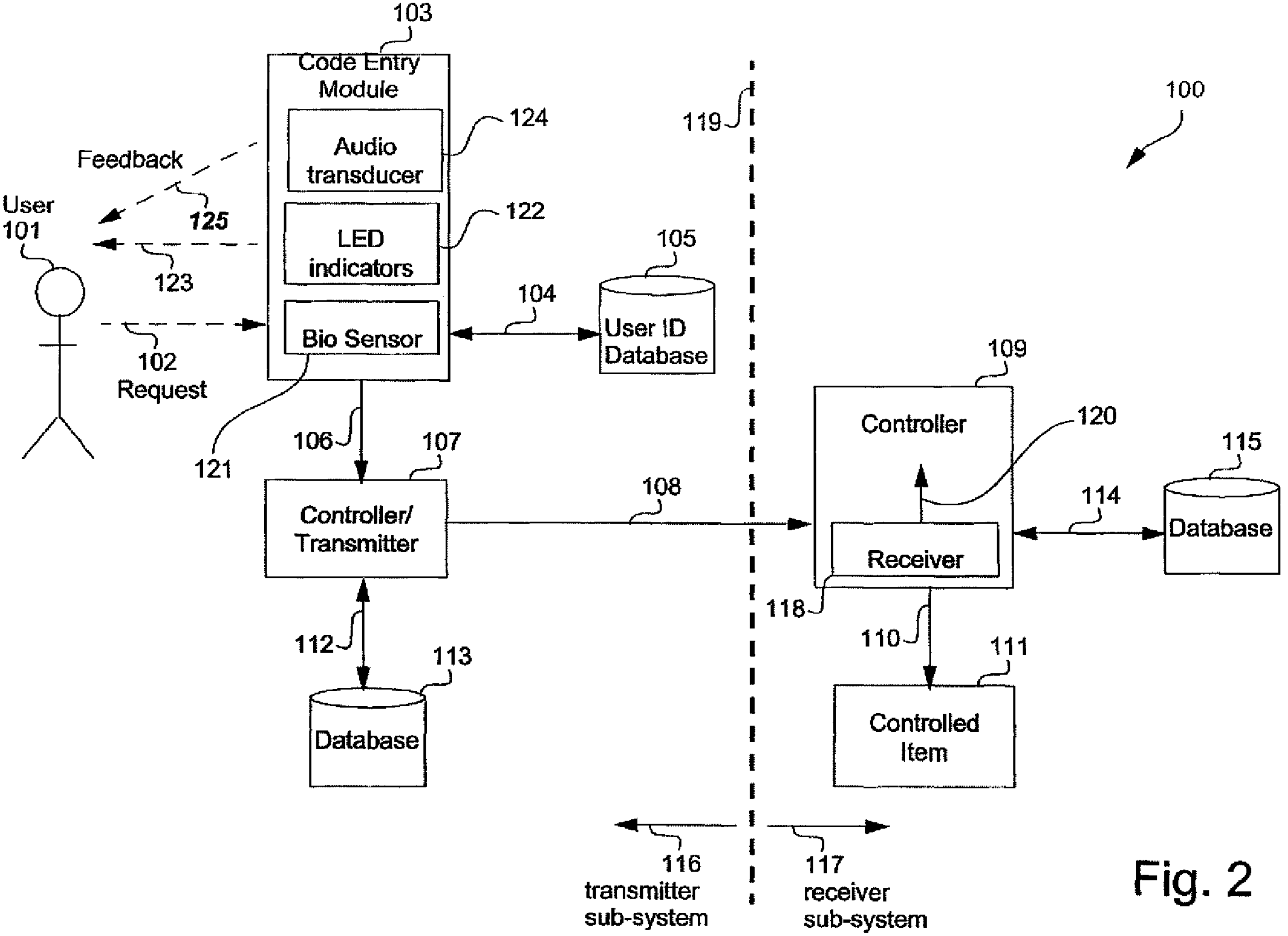

103
Code Entry Module
Audio transducer
124
LED indicators
122
Bio Sensor
121
Feedback
125
User
101
123
102
Request
104
105
User ID Database
106
107
Controller/ Transmitter
112
113
Database
108
119
100
109
Controller
120
Receiver
118
115
114
Database
110
111
Controlled Item
116
transmitter sub-system
117
receiver sub-system

Fig. 2

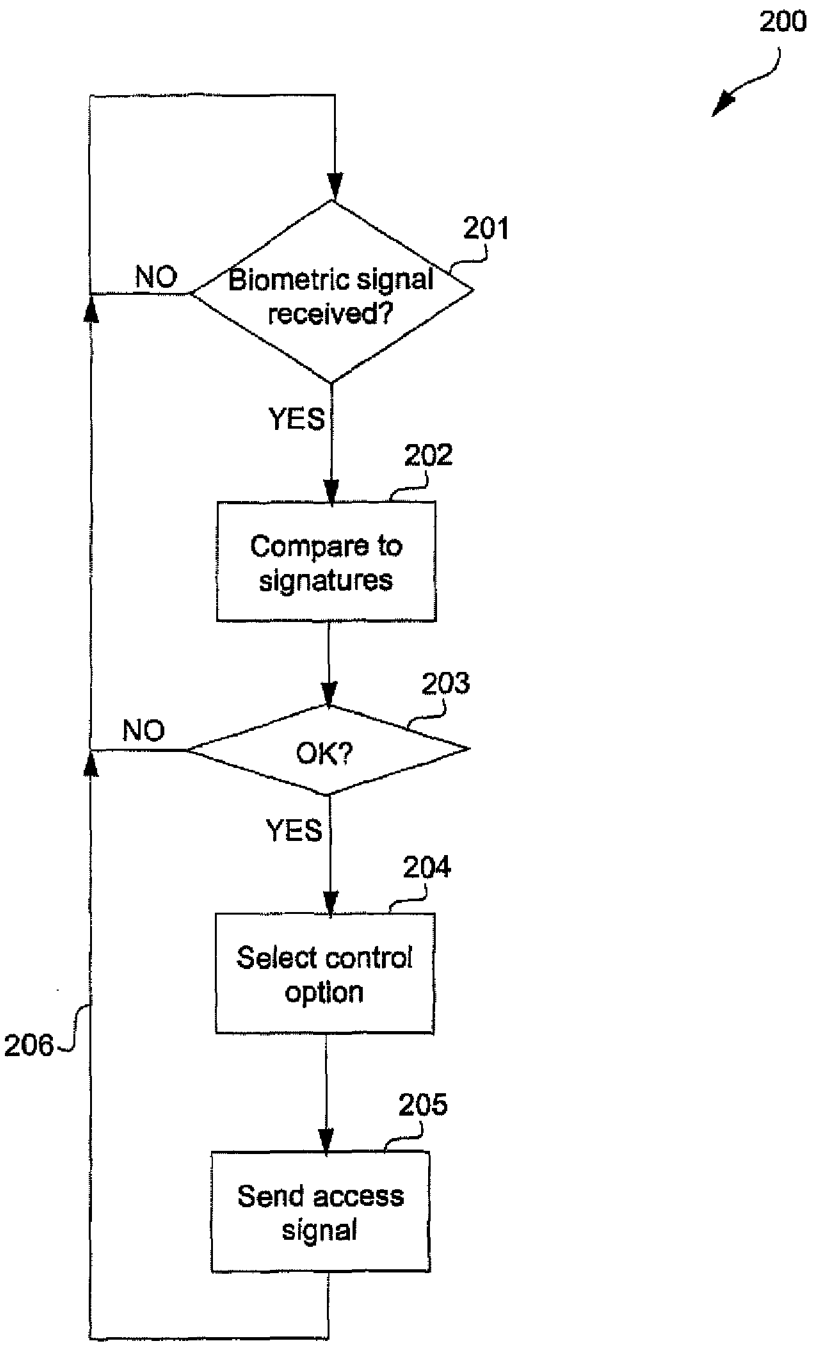

200
201
Biometric signal received?
NO
YES
202
Compare to signatures
203
OK?
NO
YES
204
Select control option
205
Send access signal
206

Fig. 3

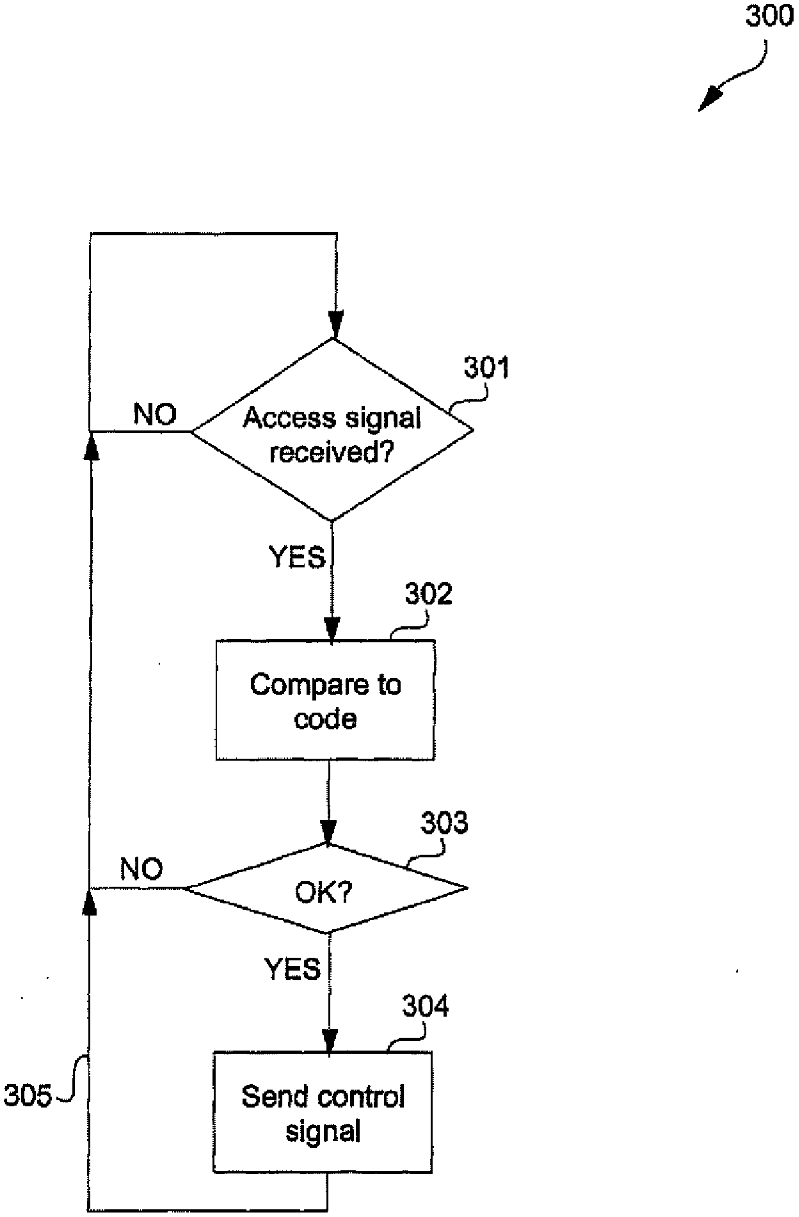

300
Access signal received?
301
NO
YES
Compare to code
302
OK?
303
NO
YES
Send control signal
304
305

Fig. 4

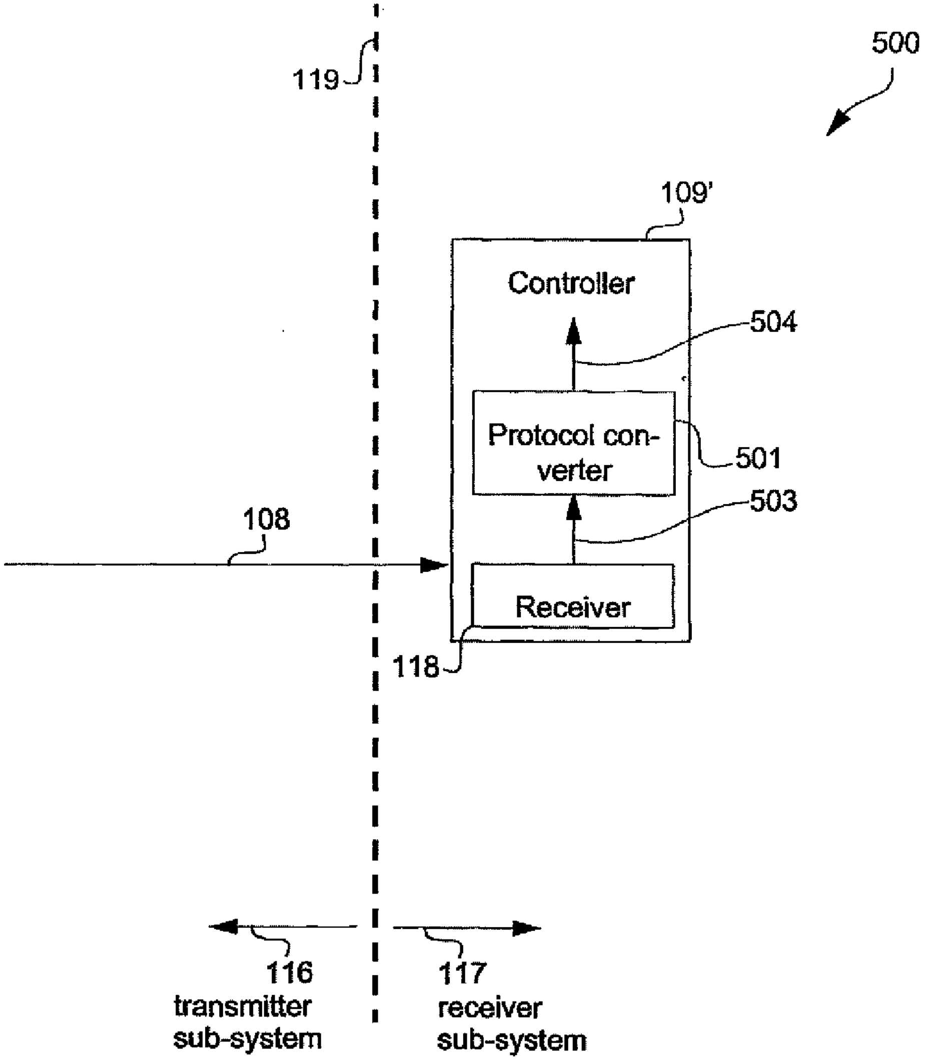

500
119
109'
Controller
504
Protocol converter
501
503
108
Receiver
118
116
transmitter sub-system
117
receiver sub-system

Fig. 5

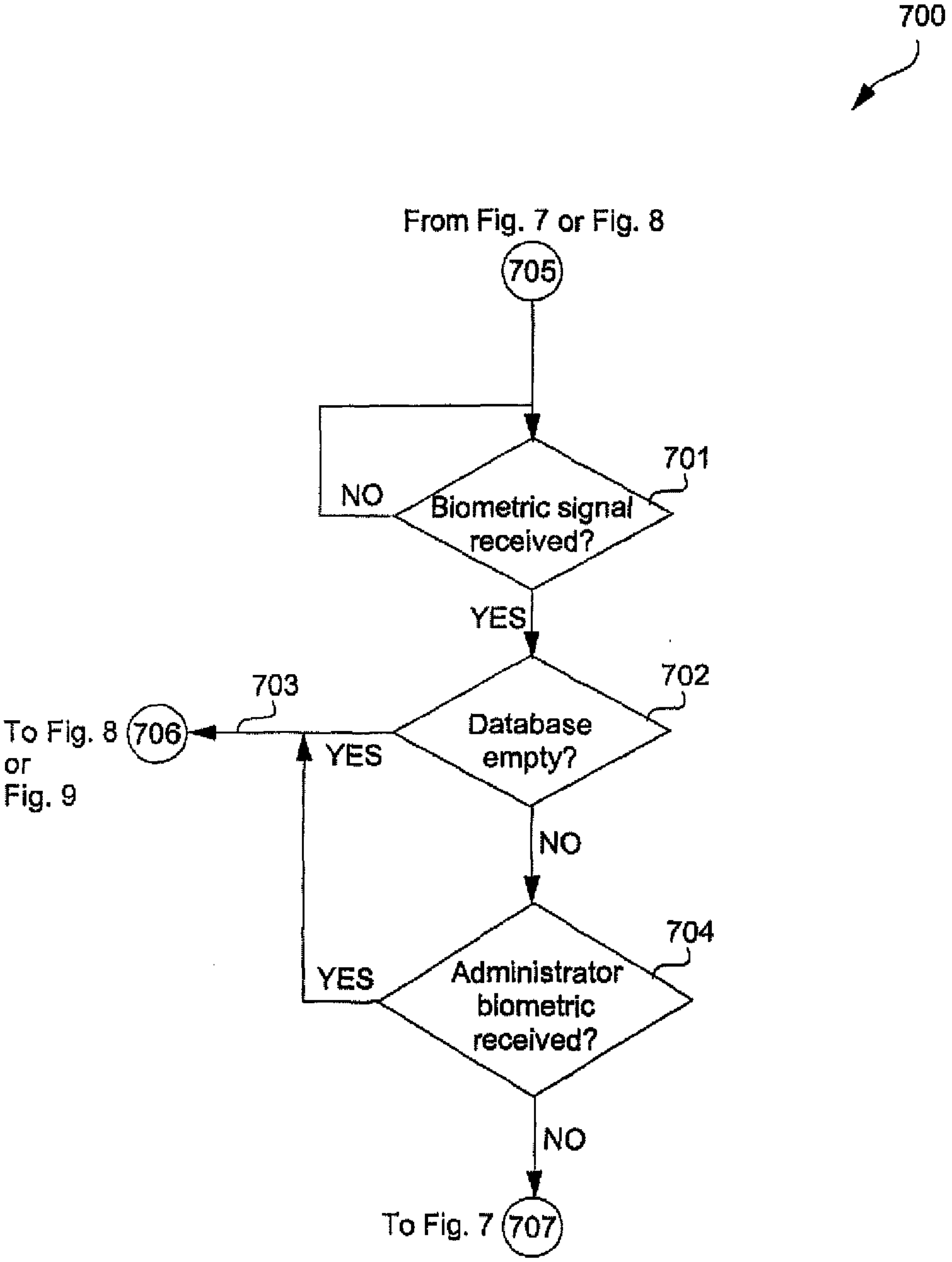

700
From Fig. 7 or Fig. 8
705
701
NO
Biometric signal received?
YES
702
703
To Fig. 8
706
or
Fig. 9
YES
Database empty?
NO
704
YES
Administrator biometric received?
NO
To Fig. 7
707

Fig. 6

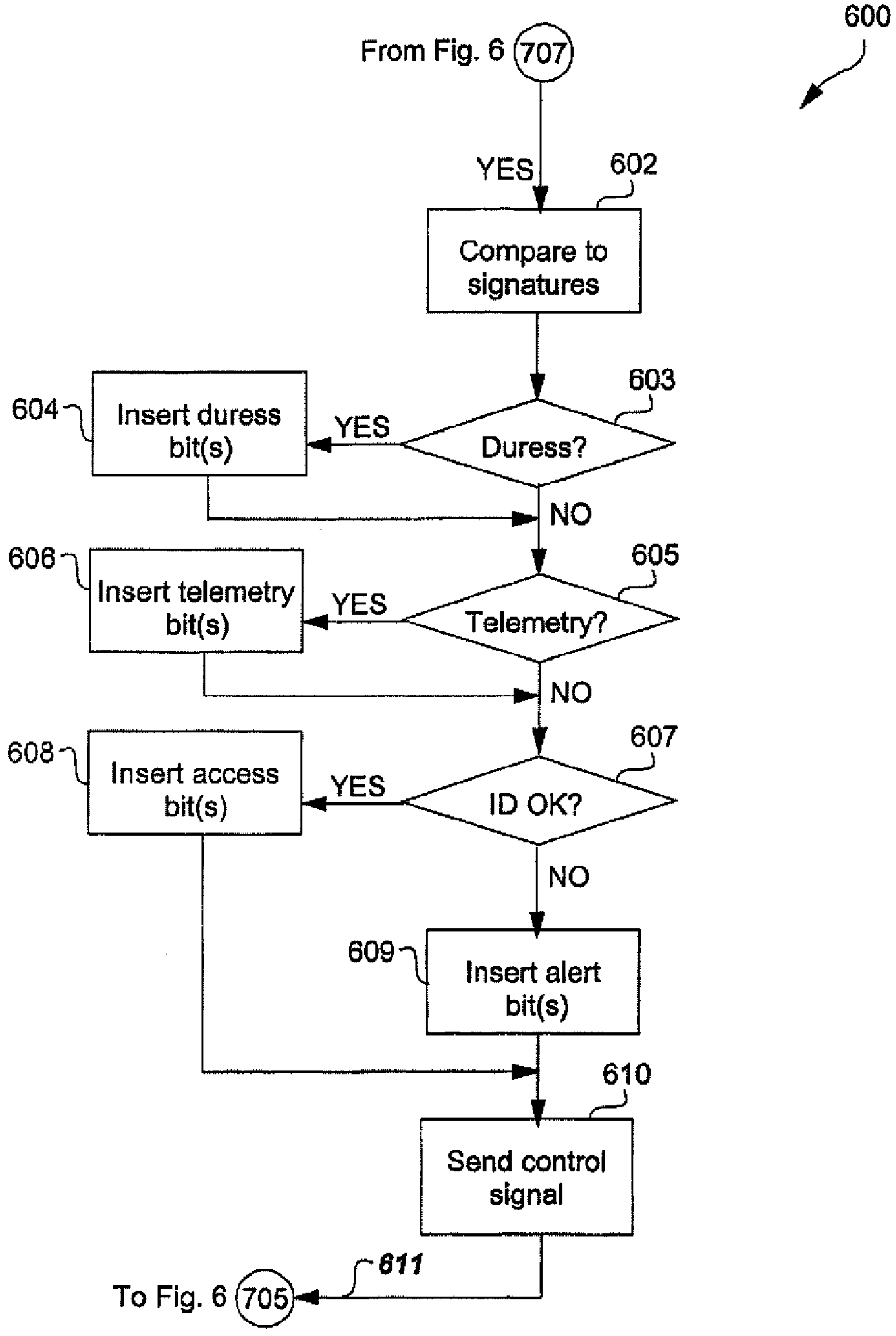

600
From Fig. 6
707
YES
602
Compare to signatures
603
Duress?
YES
604
Insert duress bit(s)
NO
605
Telemetry?
YES
606
Insert telemetry bit(s)
NO
607
ID OK?
YES
608
Insert access bit(s)
NO
609
Insert alert bit(s)
610
Send control signal
611
To Fig. 6
705

Fig. 7

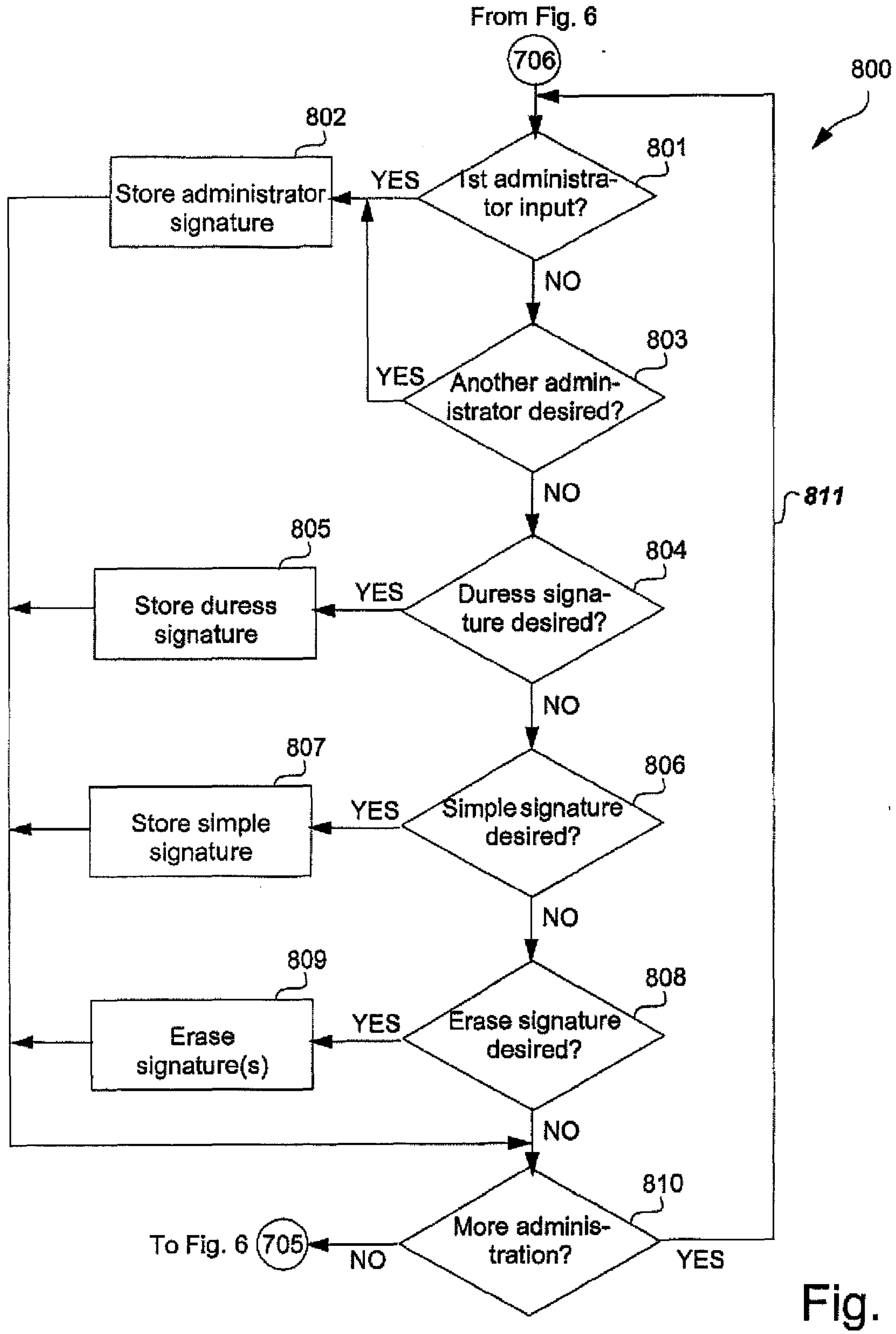

From Fig. 6
706
800
802
Store administrator signature
YES
801
1st administrator input?
NO
803
YES
Another administrator desired?
NO
811
805
Store duress signature
YES
804
Duress signature desired?
NO
807
Store simple signature
YES
806
Simple signature desired?
NO
809
Erase signature(s)
YES
808
Erase signature desired?
NO
810
To Fig. 6
705
NO
More administration?
YES

Fig. 8

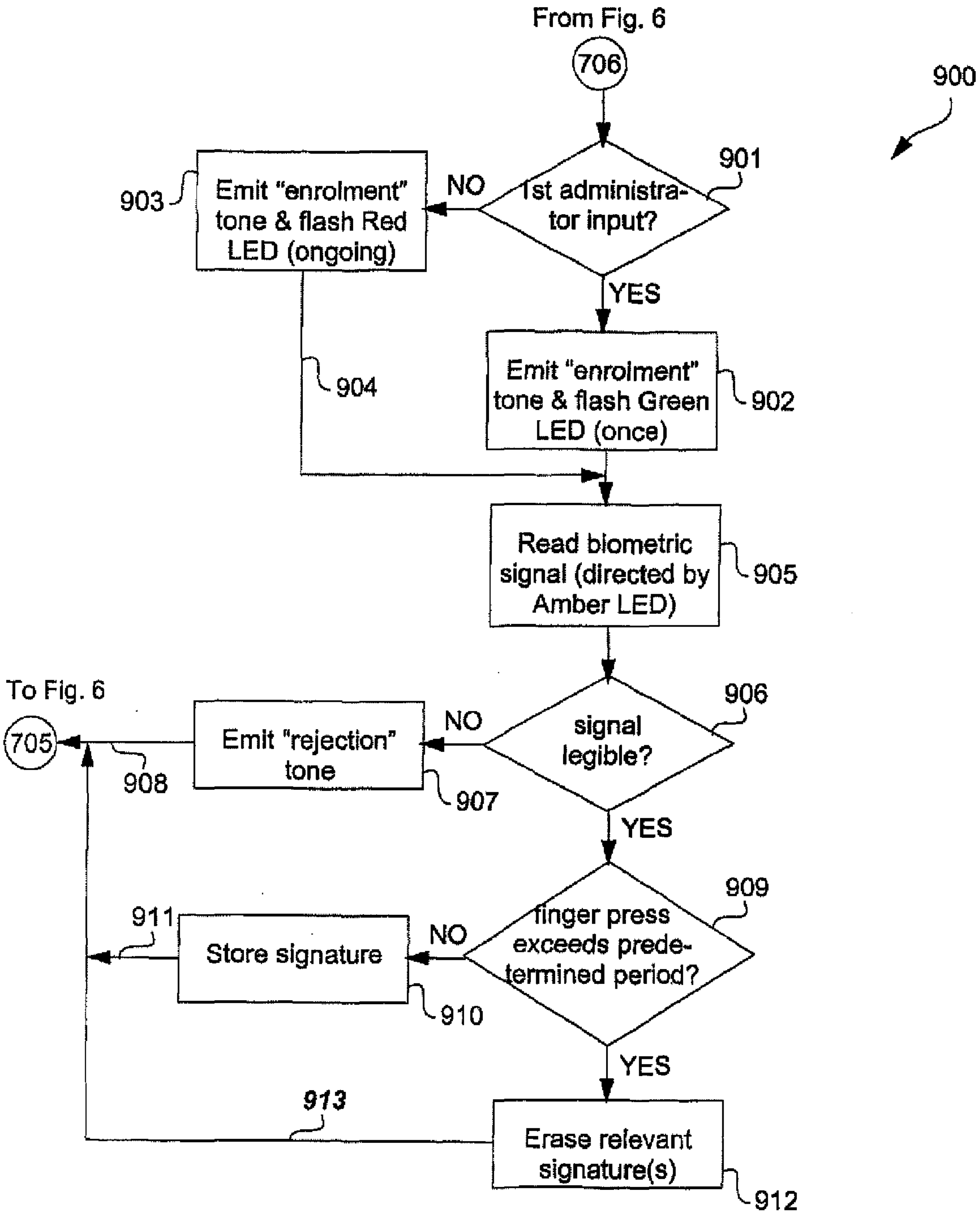

From Fig. 6
706
900
901
1st administrator input?
NO
903
Emit "enrolment" tone & flash Red LED (ongoing)
YES
Emit "enrolment" tone & flash Green LED (once)
902
904
Read biometric signal (directed by Amber LED)
905
906
signal legible?
NO
Emit "rejection" tone
907
To Fig. 6
705
908
YES
909
finger press exceeds predetermined period?
NO
Store signature
910
911
YES
913
Erase relevant signature(s)
912

Fig. 9

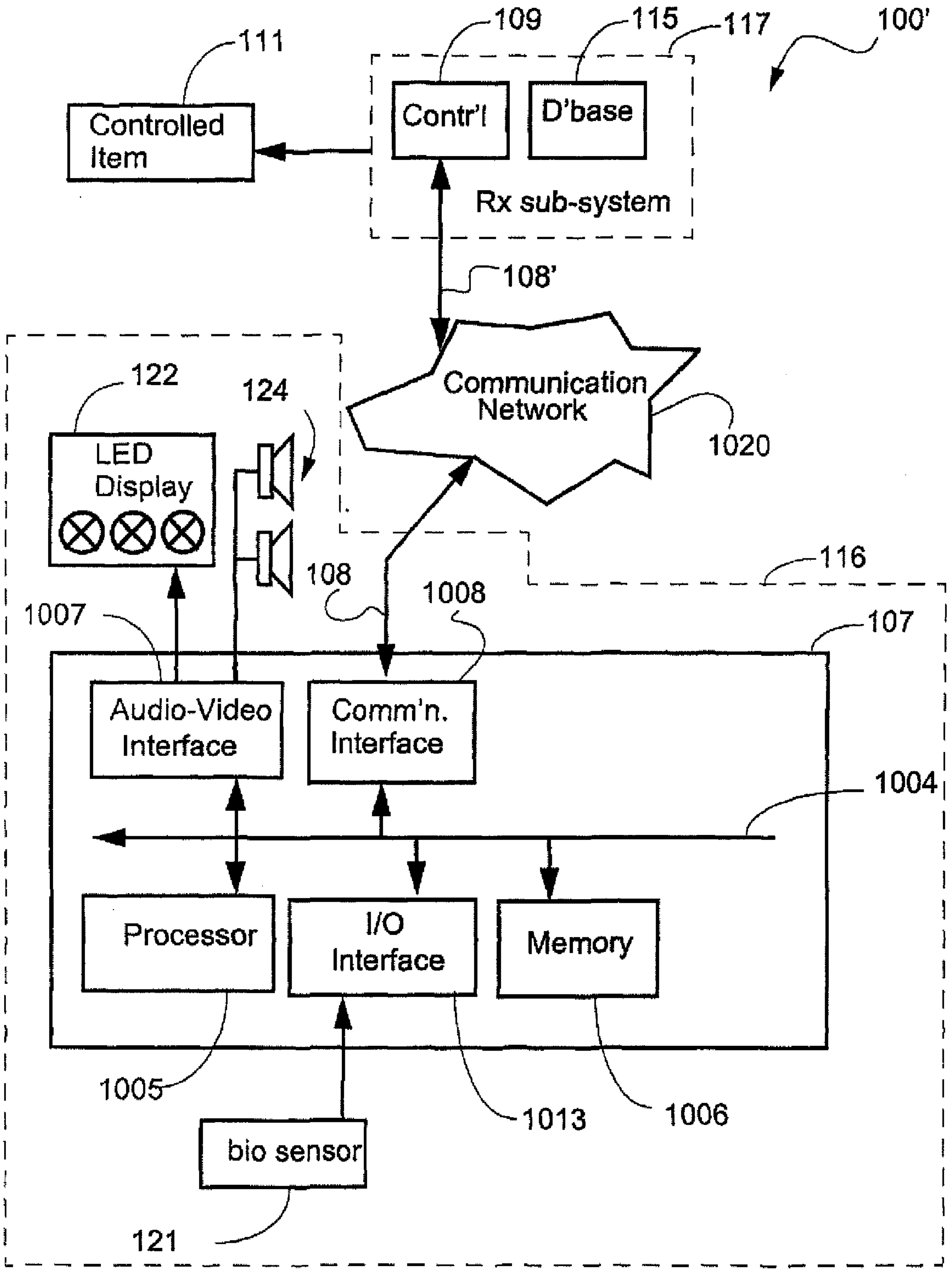

111
Controlled Item
109
115
117
100'
Contr'l
D'base
Rx sub-system
108'
Communication Network
1020
122
LED Display
124
108
1008
116
1007
107
Audio-Video Interface
Comm'n. Interface
1004
Processor
I/O Interface
Memory
1005
1013
1006
bio sensor
121

Fig. 10

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Filer:	Robert Dalton Summers/Lori Peterson
Attorney Docket Number:	12838/8

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	95	95
Utility Search Fee	2111	1	310	310
Utility Examination Fee	2311	1	125	125
Pages:				
Claims:				
Claims in excess of 20	2202	24	30	720
Independent claims in excess of 3	2201	7	125	875
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**2125**

Electronic Acknowledgement Receipt

EFS ID:	13470510
Application Number:	13572166
International Application Number:	
Confirmation Number:	9752
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Customer Number:	757
Filer:	Robert Dalton Summers/Nkosi Harvey
Filer Authorized By:	Robert Dalton Summers
Attorney Docket Number:	12838/8
Receipt Date:	10-AUG-2012
Filing Date:	
Time Stamp:	16:26:37
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2125
RAM confirmation Number	3328
Deposit Account	231925
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	128388at.pdf	99676 fea881a64594ef519ed0c57be3447e152ee4fef3	no	2
Warnings:					
Information:					
2	Oath or Declaration filed	128386dec.pdf	137784 fd4b06278e332f25730ba24a2a462a30d8eef629	no	2
Warnings:					
Information:					
3	Power of Attorney	128386poa.pdf	71577 3aba623839244e1ccc60d76ed764e314d1d51d5d	no	1
Warnings:					
Information:					
4		128388conapp.pdf	1744460 e692c948ae2e0d36a8f175b0b6fc62311e625778	yes	38
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Specification		1	23	
	Claims		24	37	
	Abstract		38	38	
Warnings:					
Information:					
5	Drawings-only black and white line drawings	128388figs.pdf	114681 faff02b1f3d1348c3ae0947f6161a20db1a6cb00	no	10
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	37866 66801513cefb51302e0d1749626d52467d352e3d	no	2
Warnings:					

Information:	
Total Files Size (in bytes):	2206044

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	13470510
Application Number:	13572166
International Application Number:	
Confirmation Number:	9752
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Customer Number:	757
Filer:	Robert Dalton Summers/Nkosi Harvey
Filer Authorized By:	Robert Dalton Summers
Attorney Docket Number:	12838/8
Receipt Date:	10-AUG-2012
Filing Date:	
Time Stamp:	16:26:37
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2125
RAM confirmation Number	3328
Deposit Account	231925
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

<table>
<tr><th>Document Number</th><th>Document Description</th><th>File Name</th><th>File Size(Bytes)/ Message Digest</th><th>Multi Part /.zip</th><th>Pages (if appl.)</th></tr>
<tr><td>1</td><td>Transmittal of New Application</td><td>128388at.pdf</td><td>99676
fea881a64594ef519ed0c57be3447e152ee4fef3</td><td>no</td><td>2</td></tr>
<tr><td colspan="6"><b>Warnings:</b></td></tr>
<tr><td colspan="6"><b>Information:</b></td></tr>
<tr><td>2</td><td>Oath or Declaration filed</td><td>128386dec.pdf</td><td>137784
fd4b06278e332f25730ba24a2a462a30d8eef629</td><td>no</td><td>2</td></tr>
<tr><td colspan="6"><b>Warnings:</b></td></tr>
<tr><td colspan="6"><b>Information:</b></td></tr>
<tr><td>3</td><td>Power of Attorney</td><td>128386poa.pdf</td><td>71577
3aba623839244e1ccc60d76ed764e314d1d51d5d</td><td>no</td><td>1</td></tr>
<tr><td colspan="6"><b>Warnings:</b></td></tr>
<tr><td colspan="6"><b>Information:</b></td></tr>
<tr><td>4</td><td></td><td>128388conapp.pdf</td><td>1744460
e692c948ae2e0d36a8f175b0b6fc62311e625778</td><td>yes</td><td>38</td></tr>
<tr><td rowspan="5"></td><td colspan="5"><b>Multipart Description/PDF files in .zip description</b></td></tr>
<tr><td colspan="2"><b>Document Description</b></td><td><b>Start</b></td><td colspan="2"><b>End</b></td></tr>
<tr><td colspan="2">Specification</td><td>1</td><td colspan="2">23</td></tr>
<tr><td colspan="2">Claims</td><td>24</td><td colspan="2">37</td></tr>
<tr><td colspan="2">Abstract</td><td>38</td><td colspan="2">38</td></tr>
<tr><td colspan="6"><b>Warnings:</b></td></tr>
<tr><td colspan="6"><b>Information:</b></td></tr>
<tr><td>5</td><td>Drawings-only black and white line drawings</td><td>128388figs.pdf</td><td>114681
faff02b1f3d1348c3ae0947f6161a20db1a6cb00</td><td>no</td><td>10</td></tr>
<tr><td colspan="6"><b>Warnings:</b></td></tr>
<tr><td colspan="6"><b>Information:</b></td></tr>
<tr><td>6</td><td>Fee Worksheet (SB06)</td><td>fee-info.pdf</td><td>37866
66801513cefb51302e0d1749626d52467d352e3d</td><td>no</td><td>2</td></tr>
<tr><td colspan="6"><b>Warnings:</b></td></tr>
</table>

Information:	
Total Files Size (in bytes):	2206044

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

BRINKS
HOFER
GILSON
&LIONE

CERTIFICATE OF EFS FILING

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS on the below date:

Date: August 10, 2012 Name: Robert D. Summers, Jr., Reg. No. 57,844 Signature: /Robert D. Summers, Jr./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: **BURKE, Christopher John**

For: **REMOTE ENTRY SYSTEM**

Attorney Docket No.: 12838/8

UTILITY PATENT APPLICATION TRANSMITTAL

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

1. TRANSMITTED HEREWITH: New application under 37 CFR §1.53(b), which is a:

☒ Continuation,

☐ Divisional, or

☐ Continuation-in-Part (CIP)

Under 37 CFR §1.53(b) of prior application no. _____.

Prior application information: Examiner: Rahman, Mohammad L. Art Unit: 2438

☐ Maintenance of copendency of prior application: A request for extension of time and the appropriate fee have been filed in the pending prior application (or are being filed in the prior application concurrently herewith) to extend the period for response until _____.

☐ Certified copy of priority document(s) has been filed in prior application no. _____.

For Continuation or Divisional Applications only: The entire disclosure of the prior application, from which an oath or declaration is supplied as indicated below, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference.

2. ATTACHMENTS: The following application elements and other papers are attached:

☐ Application Data Sheet. See 37 CFR § 1.76.

☐ Title page

☒ Specification, including claims and Abstract (38 pages)

☒ Drawings (ten (10) sheets)

☐ Appendices: _____

☒ Declaration (2 pages):

☐ newly-executed (original or copy)

☒ copy from a prior application (37 CFR §1.63(d))

☐ This application is filed by fewer than all the inventors named in the prior application, 37 CFR §1.53(d)(4). Please DELETE the following inventors(s) named in prior nonprovisional application no. _____: _____

☐ English Translation Document:

☐ is attached or ☐ has been filed in prior application no. _____.

☐ Preliminary Amendment (Note: Related application data required under 37 CFR §1.78, if any, appears in the Amendments to the Specification section of the Preliminary Amendment, including incorporations by reference.)

☐ Petition to Suspend Prosecution for the Time Necessary to File an Amendment (New Application Filed Concurrently).

☐ Information Disclosure Statement, including Form PTO-1449 (_____ sheets) and copies of references cited, if required.

☒ Assignment to: Securicom (NSW) Pty Ltd:

☒ was previously recorded on June 4, 2008 at Reel 021038, Frame 0721.

☒ Power of Attorney (1 pages; ☒ by inventor and/or Officer of the Company).

☒ The power appears in the original papers in the prior application.

☐ The power doesn't appear in the original papers in the prior application, but was filed on _____.

☐ A new power has been executed and is attached.☐ The power of attorney in the prior application is to: _____ (Reg. No. _____).

☐ Nonpublication Request under 35 USC §122(b)(2)(B)(i).

☐ Other: _____.

3. SMALL ENTITY STATUS:

☒ Applicant is small entity (per 37 CFR §1.27).

☐ A small entity statement was filed in prior application no. _____ and such status is still proper and desired.

☐ Small entity status is no longer desired.

4. FEE CALCULATION (AFTER ENTRY OF ANY PRELIMINARY AMENDMENT(S) IN ITEM #2 ABOVE):

Claims as Filed	Col. 1	Col. 2		Small Entity			Not a Small Entity	
For	No. Filed	No. Extra		Rate	Fee	or	Rate	Fee
Basic Fee					$ 95	or		$ 380
Total Claims	44-20	24		24 x $30=	$720	or	x$60=	$
Independent Claims	10-3	7		7 x $125=	$875	or	x$250=	$
Multiple Dependent Claims Present				+$225=	$	or	+$450=	$
Utility Application Size Fee (see MPEP 607 Filing Fee)				No. of pages _____ X .75 = _____ - 100 = _____ / 50 = x $155=	$	or	No. of pages _____ X .75 = _____ - 100 = _____ / 50 = x $310=	$
Search Fee				+$310=	$310	or	+$620=	$
Examination Fee				+$125=	$125	or	+$250=	$
*If the difference in col. 1 is less than zero, enter "0" in col. 2.				Total	$2125	or	Total	$

5. FEE PAYMENT:

☐ Payment by credit card in the amount of $_____ (Form PTO-2038 is attached).
WARNING: Information on this form may become public. **Credit card information should not be included on this form**

☒ Please charge Deposit Account No. 23-1925 in the amount of $2,125.00 for the filing fees.

☒ The Director is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 23-1925.

☒ Any additional filing fees required under 37 CFR § 1.16.

☒ Any patent application processing fees under 37 CFR §1.17.

☐ The Director is hereby authorized to charge payment of the following fees during the pendency of this application or credit any overpayment to Deposit Account No. 23-1925.

☐ Any filing fees under 37 CFR § 1.16 for presentation of extra claims.

☐ Any patent application processing fees under 37 CFR § 1.17.

☐ The issue fee set in 37 CFR § 1.18 at or before mailing of the Notice of Allowance, pursuant to 37 CFR § 1.311(b).

6. CORRESPONDENCE ADDRESS: Please recognize the correspondence address for this application as the address associated with the following Customer Number:

Customer No.: 00757 - Brinks Hofer Gilson Lione

7. PLEASE DIRECT all telephonic communications to: Robert D. Summers, Jr. (telephone: (312) 321-4200).

Respectfully submitted,

August 10, 2012
Date

/Robert D. Summers, Jr./
Robert D. Summers, Jr. (Reg. No. 57,844

Attorney Docket No. 12838/6

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION
(37 C.F.R. §1.63)

As a below named inventor, I hereby declare:

My residence, mailing address, and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor or an original, first and joint inventor of the subject matter that is claimed and for which a patent is sought on the invention entitled:

REMOTE ENTRY SYSTEM

the specification of which (check one)

□ is attached hereto.

☒ was filed on February, 13 2006 as United States Application No. 10/568207
and was amended on February 13, 2006 (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge my duty to disclose to the United States Patent and Trademark Office all information that I know to be material to patentability as defined in 37 C.F.R. §1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. §119(a)-(d) or (f), or §365(b) of any foreign application(s) for patent or inventor's or plant breeder's rights certificate(s), or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's or plant breeder's rights certificate(s) or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application:			Priority Not Claimed
2003904317 (Number)	Australia (Country)	08/13/2003 (Filing Date, MM/DD/YYYY)	□
(Number)	(Country)	(Filing Date, MM/DD/YYYY)	□

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below:

(Application Serial No.)	(Filing Date, MM/DD/YYYY)	(Status: pending, or abandoned)
(Application Serial No.)	(Filing Date, MM/DD/YYYY)	(Status: pending, or abandoned)

I hereby claim the benefit under 35 U.S.C. §120 of any United States applications(s), or §365(c) of any PCT International Application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in 37 C.F.R. §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

PCT/AU2004/001083 (Application Serial No.)	08/13/2004 (Filing Date, MM/DD/YYYY)	Pending (Status: patented, pending, abandoned)
(Application Serial No.)	(Filing Date, MM/DD/YYYY)	(Status: patented, pending, abandoned)
(Application Serial No.)	(Filing Date, MM/DD/YYYY)	(Status: patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. §1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole inventor
BURKE, Christopher John

Sole inventor's signature

19.5.2008
Date (DD/MM/YY)

Residence (City, State/Foreign Country)
Ramsgate NSW, Australia

Citizenship
Australia

Mailing Address
48 Margate Street, Ramsgate, New South Wales 2217, Australia

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/572,166	Filing Date 08/10/2012	□ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☒ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	**95**		N/A	
☒ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	**310**		N/A	
☒ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	**125**		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	44 minus 20 =	* 24	X $30 =	**720**	OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	10 minus 3 =	* 7	X $125 =	**875**		X $ =	
□APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
□ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	**2125**		TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))									
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT		(Column 1)		(Column 2)	(Column 3)					
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))									
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/EVA GILLIS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number
13/572,166

APPLICATION AS FILED - PART I

	(Column 1)	(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE($)	FEE($)		RATE($)	FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	95		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	310		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	125		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	44 minus 20 =	* 24	x 30 =	720	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	10 minus 3 =	* 7	x 125 =	875			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	2125		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/572,166	08/10/2012	Christopher John Burke	12838/8

CONFIRMATION NO. 9752

757
BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

IMPROPER CPOA LETTER

OC000000056095008

Date Mailed: 08/27/2012

NOTICE REGARDING POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/10/2012. The Power of Attorney in this application is not accepted for the reason(s) listed below:

- The Power of Attorney is from an assignee and the Certificate required by 37 CFR 3.73(b) has not been received.

/dnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/572,166	08/10/2012	3685	2125	12838/8	44	10

CONFIRMATION NO. 9752

757
BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

FILING RECEIPT

OC000000056141238

Date Mailed: 08/27/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Christopher John Burke, Ramsgate, AUSTRALIA;

Assignment For Published Patent Application

Securicom (NSW) Pty Ltd.

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 10/568,207 06/04/2008 PAT 8266442
which is a 371 of PCT/AU2004/001083 08/13/2004

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)
AUSTRALIA 2003904317 08/13/2003

Request to Retrieve - This application either claims priority to one or more applications filed in an intellectual property Office that participates in the Priority Document Exchange (PDX) program or contains a proper **Request to Retrieve Electronic Priority Application(s)** (PTO/SB/38 or its equivalent). Consequently, the USPTO will attempt to electronically retrieve these priority documents.

If Required, Foreign Filing License Granted: 08/22/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/572,166**

Projected Publication Date: 12/06/2012

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****
Title

REMOTE ENTRY SYSTEM

Preliminary Class

705

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS pursuant to 37 CFR §1.8 on the below date:

Date: October 01, 2012 Name: Robert D. Summers, Jr., Reg. No. 57,844 Signature: ____________________

BRINKS
HOFER
GILSON
&LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: BURKE, Christopher John

Application No.: 13/572,166

Filed: August 10, 2012

For: REMOTE ENTRY SYSTEM

Attorney Docket No: 12838/8

Examiner: Not Yet Assigned

Art Unit: 2438

Confirmation No.: 9752

TRANSMITTAL

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Attached are:

☒ Transmittal Letter; Statement Under 37 CFR §3.73(b); Power of Attorney.

Fee calculation:

☒ No additional fee is required.

☒ Small Entity.

☐ An extension fee in an amount of $____ for a ____-month extension of time under 37 CFR § 1.17(__).

☐ A petition or processing fee in an amount of $_____ under 37 CFR § 1.17(_____).

☐ An additional filing fee has been calculated as shown below:

						Small Entity			Not a Small Entity	
	Claims Remaining After Amendment		Highest No. Previously Paid For	Present Extra		Rate	Add'l Fee	OR	Rate	Add'l Fee
Total		Minus				x $30=			x $60=	$
Indep.		Minus				x 125=			x $250=	
First Presentation of Multiple Dep. Claim						+$225=			+ $450=	
						Total	$		Total	$

Fee payment:

☐ Please charge Deposit Account No. 23-1925 in the amount of $____ for the filing fee.

☐ Payment by credit card in the amount of $_____ (Form PTO-2038 is attached).

☒ The Director is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 associated with this paper (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925.

Respectfully submitted,

October 01, 2012
Date

Robert D. Summers, Jr. (Reg. No. 57,844)

Attorney Docket No. 12838/8

STATEMENT UNDER 37 CFR §3.73(b)

Applicant/Patent Owner: BURKE, Christopher John

Application/Patent No.: 13/572,166 Filed/Issue Date: August 10, 2012

Title: REMOTE ENTRY SYSTEM

Securicom (NSW) Pty Ltd a corporation
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1 ☒ the assignee of the entire right, title, and interest; or

2. □ an assignee of less than the entire right, title and interest
(The extent (by percentage) of its ownership interest is _____ %); or

3. □ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made) in the patent application/patent identified above by virtue of either:

A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the U.S. Patent and Trademark Office at Reel 021038, Frame 0721, or for which a copy thereof is attached.

OR

B. □ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows::

1. From: _____ To: _____
The document was recorded in the U.S. Patent and Trademark Office at
Reel ______, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____
The document was recorded in the U.S. Patent and Trademark Office at
Reel ______, Frame _____, or for which a copy thereof is attached.

3. From: _____ To: _____
The document was recorded in the U.S. Patent and Trademark Office at
Reel ______, Frame _____, or for which a copy thereof is attached.

□ Additional documents in the chain of title are listed on a supplemental sheet(s).

□ As required by 37 CFR §3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant **to 37 CFR §3.11.**

[NOTE: A separate copy (i.e., a true copy of the original assignment documents(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Signature

October 1, 2012
Date

Robert D. Summers, Jr.
Printed or Typed Name

312-321-4200
Telephone Number

Attorney
Title

Electronic Acknowledgement Receipt

EFS ID:	13880074
Application Number:	13572166
International Application Number:	
Confirmation Number:	9752
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Customer Number:	757
Filer:	Robert Dalton Summers/Maggie Pieczonka
Filer Authorized By:	Robert Dalton Summers
Attorney Docket Number:	12838/8
Receipt Date:	01-OCT-2012
Filing Date:	10-AUG-2012
Time Stamp:	16:36:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	128388tl.pdf	14596 61dda4a9e67218267b3df1b25957ecfe7c83f15a	no	1

Warnings:

Information:

2	Assignee showing of ownership per 37 CFR 3.73.	128388373b.pdf	11548 32629a64a4872999e755cfe36dadbb7b878d61fa	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	26144	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/572,166	08/10/2012	Christopher John Burke	12838/8

CONFIRMATION NO. 9752

POA ACCEPTANCE LETTER

Michael E. Milz
Brinks Hofer Gilson & Lione
P.O. Box 10395
Chicago, IL 60610

OC000000057036094

Date Mailed: 10/12/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/01/2012.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/ddinh/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/572,166	08/10/2012	Christopher John Burke	12838/8

CONFIRMATION NO. 9752

PUBLICATION NOTICE

OC000000058010516

Michael E. Milz
Brinks Hofer Gilson & Lione
P.O. Box 10395
Chicago, IL 60610

Title:REMOTE ENTRY SYSTEM

Publication No.US-2012-0311343-A1
Publication Date:12/06/2012

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

FORM PTO-1449	APPLICATION SERIAL NO. **13/572,166**	CASE NO. 12838/8
LIST OF PATENTS AND PUBLICATIONS FOR APPLICANTS' INFORMATION DISCLOSURE STATEMENT	FILING DATE **August 10, 2012**	GROUP ART UNIT **2438**
Confirmation No. 9752	APPLICANT: **BURKE, Christopher John**	

EXAMINER INITIAL	**OTHER ART – NON PATENT LITERATURE DOCUMENT (Include name of author, title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.**	
	A1	Notice of Acceptance dated September 18, 2012 for co-pending Australian Patent Office Application No. 2009201293 (3 pp.).

EXAMINER	DATE CONSIDERED

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS pursuant to 37 CFR §1.8 on the below date:

Date: December 13, 2012 Name: Robert D. Summers, Jr., Reg. No. 57,844 Signature: /Robert D. Summers, Jr./

BRINKS
HOFER
GILSON
&LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of:	BURKE, Christopher John	
Application No.:	13/572,166	Examiner: Not Yet Assigned
Filed:	August 10, 2012	Art Unit: 2438
For:	REMOTE ENTRY SYSTEM	Confirmation No.: 9752
Attorney Docket No:	12838/8	

TRANSMITTAL

Mail Stop Amendment
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Attached are:

☒ Transmittal Letter; Information Disclosure Statement; PTO Form 1449; copy of cited reference A1 (3 pp.).

Fee calculation:

☒ No additional fee is required.

☒ Small Entity.

☐ An extension fee in an amount of $____ for a ____-month extension of time under 37 CFR § 1.17(__).

☐ A petition or processing fee in an amount of $_____ under 37 CFR § 1.17(_____).

☐ An additional filing fee has been calculated as shown below:

						Small Entity			Not a Small Entity	
	Claims Remaining After Amendment		Highest No. Previously Paid For	Present Extra		Rate	Add'l Fee	OR	Rate	Add'l Fee
Total		Minus				x $31=			x $62=	$
Indep.		Minus				x 125=			x $250=	
First Presentation of Multiple Dep. Claim						+$225=			+ $450=	
						Total	$		Total	$

Fee payment:

☐ Please charge Deposit Account No. 23-1925 in the amount of $____ for the filing fee.

☐ Payment by credit card in the amount of $_____ (Form PTO-2038 is attached).

☒ The Director is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 associated with this paper (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925.

Respectfully submitted,

December 13, 2012
Date

/Robert D. Summers, Jr./
Robert D. Summers, Jr. (Reg. No. 57,844)

Electronic Acknowledgement Receipt

EFS ID:	14451415
Application Number:	13572166
International Application Number:	
Confirmation Number:	9752
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Correspondence Address:	Michael E. Milz Brinks Hofer Gilson & Lione P.O. Box 10395 - Chicago IL 60610 US 3123214200 -
Filer:	Robert Dalton Summers/Maggie Pieczonka
Filer Authorized By:	Robert Dalton Summers
Attorney Docket Number:	12838/8
Receipt Date:	13-DEC-2012
Filing Date:	10-AUG-2012
Time Stamp:	13:02:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	128388IDS.pdf	52815 8ee12b416b5aa1bc18475b05bb28507ef7c4e328	no	2
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	1283881449.pdf	24484 9aa347b85f5f0946baa1d7efa65b9a6e7b8b1ddd	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Non Patent Literature	128388A1.pdf	34053 b01cb0656c36147f36bc41956613249d7e9dd327	no	3
Warnings:					
Information:					
4	Miscellaneous Incoming Letter	128388tl.pdf	41662 9572f22d41694abcde66078251defdb1ce0d63ec	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	153014		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Certificate Under 37 CFR 1.8

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office, Commissioner for Patents, via the EFS on December 13, 2012.

/Robert D. Summers, Jr./
Robert D. Summers, Jr., Reg. No. 57,844

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of:	BURKE, Christopher John	
Application No.:	13/572,166	Examiner: Not Yet Assigned
Filed:	August 10, 2012	Art Unit: 2438
For:	REMOTE ENTRY SYSTEM	Confirmation No.: 9752
Attorney Docket No:	12838/8	

INFORMATION DISCLOSURE STATEMENT

In accordance with the duty of disclosure under 37 C.F.R. §1.56 and §§1.97-1.98, and more particularly in accordance with 37 C.F.R. §1.97(b), Applicant hereby cites the following reference:

OTHER ART

Notice of Acceptance dated September 18, 2012 for co-pending Australian Patent Office Application No. 2009201293 (3 pp.).

Applicant is enclosing Form PTO-1449 (one sheet), along with a copy of cited reference A1, which is required under 37 C.F.R. §1.98(a)(2). As the listed reference is in English, no further commentary is believed to be necessary, 37 C.F.R §1.98(a)(3). Applicant respectfully requests the Examiner's consideration of the above reference and entry thereof into the record of this application.

By submitting this Statement, Applicant is attempting to fully comply with the duty of candor and good faith mandated by 37 CFR §1.56. As such, this Statement is not intended to constitute an admission that the enclosed reference, or other information referred to therein, constitutes “prior art” or is otherwise "material to patentability," as that phrase is defined in 37 CFR §1.56(a).

Applicant has calculated no fee to be due in connection with the filing of this Information Disclosure Statement. However, the Director is authorized to charge any fee deficiency associated with the filing of this Information Disclosure Statement to a deposit account, as authorized in the Transmittal accompanying this Information Disclosure Statement.

Respectfully submitted,

December 13, 2012	/Robert D. Summers, Jr./
Date	Robert D. Summers, Jr. (Reg. No. 57,844)

United States Patent and Trademark Office

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/572,166	08/10/2012	Christopher John Burke	12838/8	9752

7590 03/26/2014

Michael E. Milz
Brinks Hofer Gilson & Lione
P.O. Box 10395
Chicago, IL 60610

EXAMINER	
RAHMAN, MOHAMMAD L	

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
03/26/2014	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 13/572,166	**Applicant(s)** BURKE, CHRISTOPHER JOHN	
	Examiner MOHAMMAD L. RAHMAN	**Art Unit** 2438	**AIA (First Inventor to File) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *8/10/2012*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-44* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-44* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *8/10/2012* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☒ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date *12/13/2012*.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Claims 1-44 filed 08/10/2012 presented for examination. Claims 1-44 are pending.

Information Disclosure Statement

The information disclosure statement filed 12/13/2012 has been placed in the application file and the information referred to therein has been considered as to the merits.

Oath or Declaration

The Oath filed on 08/10/2012 complies with all the requirements set forth in MPEP 602 and therefore is accepted.

Drawings

The drawings filed on 08/10/2012 have been accepted.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed **terminal disclaimer** in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-44 are provisionally rejected on the ground of **nonstatutory obviousness-type double patenting** as being unpatentable over **claims 1-14 of US Patent # 8,266,442**. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-14 of US

Patent # 8,266,442 contain every element of claims 23-42 of the instant application and thus anticipate the claim of the instant application.

Claims 1-44 of the instant application therefore is/are not patently distinct from the earlier patent claim(s) and as such is/are **unpatentable over obvious-type double patenting**. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim. "*A later patent claim is not patentably distinct from an earlier patent claim if the later claim is **obvious over**, or **anticipated by**, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus). " ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001)."Claim 12 and Claim 13 are generic to the species of invention covered by claim 3 of the patent. Thus, the generic invention is "anticipated" by the species of the patented invention. Cf., Titanium Metals Corp. v. Banner, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985) (holding that an earlier species disclosure in the prior art defeats any generic claim) 4. This court's predecessor has held that, without a terminal disclaimer, the species claims preclude issuance of the generic application. In re Van Ornum, 686 F.2d 937, 944, 214 USPQ 761, 767 (CCPA 1982). Accordingly, absent a terminal disclaimer, claims 12 and 13 were properly rejected under the doctrine of obviousness-type double patenting." (In re Goodman (CA FC) 29 USPQ2d 2010 (12/3/1993).*

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(b):
(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-26, 37-40 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

Claims 1, 3, 14, 21, 37, and 39 are directed towards “a system/an apparatus” claim. Claim elements “means for enrolling, means for receiving, means for mapping, means for matching, means for emitting, means for receiving, means for providing, means for incorporating, means for constructing” is a limitation that invokes 35 U.S.C. 112, sixth paragraph. However, the written description fails to disclose the corresponding structure, material, or acts for the claimed function. Dependent claims 2, 4-13, 15-20, 22-26, 38, and 40 do not cure the deficiencies.

Applicant may:

(a) Amend the claim so that the claim limitation will no longer be interpreted as a limitation under 35 U.S.C. 112, sixth paragraph; or

(b) Amend the written description of the specification such that it expressly recites what structure, material, or acts perform the claimed function without introducing any new matter (35 U.S.C. 132(a)).

If applicant is of the opinion that the written description of the specification already implicitly or inherently discloses the corresponding structure, material, or acts so that one of ordinary skill in the art would recognize what structure, material, or acts perform the claimed function, applicant should clarify the record by either:

(a) Amending the written description of the specification such that it expressly recites the corresponding structure, material, or acts for performing the claimed function and clearly links or associates the structure, material, or acts to the claimed function, without introducing any new matter (35 U.S.C. 132(a)); or

(b) Stating on the record what the corresponding structure, material, or acts, which are implicitly or inherently set forth in the written description of the specification, perform the claimed function. For more information, see 37 CFR 1.75(d) and MPEP §§ 608.01(o) and 2181.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under pre-AIA 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1, 9-12, 14, 21, 23, 27, 29, 31, 33, 35, 37, and 39 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hoffman et al. US 7,152,045 (hereinafter "Hoffman") in view of Igaki et al. US 5,109,428 (hereinafter "Igaki").

> Examiner Notes: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner. A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including non-preferred embodiments. *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), *cert. denied,* 493 U.S. 975 (1989). See MPEP 2123.

Regarding claim 1, Hoffman taught a system for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative***

comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.), the system comprising:

a database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***);

a transmitter subsystem (***i.e. Biometric Input Device, fig. 3 item 12]***) comprising:

a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***);

means for enrolling relevant signatures into the database using the biometric sensor (***See [7:24-26] During a registration step, the individual is to register with the system an authenticated biometric sample; [36:44-46] The purpose of the Biometric Registration Terminal (BRT) is to register new individuals including their biometric-PIC, see further 37:12-14, 49:40-42)***; and

means for enrolling relevant signatures into the database according to the instruction (***see col. 8, lines 25-26***);

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and means for emitting a secure access signal conveying information dependent upon said accessibility attribute (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual***);

said system further comprising:

a receiver sub-system comprising; means for receiving the transmitted secure access signal (***See col. 40, lines 59-62: Individual enters their biometric into the BIA, DPC is receiving biometric input by the ATM***); and

means for providing conditional access to the controlled item dependent upon said information (***see [Col. 40, lines 62-67] the Data processing center (DPC) validates the biometric-PIC and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute], see also [38:53-60] An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. Once the system verifies the individual, the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level.***, **Furthermore** ***[68:10-15] a financial transaction authorization service can decide to deny any request for over $300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. The authorization service can also use the security level as a guide on how much to charge for the transaction, based on risk.***).

Hoffman taught the claimed system. Hoffman is silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught wherein the means for enrolling relevant signatures into the database of biometric signatures comprises: means for receiving a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry; means for mapping said series into an instruction (*see Abstract, "An optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the* *single operation of pressing the fingerpad onto the inspection plate."* This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. *see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary"*).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of Hoffman with the idea of producing a sequence of fingerprint image data of Igaki *[Igaki:1:58-61]* because the use of Igaki could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data from a single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*Ikagi: Col. 1:49-51]*).

Regarding claim 9, Hoffman in view of Igaki further taught a system according to claim 1, further comprising a control panel for receiving the information and for providing the secure access requested (Hoffman, fig. 2, ref. 12).

Regarding claim 10, Hoffman in view of Igaki further taught a system according to claim 9 wherein the control panel includes a converter for receiving the secure wireless signal and for outputting the information (***Hoffman, col. 14, lines 18-24***).

Regarding claim 11, Hoffman in view of Igaki further taught a system according to claim 9, wherein the biometric sensor authenticates the identity of the user by comparing a biometric input from the user with a biometric signature for the user in the biometric database. (***See Hoffman, col. 8, lines 45-50***).

<u>Regarding claim 12</u>, Hoffman in view of Igaki further taught a system according to claim 9, wherein the secure wireless signal comprises an RF carrier and a rolling code (***Hoffman, col. 15, lines 30-36***).

<u>Regarding claim 14,</u> Hoffman taught a transmitter sub-system (***i.e. Biometric Input Device, fig. 3 item 12]***) for operating in a system for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for <u>authorization of transactions and transmissions</u>. The tokenless system and method are principally based on a <u>correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person</u> of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***), the system comprising:

a database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***);

a receiver sub-system comprising means for receiving a secure access signal transmitted by the transmitter sub-system (***See col. 40, lines 59-62: Individual enters their biometric into the BIA, DPC is receiving biometric input by the ATM***), and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal (***see [Col. 40, lines 62-67] the <u>Data processing center (DPC) validates the biometric-PIC</u> and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and <u>examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]</u>, see also [38:53-60] An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. <u>Once the system verifies the individual</u>, <u>the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level.</u>***, **Furthermore** ***[68:10-15] a financial transaction authorization service can decide to deny any request for over $300 from low security BIA, requiring individuals to use higher security***

BIA to authorize such sums. <u>The authorization service can also use the security level as a guide on how much to charge for the transaction, based on risk.</u>);

wherein the transmitter subsystem comprises:

a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***);

means for enrolling relevant signatures into the database using the biometric sensor (***See [7:24-26] During a registration step, <u>the individual is to register with the system an authenticated biometric sample</u>; [36:44-46] The purpose of the Biometric Registration Terminal (BRT) is to <u>register new individuals including their biometric-PIC</u>, see further 37:12-14, 49:40-42***); and

means for enrolling relevant signatures into the database according to the instruction (***see col. 8, lines 25-26***);

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and means for emitting the secure access signal conveying said information dependent upon said accessibility attribute (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual***).

Hoffman taught the claimed system. Hoffman is silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught wherein the means for enrolling relevant signatures into the database of biometric signatures comprises: means for receiving a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry; means for mapping said series into an instruction (*see Abstract, "An optical sensor unit optically* *produces a sequence of fingerprint image data* *during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval.* *A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data* *obtained during the single operation of pressing the fingerpad onto the inspection plate."* This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. *see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary"*).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of Hoffman with the idea of producing a sequence of fingerprint image data of Igaki *[Igaki:1:58-61]* because the use of Igaki could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data from a single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*Ikagi: Col. 1:49-51]*).

Regarding claim 21, Hoffman taught a receiver sub-system for operating in a system for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an***

authenticated biometrics sample of the same type obtained and stored previously.), the system comprising:

a database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***);

a transmitter subsystem (***i.e. Biometric Input Device, fig. 3 item 12]***) comprising:

a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***);

means for enrolling relevant signatures into the database using the biometric sensor (***See [7:24-26] During a registration step, <u>the individual is to register with the system an authenticated biometric sample</u>; [36:44-46] The purpose of the Biometric Registration Terminal (BRT) is to <u>register new individuals including their biometric-PIC</u>, see further 37:12-14, 49:40-42)***; and

means for enrolling relevant signatures into the database according to the instruction ***see col. 8, lines 25-26***),

the transmitter sub-system further comprising:

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and means for emitting a secure access signal conveying information dependent upon said accessibility attribute (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual***);

wherein the receiver sub-system comprises;

means for receiving the transmitted secure access signal; and means for providing conditional access to the controlled item dependent upon said information (***see [Col. 40, lines 62-67] the Data processing center (DPC) validates the biometric-PIC and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute], see also [38:53-60] An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. Once the system verifies the individual, the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level.***, **Furthermore** ***[68:10-15] a financial transaction authorization service can decide to deny any request for over $300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. The authorization service can also use the security level as a guide on how much to charge for the transaction, based on risk.***).

Hoffman taught the claimed system. Hoffman is silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught wherein the means for enrolling relevant signatures into the database of biometric signatures comprises: means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry; means for mapping said series into an instruction (*see Abstract, "An optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate."* This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. *see [1:40-52] "An object of the present invention is to provide* *an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary"*).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of Hoffman with the idea of producing a sequence of fingerprint image data of Igaki *[Igaki:1:58-61]* because the use of Igaki could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data from a single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*Ikagi: Col. 1:49-51]*).

Regarding claim 23, Hoffman-Igaki combination taught a receiver sub-system according to claim 21, wherein the database of biometric signatures comprises signatures in at least **one** of a system administrator class and a system user class (***Hoffman, col. 60, lines 34-43; col. 8, lines 20-55***).

Regarding claim 27, Hoffman taught a method for providing secure access to a controlled item, the method comprising the steps of (***see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***):

enrolling, by a transmitter sub-system, relevant signatures into a database using a biometric sensor (***See [7:24-26] During a registration step, the individual is to register with the system an authenticated biometric sample; [36:44-46] The purpose of the Biometric Registration Terminal (BRT) is to register new individuals including their biometric-PIC, see further 37:12-14, 49:40-42***), and enrolling relevant signatures into the database according to the instruction (***see col. 8, lines 25-26***);

receiving, by the transmitter sub-system, a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***);

matching, by the transmitter sub-system, the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; emitting, by the transmitter sub-system, a secure access signal conveying information dependent upon said accessibility attribute; and providing conditional access to the controlled item dependent upon said information (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual***).

Hoffman taught the claimed system. Hoffman is silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught by receiving a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry, mapping said series into an instruction (*see Abstract, "An optical sensor unit optically* <u>produces a sequence of fingerprint image data</u> *during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval.* <u>*A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data*</u> *obtained during the single operation of pressing the fingerpad onto the inspection plate."* This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. *see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary"*).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of Hoffman with the idea of producing a sequence of fingerprint image data of Igaki *[Igaki:1:58-61]* because the use of Igaki could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data from a single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*Ikagi: Col. 1:49-51]*).

Regarding claim 29, Hoffman-Igaki combination taught a method according to claim 27, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class (***Hoffman, col. 60, lines 34-43; col. 8, lines 20-55***).

Regarding claim 31, Hoffman taught a method for

enrolling, by a transmitter subsystem, relevant signatures into a database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***) in a system for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***), the system comprising:

said database of biometric signatures; the transmitter sub-system (***i.e. Biometric Input Device, fig. 3 item 12]***) comprising:

a biometric sensor configured for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***);

means for enrolling relevant signatures into the database using the biometric sensor (***See [7:24-26] During a registration step, <u>the individual is to register with the system an authenticated biometric sample</u>; [36:44-46] The purpose of the Biometric Registration Terminal (BRT) is to <u>register new individuals including their biometric-PIC</u>, see further 37:12-14, 49:40-42***);

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and means for emitting a secure access signal conveying information dependent upon said accessibility attribute (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual***); and

a receiver sub-system comprising: means for receiving the transmitted secure access signal; and means for providing conditional access to the controlled item dependent upon information in said secure access signal (***see [Col. 40, lines 62-67] the <u>Data processing center (DPC) validates the biometric-PIC</u> and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and <u>examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]</u>, see also [38:53-60] An individual using a***

CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. Once the system verifies the individual, the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level., **Furthermore *[68:10-15] a financial transaction authorization service can decide to deny any request for over $300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. The authorization service can also use the security level as a guide on how much to charge for the transaction, based on risk.***); said method comprising the steps of:

enrolling, by the transmitter sub-system, said relevant signatures into the database according to the instruction (***see col. 8, lines 25-26***).

Hoffman taught the claimed system. Hoffman is silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught receiving, by the transmitter sub-system, a series of entries of the biometric signal characterized according to at least one of the number of said entries and a duration of each said entry; determining, by the transmitter sub-system, at least one of the number of said entries and a duration of each said entry; mapping, by the transmitter sub-system, said series into an instruction (*see Abstract, "An optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate."* This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. *see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing* *down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary”*).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of Hoffman with the idea of producing a sequence of fingerprint image data of Igaki *[Igaki:1:58-61]* because the use of Igaki could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data from a single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*Ikagi: Col. 1:49-51]*).

Regarding claim 33, Hoffman taught a method for transmitting a secure access signal in a system for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***), the system comprising:

a database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***);

a receiver sub-system comprising: means for receiving the secure access signal transmitted by a transmitter sub-system (***See col. 40, lines 59-62: Individual enters their biometric into the BIA, DPC is receiving biometric input by the ATM***),

the transmitter sub-system (***i.e. Biometric Input Device, fig. 3 item 12]***) comprising a biometric sensor (***fig.3, ref. 12; col. 13, lines 2-8***) and being configured for enrolling relevant signatures into the database using the biometric sensor (***See [7:24-26] During a registration step, the individual is to register with the system an authenticated biometric sample; [36:44-46] The purpose of the Biometric Registration Terminal (BRT) is to register new individuals including their biometric-PIC, see further 37:12-14, 49:40-42***), enrolling relevant signatures into the database according to the instruction (***see col. 8, lines 25-26***);

means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal (***see [Col. 40, lines 62-67] the <u>Data processing center (DPC) validates the biometric-PIC</u> and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and <u>examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]</u>, see also [38:53-60] An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. <u>Once the system verifies the individual</u>, <u>the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level.</u>***, **Furthermore** ***[68:10-15] a financial transaction authorization service can decide to deny any request for over $300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. <u>The authorization service can also use the security level as a guide</u> on how much to charge for the transaction, based on risk.***);

said method comprising the steps of: receiving, by the transmitter sub-system, a biometric signal by the biometric sensor (***fig.3, ref. 12; col. 13, lines 2-8***);

matching, by the transmitter sub-system, the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and emitting, by the transmitter sub-system, the secure access signal conveying said information dependent upon said accessibility attribute (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least***

one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual).

Hoffman taught the claimed system. Hoffman is silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry, mapping said series into an instruction (*see Abstract, "An optical sensor unit optically <u>produces a sequence of fingerprint image data</u> during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. <u>A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data</u> obtained during the single operation of pressing the fingerpad onto the inspection plate."* This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. *see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary"*).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of <u>Hoffman</u> with the idea of <u>producing a sequence of fingerprint image</u> data of <u>Igaki</u> *[<u>Igaki</u>:1:58-61]* because the use of <u>Igaki</u> could provide the Biometric Input Device of <u>Hoffman</u> [*<u>Hoffman</u>, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data from a single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*<u>Ikagi</u>: Col. 1:49-51]*).

Regarding claim 35, Hoffman taught a method for receiving a secure access signal in a system for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***), the system comprising:

a database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***);

a transmitter subsystem (***i.e. Biometric Input Device, fig. 3 item 12]***), comprising:

a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***);

means for enrolling relevant signatures into the database using the biometric sensor (***See [7:24-26] During a registration step, the individual is to register with the system an authenticated biometric sample; [36:44-46] The purpose of the Biometric Registration Terminal (BRT) is to register new individuals including their biometric-PIC, see further 37:12-14, 49:40-42***),

enrolling relevant signatures into the database according to the instruction (***see col. 8, lines 25-26***);

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and means for emitting a secure access signal conveying information dependent upon said accessibility attribute (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously***

stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual),

said method comprising the steps of: receiving the transmitted secure access signal (***See col. 40, lines 59-62: Individual enters their biometric into the BIA, DPC is receiving biometric input by the ATM***); and providing conditional access to the controlled item dependent upon said information (***see [Col. 40, lines 62-67] the <u>Data processing center (DPC) validates the biometric-PIC</u> and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and <u>examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]</u>, see also [38:53-60] An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. <u>Once the system verifies the individual</u>, <u>the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level.</u>,*** **Furthermore** ***[68:10-15] a financial transaction authorization service can decide to deny any request for over $300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. <u>The authorization service can also use the security level as a guide</u> on how much to charge for the transaction, based on risk.***).

Hoffman taught the claimed system. Hoffman is silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught by receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry, mapping said series into an instruction (*see Abstract, "An optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate."* This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. *see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary"*).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of Hoffman with the idea of producing a sequence of fingerprint image data of Igaki *[Igaki:1:58-61]* because the use of Igaki could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data from a single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*Ikagi: Col. 1:49-51]*).

Regarding claim 37, Hoffman taught an apparatus for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***), said apparatus comprising:

a transmitter sub-system (***i.e. Biometric Input Device, fig. 3 item 12]***) comprising:

a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***);

means for enrolling relevant signatures into a database using the biometric sensor (***See [7:24-26] During a registration step, <u>the individual is to register with the system an authenticated biometric sample</u>; [36:44-46] The purpose of the Biometric Registration Terminal (BRT) is to <u>register new individuals including their biometric-PIC</u>, see further 37:12-14, 49:40-42)***;

means for enrolling relevant signatures into the database according to the instruction (***see col. 8, lines 25-26***);

the transmitter sub-system further comprising: means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and means for emitting a secure access signal conveying information dependent upon said accessibility attribute; and wherein conditional access is provided to the controlled item dependent upon said information (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual***).

Hoffman taught the claimed system. Hoffman is silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught wherein the means for enrolling relevant signatures into the database of biometric signatures comprises: means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry; means for mapping said series into an instruction (*see Abstract, "An optical sensor unit optically <u>produces a sequence of fingerprint image data</u> during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. <u>A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data</u> obtained during the single operation of pressing the fingerpad onto the inspection plate."* This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. *see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary"*).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of <u>Hoffman</u> with the idea of <u>producing a sequence of fingerprint image</u> data of <u>Igaki</u> *[<u>Igaki</u>:1:58-61]* because the use of <u>Igaki</u> could provide the Biometric Input Device of <u>Hoffman</u> [*<u>Hoffman</u>, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data from a single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*<u>Ikagi</u>: Col. 1:49-51]*).

<u>Regarding claim 39</u>, Hoffman taught an apparatus, in a transmitter sub-system, for enrolling relevant signatures into a database of biometric signatures in a system for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for <u>authorization of</u>***

<u>transactions and transmissions</u>. The tokenless system and method are principally based on a <u>correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person</u> of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.), the system comprising:

said database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***);

the transmitter subsystem (***i.e. Biometric Input Device, fig. 3 item 12]***), comprising:

a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***);

means for enrolling relevant signatures into the database using the biometric sensor (***See [7:24-26] During a registration step, <u>the individual is to register with the system an authenticated biometric sample</u>; [36:44-46] The purpose of the Biometric Registration Terminal (BRT) is to <u>register new individuals including their biometric-PIC</u>, see further 37:12-14, 49:40-42***);

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and means for emitting a secure access signal conveying information dependent upon said accessibility attribute (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and***

displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual);

the system further comprising:

a receiver sub-system comprising: means for receiving the transmitted secure access signal (***See col. 40, lines 59-62: Individual enters their biometric into the BIA, DPC is receiving biometric input by the ATM***); and

means for providing conditional access to the controlled item dependent upon information in said secure access signal (***see [Col. 40, lines 62-67] the Data processing center (DPC) validates the biometric-PIC and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute], see also [38:53-60] An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. Once the system verifies the individual, the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level.***, **Furthermore** ***[68:10-15] a financial transaction authorization service can decide to deny any request for over $300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. The authorization service can also use the security level as a guide on how much to charge for the transaction, based on risk.***);

means for enrolling relevant signatures into the database according to the instruction (***see col. 8, lines 25-26***)

Hoffman taught the claimed system. Hoffman is silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught said apparatus comprising: means for receiving a series of entries of the biometric signal; means for determining at least one of the number of said entries and a duration of each said entry; means for mapping said series into an instruction (*see Abstract, "An optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate."* This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. *see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary"*).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of Hoffman with the idea of producing a sequence of fingerprint image data of Igaki *[Igaki:1:58-61]* because the use of Igaki could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data from a single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*Ikagi: Col. 1:49-51]*).

Claims 2, 15, 22, 28, 32, 34, 36, 38, and 40 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hoffman et al. US 7,152,045 (hereinafter "Hoffman") in view of Igaki et al. US 5,109,428 (hereinafter "Igaki") as applied to claims 1, 14, 21, 27, 31, 33, 35, 37, and 39 above and in further view of Fuks et al. US 6,992,562 hereinafter ("Fuks").

Examiner Notes: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully

> requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner. A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including non-preferred embodiments. *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), *cert. denied,* 493 U.S. 975 (1989). See MPEP 2123.

Regarding claim 2, 15, 22, 28, 32, 34, 36, 38, 40, Hoffman-Igaki combination taught a system according to claim 1 / a transmitter sub-system according to claim 14 / a receiver sub-system according to claim 21 / a method according to claim 27 / a method according to claim 31 / a method according to claim 33 / a method according to claim 35 / a method according to claim 37 / an apparatus according to claim 39, the combination is silent on but the analogous art Fuks taught wherein the biometric sensor and the transmitter are located in a remote portable key fob (***See col. 2, lines 33-35, 42-45: The wireless device (preferably a key fob) includes a transmitter, a biometric sensor***).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the applicant(s) invention was made to modify the combined invention of Hoffman & Igaki by including a remote portable key fob that includes transmitter and biometric sensor as taught by Fuks (Fuks, col. 2, lines 33-35, 42-45) for the advantage of providing a secured wireless remote keyless entry device to a system (***Fuks, col. 1, lines 35-55***).

Claims 41, 43 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hoffman et al. US 7,152,045 (hereinafter "Hoffman") in view of Igaki et al. US 5,109,428 (hereinafter "Igaki") and in further view of Koo et al. WO 02/12660 hereinafter ("Koo").

> Examiner Notes: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner. A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including non-preferred embodiments. *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), *cert. denied,* 493 U.S. 975 (1989). See MPEP 2123.

Regarding claim 41, Hoffman taught a method of enrolling a biometric signature into a database of biometric signatures in a system for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***), the system comprising:

said database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***);

a transmitter subsystem (***i.e. Biometric Input Device, fig. 3 item 12]***) for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***),

the transmitter sub-system comprising: a biometric sensor (***fig.3, ref. 12; col. 13, lines 2-8***);

means for enrolling relevant signatures into the database using the biometric sensor (***See [7:24-26] During a registration step, the individual is to register with the system an authenticated biometric sample; [36:44-46] The purpose of the Biometric Registration Terminal (BRT) is to register new individuals including their biometric-PIC, see further 37:12-14, 49:40-42***);

means for enrolling relevant signatures into the database according to the instruction (***see col. 8, lines 25-26***);

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute if the matching is authenticated; and means for emitting a secure access signal conveying information dependent upon said accessibility attribute (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that***

the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual);

the system further comprising: a receiver sub-system comprising: means for receiving the transmitted secure access signal (***See col. 40, lines 59-62: Individual enters their biometric into the BIA, DPC is receiving biometric input by the ATM***); and

means for providing conditional access to the controlled item dependent upon information in said secure access signal (***see [Col. 40, lines 62-67] the <u>Data processing center (DPC) validates the biometric-PIC</u> and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and <u>examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]</u>, see also [38:53-60] An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. <u>Once the system verifies the individual</u>, <u>the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level.</u>*, **Furthermore** *[68:10-15] a financial transaction authorization service can decide to deny any request for over $300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. <u>The authorization service can also use the security level as a guide</u> on how much to charge for the transaction, based on risk.***); said method comprising the steps of: receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***);

Hoffman taught the claimed system. Hoffman is silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught wherein the means for enrolling relevant signatures into the database of biometric signatures comprises: means for receiving a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry; means for mapping said series into an instruction (*see Abstract, "An optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate."* This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. *see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary"*).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of Hoffman with the idea of producing a sequence of fingerprint image data of Igaki *[Igaki:1:58-61]* because the use of Igaki could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data from a single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*Ikagi: Col. 1:49-51]*).

Hoffman-Igaki combination taught the method in claim 41; the combination is silent on enrolling the relevant signatures into the database using the biometric sensor as an administrator if the database of biometric signatures is empty. However, the analogous art Koo taught enrolling the relevant signatures into the database using the biometric sensor as an administrator if the database of biometric signatures is empty (*Koo, see [Page 16, lines 8-10] if no registered administrator fingerprint information exists as empty, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14*).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the applicant's invention was made to modify the combined method of Hoffman of Igaki with the teaching of Koo for enrolling the relevant signatures into the database using the biometric sensor as an administrator if the database of biometric signatures is empty because they are analogous in biometric entry.

One of ordinary skilled in the art would have been motivated to incorporate the idea of Koo *[Page, 5, lines 19-22; Page 16, lines 8-10]* within the combined method of Hoffman [fig. 1] and Igaki because the idea of Koo could provide the method of Hoffman to provide an electronic card key administration system consisted of host computer systems for administration of a plural of the electronic fingerprint recognition card keys (*Koo, Page 3, lines 21-23*).

Regarding claim 43, Hoffman-Igaki-Koo combination taught a method according to claim 41 wherein the enrolling step comprises receiving another biometric signal to confirm the enrolling of the biometric as an administrator (*Koo, see the person having inputted his fingerprint is authorized as a new administrator [Page 16, lines 12-15]; and see also [Page 11, lines 16-18] the fingerprint code of the administrator is stored by receiving the code stored in the administration system*).

One of ordinary skilled in the art would have been motivated to incorporate the idea of Koo *[Page 11, lines 16-18; Page 16, lines 12-15]* within the combined method of Hoffman [fig. 1] and Igaki because the idea of Koo could provide the method of Hoffman to provide an electronic card key administration system consisted of host computer systems for administration of a plural of the electronic fingerprint recognition card keys (*Koo, Page 3, lines 21-23*).

Claims 42 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hoffman et al. US 7,152,045 (hereinafter "Hoffman") in view of Igaki et al. US 5,109,428 (hereinafter "Igaki") as applied to claim 41 above and in further view of Fuks et al. US 6,992,562 hereinafter ("Fuks").

> Examiner Notes: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner. A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including non-preferred embodiments. *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), *cert. denied,* 493 U.S. 975 (1989). See MPEP 2123.

Regarding claim 43, Hoffman-Igaki-Koo combination taught a method according to claim 41, the combination is silent on but the analogous art Fuks taught wherein the biometric sensor and the transmitter are located in a remote portable key fob (Fuks, ***See col. 2, lines 33-35, 42-45: The wireless device (preferably a key fob) includes a transmitter, a biometric sensor***).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the applicant(s) invention was made to modify the combined invention of Hoffman, Igaki & Koo by including a remote portable key fob that includes transmitter and biometric sensor as taught by Fuks (Fuks, col. 2, lines 33-35, 42-45) for the advantage of providing a secured wireless remote keyless entry device to a system (***Fuks, col. 1, lines 35-55***).

Allowable Subject Matter

Claims 3, 13, 16, 24, 30, and 44 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), 2nd paragraph, non-statutory obviousness-type double patenting set forth in this Office action and to include all of the limitations of the base claim (1, 14, 21, 27, 41) and any intervening claims (9-10, 23, 29, 43). Dependent claims 4-8, 17-20, and 25-26 depend upon one of the above-mentioned allowed claims and would be allowable by virtue of their dependencies.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MOHAMMAD L. RAHMAN whose telephone number is (571)270-7471. The examiner can normally be reached on Monday to Friday: 9:00 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, TAGHI T. ARANI can be reached on 5712723787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MOHAMMAD L RAHMAN/
Primary Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 13/572,166	Applicant(s)/Patent Under Reexamination BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L. RAHMAN	Art Unit 2438 · Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,152,045	12-2006	Hoffman, Ned	705/43
*	B	US-5,109,428	04-1992	Igaki et al.	382/125
*	C	US-6,992,562	01-2006	Fuks et al.	340/5.52
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N	WO 0212660 A1	02-2002	World Intellect	KOO H et al.	
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

FORM PTO-1449	APPLICATION SERIAL NO. **13/572,166**	CASE NO. 12838/8
LIST OF PATENTS AND PUBLICATIONS FOR APPLICANTS' INFORMATION DISCLOSURE STATEMENT	FILING DATE **August 10, 2012**	GROUP ART UNIT **2438**
Confirmation No. 9752	APPLICANT: **BURKE, Christopher John**	

EXAMINER INITIAL	**OTHER ART – NON PATENT LITERATURE DOCUMENT (Include name of author, title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.**	
	A1	Notice of Acceptance dated September 18, 2012 for co-pending Australian Patent Office Application No. 2009201293 (3 pp.).

EXAMINER /Mohammad Rahman/	DATE CONSIDERED 03/24/2014

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.L.R

Index of Claims	**Application/Control No.** 13572166	**Applicant(s)/Patent Under Reexamination** BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	**Art Unit** 2438

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		DATE								
Final	Original	03/19/2014								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								
	35	✓								
	36	✓								

Index of Claims	**Application/Control No.** 13572166	**Applicant(s)/Patent Under Reexamination** BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	**Art Unit** 2438

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		**DATE**								
Final	Original	03/19/2014								
	37	✓								
	38	✓								
	39	✓								
	40	✓								
	41	✓								
	42	✓								
	43	✓								
	44	✓								

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 9752

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/572,166	08/10/2012 **RULE**	726	2438	12838/8

APPLICANTS

INVENTORS
Christopher John Burke, Ramsgate, AUSTRALIA;

** **CONTINUING DATA** *************************
This application is a CON of 10/568,207 06/04/2008 PAT 8266442
which is a 371 of PCT/AU2004/001083 08/13/2004

** **FOREIGN APPLICATIONS** *************************
AUSTRALIA 2003904317 08/13/2003

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** ** ** SMALL ENTITY **
08/22/2012

		STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed ☑ Yes □ No 35 USC 119(a-d) conditions met ☑ Yes □ No Verified and Acknowledged /MOHAMMAD L RAHMAN/ Examiner's Signature	□ Met after Allowance Initials	AUSTRALIA	10	44	10

ADDRESS

Michael E. Milz
Brinks Hofer Gilson & Lione
P.O. Box 10395
Chicago, IL 60610
UNITED STATES

TITLE

REMOTE ENTRY SYSTEM

FILING FEE RECEIVED 2125	FEES: Authority has been given in Paper No.____________ to charge/credit DEPOSIT ACCOUNT No.____________ for following:	□ All Fees □ 1.16 Fees (Filing) □ 1.17 Fees (Processing Ext. of time) □ 1.18 Fees (Issue) □ Other ________________ □ Credit

BIB (Rev. 05/07).

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	29	((Christopher) near2 (Burke)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/19 15:33
L2	16349	(713/182-186,168).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/03/19 15:34
L3	23869	(726/2,7,26-30).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/03/19 15:34
L4	33433	(709/224-225).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/03/19 15:35
L5	738	biometric with identif$7 same (access near2 (right privilege control)) and (((unconditional unlimited) near2 access) duress alert telemetry)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:35
L6	33	(enroll$3 register$3) with (((biometric adj image) biometric (fingrprint adj image) fingerprint) near (sequence array))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:35
L7	4829	assign$3 with (access near (right privilege))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:35
L8	1377	(access near (right privilege)) same ((biometric adj image) biometric (fingrprint adj image) fingerprint)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:36
L9	174	7 and 8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:36
L10	26	2 and 9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:36
L11	24	3 and 9	US-PGPUB; USPAT; USOCR;	OR	ON	2014/03/19 15:37

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
L12	4	4 and 9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
L13	23	5 and 9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
L14	65	2 and 5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
L15	41	3 and 5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
L16	11	4 and 5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
L17	27	5 and 7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
L18	165	5 and 8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
L19	1377	(access near (right privilege)) same ((biometric adj image) biometric (fingrprint adj image) fingerprint)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:38
L20	131	(assign$3 provid$3) with (access adj (right privilege)) same (biometric fingerprint)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:38
S1	656	(biometric fingerprint) with (key near fob)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:45
S2	275	(biometric fingerprint) with (key near fob) and (audit$ examin$3 investigat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:47
S3	49	(biometric fingerprint) with (key near fob) and (audit$ examin$3	US-PGPUB; USPAT; USOCR;	OR	ON	2014/03/18 12:48

		investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20040813"	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S4	43	(biometric fingerprint) with (key near fob) and (audit$ examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:51
S5	0	(biometric fingerprint) with (remote near key near fob) and (audit$ examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:52
S6	0	(biometric fingerprint) with (remote near2 key near fob) and (audit$ examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:53
S7	2	("8266442").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:36
S8	2	"20120278863"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:42
S9	2	"20120311346"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:43
S10	2	"20120311343"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:43

EAST Search History (Interference)

<This search history is empty>

3/19/2014 3:41:07 PM
C:\ Users\ mrahman3\ Documents\ EAST\ Workspaces\ 13572166_First.wsp

Search Notes	Application/Control No. 13572166	Applicant(s)/Patent Under Reexamination BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	Art Unit 2438

CPC- SEARCHED

Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
713	186	03/19/2014	MLR

SEARCH NOTES

Search Notes	Date	Examiner
Combined text search with classes/sub-classes (see EAST)	3/19/2014	MLR
Inventor name, Assigee	3/19/2014	MLR
NPL Search - Google Scholar IEEE ACM WIPO	3/19/2014	MLR

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

PTO/SB/122 (09-04)
Approved for use through 07/31/2006. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

CHANGE OF CORRESPONDENCE ADDRESS
Application

Address to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	**13/572,166**
Filing Date	**August 10, 2012**
First Named Inventor	**Christopher John Burke**
Art Unit	**2438**
Examiner Name	**Mohammad L. Rahman**
Attorney Docket Number	**12838/8**

Please change the Correspondence Address for the above-identified patent application to:

☑ The address associated with Customer Number: **00757**

OR

□ Firm or Individual Name

Address

City   State   Zip

Country

Telephone   Fax

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

I am the:

□ Applicant/Inventor

□ Assignee of record of the entire interest.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

☑ Attorney or agent of record. Registration Number 62,972.

□ Registered practitioner named in the application transmittal letter in an application without an executed oath or declaration. See 37 CFR 1.33(a)(1). Registration Number ________.

Signature /E. Brandon Nykiel/

Typed or Printed Name **E. Brandon Nykiel**

Date **April 4, 2014**   Telephone **312-321-4200**

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

✓ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	18673201
Application Number:	13572166
International Application Number:	
Confirmation Number:	9752
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Correspondence Address:	Michael E. Milz Brinks Hofer Gilson & Lione P.O. Box 10395 - Chicago IL 60610 US 3123214200 -
Filer:	E. Brandon Nykiel/Maggie Pieczonka
Filer Authorized By:	E. Brandon Nykiel
Attorney Docket Number:	12838/8
Receipt Date:	04-APR-2014
Filing Date:	10-AUG-2012
Time Stamp:	12:17:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		12838_8_ChangeofCorrFiling_040414.pdf	79661 aedad1dd6eb957a76c879366849b7c261104ba87	yes	2

Multipart Description/PDF files in .zip description

Document Description	Start	End
Miscellaneous Incoming Letter	1	1
Change of Address	2	2

Warnings:

Information:

Total Files Size (in bytes):	79661

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS pursuant to 37 CFR §1.8 on the below date:

Date: April 4, 2014 Name: E. Brandon Nykiel Signature: /E. Brandon Nykiel/

BRINKS
GILSON
& LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: Christopher John Burke
Appln. No.: 13/572,166
Filed: August 10, 2012
For: REMOTE ENTRY SYSTEM
Attorney Docket No.: 12838/8

Examiner: Mohammad L. Rahman
Art Unit: 2438
Conf. No.: 9752

TRANSMITTAL

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Attached is/are:

☒ Change of Correspondence Address.

Fee calculation:

☒ No additional fee is required.

□ Per 37 CFR §1.27, □ Applicant is small entity □ Applicant is micro entity.

□ An extension fee in an amount of $_____ for a _____-month extension of time under 37 CFR § 1.136(a).

□ A petition or processing fee in an amount of $_____ under 37 CFR § 1.17(_____).

□ An additional filing fee has been calculated as shown below:

					Fee		Small Entity Fee		Micro Entity Fee	
	Claims Remaining After Amendment		Highest No. Previously Paid	Present Extra	Rate	Add'l Fee	Rate	Add'l Fee	Rate	Add'l Fee
Total		Minus			x $ 80 =	$	x $ 40 =	$	x $20 =	$
Independent		Minus			x $420 =	$	x $210 =	$	x $105 =	$
First Presentation of Multiple Dep. Claim					+ $780 =	$	+ $390 =	$	+ $195 =	$
					Total	$	Total	$	Total	$

Fee payment:

□ Please charge Deposit Account No. 23-1925 in the amount of $_____ for _____.

□ Payment by credit card in the amount of $_____ (Form PTO-2038 is attached).
WARNING: Information on this form may become public. **Credit card information should not be included on this form.**

☒ The Director is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925.

Respectfully submitted,

April 4, 2014
Date

/E. Brandon Nykiel/
E. Brandon Nykiel (Reg. No. 62,972)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

PRIORITY DOCUMENT EXCHANGE

FAILURE STATUS REPORT

An attempt by the Office to electronically retrieve, under the Priority Document Exchange programs (PDX and DAS), 2003904317 to which priority is claimed has FAILED on 05/21/2014.

For further questions or assistance, please contact our EBC Customer Support Center at

1-866-217-9197 (toll-free)

571-272-4100 (local)

M-F 6AM - Midnight (Eastern Time)

pdx@uspto.gov (email)

Priority Document Exchange Website: http://www.uspto.gov/patents/process/file/pdx/pdx_index.jsp

PTO/SB/26 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 12838/8

In re Application of: Christopher John Burke

Application No.: 13/572,166

Filed: August 10, 2012

For: REMOTE ENTRY SYSTEM

The owner*, SECURICOM (NSW) PTY LTD, of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 8,266,442 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. □ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 62,972

/E. Brandon Nykiel/
Signature

August 26, 2014
Date

E. Brandon Nykiel
Typed or printed name

(312) 321-4200
Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	13572166
Filing Date:	10-Aug-2012
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Filer:	E. Brandon Nykiel/Patricia Chiovari
Attorney Docket Number:	12838/8

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 2 months with $0 paid	2252	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Statutory or Terminal Disclaimer	1814	1	160	160
	Total in USD ($)			**460**

Electronic Acknowledgement Receipt

EFS ID:	19967147
Application Number:	13572166
International Application Number:	
Confirmation Number:	9752
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Correspondence Address:	Michael E. Milz Brinks Hofer Gilson & Lione P.O. Box 10395 - Chicago IL 60610 US 3123214200 -
Filer:	E. Brandon Nykiel/Maggie Pieczonka
Filer Authorized By:	E. Brandon Nykiel
Attorney Docket Number:	12838/8
Receipt Date:	26-AUG-2014
Filing Date:	10-AUG-2012
Time Stamp:	15:02:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$460

RAM confirmation Number	1351
Deposit Account	231925
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		12838_8_ResponseFiling_082614.pdf	650282 c804d8fb61a92e40c88407f68de56ee95342fb40	yes	18

Multipart Description/PDF files in .zip description

Document Description	Start	End
Miscellaneous Incoming Letter	1	1
Extension of Time	2	3
Amendment/Req. Reconsideration-After Non-Final Reject	4	4
Claims	5	11
Applicant Arguments/Remarks Made in an Amendment	12	17
Terminal Disclaimer Filed	18	18

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Fee Worksheet (SB06)	fee-info.pdf	32104 5be44cb8235ff022a6369be1e67029587507887d	no	2

Warnings:

Information:

Total Files Size (in bytes):	682386

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS pursuant to 37 CFR §1.8 on the below date:

Date: August 26, 2014 Name: E. Brandon Nykiel Signature: /E. Brandon Nykiel/

BRINKS
GILSON
& LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: Christopher John Burke
Appln. No.: 13/572,166
Filed: August 10, 2012
For: REMOTE ENTRY SYSTEM
Attorney Docket No.: 12838/8

Examiner: Rahman, Mohammad L.
Art Unit: 2438
Conf. No.: 9752

TRANSMITTAL

Mail Stop Amendment
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Attached is/are:

☒ Petition and Fee for Extension of Time (2 months); Amendment and Response to Office Action Mailed March 26, 2014, and Terminal Disclaimer to Obviate a Double Patenting Rejection Over a "Prior" Patent.

Fee calculation:

☐ No additional fee is required.

☒ Per 37 CFR §1.27, ☒ Applicant is small entity ☐ Applicant is micro entity.

☒ An extension fee in an amount of $300 for a 2-month extension of time under 37 CFR § 1.136(a).

☒ A petition or processing fee in an amount of $160 under 37 CFR § 1.20(d).

☐ An additional filing fee has been calculated as shown below:

					Fee		Small Entity Fee		Micro Entity Fee	
	Claims Remaining After Amendment		Highest No. Previously Paid	Present Extra	Rate	Add'l Fee	Rate	Add'l Fee	Rate	Add'l Fee
Total		Minus			x $ 80 =	$	x $ 40 =	$	x $20 =	$
Independent		Minus			x $420 =	$	x $210 =	$	x $105 =	$
First Presentation of Multiple Dep. Claim					+ $780 =	$	+ $390 =	$	+ $195 =	$
					Total	$	Total	$	Total	$

Fee payment:

☒ Please charge Deposit Account No. 23-1925 in the amount of $460 for Extension of Time (2 months) and Terminal Disclaimer.

☐ Payment by credit card in the amount of $_____ (Form PTO-2038 is attached).
WARNING: Information on this form may become public. **Credit card information should not be included on this form.**

☒ The Director is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925.

Respectfully submitted,

August 26, 2014
Date

/E. Brandon Nykiel/
E. Brandon Nykiel (Reg. No. 62,972)

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS pursuant to 37 CFR §1.8 on the below date:

Date: August 26, 2014 Name: E. Brandon Nykiel Signature: /E. Brandon Nykiel/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of:	Christopher John Burke		
Appln. No.:	13/572,166	Examiner:	Rahman, Mohammad L.
Filed:	August 10, 2012	Art Unit:	2438
For:	REMOTE ENTRY SYSTEM	Conf. No.:	9752
Attorney Docket No.:	12838/8		

PETITION AND FEE FOR EXTENSION OF TIME (37 CFR § 1.136(a))

Mail Stop Amendment
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

This is a petition for an extension of the time to respond to the Office Action dated March 26, 2014 for a period of 2 month(s).

Per 37 CFR §1.27, ☒ Applicant is small entity ☐ Applicant is micro entity.

	Extension Months	Fee	Small Entity Fee	Micro Entity Fee
☐	One Month	$ 200	$ 100	$ 50
☒	Two Months	$ 600	$ 300	$150
☐	Three Months	$1,400	$ 700	$350
☐	Four Months	$2,200	$1,100	$550
☐	Five Months	$3,000	$1,500	$750

Payment Method:

☐ Payment by credit card in the amount of $_____ to cover the fees listed above. Form PTO-2038 is enclosed for this purpose.

☒ The Commissioner is hereby authorized to charge $300 to cover the fees listed above to Deposit Account No. 23-1925.

☒ The Commissioner is hereby authorized to charge any deficiencies in fees or credit overpayment to Deposit Account No. 23-1925.

Respectfully submitted,

Dated: August 26, 2014

/E. Brandon Nykiel/
E. Brandon Nykiel, Reg. No. 62,972
Attorney for Applicant(s)

BRINKS GILSON & LIONE
PO BOX 10395
CHICAGO, IL 60610
(312) 321-4200

CERTIFICATE OF ELECTRONIC FILING
I hereby certify that this correspondence is being filed electronically with the U.S. Patent and Trademark Office on

Date: August 26, 2014 Name: E. Brandon Nykiel Signature: /E. Brandon Nykiel/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of:	Christopher John Burke	
Appln. No.:	13/572,166	Examiner: Rahman, Mohammad L.
Filed:	August 10, 2012	Art Unit: 2438
For:	REMOTE ENTRY SYSTEM	Confirmation No. 9752
Attorney Docket No:	12838/8	

AMENDMENT AND RESPONSE TO OFFICE ACTION MAILED MARCH 26, 2014

MAIL STOP - Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir or Madam:

In response to the Office Action mailed March 26, 2014, please enter the following amendments and consider the following remarks.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 9 of this paper.

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of the Claims:

What is claimed is:

1-44. (Cancelled)

45. (New) A transmitter sub-system for providing secure access to a controlled item, the transmitter sub-system comprising:

a processor, a memory, and a processor executable software program;

a database of biometric signatures;

a biometric sensor for receiving a biometric signal, wherein said transmitter sub-system is operable for:

matching the biometric signal against members of the database of biometric signatures; and

sending an access signal dependent upon the results of the matching, said secure access being provided dependent upon the access signal.

46. (New) A system for providing secure access to a controlled item, the system comprising:

a processor, a memory, and a processor executable software program;

a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor for receiving a biometric signal, wherein said transmitter sub-system is operable for;

matching the biometric signal against members of the database of biometric signatures; and

sending an access signal dependent upon the matching; and

a receiver sub-system operable for;

receiving the access signal; and

providing conditional access to the controlled item dependent upon the access signal;

wherein the transmitter sub-system is further operable for populating the database of biometric signatures by performing the steps of:

receiving, by the biometric sensor, a succession of entries of the biometric signal; and

populating the database with biometric information derived from the succession of entries.

47. (New) A system according to claim 45, wherein the step of populating the database comprises the steps of:

accepting the succession of entries as control information; and

populating the database dependent upon the control information.

48. (New) A system according to claim 45, further operable for:

providing a signal for directing input of the succession of entries of the biometric signal; and

incorporating into the access signal an identification field identifying the biometric signal if the signal matches a member of the database.

49. (New) A system according to claim 45, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class and a system user class, the access signal comprising:

an access attribute if the biometric signal matches a member of the database of biometric signatures; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

50. (New) A system according to claim 45, wherein the controlled item is one of:

a locking mechanism for providing physical access; and a locking mechanism for providing electronic access.

51. (New) A system according to claim 45, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration, and/or the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

52. (New) A system according to claim 45, wherein said conditional access comprises one of:

provision of access to the controlled item if the access signal comprises an access attribute;

provision of access to the controlled item and sounding of an alert if the access signal comprises a duress attribute; and

denial of access to the controlled item and sounding of an alert if the access signal comprises an alert attribute.

53. (New) A system as claimed in claim 45, wherein:

the transmitter sub-system is further operative for transmitting information capable of granting more than two types of access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and the system further comprises a control panel for receiving the information and for providing the secure access requested.

54. (New) A system according to claim 52, wherein the control panel includes a converter for receiving the secure wireless signal and for outputting the information, and/or the biometric sensor authenticates the identity of the user by comparing a biometric input from the user with a biometric signature for the user in the biometric database.

55. (New) A system according to claim 52, wherein the secure wireless signal comprises an RF carrier and a rolling code, encrypted Bluetooth or other communications protocol, and

the converter converts the secure wireless signal to a Wiegand protocol or other protocol required by the system.

56. (New) A system according to claim 45, wherein the biometric sensor and the transmitter sub-system are located in a portable device.

57. (New) A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:

a processor, a memory, and a processor executable software program;

a biometric sensor for receiving a biometric signal, wherein said transmitter sub-system is operable for;

matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute;

emitting an access signal conveying information dependent upon said accessibility attribute; and

populating the database of biometric signatures by:

receiving, by the biometric sensor, a succession of entries of the biometric signal, said succession being characterised according to at least one of the number of said entries and a duration of each said entry; and

populating the database dependent upon the succession of entries.

58. (New) A method for providing secure access to a controlled item in a system comprising a processor, a memory, and a processor executable software program, a database of biometric signatures, a transmitter sub-system comprising a biometric sensor for receiving a biometric signal, the transmitter sub-system being operable for emitting a secure access signal, and a receiver sub-system operable for receiving the transmitted secure access signal and for providing conditional access to the controlled item dependent upon information in said secure access signal, the method comprising the steps of:

populating the database of biometric signatures by:

receiving, by the biometric sensor, a succession of entries of the biometric signal;

determining at least one of the number of said entries and a duration of each said entry; and

populating the database dependent upon the succession of entries;

receiving a biometric signal;

matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;

emitting an access signal conveying information dependent upon said accessibility attribute; and

providing conditional access to the controlled item dependent upon said information.

59. (New) A method according to claim 57, wherein the step of populating the database of biometric signatures further comprises the step of enrolling a biometric signature into the database of biometric signatures by:

receiving a biometric signal; and

enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty.

60. (New) A method according to claim 57, wherein the step of enrolling the biometric signature further comprises receiving another biometric signal to confirm the enrolling of the biometric signal as an administrator signature dependent upon generation of a feedback signal adapted to direct provision of at least one of the biometric signal and the other biometric signal.

61. (New) A method according to claim 57, wherein the biometric sensor and the transmitter sub-system are located in a portable device.

62. (New) A non-transitory computer readable medium for storing a computer program comprising instructions or code, which when executed by processors, causes the processors to perform the steps of the method of any one of claims 14 to 17.

63. (New) A system for populating a database of biometric signatures, the system comprising:

a processor, a memory, and a processor executable software program;

a database of biometric signatures; and

a biometric sensor for receiving a biometric signal, wherein said system is operable for populating the database of biometric signatures by performing the steps of:

receiving, by the biometric sensor, a succession of entries of the biometric signal, the succession being characterised according to at least one of the number of said entries and a duration of each said entry; and

populating the database dependent upon the succession of entries

64. (New) A system according to claim 62, wherein the system is further operable for enrolling a biometric signature into the database of biometric signatures by:

receiving a biometric signal; and

enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty.

65. (New) A method for populating a database of biometric signatures, the method comprising the steps of:

receiving, by a biometric sensor, a succession of entries of the biometric signal;

determining at least one of the number of said entries and a duration of each said entry; and

populating the database dependent upon the succession of entries.

66. (New) A method according to claim 64, wherein the step of populating the database further comprises the steps of:

receiving a biometric signal; and

enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty.

67. (New) A system according to claim 49, wherein:

physical access is provided to one of a door, a gate, and a hatch; and

electronic access is provided to one of a Personal Computer, a smart phone, a network, and a payment system.

Remarks

Introduction

Claims 45-67 are pending. In this Amendment and Response, claims 1-44 are cancelled. Claims 45-67 are added. Support for the added claims is found in the Specification at least in paragraphs [0079], [0109], [0080], and [0085]. No new matter is added. Applicant respectfully requests reconsideration in view of the amendments and the following remarks.

Double Patenting

The Office Action on page 2 provisionally rejects claims 1-44 on the grounds of non-statutory obviousness-type double patenting, as being unpatentable over claims 1-14 of US Patent No. 8,266,442.

The Applicant does not concede that this objection has been properly taken. However, in order to expedite prosecution in the event that pending claims 45-67 are similarly rejected on grounds of non-statutory obviousness type double patenting, Applicant submits herewith a terminal disclaimer.

Claim Rejections Under 35 U.S.C. § 112

The Office Action on page 4 rejects claims 1-26 and 37-40 under 35 USC 112(b) or 35 USC 112 (pre-AIA) as being indefinite. Pending claims 45-67 do not recite "means for" language, which obviates the rejection. Reconsideration is respectfully requested.

Claim Rejections Under 35 U.S.C. § 103

The Office Action at page 5 rejects claims 1, 9-12, 14, 21, 23, 27, 29, 31, 33, 35, 37 and 39 under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hoffman et al (US 7,152,045) in view of Igaki et al (US 5,109,428).

Hoffman

Hoffman is directed to a token-less identification system and method for authorization of transactions and transmissions (Abstract). A "token" in this citation is an inanimate object such as a plastic card which confers a capability to the individual presenting the object (column 1 lines 25-29).

Fig. 1 of Hoffman shows the overall configuration of the described arrangement. A Data Processing Centre DPC 1 is connected to terminals 2 through various communication means 3 (column 12 lines 52-54).

The citation refers to a number of different terminals (column 27 line 21 – column 28 line 7). Each terminal is associated with a Biometric Input Apparatus (BIA) which is a combination of hardware and software whose job is to gather, encode, and encrypt biometric input for use in individual identification (column 14 lines 38-45).

Registration is performed in Hoffman using a Biometric Registration Terminal (BRT) (column 27 lines 25-29). The purpose of the BRT (column 36 lines 44-50) is to register new individuals including their biometric-PIC (Personal Identification Code – see column 2 line 9), mailing address, etc. It is submitted that this amount of data entry requires, as well as a biometric sensor for inputting the biometric-PIC, a standard keyboard for entering the data. Clearly, Hoffman is a hard-wired network-based system that is suitable for the "back end" of banking systems for electronic banking purposes (eg see BRTs that are located in places that are physically secure such as retail banking outlets (column 36 line 66 – column 37 line 3)).

In contrast, claim 45 is directed to a "transmitter sub-system", which is clearly part of a wireless based system when the claim is read in the context of the specification as a whole (see Fig. 2 of the present specification for example).

Given the significant constraints of a wireless system in comparison to a hard-wired network system, the Applicant submits that the person of ordinary skill would not find it obvious or straightforward to modify the system of Hoffman in order to arrive at the system recited in claim 45.

Accordingly, the Applicant submits that claim 45 is patentable over Hoffman.

The Office Action concedes that Hoffman is silent in regard to "*means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry; means for mapping said series into an instruction*" and refers to analogous art in Igaki in this regard.

Igaki

The Office Action makes reference to the Abstract in Igaki in this regard, which states that an optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate.

However, claim 46 of the present application recites, among other features, "*receiving by the biometric sensor a* succession *of entries* (emphasis added) *of the biometric signal, the* succession *being characterised according to at least one of the number of said entries and a duration of each said entry*".

In other words, the biometric sensor of the claimed invention receives a succession of entries of the biometric signal during the enrolment process. In contrast the biometric sensor in Igaki receives only a single fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate (Abstract).

The invention defined by claim 46 as amended is able to receive a succession of biometric signals which the user ensures are of predetermined duration, predetermined quantity, and being input within a predetermined time, and the system uses this information for enrolment purposes. The fact that the user has total control over the succession of biometric signal entries necessarily implies that the signals in the succession of signals are independent of each other.

In contrast Igaki receives only a single biometric signal, and processes the single biometric signal to form a sequence of image data. Since the sequence of derived image data are all derived from (and thus dependent upon) the single biometric signal, the sequence of image data in Igaki are clearly not independent of each other.

The object of Igaki is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary (emphasis added) (column 12 lines 40-45).

Igaki thus explicitly teaches away from successive multiple pressing down operations, which is consistent with the fact that Igaki is concerned with extracting minutia data from fingerprint image data, and not with enrolling users using a succession of entries of the biometric signal as recited in claim 46 as amended.

Establishment of a prima facie case of obviousness requires that Hoffman when combined with Igaki must teach or suggest all the claim limitations. However, even if Hoffman is combined with Igaki, and the Applicant does not concede that there is any apparent reason for asserting this combination, it is submitted that there is no teaching or suggestion of **EITHER** *receiving, by the biometric sensor, a succession of entries of the biometric signal, the succession being characterised according to at least one of the number of said entries and a duration of each said entry;* **OR** *populating the database dependent upon the succession of entries.*

For at least the reasons noted above, it is submitted that claim 46 as amended is patentable over Hoffman and Igaki whether these documents are considered alone or in combination.

Claims 47-67 recite, either explicitly or through dependence, the same or equivalent features to those referred to above in regard to claim 46 as amended. Accordingly, for at least the reasons noted above, it is submitted that claims 46-67 are patentable over Hoffman and Igaki whether these documents are considered alone or in combination.

The Office Action at page 29 rejects claims 2, 15, 22, 28, 32, 34, 36, 38 and 40 under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hoffman in view of Igaki and further in view of Fuks et al (US 6,992,562).

The Office Action concedes that Hoffman and Igaki are silent in regard to "*wherein the biometric sensor and the transmitter sub-system are located in a remote portable key fob*", and refer to Fuks in this regard.

New claims 56 and 61 recite *wherein the biometric sensor and the transmitter sub-system are located in a portable device*, however they also recite, by dependence, the features referred to above in regard to claim 46 as amended, and the Applicant is of the opinion that Fuks does not remedy the deficiencies of Hoffman and Igaki in this regard.

Establishment of a prima facie case of obviousness requires that Hoffman when combined with Igaki and Fuks must teach or suggest all the claim limitations. However, even if Hoffman is combined with Igaki and Fuks, and the Applicant does not concede that there is any apparent reason for asserting this combination, it is submitted that there is no teaching or suggestion of **EITHER** *receiving, by the biometric sensor, a succession of entries of the biometric signal, the succession being characterised according to at least one of the number of said entries and a duration of each said entry;* **OR** *populating the database dependent upon the succession of entries.*

For at least the reasons noted above, it is submitted that claims 56 and 61 are patentable over Hoffman and Igaki and Fuks whether these documents are considered alone or in combination.

The Office Action at page 30 rejects claims 41, 43 under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hoffman in view of Igaki and further in view of Koo et al (WO 02/12660).

The Office Action concedes that Hoffman and Igaki are silent in regard to "*enrolling the relevant signatures into the database using the biometric sensor as an administrator if the database of biometric signatures is empty*", and refer to Koo in this regard.

New claim 59 recites the noted feature, however it also recites, by dependence, the features referred to above in regard to claim 46 as amended, and the Applicant is of the opinion that Koo does not remedy the deficiencies of Hoffman and Igaki in this regard.

Establishment of a prima facie case of obviousness requires that Hoffman when combined with Igaki and Koo must teach or suggest all the claim limitations. However, even if Hoffman is combined with Igaki and Koo, and the Applicant does not concede that there is any apparent reason for asserting this combination, it is submitted that there is no teaching or suggestion of **EITHER** *receiving, by the biometric sensor, a succession of entries of the biometric signal, the succession being characterised according to at least one of the number of said entries and a duration of each said entry;* **OR** *populating the database dependent upon the succession of entries.*

For at least the reasons noted above, it is submitted that claim 59 is patentable over Hoffman and Igaki and Koo whether these documents are considered alone or in combination.

Conclusion

With this amendment and response, the present pending claims of this application are allowable, and Applicants respectfully request the Examiner to issue a Notice of Allowance for this application. Should the Examiner deem a telephone conference to be beneficial in expediting allowance/examination of this application, the Examiner is invited to call the undersigned attorney at the telephone number listed below.

Respectfully submitted,

/E. Brandon Nykiel/

Date: August 26, 2014

E. Brandon Nykiel
Attorney Reg. No. 62,972
Attorney for Applicant

BRINKS GILSON & LIONE
P.O. Box 10395
Chicago, Illinois 60610
(312) 321-4200

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/572,166	Filing Date 08/10/2012	□ To be Mailed

ENTITY: □ LARGE ☒ SMALL □ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
□ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
□APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
□ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT	08/26/2014	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 23	Minus	** 44	= 0	x $40 =	0
	Independent (37 CFR 1.16(h))	* 6	Minus	***10	= 0	x $210 =	0
	□ Application Size Fee (37 CFR 1.16(s))						
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**0**

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))						
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/THUY TA/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination
	13/572,166	BURKE, CHRISTOPHER JOHN

Document Code - DISQ	**Internal Document – DO NOT MAIL**

TERMINAL DISCLAIMER	□ APPROVED	☒ DISAPPROVED
Date Filed : 08/26/2014	**This patent is subject to a Terminal Disclaimer**	

Approved/Disapproved by:

Dorethea Lawrence

The person who signed the terminal disclaimer (only for application filed before September 16, 2012): does not have power of attorney, and thus, is not of record. (See FP 14.29. fti).

Resubmit a new terminal disclaimer at no additional fee.

U.S. Patent and Trademark Office

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/572,166	08/10/2012	Christopher John Burke	12838/8	9752

7590 11/10/2014

Michael E. Milz
Brinks Hofer Gilson & Lione
P.O. Box 10395
Chicago, IL 60610

EXAMINER	
RAHMAN, MOHAMMAD L	
ART UNIT	PAPER NUMBER
2438	
MAIL DATE	DELIVERY MODE
11/10/2014	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 13/572,166	**Applicant(s)** BURKE, CHRISTOPHER JOHN	
	Examiner MOHAMMAD L. RAHMAN	**Art Unit** 2438	**AIA (First Inventor to File) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *8/26/2014*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-67* is/are pending in the application.

5a) Of the above claim(s) *1-44* is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *44-67* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

This office action is in response to applicant's argument/amendment filed 08/26/2014. Claims 1-44 have been canceled. New claims 45-67 have been added.

Response to Arguments

Regarding Double Patenting Rehection:

The terminal disclaimer identifies a party who is not the applicant (only for applications filed on or after September 16, 2012). For cases filed on/after 9/16/12, 37 CFR 1.321 specifies that the applicant can disclaim, and the terminal disclaimer must specify the extent of the applicant's ownership. A request under 37 CFR 1.46(c) to change the applicant needs to be filed, which is (1) a request, signed by a 1.33(b) party, (2) a corrected ADS (37 CFR 1.76(c)) that identifies the "new" applicant in the applicant information, and is underlined since it is new, and (3) a 3.73(c) statement showing chain of title to the new applicant. Along with the paragraph 1.46(c) request, it is required to file a POA that gives power of the attorney who is signing the TD along with another copy of the TD unless a TD signed by the applicant. Therefore, the rejection on the ground of non-statutory obviousness-type double patenting rejection is maintained. See the attached review decision or in PAIR on 08/28/2014.

Regarding Prior Art rejections:

Applicant argued, see page 10 of remarks, Hoffman et al. is a hard-wired network-based system but in contrast, claim 45 is directed to a "transmitter sub-system", which is clearly part of a wireless based system when the claim is read on the context of the specification as a whole.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., ***transmitter sub-system, which is clearly part of a wireless based system***) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir.1993). Claim does not limit transmitter sub-system to only a wireless system or a part of wireless based system. Specification discloses, a transmitter subsystem comprises: a biometric sensor for receiving a biometric signal, means for matching..., means for emitting... etc. (see specification ¶0013-¶0018, ¶0023) OR FIG. 2 shows the transmitter sub-system 116 communicating with the receiver sub-system 117 **using** a direct wireless link for the access signal 108 (see specification ¶0135). Under MPEP § 2111, pending claims must be given their broadest reasonable interpretation consistent with the specification. Given the broadest reasonable interpretation, a transmitter sub-system can be a system which comprises biometric sensor and can communicate with other system using wired or wireless signal. Hoffman clearly teaches the biometric input apparatus (i.e. transmitter-subsystem) hardware comes in four basic versions: standard, **wireless**, integrated phone/cable television (or "CATV")/fax, and ATM. See Hoffman, col. 13, lines 37-50. See further **BIA/Wireless** under BIA Models in col. 14, lines 27-40.

Applicant argued, see page 11 of remarks, Igaki et al. does not teach claim 46 of the present application recites, among other features, "*receiving by the biometric sensor a succession of the biometric signal, the succession being characterized according to at least one of the said entries and a duration of each said entry*"

Claim 46 does not recites, "*the succession being characterized according to at least one of the said entries and a duration of each said entry*". Specification discloses, see ¶0109, " *The first administrator can provide control information to the code entry module by providing a succession of finger presses to the biometric sensor 121, providing that these successive presses are of the appropriate duration, the appropriate quantity, and are input within a predetermined time.*" As the claim does not characterize the "succession of entries of the biometric signal", it could be interpreted as succession of entries of any kind of biometric signal or succession of finger presses of appropriate duration or appropriate quantity or input within a predetermined time. Igaki discloses, "*An optical sensor unit optically **produces a sequence of fingerprint image data** during a single operation of **pressing a fingerpad onto an inspection plate** in a direction substantially transverse to the plate and with increasing pressure **over a time interval** (Abstract).*" Further, Igaki clearly discloses S*ee [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a* *sensor the alignment between* ***successive fingerprint image data produced in successive, multiple fingerprint pressing down operations*** *as in the prior art becomes unnecessary"*). Igaki clearly mentioned that ***successive fingerprint image data produced in successive, multiple fingerprint pressing down operations*** was known in the art. A known operation cannot add any novelty or non-obviousness to the invention.

Applicants present no further arguments.

For the above reasons, it is believed that the rejections should be sustained.

Accordingly, THIS ACTION IS MADE FINAL. See MPEP 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(d):

(d) REFERENCE IN DEPENDENT FORMS.—Subject to subsection (e), a claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed. A claim in dependent form shall be construed to incorporate by reference all the limitations of the claim to which it refers.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), fourth paragraph:

Subject to the [fifth paragraph of 35 U.S.C. 112 (pre-AIA)], a claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed. A claim in dependent form shall be construed to incorporate by reference all the limitations of the claim to which it refers.

Claim 62 is rejected under 35 U.S.C. 112(d) or 35 U.S.C. 112 (pre-AIA), 4th paragraph, as being of improper dependent form for failing to further limit the subject matter of the claim upon which it depends, or for failing to include all the limitations of the claim upon which it depends.

Dependent claim 12 recites "*A non-transitory computer readable medium for storing a computer program comprising instructions or code, which when executed by……the steps of the method of any one of claims 14 to 17.*" In this case, claim fails the infringement test under 35 USC § 112 ¶4th as it can be infringed by owning the medium without executing the method. The test as to whether a claim is a proper dependent claim is that it shall include every limitation of the claim from which it depends (35 U.S.C. 112, fourth paragraph) or in other words that it shall not conceivably be infringed by anything which would not also infringe the basic claim. See MPEP 608.01 (n) III (Infringement Test). There are no claims 14 to 17 because they were canceled in the amendment..

Applicant may cancel the claim(s), amend the claim(s) to place the claim(s) in proper dependent form, rewrite the claim(s) in independent form, or present a sufficient showing that the dependent claim(s) complies with the statutory requirements.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed **terminal disclaimer** in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 45-67 are provisionally rejected on the ground of **nonstatutory obviousness-type double patenting** as being unpatentable over **claims 1-14 of US Patent # 8,266,442**. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-14 of US Patent # 8,266,442 contain every element of claims 23-42 of the instant application and thus anticipate the claim of the instant application.

Claims 45-67 of the instant application therefore is/are not patently distinct from the earlier patent claim(s) and as such is/are unpatentable over obvious-type double patenting. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim. "*A later patent claim is not patentably distinct from an earlier patent claim if the later claim is* ***obvious over****, or* ***anticipated by****, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus). " ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001)."Claim 12 and Claim 13 are generic to the species of invention covered by claim 3 of the patent. Thus, the generic invention is "anticipated" by the species of the patented invention. Cf., Titanium Metals Corp. v. Banner, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985) (holding that an earlier species disclosure in the prior art defeats any generic claim) 4. This court's predecessor has held that, without a terminal disclaimer, the species claims preclude issuance of the generic application. In re Van Ornum, 686 F.2d 937, 944, 214 USPQ 761, 767 (CCPA 1982). Accordingly, absent a terminal disclaimer, claims 12 and 13 were properly rejected under the doctrine of obviousness-type double patenting." (In re Goodman (CA FC) 29 USPQ2d 2010 (12/3/1993).*

<u>Claim Rejections - 35 USC § 102</u>

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 45, 49-56, and 67 are rejected under pre-AIA 35 U.S.C. 102 (e/a) as being anticipated by Hoffman et al. US 7,152,045 B2 (filed Sep. 10, 2002, PgPub US 2003/0105725 published Jun 5, 2003) hereinafter "Hoffman".

> Examiner Notes: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner. A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including non-preferred embodiments. *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), *cert. denied,* 493 U.S. 975 (1989). See MPEP 2123.

Regarding claim 45, (New) A transmitter sub-system for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***), the transmitter sub-system comprising:

a processor, a memory, and a processor executable software program; a database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***);

a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***), wherein said transmitter sub-system is operable for:

matching the biometric signal against members of the database of biometric signatures;

and sending an access signal dependent upon the results of the matching, said secure access being provided dependent upon the access signal (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the***

previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual).

Regarding claim 49, (New) Hoffman in view of Igaki further teaches a system according to claim 45, wherein the database of biometric signatures comprises signatures in at least **one** of a system administrator class and a system user class (***Hoffman, col. 60, lines 34-43; col. 8, lines 20-55***), the access signal comprising: an access attribute if the biometric signal matches a member of the database of biometric signatures; and an alert attribute if the biometric signal does not match a member of the database of biometric signatures (***Hoffman, col. 8, lines 45-51: successful or failed identification result***).

Regarding claim 50, (New) Hoffman in view of Igaki further teaches a system according to claim 45, wherein the controlled item is **one** of: a locking mechanism for providing physical access; and a locking mechanism for providing electronic access (***Hoffman, col. 9, lines 1-5***).

Regarding claim 51, (New) Hoffman in view of Igaki further teaches a system according to claim 45, wherein the biometric sensor is responsive to **one** of voice, retinal pattern, iris pattern, face pattern, and palm configuration, and/or the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system (***Hoffman, col. 60, lines 34-43; col. 8, lines 20-55***).

Regarding claim 52, (New) Hoffman in view of Igaki further teaches a system according to claim 45, wherein said conditional access comprises one of: provision of access to the controlled item if the access signal comprises an access attribute; provision of access to the controlled item and sounding of an alert if the access signal comprises a duress attribute; and denial of access to the controlled item and sounding of an alert if the access signal comprises an alert attribute (***Hoffman, col. 8, lines 45-51: successful or failed identification result***).

Regarding claim 53, (New) Hoffman in view of Igaki further teaches a system as claimed in claim 45, wherein: the transmitter sub-system is further operative for transmitting information capable of granting more than two types of access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and the system further comprises a control panel for receiving the information and for providing the secure access requested (***Hoffman, BIA models – BIA wireless, CATV, col. 14, lines 30-51***).

Regarding claim 54, (New) Hoffman in view of Igaki further teaches a system according to claim 52, wherein the control panel includes a converter for receiving the secure wireless signal and for outputting the information, and/or the biometric sensor authenticates the identity of the user by comparing a biometric input from the user with a biometric signature for the user in the biometric database (***Hoffman, col. 8, lines 29-50, comparison of entered biometric sample with the stored biometric sample***).

Regarding claim 55, (New) Hoffman in view of Igaki further teaches a system according to claim 52, wherein the secure wireless signal (***col. 17, lines 15***) comprises an RF carrier and a rolling code, encrypted Bluetooth or other communications protocol, and the converter converts the secure wireless signal to a Wiegand protocol **or** other protocol required by the system (***Hoffman, col. 14, lines 18-24***).

Regarding claim 56, (New) Hoffman in view of Igaki further teaches a system according to claim 45, wherein the biometric sensor and the transmitter sub-system are located in a portable device (***Hoffman, col. 17, lines 64-67, The phone/CATV version of BIA hardware***).

Regarding claim 67, (New) Hoffman further teaches a system according to claim 49, wherein: physical access is provided to one of a door, a gate, and a hatch; and electronic access is provided to one of a Personal Computer, a smart phone, a network, and a payment (***Hoffman, fig. 3, col. 14, section 1.1.2 BIA models***)

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim 65 is ejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Igaki et al. US 5,109,428 hereinafter "Igaki".

> Examiner Notes: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner. A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including non-preferred embodiments. *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), *cert. denied,* 493 U.S. 975 (1989). See MPEP 2123.

Regarding claim 65, (New) Igaki teaches a method for populating a database of biometric signatures, the method comprising the steps of:

receiving, by a biometric sensor (fig. 8, ref. 110), a succession of entries of the biometric signal; determining at least one of the number of said entries and a duration of each said entry; and populating the database dependent upon the succession of entries (***see Abstract, "An optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate." This method is the improvement from already***

known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between <u>successive fingerprint image data produced in successive, multiple fingerprint pressing down operations</u> as in the prior art becomes unnecessary"; See further fig. 5A-5D).

<u>Claim Rejections - 35 USC § 103</u>

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under pre-AIA 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 46-48, 57-58, 60-61, and 63 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hoffman in view of Igaki et al. US 5,109,428 hereinafter "Igaki".

Examiner Notes: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner. A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including non-preferred embodiments. *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), *cert. denied,* 493 U.S. 975 (1989). See MPEP 2123.

Regarding claim 46, (New) A system for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***), the system comprising:

a processor, a memory, and a processor executable software program; a database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***);

a transmitter sub-system (***i.e. Biometric Input Device, fig. 3 item 12]***) comprising:

a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***), wherein said transmitter sub-system is operable for;

matching the biometric signal against members of the database of biometric signatures; and sending an access signal dependent upon the matching (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result***

or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual); and

a receiver sub-system operable for;

receiving the access signal(***See col. 40, lines 59-62: Individual enters their biometric into the BIA, DPC is receiving biometric input by the ATM***); and

providing conditional access to the controlled item dependent upon the access signal (***see [Col. 40, lines 62-67] the <u>Data processing center (DPC) validates the biometric-PIC</u> and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and <u>examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]</u>, see also [38:53-60] An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. <u>Once the system verifies the individual</u>, <u>the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level.</u>*, **Furthermore** *[68:10-15] a financial transaction authorization service can decide to deny any request for over $300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. <u>The authorization service can also use the security level as a guide</u> on how much to charge for the transaction, based on risk.***)

Hoffman taught the claimed system. Hoffman is silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught wherein the transmitter sub-system is further operable for populating the database of biometric signatures by performing the steps of: receiving, by the biometric sensor, a succession of entries of the biometric signal; and populating the database with biometric information derived from the succession of entries (***see Abstract, "An optical sensor unit optically <u>produces a sequence of fingerprint image data</u> during a single***

operation of <u>pressing a fingerpad onto an inspection plate</u> in a direction substantially transverse to the plate and with increasing pressure <u>over a time interval</u>. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate." This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between <u>successive fingerprint image data produced in successive, multiple fingerprint pressing down operations</u> as in the prior art becomes unnecessary").

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of <u>Hoffman</u> with the idea of producing a sequence of fingerprint image data of <u>Igaki</u> *[<u>Igaki</u>:1:58-61]* because the use of <u>Igaki</u> could provide the Biometric Input Device of <u>Hoffman</u> [*<u>Hoffman</u>, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*<u>igaki</u>: Col. 1:49-51]*).

<u>Regarding claim 47</u>, (New) Hoffman-Igaki combination further teaches a system according to claim 45, wherein the step of populating the database comprises the steps of: accepting the succession of entries as control information; and populating the database dependent upon the control information (***Igaki, col. 1, line 40- col.2, line 2***).

<u>Regarding claim 48</u>, (New) Hoffman-Igaki combination further teaches a system according to claim 45, further operable for: providing a signal for directing input of the succession of entries of the biometric signal; and incorporating into the access signal an identification field identifying the biometric signal (***Igaki, col. 1, line 40- col.2, line 2***). if the signal matches a member of the database (***Hoffman, see col. 8, lines 29-33***).

Regarding claim 57, (New) Hoffman teaches a transmitter sub-system for operating in a system for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***), wherein the transmitter sub-system comprises:

a processor, a memory, and a processor executable software program; a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***), wherein said transmitter sub-system is operable for;

matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; emitting an access signal conveying information dependent upon said accessibility attribute (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual***);

Hoffman taught the claimed system. Hoffman was silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught populating the database of biometric signatures by: receiving, by the biometric sensor, a succession of entries of the biometric signal, said succession being characterised according to at least one of the number of said entries and a duration of each said entry; and populating the database dependent upon the succession of entries (***see Abstract, "An optical sensor unit optically <u>produces a sequence of fingerprint image data</u> during a single operation of <u>pressing a fingerpad onto an inspection plate</u> in a direction substantially transverse to the plate and with increasing pressure <u>over a time interval</u>. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate." This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between <u>successive fingerprint image data produced in successive, multiple fingerprint pressing down operations</u> as in the prior art becomes unnecessary"***).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of <u>Hoffman</u> with the idea of producing a sequence of fingerprint image data of <u>Igaki</u> *[<u>Igaki</u>:1:58-61]* because the use of <u>Igaki</u> could provide the Biometric Input Device of <u>Hoffman</u> [*<u>Hoffman</u>, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*<u>igaki</u>: Col. 1:49-51]*).

<u>**Regarding claim 58**</u>, (New) Hoffman teaches a method for providing secure access to a controlled item ***see [Abstract] A tokenless identification system and method for <u>authorization of transactions and transmissions</u>. The tokenless system and method are principally based on a <u>correlative comparison of a unique biometrics sample, such as a finger print or voice recording,</u>***

gathered directly from the person ***of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***) in a system comprising a processor, a memory, and a processor executable software program, a database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***), a transmitter sub-system comprising a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***), the transmitter sub-system being operable for emitting a secure access signal, and a receiver sub-system operable for receiving the transmitted secure access signal (***See col. 40, lines 59-62: Individual enters their biometric into the BIA, DPC is receiving biometric input by the ATM***) and for providing conditional access to the controlled item dependent upon information in said secure access signal (***see [Col. 40, lines 62-67] the*** ***Data processing center (DPC) validates the biometric-PIC*** ***and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and*** ***examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]***, ***see also [38:53-60] An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification.*** ***Once the system verifies the individual, the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level.***, **Furthermore** ***[68:10-15] a financial transaction authorization service can decide to deny any request for over $300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums.*** ***The authorization service can also use the security level as a guide*** ***on how much to charge for the transaction, based on risk.***), the method comprising the steps of: populating the database of biometric signatures by:

receiving a biometric signal; matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; emitting an access signal conveying information dependent upon said accessibility attribute; and providing conditional access to the controlled item dependent upon said information attribute (***see col. 8, lines 29-33: comparison of the biometric***

sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual).

Hoffman taught the claimed system. Hoffman was silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught receiving, by the biometric sensor, a succession of entries of the biometricsignal; determining at least one of the number of said entries and a duration of each said entry; and populating the database dependent upon the succession of entries; (***see Abstract, "An optical sensor unit optically <u>produces a sequence of fingerprint image data</u> during a single operation of <u>pressing a fingerpad onto an inspection plate</u> in a direction substantially transverse to the plate and with increasing pressure <u>over a time interval</u>. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate." This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor***

the alignment between <u>successive fingerprint image data produced in successive, multiple fingerprint pressing down operations</u> as in the prior art becomes unnecessary”).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of <u>Hoffman</u> with the idea of producing a sequence of fingerprint image data of <u>Igaki</u> *[<u>Igaki</u>:1:58-61]* because the use of <u>Igaki</u> could provide the Biometric Input Device of <u>Hoffman</u> [*<u>Hoffman</u>, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*<u>igaki</u>: Col. 1:49-51]*).

<u>Regarding claim 60</u>, (New) Hoffman in view of Igaki further teaches a method according to claim 57, wherein the step of enrolling the biometric signature further comprises receiving another biometric signal to confirm the enrolling of the biometric signal as an administrator signature dependent upon generation of a feedback signal adapted to direct provision of at least one of the biometric signal and the other biometric signal (***Hoffman, col. 60, lines 34-43; col. 8, lines 20-55***).

<u>Regarding claim 61</u>, (New) Hoffman in view of Igaki further taught a method according to claim 57, wherein the biometric sensor and the transmitter sub-system are located in a portable device (***Hoffman, col. 17, lines 64-67, The phone/CATV version of BIA hardware***).

<u>Regarding claim 63</u>, (New) Hoffman taught a system for populating a database of biometric signatures (***see [Abstract] A tokenless identification system and method for <u>authorization of transactions and transmissions</u>. The tokenless system and method are principally based on a <u>correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person</u> of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***), the system comprising:

a processor, a memory, and a processor executable software program; a database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***); and a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***), wherein said system is operable for populating the database of biometric signatures by performing the steps of: receiving, by the biometric sensor(***fig.3, ref. 12; col. 13, lines 2-8***),

Hoffman was silent on but the analogous art Igaki taught a succession of entries of the biometric signal, the succession being characterised according to at least one of the number of said entries and a duration of each said entry; and populating the database dependent upon the succession of entries(***see Abstract, "An optical sensor unit optically <u>produces a sequence of fingerprint image data</u> during a single operation of <u>pressing a fingerpad onto an inspection plate</u> in a direction substantially transverse to the plate and with increasing pressure <u>over a time interval</u>. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate." This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between <u>successive fingerprint image data produced in successive, multiple fingerprint pressing down operations</u> as in the prior art becomes unnecessary"***).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of <u>Hoffman</u> with the idea of producing a sequence of fingerprint image data of <u>Igaki</u> *[<u>Igaki</u>:1:58-61]* because the use of <u>Igaki</u> could provide the Biometric Input Device of <u>Hoffman</u> [*<u>Hoffman</u>, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*<u>igaki</u>: Col. 1:49-51]*).

Claims 59, 62, 64 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hoffman in view of Igaki as applied to claim 57 above, and further in view of Koo et al. WO 02/12660 hereinafter "Koo".

Regarding claim 59, (New) Hoffman-Igaki combination teaches a method according to claim 57, the combination is silent on but the analogous art Koo taught wherein the step of populating the database of biometric signatures further comprises the step of enrolling a biometric signature into the database of biometric signatures by: receiving a biometric signal; and enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty (***Koo, see [Page 16, lines 8-10] if no registered administrator fingerprint information exists as empty, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14***).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the applicant's invention was made to modify the combined method of Hoffman of Igaki with the teaching of Koo for enrolling the relevant signatures into the database using the biometric sensor as an administrator if the database of biometric signatures is empty because they are analogous in biometric entry.

One of ordinary skilled in the art would have been motivated to incorporate the idea of Koo ***[Page, 5, lines 19-22; Page 16, lines 8-10]*** within the combined method of Hoffman [fig. 1] and Igaki because the idea of Koo could provide the method of Hoffman to provide an electronic card key administration system consisted of host computer systems for administration of a plural of the electronic fingerprint recognition card keys (***Koo, Page 3, lines 21-23***).

Regarding claim 62, (New) A non-transitory computer readable medium for storing a computer program comprising instructions or code, which when executed by processors, causes the processors to perform the steps of the method of any **one of claims 14 to 17**.(***Claims 14-17 was canceled. For examining purpose, examiner construe claims 58-61 and see the same rational cited in the above claims***).

Regarding claim 64, (New) Hoffman-Igaki-Koo combination further teaches a system according to claim 62, wherein the system is further operable for enrolling a biometric signature into the database of biometric signatures by: receiving a biometric signal; and enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty (***Koo, see [Page 16, lines 8-10] if no registered administrator fingerprint information exists as empty, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14***).

Claim 66 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Igaki in view of Koo.

Regarding claim 66, (New) Igaki teaches a method according to claim 64, wherein the step of populating the database further comprises the steps of:

receiving a biometric signal (***Igaki, fig.6, ref. S1***); Igaki is silent on but the analogous art Koo teaches enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty (***Koo, see [Page 16, lines 8-10] if no registered administrator fingerprint information exists as empty, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14***).

One of ordinary skilled in the art would have been motivated to incorporate the idea of Koo ***[Page, 5, lines 19-22; Page 16, lines 8-10]*** within the combined method of Igaki because the idea of Koo could provide the method of Igaki to provide an electronic card key administration system consisted of host computer systems for administration of a plural of the electronic fingerprint recognition card keys (***Koo, Page 3, lines 21-23***).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MOHAMMAD L. RAHMAN whose telephone number is (571)270-7471. The examiner can normally be reached on Monday to Friday: 9:00 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, TAGHI T. ARANI can be reached on 5712723787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MOHAMMAD L RAHMAN/
Primary Examiner, Art Unit 2438

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination	
	13/572,166	BURKE, CHRISTOPHER JOHN	

Document Code - DISQ	**Internal Document – DO NOT MAIL**

TERMINAL DISCLAIMER	☐ APPROVED	☒ DISAPPROVED
Date Filed : 08/26/2014	**This patent is subject to a Terminal Disclaimer**	

Approved/Disapproved by:

Dorethea Lawrence

The person who signed the terminal disclaimer (only for application filed before September 16, 2012): does not have power of attorney, and thus, is not of record. (See FP 14.29. fti).
Resubmit a new terminal disclaimer at no additional fee.

U.S. Patent and Trademark Office

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	94	(biometric fingerprint) with ((multiple plural consecutive sequential successive) near2 entr$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/11/06 13:34
L2	33	(biometric fingerprint) with ((multiple plural consecutive sequential successive) near2 entr$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/11/06 13:34
L3	18809	(713/182-186,168).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/11/06 13:35
L4	2	L3 and L2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/11/06 13:35
L5	29312	(726/2,7,26-30).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/11/06 13:35
L6	0	L5 and L2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/11/06 13:35
L7	39035	(709/224-225).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/11/06 13:35
L8	0	L7 and L2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/11/06 13:35
L9	36	((Christopher) near2 (Burke)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2014/11/06 13:35
L10	0	L9 and L1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/11/06 13:35
L11	10	(biometric fingerprint) with ((consecutive sequential	US-PGPUB; USPAT; USOCR;	OR	ON	2014/11/06 13:36

		successive) near2 entr$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S1	656	(biometric fingerprint) with (key near fob)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:45
S2	275	(biometric fingerprint) with (key near fob) and (audit$ examin$3 investigat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:47
S3	49	(biometric fingerprint) with (key near fob) and (audit$ examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20040813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:48
S4	43	(biometric fingerprint) with (key near fob) and (audit$ examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:51
S5	0	(biometric fingerprint) with (remote near key near fob) and (audit$ examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:52
S6	0	(biometric fingerprint) with (remote near2 key near fob) and (audit$ examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:53
S7	2	("8266442").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:36
S8	2	"20120278863"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:42
S9	2	"20120311346"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:43
S10	2	"20120311343"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:43
S11	29	((Christopher) near2 (Burke)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/19 15:33
S12	16349	(713/182-186,168).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/03/19 15:34

S13	23869	(726/2,7,26-30).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/03/19 15:34
S14	33433	(709/224-225).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/03/19 15:35
S15	738	biometric with identif$7 same (access near2 (right privilege control)) and (((unconditional unlimited) near2 access) duress alert telemetry)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:35
S16	33	(enroll$3 register$3) with (((biometric adj image) biometric (fingrprint adj image) fingerprint) near (sequence array))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:35
S17	4829	assign$3 with (access near (right privilege))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:35
S18	1377	(access near (right privilege)) same ((biometric adj image) biometric (fingrprint adj image) fingerprint)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:36
S19	174	S17 and S18	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:36
S20	26	S12 and S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:36
S21	24	S13 and S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S22	4	S14 and S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S23	23	S15 and S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S24	65	S12 and S15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37

S25	41	S13 and S15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S26	11	S14 and S15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S27	27	S15 and S17	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S28	165	S15 and S18	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S29	1377	(access near (right privilege)) same ((biometric adj image) biometric (fingrprint adj image) fingerprint)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:38
S30	131	(assign$3 provid$3) with (access adj (right privilege)) same (biometric fingerprint)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:38

EAST Search History (Interference)

<This search history is empty>

11/6/2014 1:37:01 PM
C:\Users\mrahman3\Documents\EAST\Workspaces\13572166_First.wsp

Index of Claims	**Application/Control No.** 13572166	**Applicant(s)/Patent Under Reexamination** BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	**Art Unit** 2438

✓	**Rejected**		**-**	**Cancelled**		**N**	**Non-Elected**		**A**	**Appeal**
=	**Allowed**		**÷**	**Restricted**		**I**	**Interference**		**O**	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		**DATE**								
Final	Original	03/19/2014	11/06/2014							
	1	✓	-							
	2	✓	-							
	3	✓	-							
	4	✓	-							
	5	✓	-							
	6	✓	-							
	7	✓	-							
	8	✓	-							
	9	✓	-							
	10	✓	-							
	11	✓	-							
	12	✓	-							
	13	✓	-							
	14	✓	-							
	15	✓	-							
	16	✓	-							
	17	✓	-							
	18	✓	-							
	19	✓	-							
	20	✓	-							
	21	✓	-							
	22	✓	-							
	23	✓	-							
	24	✓	-							
	25	✓	-							
	26	✓	-							
	27	✓	-							
	28	✓	-							
	29	✓	-							
	30	✓	-							
	31	✓	-							
	32	✓	-							
	33	✓	-							
	34	✓	-							
	35	✓	-							
	36	✓	-							

Index of Claims

	Application/Control No. 13572166	**Applicant(s)/Patent Under Reexamination** BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	**Art Unit** 2438

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		**DATE**								
Final	Original	03/19/2014	11/06/2014							
	37	✓	-							
	38	✓	-							
	39	✓	-							
	40	✓	-							
	41	✓	-							
	42	✓	-							
	43	✓	-							
	44	✓	-							
	45		✓							
	46		✓							
	47		✓							
	48		✓							
	49		✓							
	50		✓							
	51		✓							
	52		✓							
	53		✓							
	54		✓							
	55		✓							
	56		✓							
	57		✓							
	58		✓							
	59		✓							
	60		✓							
	61		✓							
	62		✓							
	63		✓							
	64		✓							
	65		✓							
	66		✓							
	67		✓							

Search Notes	**Application/Control No.** 13572166	**Applicant(s)/Patent Under Reexamination** BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	**Art Unit** 2438

CPC- SEARCHED

Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
713	186	03/19/2014	MLR
Updated Search			
713	186	11/6/2014	MLR

SEARCH NOTES

Search Notes	Date	Examiner
Combined text search with classes/sub-classes (see EAST)	3/19/2014	MLR
Inventor name, Assigee	3/19/2014	MLR
NPL Search - Google Scholar IEEE ACM WIPO	3/19/2014	MLR
Updated Search		
Updated keywords combined with classes/sub-classes	11/6/2014	MLR
Inventor name, Assignee	11/6/2014	MLR
NPL Search - Google Scholar IEEE ACM WIPO	11/6/2014	MLR

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 12838/8

In re Application of: Christopher John Burke

Application No.: 13/572,166

Filed: August 10, 2012

For: REMOTE ENTRY SYSTEM

The owner*, SECURICOM (NSW) PTY LTD, of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 8,266,442 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. □ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 34,880

/Michael E. Milz/
Signature

March 10, 2014
Date

Michael E. Milz
Typed or printed name

(312) 321-4200
Telephone Number

□ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner). Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	13572166
Filing Date:	10-Aug-2012
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Filer:	Michael Edward Milz/kathy kerns
Attorney Docket Number:	12838/8

Filed as Small Entity

Filing Fees for **Utility under 35 USC 111(a)**

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	2202	1	40	40
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Extension - 1 month with $0 paid	2251	1	100	100
Miscellaneous:				
Request for Continued Examination	2801	1	600	600
	Total in USD ($)			**740**

Electronic Acknowledgement Receipt

EFS ID:	21728234
Application Number:	13572166
International Application Number:	
Confirmation Number:	9752
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Correspondence Address:	Michael E. Milz Brinks Hofer Gilson & Lione P.O. Box 10395 - Chicago IL 60610 US 3123214200 -
Filer:	Michael Edward Milz/Maggie Krause
Filer Authorized By:	Michael Edward Milz
Attorney Docket Number:	12838/8
Receipt Date:	10-MAR-2015
Filing Date:	10-AUG-2012
Time Stamp:	16:27:26
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$740

RAM confirmation Number	3283
Deposit Account	231925
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		12838-8-Amendment-TD-EOT-RCE.pdf	905210 de59c4aecc5983c3d2f230d5d02297b014a015db	yes	19

Multipart Description/PDF files in .zip description

Document Description	Start	End
Transmittal Letter	1	1
Extension of Time	2	3
Request for Continued Examination (RCE)	4	5
Amendment Submitted/Entered with Filing of CPA/RCE	6	6
Claims	7	13
Applicant Arguments/Remarks Made in an Amendment	14	19

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Terminal Disclaimer Filed	12838-8-TerminalDisclaimer.pdf	374497 e1b2a8ea2bfd24dc9d1738dea326e74ca9850033	no	2

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
3	Fee Worksheet (SB06)	fee-info.pdf	33770 81de730e4bd4fe68c2cbcac844359dfdf256483f	no	2

Warnings:

Information:

Total Files Size (in bytes):	1313477

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8
I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS pursuant to 37 CFR §1.8 on the below date:

Date: March 10, 2015 Name: Michael E. Milz (Reg. No. 34,880) Signature: /Michael E. Milz/

BRINKS
GILSON
& LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: Christopher John Burke
Appln. No.: 13/572,166
Filed: August 10, 2012
For: REMOTE ENTRY SYSTEM
Attorney Docket No.: 12838/8

Examiner: Rahman, Mohammad L.
Art Unit: 2438
Conf. No.: 9752

TRANSMITTAL

Mail Stop RCE
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Attached is/are:

☒ Petition and Fee for Extension of Time (1 month); Request for Continued Examination; Amendment and Response to Final Office Action Mailed November 10, 2014; and Terminal Disclaimer to Obviate a Double Patenting Rejection Over a "Prior" Patent.

Fee calculation:

□ No additional fee is required.

☒ Per 37 CFR §1.27, ☒ Applicant is small entity □ Applicant is micro entity.

☒ An extension fee in an amount of $100 for a 1-month extension of time under 37 CFR § 1.136(a).

☒ A petition or processing fee in an amount of $600 under 37 CFR §1.17(e)(1).

☒ An additional filing fee has been calculated as shown below:

					Fee		Small Entity Fee		Micro Entity Fee	
	Claims Remaining After Amendment		Highest No. Previously Paid	Present Extra	Rate	Add'l Fee	Rate	Add'l Fee	Rate	Add'l Fee
Total	68	Minus	67	1	x $ 80 =	$	1x $ 40 =	$40	x $20 =	$
Independent		Minus			x $420 =	$	x $210 =	$	x $105 =	$
First Presentation of Multiple Dep. Claim					+ $780 =	$	+ $390 =	$	+ $195 =	$
					Total	$	Total	$40	Total	$

Fee payment:

☒ Please charge Deposit Account No. 23-1925 in the amount of $740 for 1-month Extension of Time ($100); Request for Continued Examination ($600); and 1 additional dependent claim ($40).

□ Payment by credit card in the amount of $______ (Form PTO-2038 is attached).
WARNING: Information on this form may become public. **Credit card information should not be included on this form.**

☒ The Director is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925.

Respectfully submitted,

March 10, 2015
Date

/Michael E. Milz/
Michael E. Milz (Reg. No. 34,880)

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS pursuant to 37 CFR §1.8 on the below date:

Date: March 10, 2015 Name: Michael E. Milz (Reg. No. 34,880) Signature: /Michael E. Milz/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of:	Christopher John Burke		
Appln. No.:	13/572,166	Examiner:	Rahman, Mohammad L.
Filed:	August 10, 2012	Art Unit:	2438
For:	REMOTE ENTRY SYSTEM	Conf. No.:	9752
Attorney Docket No.:	12838/8		

PETITION AND FEE FOR EXTENSION OF TIME (37 CFR § 1.136(a))

Mail Stop RCE
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

This is a petition for an extension of the time to respond to the final Office Action dated November 10, 2014 for a period of 1 month(s).

Per 37 CFR §1.27, ☒ Applicant is small entity □ Applicant is micro entity.

	Extension Months	Fee	Small Entity Fee	Micro Entity Fee
☒	One Month	$ 200	$ 100	$ 50
□	Two Months	$ 600	$ 300	$150
□	Three Months	$1,400	$ 700	$350
□	Four Months	$2,200	$1,100	$550
□	Five Months	$3,000	$1,500	$750

Payment Method:

□ Payment by credit card in the amount of $_____ to cover the fees listed above. Form PTO-2038 is enclosed for this purpose.

☒ The Commissioner is hereby authorized to charge $100 to cover the fees listed above to Deposit Account No. 23-1925.

☒ The Commissioner is hereby authorized to charge any deficiencies in fees or credit overpayment to Deposit Account No. 23-1925.

Respectfully submitted,

Dated: March 10, 2015

/Michael E. Milz/
Michael E. Milz, Reg. No. 34,880
Attorney for Applicant(s)

BRINKS GILSON & LIONE
PO BOX 10395
CHICAGO, IL 60610
(312) 321-4200

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS pursuant to 37 CFR §1.8 on the below date:

Date: March 10, 2015 Name: Michael E. Milz (Reg. No. 34,880) Signature: /Michael E. Milz/

BRINKS
GILSON
& LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of:	Christopher John Burke		
Appln. No.:	13/572,166	Examiner:	Rahman, Mohammad L.
Filed:	August 10, 2012	Art Unit:	2438
For:	REMOTE ENTRY SYSTEM	Conf. No.:	9752
Attorney Docket No.:	12838/8		

Mail Stop RCE
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

REQUEST FOR CONTINUED EXAMINATION (37 CFR § 1.114)

Dear Sir/Madam:

Applicant(s) requests continued examination of the above-identified application under 37 CFR §1.114.

☒ This is the FIRST request under 37 CFR §1.17(e) in this application.

☒ Submission under 37 CFR 1.114 (*check at least one of the following*):

- □ Previously submitted:
  - □ Applicant(s) requests nonentry of any previously-filed unentered amendments.
  - □ Please enter and consider the Amendment After Final Under 37 CFR §1.116 previously filed on _____.
  - □ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____.
  - □ Other: _____.
- ☒ Attached is/are:
  - □ An Information Disclosure Statement
  - ☒ An Amendment to the written description, claims, or drawings
  - □ New Arguments and/or New Evidence in support of Patentability
  - ☒ Other: Terminal Disclaimer

☐ Request for suspension of action:

Applicant(s) hereby requests suspension of action on the above-identified application under 37 CFR §1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; requires Processing Fee under 37 CFR §1.17(i)).

☒ Small/Micro Entity Status:

☒ Applicant(s) hereby asserts entitlement to claim ☒ small or ☐ micro entity status under 37 CFR §§ 1.9 and 1.27.

☐ A small/micro entity statement or assertion of entitlement to claim small/micro entity status was filed in prior application no. _____/_____ and such status is still proper and desired.

☐ Is no longer desired.

☒ Applicant(s) calculates the following fees to be due in connection with this Request:

☒ A request fee of $600 under 37 CFR §1.17(e)(1) or (2).

☐ A suspension processing fee of $_____ under 37 CFR §1.17(i).

☒ An additional filing fee of $40 under 37 CFR §1.16 (1 additional dependent claim).

☒ An extension fee of $100 under 37 CFR §1.17(a) for a 1-month extension of time.

☒ Fee payment to cover the above-enumerated fee(s):

☒ Please charge Deposit Account No. 23-1925 (BRINKS GILSON & LIONE) in the amount of $740.

☐ A payment by credit card in the amount of $_____ (Form PTO-2038 is attached).

☒ The Commissioner is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 associated with this paper (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925 (BRINKS GILSON & LIONE).

Respectfully submitted,

March 10, 2015
Date

/Michael E. Milz/
Michael E. Milz (Reg. No. 34,880)

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being filed electronically with the U.S. Patent and Trademark Office on

Date: March 10, 2015 Name: Michael E. Milz (Reg. No. 34,880) Signature: /Michael E. Milz/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: Christopher John Burke
Appln. No.: 13/572,166
Filed: August 10, 2012
For: REMOTE ENTRY SYSTEM
Attorney Docket No: 12838/8

Examiner: Rahman, Mohammad L.
Art Unit: 2438
Confirmation No. 9752

AMENDMENT AND RESPONSE TO FINAL OFFICE ACTION MAILED NOVEMBER 10, 2014

MAIL STOP - RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir or Madam:

In response to the final Office Action mailed November 10, 2014, please enter the following amendments and consider the following remarks.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 9 of this paper.

A terminal disclaimer is being submitted with this Amendment and Response.

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of the Claims:

What is claimed is:

1-44. (Cancelled)

45. (Currently amended) A transmitter sub-system for providing secure access to a controlled item, the transmitter sub-system comprising:

a processor, a memory, and a processor executable software program;

a database of biometric signatures;

a biometric sensor for receiving a biometric signal, wherein said transmitter sub-system is operable for:

matching the biometric signal against members of the database of biometric signatures; and

sending, using a wireless communication channel, an access signal dependent upon the results of the matching, said secure access being provided dependent upon the access signal.

46. (Currently amended) A system for providing secure access to a controlled item, the system comprising:

a processor, a memory, and a processor executable software program;

a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor for receiving a biometric signal, wherein said transmitter sub-system is operable for;

matching the biometric signal against members of the database of biometric signatures; and

sending an access signal dependent upon the matching; and

a receiver sub-system operable for;

receiving the access signal; and

providing conditional access to the controlled item dependent upon the access signal;

wherein the transmitter sub-system is further operable for populating the database of biometric signatures by performing the steps of:

receiving, by the biometric sensor, a succession of entries of the biometric signal, said succession being characterized according to at least one of the number of said entries and a duration of each said entry; and

populating the database with biometric information derived from the succession of entries provided that the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration.

47. (Currently amended) A system according to claim [[45]] 46, wherein the step of populating the database comprises the steps of:

accepting the succession of entries as control information; and

populating the database dependent upon the control information.

48. (Currently amended) A system according to claim [[45]] 46, further operable for:

providing a signal for directing input of the succession of entries of the biometric signal; and

incorporating into the access signal an identification field identifying the biometric signal if the signal matches a member of the database.

49. (Currently amended) A system according to claim [[45]] 46, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class and a system user class, the access signal comprising:

an access attribute if the biometric signal matches a member of the database of biometric signatures; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

50. (Currently amended) A system according to claim [[45]] 46, wherein the controlled item is one of:

a locking mechanism for providing physical access; and

a locking mechanism for providing electronic access.

51. (Currently amended) A system according to claim [[45]] 46, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration, and/or the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

52. (Currently amended) A system according to claim [[45]] 46, wherein said conditional access comprises one of:

provision of access to the controlled item if the access signal comprises an access attribute;

provision of access to the controlled item and sounding of an alert if the access signal comprises a duress attribute; and

denial of access to the controlled item and sounding of an alert if the access signal comprises an alert attribute.

53. (Currently amended) A system as claimed in claim [[45]] 46, wherein:

the transmitter sub-system is further operative for transmitting information capable of granting more than two types of access to the controlled item using a ~~secure wireless~~ signal dependent upon a request from the user and the authentication of the user identity; and the system further comprises a control panel for receiving the information and for providing the secure access requested.

54. (Currently amended) A system according to claim [[52]] 53, wherein the control panel includes a converter for receiving the ~~secure wireless~~ signal and for outputting the information, and/or the biometric sensor authenticates the identity of the user by comparing a biometric input from the user with a biometric signature for the user in the biometric database.

55. (Currently amended) A system according to claim [[52]] 53, wherein the secure wireless signal comprises an RF carrier and a rolling code, encrypted Bluetooth or other communications protocol, and the converter converts the secure wireless signal to a Wiegand protocol or other protocol required by the system.

56. (Currently amended) A system according to claim [[45]] 46, wherein the biometric sensor and the transmitter sub-system are located in a portable device.

57. (Currently amended) A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:

a processor, a memory, and a processor executable software program;

a biometric sensor for receiving a biometric signal, wherein said transmitter sub-system is operable for;

matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute;

emitting an access signal conveying information dependent upon said accessibility attribute; and

populating the database of biometric signatures by:

receiving, by the biometric sensor, a succession of entries of the biometric signal, said succession being characterised according to at least one of the number of said entries and a duration of each said entry; and

populating the database dependent upon the succession of entries provided that the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration.

58. (Currently amended) A method for providing secure access to a controlled item in a system comprising a processor, a memory, and a processor executable software program, a database of biometric signatures, a transmitter sub-system comprising a biometric sensor for receiving a biometric signal, the transmitter sub-system being operable for emitting a secure access signal, and a receiver sub-system operable for receiving the transmitted secure access

signal and for providing conditional access to the controlled item dependent upon information in said secure access signal, the method comprising the steps of:

populating the database of biometric signatures by:

receiving, by the biometric sensor, a succession of entries of the biometric signal, said succession being characterized according to at least one of the number of said entries and a duration of each said entry;

determining at least one of the number of said entries and a duration of each said entry; and

populating the database dependent upon the succession of entries provided that the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration;

receiving a biometric signal;

matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;

emitting an access signal conveying information dependent upon said accessibility attribute; and

providing conditional access to the controlled item dependent upon said information.

59. (Currently amended) A method according to claim [[57]] 58, wherein the step of populating the database of biometric signatures further comprises the step of enrolling a biometric signature into the database of biometric signatures by:

receiving a biometric signal; and

enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty.

60. (Currently amended) A method according to claim [[57]] 58, wherein the step of enrolling the biometric signature further comprises receiving another biometric signal to confirm the enrolling of the biometric signal as an administrator signature dependent upon generation of a feedback signal adapted to direct provision of at least one of the biometric signal and the other biometric signal.

61. (Currently amended) A method according to claim [[57]] 58, wherein the biometric sensor and the transmitter sub-system are located in a portable device.

62. (Currently amended) A non-transitory computer readable medium for storing a computer program comprising instructions or code, which when executed by processors, causes the processors to perform the steps of the method of any one of claims [[14]] 58 to [[17]] 61.

63. (Currently amended) A system for populating a database of biometric signatures, the system comprising:

a processor, a memory, and a processor executable software program;

a database of biometric signatures; and

a biometric sensor for receiving a biometric signal, wherein said system is operable for populating the database of biometric signatures by performing the steps of:

receiving, by the biometric sensor, a succession of entries of the biometric signal, the succession being characterised according to at least one of the number of said entries and a duration of each said entry; and

populating the database dependent upon the succession of entries provided that the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration.

64. (Currently amended) A system according to claim [[62]] 63, wherein the system is further operable for enrolling a biometric signature into the database of biometric signatures by:

receiving a biometric signal; and

enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty.

65. (Currently amended) A method for populating a database of biometric signatures, the method comprising the steps of:

receiving, by a biometric sensor, a succession of entries of the biometric signal, said succession being characterized according to at least one of the number of said entries and a duration of each said entry;

determining at least one of the number of said entries and a duration of each said entry; and

populating the database dependent upon the succession of entries provided that the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration.

66. (Currently amended) A method according to claim [[64]] 65, wherein the step of populating the database further comprises the steps of:

receiving a biometric signal; and

enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty.

67. (Currently amended) A system according to claim [[49]] 50, wherein:

physical access is provided to one of a door, a gate, and a hatch; and

electronic access is provided to one of a Personal Computer, a smart phone, a network, and a payment system.

68. (New) A system according to claim 46, wherein the succession of entries of the biometric signal comprises four entries, the first three of which are of 1 second duration, and the last of which is of 2 second duration.

Remarks

Introduction

Claims 45-68 are pending. In this Amendment and Response, Claims 45-67 are amended. Claim 68 is added. Support for the amendments is found in the Specification at least in paragraphs [0085] and [0109]. No new matter is added. Applicant respectfully requests reconsideration in view of the amendments and the following remarks.

Double Patenting

The Office Action provisionally rejects claims 45-67 on grounds of non-statutory obviousness-type double patenting, as being unpatentable over claims 1-14 of US Patent No. 8,266,442. Applicant submits herewith a terminal disclaimer to overcome the double patenting rejection. Reconsideration is respectfully requested.

Claim Rejections Under 35 U.S.C. § 112

The Office Action rejected claim 62 under 35 U.S.C. § 112, fourth paragraph on grounds that claim 62 recited that it depended on any of claims 14 to 17, even though those claims were cancelled. In this Amendment and Response, claim 62 is amended so that it depends on "any one of claims 58 to 61," which are currently pending. Reconsideration of the § 112 rejections is respectfully requested.

Claim Rejections Under 35 U.S.C. §§ 102, 103

The Office Action rejected claims 45, 49-56, and 67 under 35 U.S.C. 102(e/a) as being anticipated by U.S. Patent No. 7,152,045 ("Hoffman"). Claim 65 was rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,109,428 ("Igaki"). Claims 46-48, 57-58, 60-61, and 63 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hoffman in view of Igaki. Claims 59, 62, and 64 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hoffman in view of Igaki, and further in view of WO 02/12660 ("Koo"). Claim 66 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Igaki in view of Koo.

Claim 45

Independent claim 45 is directed to a transmitter sub-system for providing secure access to a controlled item. Said transmitter sub-system is operable for matching a biometric signal against members of a database of biometric signatures, and sending, using a wireless communication channel, an access signal dependent upon the results of the matching, said secure access being provided dependent upon the access signal.

Hoffman fails to teach these limitations.

Hoffman describes a hard-wired network-based system that is suitable for the "back end" of banking systems for electronic banking purposes (see, e.g., BRTs that are located in places that are physically secure such as retail banking outlets). Hoffman, col. 36, line 66—col. 37, line 3). However, Hoffman, fails to teach or suggest at least sending, using a wireless communication channel, an access signal dependent upon results of matching.

For at least this reason, Hoffman fails to render unpatentable claim 45. Reconsideration is respectfully is respectfully requested.

Claim 46

Independent claim 46 is directed to a system for providing secure access to a controlled item. The system comprises a transmitter sub-system operable for populating a database of biometric signatures by performing the steps of populating the database with biometric information derived from succession of entries provided that the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration.

The combination of Hoffman and Igaki fails to teach these limitations.

As acknowledged in the Office Action, Hoffman fails to teach populating a database of biometric signatures. *See* Office Action mailed November 10, 2014, p. 13. Igaki fails to remedy the deficiencies of Hoffman.

Igaki describes an optical sensor unit that optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate. Igaki, Abstract. In particular, minutia data from fingerprint image data is extracted in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down on the fingerpad so that multiple fingerprint pressing down operations becomes unnecessary. *Id.* col. 1, lines 40-42.

However, despite Igaki describing a "sequence of fingerprint image data," Igaki describes that this is generated from only a "single operation of pressing a fingerpad." It necessarily follows then that since there is only single operation of pressing a fingerpad, any alleged database in Igaki would not be populated due to repeated fingerprint pressing, and as such any alleged database in Igaki would not be populated with biometric information derived from a succession of entries, as recited in claim 46. As such, even if Igaki is combined with Hoffman, the combination fails to teach a transmitter sub-system operable for populating a database of biometric signatures by performing the steps of populating the database with biometric information derived from succession of entries provided that the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration.

For at least these reasons, the combination of Hoffman and Igaki fails to render unpatentable claim 46 or any claim that depends on claim 46. Reconsideration is respectfully requested.

Claim 57

Independent claim 57 is directed to a transmitter sub-system for operating in a system for providing secure access to a controlled item. Said transmitter sub-system is operable for populating a database of biometric signatures by: receiving, by a biometric sensor, a succession of entries of a biometric signal, said succession being characterised according to at least one of the number of said entries and a duration of each said entry; and populating the database dependent upon the succession of entries provided that the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration.

The combination of Hoffman and Igaki fails to teach these limitations. Instead, at best, the combination describes producing fingerprint image data based on a single operation of pressing a fingerpad.

For at least these reasons, the combination of Hoffman and Igaki fails to render unpatentable claim 57. Reconsideration is respectfully requested.

Claim 58

Independent claim 58 is directed to a method for providing secure access to a controlled item in a system. The method comprising the steps of: populating a database of biometric signatures by: receiving, by a biometric sensor, a succession of entries of a biometric signal, said succession being characterized according to at least one of the number of said entries and a duration of each said entry; determining at least one of the number of said entries and a duration of each said entry; and populating the database dependent upon the succession of entries provided that the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration.

The combination of Hoffman and Igaki fails to teach these limitations. Instead, at best, the combination describes producing fingerprint image data based on a single operation of pressing a fingerpad.

For at least these reasons, the combination of Hoffman and Igaki fails to render unpatentable claim 58 or any claim that depends on claim 58. Reconsideration is respectfully requested.

Claim 63

Independent claim 63 is directed to a system for populating a database of biometric signatures. Said system is operable for populating the database of biometric signatures by performing the steps of: receiving, by a biometric sensor, a succession of entries of the biometric signal, the succession being characterised according to at least one of the number of said entries and a duration of each said entry; and populating a database dependent upon the succession of entries provided that the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration.

The combination of Hoffman and Igaki fails to teach these limitations. Instead, at best, the combination describes producing fingerprint image data based on a single operation of pressing a fingerpad.

For at least these reasons, the combination of Hoffman and Igaki fails to render unpatentable claim 63 or any claim that depends on claim 63. Reconsideration is respectfully requested.

Claim 65

Independent claim 65 is directed to a method for populating a database of biometric signatures. The method includes the steps of: receiving, by a biometric sensor, a succession of entries of the biometric signal, said succession being characterized according to at least one of the number of said entries and a duration of each said entry; determining at least one of the number of said entries and a duration of each said entry; and populating the database dependent upon the succession of entries provided that the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration.

Igaki fails to teach these limitations at least because Igaki merely describes producing fingerprint image data based on a single operation of pressing a fingerpad.

For at least these reasons, Igaki fails to render unpatentable claim 65 or any claim that depends on claim 65. Reconsideration is respectfully requested.

New Claim 68

Newly added claim 68 depends on independent claim 46 and further recites that the succession of entries of the biometric signal comprises four entries, the first three of which are of 1 second duration, and the last of which is of 2 second duration. Applicant submits that claim 68 is patentable at least by virtue of its dependency on claim 46. Favorable consideration of newly added claim 68 is respectfully requested.

Conclusion

With this amendment and response, the present pending claims of this application are allowable, and Applicants respectfully request the Examiner to issue a Notice of Allowance for this application. Should the Examiner deem a telephone conference to be beneficial in expediting allowance/examination of this application, the Examiner is invited to call the undersigned attorney at the telephone number listed below.

Respectfully submitted,

/Michael E. Milz/
Michael E. Milz
Attorney Reg. No. 34,880
Attorney for Applicant

Date: March 10, 2015

BRINKS GILSON & LIONE
P.O. Box 10395
Chicago, Illinois 60610
(312) 321-4200

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/572,166	Filing Date 08/10/2012	□ To be Mailed

ENTITY: □ LARGE ☒ SMALL □ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
□ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
□ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
□ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT	03/10/2015	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 24	Minus	** 44	= 0	x $40 =	0
	Independent (37 CFR 1.16(h))	* 6	Minus	***10	= 0	x $210 =	0
	□ Application Size Fee (37 CFR 1.16(s))						
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**0**

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))						
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/STEFANIE BRYCE/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Application Number	**Application/Control No.** 13/572,166	**Applicant(s)/Patent under Reexamination** BURKE, CHRISTOPHER JOHN

Document Code - DISQ	**Internal Document – DO NOT MAIL**

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 3/10/15	**This patent is subject to a Terminal Disclaimer**	

Approved/Disapproved by:

jean proctor

U.S. Patent and Trademark Office

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/572,166	08/10/2012	Christopher John Burke	12838/8	9752

7590 04/27/2015

Michael E. Milz
Brinks Hofer Gilson & Lione
P.O. Box 10395
Chicago, IL 60610

EXAMINER	
RAHMAN, MOHAMMAD L	

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
04/27/2015	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 13/572,166	**Applicant(s)** BURKE, CHRISTOPHER JOHN	
	Examiner MOHAMMAD L. RAHMAN	**Art Unit** 2438	**AIA (First Inventor to File) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *3/10/2015*.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *45-68* is/are pending in the application.
5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *45-68* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

The present application is being examined under the pre-AIA first to invent provisions.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on March 10, 2015 has been entered. Claims 1-44 were previously canceled. Claims 45-68 are pending.

Response to Arguments

a) The terminal disclaimer filed on 03/10/2015 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of any patent granted on US Patent # 8,266,442 has/have been reviewed and is accepted. The terminal disclaimer has been recorded.

b) Applicant argued in page 10 of Remarks (filed 3/10/2015), Hoffman fails to teach or suggest at least sending, using a wireless communication channel, an access signal dependent upon the results of the matching. In support of the argument, applicant mentioned BRTs are located in places that are physically secure such as retail banking outlets (col. 36, lines 66 – col. 37, lines 3).

Examiner respectfully disagrees. Hoffman evidently teaches

> Biometric Input Apparatus (BIA) hardware comes in four basic versions: standard, **wireless**, integrated phone/cable television (or "CATV")/fax and ATM (col. 13, lines 46-48).

Hoffman further teaches the BRT uses an attached BIA for biometric entry and

> BIA/Wireless
> Standard model, but serial line replaced with **spread-spectrum wireless communications module using external antenna. Used in restaurant point of sale** (col. 14, lines 37-40).

c) The newly added limitations to independent claims 46, 57, 58, 63, and 65, changes the scope, necessitated new ground(s) of rejection.

Claim Objections

Claims 46-57, 59-61, 64, 66-68 are objected to because of the following informalities:

a) Claims 47-56, 59-61, 64, 66-68 are all dependent claims that recite the limitation "A method/ A system according to..." in the preamble. It is suggested the limitation be amended to "[[A]] The method / The System according to..."

b) Claims 46, 57 recite **"operable for;"** which is an incomplete sentence.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(b):
(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 45-46, 48, 53, 57-58, 63, and 65 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

a) Claims 45-46, 48, 53, 57-58 recite "**operable for**" in preamble and couple of places which is considered as the applicant merely constitutes a statement of intended use and do not impose any positive limitation on the scope of the claim.

b) The terms "**appropriate number**", "**appropriate duration**" in claims 46, 57, 58, 63, and 65 is a relative term which renders the claim indefinite. The term "appropriate" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 45-68 are rejected under 35 U.S.C. 101 because the claimed invention is directed to a judicial exception (i.e. an abstract idea) without significantly more.

Independent claims 45, 46, 57, 58, 63, and 65 are directed towards a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more because the claim(s) as a whole, considering all claim elements both individually and in combination, do not amount to significantly more than an abstract idea. Claims are directed towards performing *a simple biometric authentication*. The underlying invention is merely *a simple biometric matching operation to access a controlled item*. The claim(s) does/do not include additional elements that are sufficient to amount to significantly more than the judicial exception because the additional element(s) or combination of elements in the claim(s) other than the abstract idea per se amount(s) to no more than recitation of generic computer structure (e.g. *transmitter sub-system, receiver sub-system, biometric sensor, wireless communication channel*) that serves to perform generic computer functions (e.g. *receiving biometric signal, receiving more than one biometric entry, matching the received signal with database, providing access to a controlled item*) that are well-understood, routine, and conventional activities previously known to the pertinent industry. Further, the claims do not recite an improvement to another technology or technical field, an improvement to the functioning of the computer itself, or meaningful limitations beyond generally linking the use of an abstract idea to a particular technological environment. Therefore, the claim(s) 1 is rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter.

See

1. Preliminary Examination Instructions in view of the Supreme Court Decision in *Alice Corporation Pty. Ltd. C. CLS Bank International et al.* (http://www.uspto.gov/patents/announce/alice_pec_25jun2014.pdf).

2. Federal Register Notice: 2014 Interim Guidance on Patent Subject Matter Eligibility

(http://www.gpo.gov/fdsys/pkg/FR-2014-12-16/pdf/2014-29414.pdf).

3. Abstract Idea Examples (http://www.uspto.gov/patents/law/exam/abstract_idea_examples.pdf)

Dependent claims 2-11 depends from claim 1 do cure the deficiencies set forth above.

Dependent claim(s) 47-56, 59-62, 64, 66-68 when analyzed as a whole are held to be patent ineligible under 35 U.S.C. 101 because the additional recited limitation(s) fail(s) to establish that the claim(s) is/are not directed to an abstract idea. The claims do not include additional elements that are sufficient to amount to significantly more than the judicial exception because the additional limitations are merely instructions to implement the abstract idea on a computer and require no more than a generic computer to perform generic computer functions that are well-understood, routine and conventional activities previously known to the industry (e.g. accepting, populating biometric entries, sending an alert, provision or denial of access).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claim 45 is rejected under pre-AIA 35 U.S.C. 102 (e/a) as being anticipated by Hoffman et al. US 7,152,045 B2 (filed Sep. 10, 2002, PgPub US 2003/0105725 published Jun 5, 2003) hereinafter "Hoffman".

> Examiner Notes: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner. A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including non-preferred embodiments. *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), *cert. denied,* 493 U.S. 975 (1989). See MPEP 2123.

<u>**Regarding claim 45**</u>, (New) A transmitter sub-system for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for <u>authorization of transactions and transmissions</u>. The tokenless system and method are principally based on a <u>correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person</u> of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***), the transmitter sub-system comprising:

a processor, a memory, and a processor executable software program; a database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***);

a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***), wherein said transmitter sub-system is operable for:

matching the biometric signal against members of the database of biometric signatures; and sending, <u>using a wireless communication channel</u> (***Biometric Input Apparatus (BIA) hardware comes in four basic versions: standard, <u>wireless</u>, integrated phone/cable television (or "CATV")/fax and ATM [col. 13, lines 46-48]; BIA/Wireless : Standard model, but serial line replaced with <u>spread-spectrum wireless communications module using external antenna. Used in restaurant point of sale</u> [col. 14, lines 37-40]***), an access signal dependent upon the results of the matching, said secure access being provided dependent upon the access signal (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of***

the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual).

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under pre-AIA 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 46-58, 60-63, and 67-68 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hoffman in view of Igaki et al. US 5,109,428 hereinafter "Igaki" and in further view of Pu et al. US 6,229,906 hereinafter "Pu".

Examiner Notes: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner. A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including non-preferred embodiments. *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), *cert. denied,* 493 U.S. 975 (1989). See MPEP 2123.

Regarding claim 46, (Currently Amended) Hoffman teaches a system for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***), the system comprising:

a processor, a memory, and a processor executable software program; a database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***);

a transmitter sub-system (***i.e. Biometric Input Device, fig. 3 item 12]***) comprising:

a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***), wherein said transmitter sub-system is operable for;

matching the biometric signal against members of the database of biometric signatures; and sending an access signal dependent upon the matching (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on***

successful identification of said first individual, said private code is presented to said first individual); and

a receiver sub-system operable for;

receiving the access signal(***See col. 40, lines 59-62: Individual enters their biometric into the BIA, DPC is receiving biometric input by the ATM***); and

providing conditional access to the controlled item dependent upon the access signal (***see [Col. 40, lines 62-67] the <u>Data processing center (DPC) validates the biometric-PIC</u> and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and <u>examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]</u>, see also [38:53-60] An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. <u>Once the system verifies the individual</u>, <u>the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level.</u>***, **Furthermore** ***[68:10-15] a financial transaction authorization service can decide to deny any request for over $300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. <u>The authorization service can also use the security level as a guide</u> on how much to charge for the transaction, based on risk.***)

Hoffman taught the claimed system. Hoffman is silent on but the analogous art <u>Igaki</u> which addressed the same field of endeavor in fingerprint identification explicitly taught wherein the transmitter sub-system is further operable for populating the database of biometric signatures by performing the steps of: receiving, by the biometric sensor, a succession of entries of the biometric signal; and populating the database with biometric information derived from the succession of entries (***see Abstract, "An optical sensor unit optically <u>produces a sequence of fingerprint image data</u> during a single operation of <u>pressing a fingerpad onto an inspection plate</u> in a direction substantially transverse***

to the plate and with increasing pressure <u>over a time interval</u>. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate." This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between <u>successive fingerprint image data produced in successive, multiple fingerprint pressing down operations</u> as in the prior art becomes unnecessary").

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of <u>Hoffman</u> with the idea of producing a sequence of fingerprint image data of <u>Igaki</u> *[<u>Igaki</u>:1:58-61]* because the use of <u>Igaki</u> could provide the Biometric Input Device of <u>Hoffman</u> [*<u>Hoffman</u>, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*<u>igaki</u>: Col. 1:49-51]*).

Hoffman-Igaki combination is silent on but the analogous art **<u>Pu</u>** teaches <u>said succession being characterized according to at least **one** of the number of said entries</u> (***Pu, col. 2, lines 18-22; 5, lines 25-46)*** <u>and a duration of each said entry</u> (***Pu, col. 5, lines 50-55***); <u>the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration</u> (***Pu, col. 2, lines 40-43; col. 4, lines 30-33, 40-67; col. 5, lines 50-55***).

Therefore, one of ordinary skilled artisan would have been motivated to modify the combined system of <u>Hoffman & Igaki</u> with the idea of succession being characterized according to at least one of the number of said entries and a duration of each said entry, the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration as taught by Pu because the use of Pu could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to include at least one of the number of said entries and a duration of each said entry, the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration to implement high security of the system by using secret sequence codes formed by body parts (***Pu, col. 3, lines 21-23***).

Regarding claim 47, (Currently Amended) Hoffman-Igaki-Pu combination further teaches a system according to claim 46, wherein the step of populating the database comprises the steps of: accepting the succession of entries as control information; and populating the database dependent upon the control information (***Igaki, col. 1, line 40- col.2, line 2***).

Regarding claim 48, (Currently Amended) Hoffman-Igaki-Pu combination further teaches a system according to claim 46, further operable for: providing a signal for directing input of the succession of entries of the biometric signal; and incorporating into the access signal an identification field identifying the biometric signal (***Igaki, col. 1, line 40- col.2, line 2***). if the signal matches a member of the database (***Hoffman, see col. 8, lines 29-33***).

Regarding claim 49, (Currently Amended) Hoffman in view of Igaki & Pu further teaches a system according to claim 46, wherein the database of biometric signatures comprises signatures in at least **one** of a system administrator class and a system user class (***Hoffman, col. 60, lines 34-43; col. 8, lines 20-55***), the access signal comprising: an access attribute if the biometric signal matches a member of the database of biometric signatures; and an alert attribute if the biometric signal does not match a member of the database of biometric signatures (***Hoffman, col. 8, lines 45-51: successful or failed identification result***).

Regarding claim 50, (Currently Amended) Hoffman in view of Igaki & Pu further teaches a system according to claim 46, wherein the controlled item is **one** of: a locking mechanism for providing physical access; and a locking mechanism for providing electronic access (***Hoffman, col. 9, lines 1-5***).

Regarding claim 51, (Currently Amended) Hoffman in view of Igaki & Pu further teaches a system according to claim 46, wherein the biometric sensor is responsive to **one** of voice, retinal pattern, iris pattern, face pattern, and palm configuration, and/or the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system (***Hoffman, col. 60, lines 34-43; col. 8, lines 20-55***).

Regarding claim 52, (Currently Amended) Hoffman in view of Igaki & Pu further teaches a system according to claim 46, wherein said conditional access comprises one of: provision of access to the controlled item if the access signal comprises an access attribute; provision of access to the controlled item and sounding of an alert if the access signal comprises a duress attribute; and denial of access to the controlled item and sounding of an alert if the access signal comprises an alert attribute (***Hoffman, col. 8, lines 45-51: successful or failed identification result***).

Regarding claim 53, (Currently Amended) Hoffman in view of Igaki & Pu further teaches a system as claimed in claim 46, wherein: the transmitter sub-system is further operative for transmitting information capable of granting more than two types of access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and the system further comprises a control panel for receiving the information and for providing the secure access requested (***Hoffman, BIA models – BIA wireless, CATV, col. 14, lines 30-51***).

Regarding claim 54, (Currently Amended) Hoffman in view of Igaki & Pu further teaches a system according to claim 53, wherein the control panel includes a converter for receiving the secure wireless signal and for outputting the information, and/or the biometric sensor authenticates the identity of the user by comparing a biometric input from the user with a biometric signature for the user in the biometric database (***Hoffman, col. 8, lines 29-50, comparison of entered biometric sample with the stored biometric sample***).

Regarding claim 55, (Currently Amended) Hoffman in view of Igaki & Pu further teaches a system according to claim 53, wherein the secure wireless signal (***col. 17, lines 15***) comprises an RF carrier and a rolling code, encrypted Bluetooth or other communications protocol, and the converter converts the secure wireless signal to a Wiegand protocol **or** other protocol required by the system (***Hoffman, col. 14, lines 18-24***).

Regarding claim 56, (Currently Amended) Hoffman in view of Igaki & Pu further teaches a system according to claim 46, wherein the biometric sensor and the transmitter sub-system are located in a portable device (***Hoffman, col. 17, lines 64-67, The phone/CATV version of BIA hardware***).

Regarding claim 57, (New) Hoffman teaches a transmitter sub-system for operating in a system for providing secure access to a controlled item (***see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***), wherein the transmitter sub-system comprises:

a processor, a memory, and a processor executable software program; a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***), wherein said transmitter sub-system is operable for;

matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; emitting an access signal conveying information dependent upon said accessibility attribute (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at***

least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual);

Hoffman taught the claimed system. Hoffman was silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught populating the database of biometric signatures by: receiving, by the biometric sensor, a succession of entries of the biometric signal, said succession being characterised according to at least one of the number of said entries and a duration of each said entry; and populating the database dependent upon the succession of entries (***see Abstract, "An optical sensor unit optically <u>produces a sequence of fingerprint image data</u> during a single operation of <u>pressing a fingerpad onto an inspection plate</u> in a direction substantially transverse to the plate and with increasing pressure <u>over a time interval</u>. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate." This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between <u>successive fingerprint image data produced in successive, multiple fingerprint pressing down operations</u> as in the prior art becomes unnecessary"***).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of <u>Hoffman</u> with the idea of producing a sequence of fingerprint image data of <u>Igaki</u> *[<u>Igaki</u>:1:58-61]* because the use of Igaki could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*igaki: Col. 1:49-51]*).

Hoffman-Igaki combination is silent on but the analogous art **Pu** teaches the number of said entries (***Pu, col. 2, lines 18-22; 5, lines 25-46)*** is the appropriate number of entries, and the duration of each said entry (***Pu, col. 5, lines 50-55***) is of the appropriate duration (***Pu, col. 2, lines 40-43; col. 4, lines 30-33, 40-67; col. 5, lines 50-55***).

Therefore, one of ordinary skilled artisan would have been motivated to modify the combined system of Hoffman & Igaki with the idea of the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration as taught by Pu because the use of Pu could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to include the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration to implement high security of the system by using secret sequence codes formed by body parts (***Pu, col. 3, lines 21-23***).

Regarding claim 58, (Currently Amended) Hoffman teaches a method for providing secure access to a controlled item ***see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***) in a system comprising a processor, a memory, and a processor executable software program, a database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***), a transmitter sub-system comprising a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***), the transmitter sub-system being operable for emitting a secure access signal, and a receiver sub-system operable for receiving the transmitted secure access signal (***See col. 40, lines 59-62: Individual enters their biometric into the BIA, DPC is receiving biometric input by the ATM***) and for providing conditional access to the controlled item dependent upon information in said secure access signal (***see [Col. 40, lines 62-67] the <u>Data processing center (DPC) validates the biometric-PIC</u> and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and <u>examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]</u>, see also [38:53-60] An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. <u>Once the system verifies the individual</u>, <u>the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level.</u>***, **Furthermore** ***[68:10-15] a financial transaction authorization service can decide to deny any request for over $300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. <u>The authorization service can also use the security level as a guide</u> on how much to charge for the transaction, based on risk.***), the method comprising the steps of: populating the database of biometric signatures by:

receiving a biometric signal; matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; emitting an access signal conveying information dependent upon said accessibility attribute; and providing conditional access to the controlled item dependent upon said information attribute (***see col. 8, lines 29-33: comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; see col. 8, lines 46-50, 54-55: comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-***

basket for producing either a successful or failed identification result; an output step wherein said identification result or said determination is externalized and displayed, and; a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual).

Hoffman taught the claimed system. Hoffman was silent on but the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught receiving, by the biometric sensor, a succession of entries of the biometricsignal; determining at least one of the number of said entries and a duration of each said entry; and populating the database dependent upon the succession of entries; (***see Abstract, "An optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate." This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary"***).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of Hoffman with the idea of producing a sequence of fingerprint image data of Igaki *[Igaki:1:58-61]* because the use of Igaki could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*igaki: Col. 1:49-51]*).

Hoffman-Igaki combination is silent on but the analogous art **Pu** teaches said succession being characterized according to at least **one** of the number of said entries (***Pu, col. 2, lines 18-22; 5, lines 25-46)*** and a duration of each said entry (***Pu, col. 5, lines 50-55***); the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration (***Pu, col. 2, lines 40-43; col. 4, lines 30-33, 40-67; col. 5, lines 50-55***).

Therefore, one of ordinary skilled artisan would have been motivated to modify the combined system of Hoffman & Igaki with the idea of succession being characterized according to at least one of the number of said entries and a duration of each said entry, the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration as taught by Pu because the use of Pu could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to include at least one of the number of said entries and a duration of each said entry, the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration to implement high security of the system by using secret sequence codes formed by body parts (***Pu, col. 3, lines 21-23***).

Regarding claim 60, (Currently Amended) Hoffman in view of Igaki & Pu further teaches a method according to claim 58, wherein the step of enrolling the biometric signature further comprises receiving another biometric signal to confirm the enrolling of the biometric signal as an administrator signature dependent upon generation of a feedback signal adapted to direct provision of at least one of the biometric signal and the other biometric signal (***Hoffman, col. 60, lines 34-43; col. 8, lines 20-55***).

Regarding claim 61, (Currently Amended) Hoffman in view of Igaki & Pu further taught a method according to claim 58, wherein the biometric sensor and the transmitter sub-system are located in a portable device (***Hoffman, col. 17, lines 64-67, The phone/CATV version of BIA hardware***).

<u>Regarding claim 62</u>, (Currently Amended) Hoffman-Igaki-Pu combination teaches a non-transitory computer readable medium for storing a computer program comprising instructions or code, which when executed by processors, causes the processors to perform the steps of the method of any one of claims 58 to 61.(***see the same rational cited in the above claims 58-61***).

<u>Regarding claim 63</u>, (New) Hoffman taught a system for populating a database of biometric signatures (***see [Abstract] A tokenless identification system and method for <u>authorization of transactions and transmissions</u>. The tokenless system and method are principally based on a <u>correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person</u> of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.***), the system comprising:

a processor, a memory, and a processor executable software program; a database of biometric signatures (***col. 44, lines 34-36: IBD individual biometric database; see col. 8, lines 30-36***); and a biometric sensor for receiving a biometric signal (***fig.3, ref. 12; col. 13, lines 2-8***), wherein said system is operable for populating the database of biometric signatures by performing the steps of: receiving, by the biometric sensor(***fig.3, ref. 12; col. 13, lines 2-8***),

Hoffman was silent on but the analogous art Igaki taught a succession of entries of the biometric signal, the succession being characterised according to at least one of the number of said entries and a duration of each said entry; and populating the database dependent upon the succession of entries(***see Abstract, "An optical sensor unit optically <u>produces a sequence of fingerprint image data</u> during a single operation of <u>pressing a fingerpad onto an inspection plate</u> in a direction substantially transverse to the plate and with increasing pressure <u>over a time interval</u>. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate." This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in***

fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary").

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of Hoffman with the idea of producing a sequence of fingerprint image data of Igaki *[Igaki:1:58-61]* because the use of Igaki could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to produce a sequence of fingerprint image data of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*igaki: Col. 1:49-51]*).

Hoffman-Igaki combination is silent on but the analogous art **Pu** teaches the number of said entries (***Pu, col. 2, lines 18-22; 5, lines 25-46)*** is the appropriate number of entries, and the duration of each said entry (***Pu, col. 5, lines 50-55***) is of the appropriate duration (***Pu, col. 2, lines 40-43; col. 4, lines 30-33, 40-67; col. 5, lines 50-55***).

Therefore, one of ordinary skilled artisan would have been motivated to modify the combined system of Hoffman & Igaki with the idea of the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration as taught by Pu because the use of Pu could provide the Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] the ability to include the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration to implement high security of the system by using secret sequence codes formed by body parts (***Pu, col. 3, lines 21-23***).

Regarding claim 67, (Currently Amended) Hoffman in view of Igaki and Pu further teaches a system according to claim 50, wherein: physical access is provided to one of a door, a gate, and a hatch;

and electronic access is provided to one of a Personal Computer, a smart phone, a network, and a payment (***Hoffman, fig. 3, col. 14, section 1.1.2 BIA models***).

Regarding claim 68, (Currently Amended) Hoffman-Igaki-Pu combination further teaches a system according to claim 46, wherein the succession of entries of the biometric signal comprises four entries, the first three of which are of 1 second duration, and the last of which is of 2 second duration (***Pu, col. 5, lines 50-55, By removing and placing the user's fingerprint on the input device for a plurality of times with different duration, a fingerprint Morse Code is generated.*** Based on the specification application uses dit, dit, dit, dah entry which is a Morse code).

Claim 65 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Igaki in view of Pu.

> Examiner Notes: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner. A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including non-preferred embodiments. *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), *cert. denied,* 493 U.S. 975 (1989). See MPEP 2123.

Regarding claim 65, (New) Igaki teaches a method for populating a database of biometric signatures, the method comprising the steps of:

receiving, by a biometric sensor (fig. 8, ref. 110), a succession of entries of the biometric signal; determining at least one of the number of said entries and a duration of each said entry; and populating the database dependent upon the succession of entries (***see Abstract, "An optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of***

pressing the fingerpad onto the inspection plate." This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad. see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between <u>successive fingerprint image data produced in successive, multiple fingerprint pressing down operations</u> as in the prior art becomes unnecessary"; See further fig. 5A-5D).

Igaki is silent on but the analogous art <u>**Pu**</u> teaches <u>said succession being characterized according to at least **one** of the number of said entries</u> (***Pu, col. 2, lines 18-22; 5, lines 25-46)*** <u>and a duration of each said entry</u> (***Pu, col. 5, lines 50-55***); <u>the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration</u> (***Pu, col. 2, lines 40-43; col. 4, lines 30-33, 40-67; col. 5, lines 50-55***).

Therefore, one of ordinary skilled artisan would have been motivated to modify the combined system of <u>Hoffman & Igaki</u> with the idea of succession being characterized according to at least one of the number of said entries and a duration of each said entry, the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration as taught by <u>Pu</u> because the use of <u>Pu</u> could provide the Biometric Input Device of <u>Hoffman</u> [*<u>Hoffman</u>, fig. 3, item 12*] the ability to include at least one of the number of said entries and a duration of each said entry, the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration to implement high security of the system by using secret sequence codes formed by body parts (***Pu, col. 3, lines 21-23***).

Claim 66 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Igaki in view of Pu as claimed 65 above and in further view of Koo.

Examiner Notes: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner. A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including non-preferred embodiments. *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), *cert. denied,* 493 U.S. 975 (1989). See MPEP 2123.

Regarding claim 66, (New) Igaki-Pu-Koo combination teaches a method according to claim 64, wherein the step of populating the database further comprises the steps of:

receiving a biometric signal (***Igaki, fig.6, ref. S1***); Igaki is silent on but the analogous art Koo teaches enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty (***Koo, see [Page 16, lines 8-10] if no registered administrator fingerprint information exists as empty, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14***).

One of ordinary skilled in the art would have been motivated to incorporate the idea of Koo ***[Page, 5, lines 19-22; Page 16, lines 8-10]*** within the combined method of Igaki because the idea of Koo could provide the method of Igaki to provide an electronic card key administration system consisted of host computer systems for administration of a plural of the electronic fingerprint recognition card keys (***Koo, Page 3, lines 21-23***).

Claims 59, 64 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hoffman in view of Igaki & Pu as applied to claims 58, 63 above, and further in view of Koo et al. WO 02/12660 hereinafter "Koo".

Examiner Notes: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner. A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including non-preferred embodiments. *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), *cert. denied,* 493 U.S. 975 (1989). See MPEP 2123.

Regarding claim 59, (Currently Amended) Hoffman-Igaki-Pu combination teaches a method according to claim 58, the combination is silent on but the analogous art Koo taught wherein the step of populating the database of biometric signatures further comprises the step of enrolling a biometric signature into the database of biometric signatures by: receiving a biometric signal; and enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty (***Koo, see [Page 16, lines 8-10] if no registered administrator fingerprint information exists as empty, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14***).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the applicant's invention was made to modify the combined method of Hoffman, Igaki, and Pu with the teaching of Koo for enrolling the relevant signatures into the database using the biometric sensor as an administrator if the database of biometric signatures is empty because they are analogous in biometric entry.

One of ordinary skilled in the art would have been motivated to incorporate the idea of Koo ***[Page, 5, lines 19-22; Page 16, lines 8-10]*** within the combined method of Hoffman [fig. 1], Igaki, and Pu because the idea of Koo could provide the method of Hoffman to provide an electronic card key administration system consisted of host computer systems for administration of a plural of the electronic fingerprint recognition card keys (***Koo, Page 3, lines 21-23***).

Regarding claim 64, (New) Hoffman-Igaki-Koo combination further teaches a system according to claim 63, wherein the system is further operable for enrolling a biometric signature into the database of biometric signatures by: receiving a biometric signal; and enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty (***Koo, see [Page 16, lines 8-10] if no registered administrator fingerprint information exists as empty, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14***).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: US 6,992,562 (Fuks), US 7,174,017 (Bantz), US 6,195,447 (Ross).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MOHAMMAD L. RAHMAN whose telephone number is (571)270-7471. The examiner can normally be reached on Monday to Friday: 9:00 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, TAGHI T. ARANI can be reached on 5712723787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MOHAMMAD L RAHMAN/
Primary Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 13/572,166	Applicant(s)/Patent Under Reexamination BURKE, CHRISTOPHER JOHN	
	Examiner MOHAMMAD L. RAHMAN	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,195,447 B1	02-2001	Ross, Paul C.	382/125
*	B	US-6,229,906 B1	05-2001	Pu et al.	382/116
*	C	US-6,992,562 B2	01-2006	Fuks et al.	340/5.52
*	D	US-7,174,017 B2	02-2007	Bantz et al.	380/255
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	**Application/Control No.** 13572166	**Applicant(s)/Patent Under Reexamination** BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	**Art Unit** 2438

CPC- SEARCHED

Symbol	Date	Examiner
H04L63/0861	4/22/2015	MLR
G06F21/32	4/22/2015	MLR

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
713	186	03/19/2014	MLR
Updated Search			
713	186	11/6/2014	MLR

SEARCH NOTES

Search Notes	Date	Examiner
Combined text search with classes/sub-classes (see EAST)	3/19/2014	MLR
Inventor name, Assigee	3/19/2014	MLR
NPL Search - Google Scholar IEEE ACM WIPO	3/19/2014	MLR
Updated Search		
Updated keywords combined with classes/sub-classes	11/6/2014	MLR
Inventor name, Assignee	11/6/2014	MLR
NPL Search - Google Scholar IEEE ACM WIPO	11/6/2014	MLR
Updated Text search combined with CPC symbols (see EAST)	4/22/2015	MLR
Inventor name, Assignee	4/22/2015	MLR
NPL Search - Google Scholar IEEE ACM WIPO	4/22/2015	MLR

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	93012	(G07C9/00158 or G06F21/35 or H04W12/08 or H04L63/0861 or G06F21/32 or H04W84/18 or H04W84/12).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/22 21:24
L2	55	(duration (time near5 (period length span))) with ((biometric fingerprint (retina near2 scan)) near5 entr$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/22 21:25
L3	17	L1 and L2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/22 21:25
S1	656	(biometric fingerprint) with (key near fob)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:45
S2	275	(biometric fingerprint) with (key near fob) and (audit$ examin$3 investigat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:47
S3	49	(biometric fingerprint) with (key near fob) and (audit$ examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20040813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:48
S4	43	(biometric fingerprint) with (key near fob) and (audit$ examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:51
S5	0	(biometric fingerprint) with (remote near key near fob) and (audit$ examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:52
S6	0	(biometric fingerprint) with (remote near2 key near fob) and (audit$	US-PGPUB; USPAT; USOCR;	OR	ON	2014/03/18 12:53

		examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S7	2	("8266442").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:36
S8	2	"20120278863"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:42
S9	2	"20120311346"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:43
S10	2	"20120311343"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:43
S11	29	((Christopher) near2 (Burke)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/19 15:33
S12	16349	(713/182-186,168).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/03/19 15:34
S13	23869	(726/2,7,26-30).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/03/19 15:34
S14	33433	(709/224-225).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/03/19 15:35
S15	738	biometric with identif$7 same (access near2 (right privilege control)) and (((unconditional unlimited) near2 access) duress alert telemetry)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:35
S16	33	(enroll$3 register$3) with (((biometric adj image) biometric (fingrprint adj image) fingerprint) near (sequence array))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:35

S17	4829	assign$3 with (access near (right privilege))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:35
S18	1377	(access near (right privilege)) same ((biometric adj image) biometric (fingrprint adj image) fingerprint)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:36
S19	174	S17 and S18	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:36
S20	26	S12 and S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:36
S21	24	S13 and S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S22	4	S14 and S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S23	23	S15 and S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S24	65	S12 and S15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S25	41	S13 and S15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S26	11	S14 and S15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37

S27	27	S15 and S17	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/03/19
						15:37

S28	165	S15 and S18	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/03/19
						15:37

S29	1377	(access near (right privilege)) same ((biometric adj image) biometric (fingrprint adj image) fingerprint)	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/03/19
						15:38

S30	131	(assign$3 provid$3) with (access adj (right privilege)) same (biometric fingerprint)	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/03/19
						15:38

S31	94	(biometric fingerprint) with ((multiple plural consecutive sequential successive) near2 entr$3)	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/11/06
						13:34

S32	33	(biometric fingerprint) with ((multiple plural consecutive sequential successive) near2 entr$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/11/06
						13:34

S33	18809	(713/182-186,168).CCLS.	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2014/11/06
						13:35

S34	2	S33 and S32	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/11/06
						13:35

S35	29312	(726/2,7,26-30).CCLS.	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2014/11/06
						13:35

S36	0	S35 and S32	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/11/06
						13:35

S37	39035	(709/224-225).CCLS.	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2014/11/06
						13:35

S38	0	S37 and S32	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/11/06
						13:35

S39	36	((Christopher) near2 (Burke)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2014/11/06 13:35

S40	0	S39 and S31	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/11/06
						13:35

S41	10	(biometric fingerprint) with ((consecutive sequential successive) near2 entr$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/11/06
						13:36

S42	17	(calculat$3 detect$3 identify$3) with (number near5 (biometric near2 entr$3))	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/20
						21:40

S43	0	(calculat$3 detect$3 identify$3) with (duration near5 (biometric near2 entr$3))	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/20
						21:40

S44	1	(calculat$3 detect$3 identify$3) with ((duration period time) near5 (biometric near2 entr$3))	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/20
						21:40

S45	1	(calculat$3 detect$3 identify$3) with ((duration period time length span) near5 (biometric near2 entr$3))	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/20
						21:41

S46	14	((duration period time length span) near5 (biometric near2 entr$3))	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/21
						10:42

S47	0	(duration (time near2 (period length span))) with ((each multiple plural) near5 (biometric near2 entr$3))	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
				OR	ON	2015/04/21
						10:47

			DERWENT; IBM_TDB			

S48	0	(duration (time near5 (period length span))) with ((each multiple plural) near5 (biometric near2 entr$3))	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/21
						10:47

S49	23	(duration (time near5 (period length span))) with (biometric near2 entr$3)	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/21
						10:47

S50	8	(biometric fingerprint) SAME ((consecutive sequential successive) near2 entr$3) SAME ((number count$3) near5 entr$3) AND (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/21
						11:15

S51	13	(biometric fingerprint) SAME ((consecutive sequential successive) near2 entr$3) AND ((number count$3) near5 entr$3) AND (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/21
						11:16

S52	55	(duration (time near5 (period length span))) with ((biometric fingerprint (retina near2 scan)) near5 entr$3)	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/21
						11:25

S53	19	(duration (time near5 (period length span))) with ((biometric fingerprint (retina near2 scan)) near5 entr$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/21
						11:25

S54	161	"5109428"	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/21
						12:15

S55	4	"5109428".PN.	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/21
						12:15

S56	3	(biometric fingerprint) same ((consecutive successive) near2 entr$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/21
						12:20

S57	43	(biometric fingerprint) same ((consecutive successive multiple) near2 entr$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
				OR	ON	2015/04/21
						12:22

			DERWENT; IBM_TDB			

S58	2	"6195447 ".PN.	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/21
						13:12

S59	2	"6229906".PN.	US-PGPUB;
			USPAT; USOCR;
			FPRS; EPO;
			JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2015/04/21
						13:41

EAST Search History (Interference)

<This search history is empty>

4/22/2015 9:29:15 PM
C:\Users\mrahman3\Documents\EAST\Workspaces\13572166_First.wsp

Index of Claims	**Application/Control No.** 13572166	**Applicant(s)/Patent Under Reexamination** BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	**Art Unit** 2438

✓	**Rejected**	-	**Cancelled**	**N**	**Non-Elected**	**A**	**Appeal**
=	**Allowed**	÷	**Restricted**	**I**	**Interference**	**O**	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		**DATE**								
Final	Original	03/19/2014	11/06/2014	04/22/2015						
	1	✓	-	-						
	2	✓	-	-						
	3	✓	-	-						
	4	✓	-	-						
	5	✓	-	-						
	6	✓	-	-						
	7	✓	-	-						
	8	✓	-	-						
	9	✓	-	-						
	10	✓	-	-						
	11	✓	-	-						
	12	✓	-	-						
	13	✓	-	-						
	14	✓	-	-						
	15	✓	-	-						
	16	✓	-	-						
	17	✓	-	-						
	18	✓	-	-						
	19	✓	-	-						
	20	✓	-	-						
	21	✓	-	-						
	22	✓	-	-						
	23	✓	-	-						
	24	✓	-	-						
	25	✓	-	-						
	26	✓	-	-						
	27	✓	-	-						
	28	✓	-	-						
	29	✓	-	-						
	30	✓	-	-						
	31	✓	-	-						
	32	✓	-	-						
	33	✓	-	-						
	34	✓	-	-						
	35	✓	-	-						
	36	✓	-	-						

Index of Claims	**Application/Control No.** 13572166	**Applicant(s)/Patent Under Reexamination** BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	**Art Unit** 2438

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		DATE								
Final	Original	03/19/2014	11/06/2014	04/22/2015						
	37	✓	-	-						
	38	✓	-	-						
	39	✓	-	-						
	40	✓	-	-						
	41	✓	-	-						
	42	✓	-	-						
	43	✓	-	-						
	44	✓	-	-						
	45		✓	✓						
	46		✓	✓						
	47		✓	✓						
	48		✓	✓						
	49		✓	✓						
	50		✓	✓						
	51		✓	✓						
	52		✓	✓						
	53		✓	✓						
	54		✓	✓						
	55		✓	✓						
	56		✓	✓						
	57		✓	✓						
	58		✓	✓						
	59		✓	✓						
	60		✓	✓						
	61		✓	✓						
	62		✓	✓						
	63		✓	✓						
	64		✓	✓						
	65		✓	✓						
	66		✓	✓						
	67		✓	✓						
	68			✓						

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS on the below date:

Date: May 15, 2015 Name: E. Brandon Nykiel Signature: /E. Brandon Nykiel/

BRINKS
GILSON
& LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of:	Christopher John Burke		
Appln. No.:	13/572,166	Examiner:	Rahman, Mohammad L.
Filed:	August 10, 2012	Art Unit:	2438
For:	REMONTE ENTRY SYSTEM	Conf. No.:	9752
Attorney Docket No.:	12838-8		

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

In accordance with the duty of disclosure, Applicant(s) hereby cites the following references:

US PATENT REFERENCES

EXAMINER INITIAL		DOCUMENT NUMBER Number-Kind Code (if known)	DATE	NAME
	B1	2002/0038818 A1	04-04-2002	Zingher et al.
	B2	2003/0126439 A1	07-03-2003	Wheeler et al.

FOREIGN PATENT REFERENCES

EXAMINER INITIAL		DOCUMENT NUMBER Number-Kind Code (if known)	DATE	COUNTRY	TRANSLATION YES OR NO
	B3	WO 02/095589 A1	11-28-2002	PCT	N/A

OTHER ART – NON PATENT LITERATURE DOCUMENTS

EXAMINER INITIAL	Include name of author, title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	B4	Extended European Search Report for corresponding EP application number 14188004 dated April 22, 2015
	B5	Office Action for corresponding Canadian application number 2,535,434 dated March 27, 2015

Examiner Signature		Date Considered	

1. PRIORITY INFORMATION:

□ This application claims priority under 35 USC §120 to the following United States patent application(s):. In accordance with 37 CFR §1.98(d), copies of the references cited herein which were submitted to, or cited by, the office, in compliance with 37 CFR §1.98(a)-(c) in the earlier application are not provided herewith. The Examiner is directed to those references cited in all Information Disclosure Statements filed in the priority United States patent application(s) cited above in addition to the references cited herein.

2. CERTIFICATIONS: (CHECK ALL THAT APPLY)

□ For purposes of 37 CFR §1.704(d)(i), Applicant hereby certifies that each item of information contained in this Information Disclosure Statement was first cited in any communication from a patent office in a counterpart foreign or international application or from the Office, and that this communication was not received by any individual designated in 37 CFR §1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement.

□ For purposes of 37 CFR §1.704(d)(ii), Applicant hereby certifies that each item of information contained in this Information Disclosure Statement is a communication that was issued by a patent office in a counterpart foreign or international application or by the Office, and that this communication was not received by any individual designated in 37 CFR §1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement.

☒ Applicant hereby certifies pursuant to 37 CFR §1.97(e)(1) that each item of information in this Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

□ Applicant hereby certifies pursuant to 37 CFR §1.97(e)(2) that no item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated in 37 CFR §1.56(c), more than three months prior to the filing of this Information Disclosure Statement.

3. FEE INFORMATION: (CHECK IF FEE REQUIRED)

□ Applicant has calculated a processing fee in the amount of ________ to be due under 37 CFR §1.17(p) in connection with the filing of this Information Disclosure Statement. Applicant authorizes charging the fee to Deposit Account ________.

☒ The Director is hereby authorized to charge any fee deficiency associated with the filing of this Information Disclosure Statement to Deposit Account 23-1925.

Pursuant to the undersigned attorney's obligation and duties under 37 CFR §§ 1.56 and 1.98(a)(3) and (c), either English language abstracts, partial translations, or full translations are included for patent documents which are not in English for the express purpose of providing a concise explanation of the references to the Patent and Trademark Office with the opportunity to evaluate the same. Applicant respectfully requests the Examiner's consideration of the above reference(s) and entry thereof into the record of this application.

By submitting this Statement, Applicant is attempting to fully comply with the duty of candor and good faith mandated by 37 CFR §1.56. As such, this Statement is not intended to constitute an admission that any of the enclosed references, or other information referred to therein, constitutes "prior art" or is otherwise "material to patentability," as that phrase is defined in 37 CFR §1.56(a).

Respectfully submitted,
May 15, 2015 /E. Brandon Nykiel/
Date E. Brandon Nykiel (Reg. No. 62,972)

xaminer Signature		Date Considered	

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 November 2002 (28.11.2002)

PCT

(10) International Publication Number
WO 02/095589 A1

(51) International Patent Classification⁷: G06F 11/30

(21) International Application Number: PCT/US02/15843

(22) International Filing Date: 17 May 2002 (17.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/858,887 17 May 2001 (17.05.2001) US

(71) Applicant: IDENTIX INCORPORATED [US/US]; 5600 Rowland Road, Minnetonka, MN 55343 (US).

(72) Inventors: SANCHEZ, Juan, Federico; 329 N First Street #312, San Jose, CA 95110 (US). LEDEEN, William, Present; 10265 Parkwood Drive, #1, Cupertino, CA 95014 (US).

(74) Agents: EGAN, William, J. et al.; Fish & Richardson, P.C., 500 Arguello Street, Suite 500, Redwood City, CA 94063 (US).

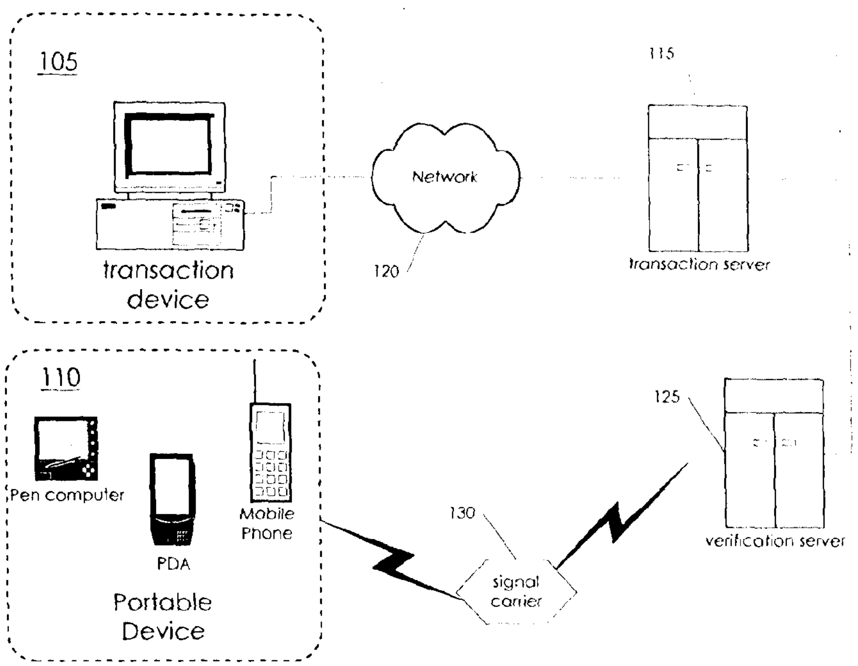
(81) Designated States *(national)*: AU, CA, JP, KR.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: MOBILE IDENTITY VERIFICATION



(57) Abstract: A method performed at a verification server of verifying an identity of a user attempting to access a transaction hosted by a server includes a receiving a biometric signal from a verification system that is housed within a portable device and that is separate from the transaction server and the verification server. The received biometric signal is validated, and acknowledgement of validation is sent to the transaction server. The received biometric signal includes information relating to the user's identity that was obtained using biometric verification.

WO 02/095589 A1

MOBILE IDENTITY VERIFICATION

TECHNICAL FIELD

This invention relates to identity verification, and more particularly to universal mobile identity verification.

BACKGROUND

Biometric identity verification is a useful tool for validating a user's identity without the annoyance of remembering a password and with the convenience and safety of biometric identification.

Fingerprint identity verification is one example of a biometric identity verification system. Fingerprint identity verification includes, among other steps, acquiring fingerprint data using a fingerprint reader. Typically, fingerprint data are obtained by reflecting or scattering an image of a finger surface onto an image sensor, such as a charge coupled device. Fingerprint readers are described in, for example, U.S. Pat. No. 4,924,085 to Kato et al., U.S. Pat. No. 5,088,817 to Igaki et al., and U.S. Pat. No. 5,067,162 to Driscoll, Jr., et al. In each of these fingerprint readers, a light source is irradiated at an angle onto the ridge and valley portions of a fingerprint that has been pressed against a light conducting plate. Depending upon the particular orientation of the light source with respect to the light conducting plate, and the location of the image sensing device, either the reflected or the scattered light from the fingerprint is transferred. The image sensor captures the transferred light so that the captured fingerprint data can be stored.

SUMMARY

In one general aspect, a method is performed at a verification server for verifying an identity of a user attempting to access a transaction hosted by a server. The method includes receiving a biometric signal from a verification system that is housed in a portable device and that is separate from the transaction server and the verification server. The method further includes validating the received biometric signal, and sending acknowledgement of validation to the transaction server. The received biometric signal includes information relating to the user's identity that was obtained using biometric verification.

Implementations may include one or more of the following features. The method may include receiving a user identifier from the transaction server and generating an access identifier in response to the received user identifier. The method may also include sending the access identifier to the transaction server for presentation to the user and prompting a user to enter the access identifier. The access identifier may be received from the user and validated, and the user may be prompted to produce the biometric signal by performing a verification action. Validating the received access identifier may include determining if the received access identifier corresponds to the generated access identifier.

The received biometric signal may be validated by determining if the received biometric signal corresponds to a predetermined biometric template for the user. A biometric signal may be transmitted through a wireless channel. A biometric signal may include information relating to a physical feature of the user.

The portable device may be a cellular telephone. The portable device may be a personal digital assistant.

In another general aspect, a system for verifying an identity of a user attempting to access a transaction hosted by a server includes a device and a verification server. The device is separate from the transaction server and carried by the user, and the device includes a verification system. The verification server is separate from the transaction server and the device. The verification server includes a processor having a communication link that transmits content to and from the user device and to and from the transaction server, and memory. The memory stores instructions performed by the processor (i) to receive a biometric signal from the verification system; (ii) to validate the received biometric signal; and (iii) to send acknowledgement of validation to the transaction server. The received biometric signal includes information relating to the user's identity that was obtained using biometric verification.

Implementations may include one or more of the following features. The verification system may include an imager, a processor, and memory. The memory stores instructions performed by the verification system processor (i) to image a finger; (ii) to convert the finger image into a biometric template; and (iii) to prepare the biometric template for subsequent transmission.

The transaction server may include a processor having a communication link that transmits content to and from the user device and to and from the verification server, and memory. The memory stores instructions performed by the transaction server processor (i) to receive a user request to access the transaction; (ii) to receive a user identifier; (iii) to send the user identifier to the verification server; (iv) to receive an access identifier from the verification server; (v) to present the access identifier to the portable device; (vi) to receive acknowledgement verifying the user identity from the verification server; and (vii) to grant the user access to the transaction.

In another general aspect, a system for converting a portable device into a portable verification device includes a body that houses components needed to perform a first function of the portable device, a compartment in the body of the portable device, and an adapted compartment. The compartment stores an energy source to power the housed components of the portable device. The adapted compartment is designed to encapsulate a fingerprint reader. The adapted compartment fits in the compartment of the portable device to convert the portable device into a portable verification device that performs the first function and a second verification function.

Implementations may include one or more of the following features. The portable device may be a cellular telephone. The compartment may include a battery pack. The adapted compartment may include a battery pack.

The fingerprint reader may include an imager, a processor, and memory. The memory stores instructions performed by the processor (i) to image a finger, (ii) to convert the finger image into a biometric template, and (iii) to prepare the biometric template for transmission.

In another general aspect, a method of converting a portable device into a portable verification device includes forming a mold cavity shaped like a compartment in a body of the portable device to to store an energy source to power elements needed to perform a first function of of the portable device. The method also includes inserting a fingerprint reader into the mold cavity and injecting a material into the mold cavity to encapsulate the fingerprint reader. The injected material is permitted to solidify to form an adapted compartment. The adapted compartment is attached to the portable device to convert the portable device into a portable verification device that performs the first function and a verification function.

Implementations may include one or more of the following features. The portable device may be a cellular telephone and the compartment may include a battery pack.

The systems and methods of biometric identity verification have several advantages. The biometric identity verification system and method exploits the ubiquity of wireless telephony and Internet access, thus enabling biometric identity verification with minimal modification to existing infrastructure. Accordingly, such a biometric identity verification system and method increases or promotes use of biometric verification to add security to many transactions.

Other features and advantages will be apparent from the following detailed description, the accompanying drawings, and the claims.

DESCRIPTION OF DRAWINGS

The invention is described by way of examples with reference to the accompanying drawings wherein:

Fig. 1 is a block diagram of a mobile identity verification system.

Fig. 2 is a block diagram of a portable device that may be used in the mobile identity verification system of Fig. 1.

Fig. 3 and 4 are front and back schematic views, respectively, of a portable device used in the mobile identity verification system of Fig. 1.

Fig. 5 is a flow chart of a procedure for forming a battery pack in the portable device of Figs. 3 and 4.

Figs. 6 and 7 are flow charts of procedures performed by the mobile identity verification system.

Like reference symbols in the various drawings indicate like elements.

DETAILED DESCRIPTION

Widespread adoption of fingerprint identity verification is inhibited because of a lack of installed infrastructure of fingerprint readers into various form factors such as, for example, personal computers, personal digital assistants (PDAs), and public data terminals. Although fingerprint reader technology is now available in small and moderately priced form factors, the technical complexity of installation into a wide variety and number form factors has had a negative effect on deployment of applications that may benefit from biometric verification of identity.

For example, portable personal identification devices (PIDs) may be used to provide secure access to a host facility such as a home security system, an automated teller machine, an automobil alarm system, or a garage door opener. The PID may include a biometric sensor system capable of sensing a biometric trait (such as a fingerprint) of a user that is unique to the user. The PID then provides a biometric signal indicative of the user's identity to the host facility. Such systems are described in U.S. Application No. 09/066,643, titled "PERSONAL IDENTIFICATION SYSTEM," and filed on April 24, 1998, and U.S. Application No. 09/298,326, titled "PERSONAL IDENTIFICATION SYSTEM AND METHOD," and filed on April 23, 1999, assigned to the assignee of the subject application and both of which are incorporated herein by reference.

Referring to Fig. 1, a mobile identity verification system 100 exploits the ubiquity of wireless communications to enable biometric identity verification with minimal modifications to existing infrastructure, thus increasing the possibility of using biometric identity verification in every day transactions. In general, a user enters biometric information into a portable device (such as a cellular telephone) when trying to enter a transaction at a transaction device (such as an Internet web page, a personal computer, or an automated teller machine). Using wireless communication, the portable device sends a biometric signal to an independent verification server (that may be separate from the portable device), which performs verification services and indicates such user verification to a transaction server in communication with the transaction device.

In wireless communications, electromagnetic waves (rather than some form of wire or cable) carry the propagation signal over part or all of the communication path. Some devices, such as intrusion alarms, employ acoustic waves at frequencies above the range of human hearing; these devices are also sometimes classified as wireless. Standard wireless communications systems include radio wave systems, microwave systems, and infrared systems. Standard applications using wireless communications include cellular telephones and pagers, global positioning systems, cordless computer peripherals, cordless telephone sets, home entertainment system control boxes, satellite television, and wireless local area networks.

The mobile identity verification system 100 includes a transaction device 105, a portable device 110, a transaction server 115 coupled to the transaction device 105 through a network 120, and a verification server 125 coupled to the portable device 110 using any signal carrier 130 such as a radio tower, microwave antenna, or infrared transmitter/receiver.

The transaction device 105 may be any device at which the user wishes to access a transaction. Examples of transaction devices 105 include personal computers, credit card terminals, and automatic teller machines. For example, the user may wish to access a web site that is enabled for fingerprint identity verification. As another example, the user may wish to use a credit card at a credit card terminal that requires biometric verification of the authorized card holder.

In any case, the transaction device 105 controls operations of the transaction and is enabled for biometric verification. To achieve these functions, the transaction device 105 may include various input/output (I/O) devices (for example, a mouse, a keyboard, a display, or a microphone) and a general purpose computer having a central processor unit (CPU), an I/O unit, and a memory that stores data and various programs such as an operating system, and one or more application programs. The memory stores a program that controls transactions enabled for biometric verification. The computer system may also include some sort of communications card or device (for example, a modem or network adapter) for exchanging data with a network via a communications link (for example, a telephone line or cable).

The transaction server 115 communicates with the transaction device 105 through the network 120 and with the verification server 125 either through a direct connection or through a wireless connection. The transaction server 115 may include one or more general-purpose computers (for example, personal computers), one or more special-purpose computers (for example, devices specifically programmed to communicate with each other), or a combination of one or more general-purpose computers and one or more special-purpose computers. The transaction server 115 may be arranged to operate within or in concert with one or more other systems, such as for example, one or more Local Area Networks (LANs) and/or one or more Wide Area Networks (WANs). The transaction server 115 is generally capable of executing instructions under the command of a transaction controller (not shown). The transaction server 115 is connected to the transaction controller by a wired or wireless data pathway capable of delivering data.

The portable device 110 may be any wireless device that a user is likely to carry such as a cellular telephone, a PDA, or a pen computer. The portable device 110 includes wireless communication equipment such as, for example, a transceiver (receiver/transmitter), audio circuitry (such as microphone or speaker), and various controller circuits for controlling communications. In addition to including necessary wireless communication equipment, the portable device 110 may include various input/output (I/O) devices (for example, a pointing device, a keyboard, or a display), a central processor unit (CPU), an I/O unit, and a memory that stores data and various programs such as an operating system, and one or more application programs.

The portable device 110 may include an externally-accessible (analog or digital) data connector for accessory devices such as, for example, headsets. When an accessory device is attached to the data connector, and once a predetermined event (for example, an initiation of a call on a cellular telephone) occurs, that accessory device operates as an input/output device for the portable device 110. In this case, the accessory device may override operation of internal devices of the portable device 110. For example, the accessory device may cause some internal devices of the portable device 110 to bypass a microphone.

Referring also to Fig. 2, the portable device 110 is equipped with a verification system 200 that includes all the necessary components for fingerprint identification, signal conversion, compression, encryption, and communication. The verification system 200 includes a fingerprint reader 205 that images the finger, image capture electronics 210 for receiving the output from the fingerprint reader 205 and for converting the output into a format readable by a controller 215.

The fingerprint reader 205 includes the necessary optics and illuminating sources for illuminating the finger. Fingerprint readers are described in U.S. Application No. 09/571,741, titled "FINGERPRINT IMAGING DEVICE" and filed on May 15, 2000, and U.S. Application No. 09/637,063, titled "FINGERPRINT IMAGING DEVICE" and filed on August 11, 2000, assigned to the assignee of the subject application and both of which are incorporated herein by reference.

The controller 215 may include a processor 220 and memory 225 storing software for converting image data from the image capture electronics 210 into a biometric template, and for compressing and encrypting the template to avoid interception during data communication. Thus, the memory 225 may store software 230 for capturing and imaging, software 235 for biometric template extraction, software 240 for data encryption and packaging, and software 245 for call control and protocol. The memory 225 may be used to store finger images and other suitable data that may be accessed by the processor 220. The verification system 200 may also include a modulator/demodulator (or a high speed touch tone generator) 250 for preparing data from the controller 215 for transmission.

Any suitable data communications system 255 may be implemented within the device 110 to transmit the template to a central verification server. For example, as discussed above, a suitable data communication system 255 may include analog and digital radio systems such as are used in cellular telephones. The communication system 255 may include a data or voice connector 260 for communicating with the modulator/demodulator 250 and standard wireless communication electronics 265 for use in portable devices and telephony applications. Additionally, the device 110 includes other various components 270 that control standard operation of the device 110. The various electronic components of the verification system 200 may be configured on a PC card or any suitable device.

The verification server 125 may include one or more general-purpose computers (for example, personal computers), one or more special-purpose computers (for example, devices specifically programmed to communicate with each other), or a combination of one or more general-purpose computers and one or more special-purpose computers. The verification server 125 may be arranged to operate within or in concert with one or more other systems, such as for example, one or more Local Area Networks (LANs) and/or one or more Wide Area Networks (WANs). The verification server 125 is generally capable of executing instructions under the command of a verification controller (not shown), which may be connected to the verification server by a wired or wireless data pathway capable of delivering data. In general, the verification server 125 performs the user identity verification that will be used by the transaction device 105 to grant access of a transaction to the user.

Referring also to Figs. 3 and 4, in one implementation, the portable device 110 may be a cellular telephone 300 that includes a telephone body 302 and a battery compartment 304. The battery compartment 304 contains the batteries used to power the cellular telephone. To facilitate fingerprint identity verification, the fingerprint reader

205 may be molded into an adapted battery component 410 that attaches to the telephone body 302 and fits within the battery compartment 304.

An externally-accessible data connector 306 may protrude into the battery compartment 304. In this case, the adapted battery component 410 may interface with the data connector 306 through a matching connector. In another design, the adapted battery component 410 may include a cable lead and a mating connector that connects into the data connector 306.

In some designs, a battery is also molded into the adapted battery component 410. In other designs, a battery is secured by the adapted battery component 410 into the battery compartment 304 of the telephone body 302. In any case, no modifications to the body 302 are required using the adapted battery component 410. Moreover, no approval (for example, FCC) is required to gain regulatory acceptance. Users may purchase the adapted battery component 410 to upgrade their existing cellular telephone to provide mobile identity verification at any time.

The adapted battery component 410 may be formed of any material suitable for use in the cellular telephone. For example, the adapted battery component 410 may be made from a non-conductive material using a variety of known techniques, such as a strong thermoplastic (for example, acrylonitrile-butadiene-styrene (ABS)) that may be injection molded or compression molded. Accordingly, the fingerprint reader 205 may be integrally formed with the battery component 410, during injection molding. The battery component 410 may also be formed, for example, from a lightweight metal having an electrically non-conductive coating. Specific dimensions of the battery component 410 depend on the size of the cellular telephone 300.

Referring also to Fig. 5, in one implementation, the adapted battery component 410 is formed using a production procedure 500 such as injection molding. The fingerprint reader is inserted and appropriately positioned into a mold cavity shaped like the battery component (step 505). Other components such as a battery and wires are inserted and positioned into the mold cavity (step 510). A prepared material such as a plastic resin or a polymer is injected under pressure into the mold cavity to encapsulate the fingerprint reader and the other positioned components (step 515). The prepared and injected material is permitted to solidify to form the adapted battery component (step 520) and the mold cavity is subsequently removed (step 525). The adapted battery component may then be integrated into the battery compartment of, for example, a cellular telephone..

Typically, the user programs a personal identification number (PIN) into the portable device 110 immediately after purchase of the portable device 110. This PIN is also stored, for example, into the memory of the fingerprint reader of the portable device 110 for future transmission and reference.

Referring to Figs. 6 and 7, the system 100 performs a procedure 600 for mobile identity verification. Initially, the transaction server 115 receives from a user at the transaction device 105 a request to access a verification-enabled transaction (step 605). For example, the user may access a web site that is enabled for biometric verification. Next, the transaction server 115 receives a user identifier (step 610). For example, the user may enter a user ID and then press a "verify" button at a web site instead of entering a password.

The transaction server 115 sends the user identifier to the verification server 125 (step 615). Upon receipt of the user identifier (step 620), the verification server 125 generates and sends an access identifier (for example, a randomly-generated multi-digit token) to the transaction server 115 (step 625). Upon receipt of the access identifier, the transaction server 115 presents the access identifier to the user at the transaction device 105 and requests that the user enter this access identifier when subsequently verifying her identity (step 630).

Next, the portable device 110 receives a user initiation to access the verification server 125 (step 635). For example, a user initiation may include the user pressing a speed dial button on her cellular telephone to access the verification server. The verification server 125 receives the initiation, initiates a connection by establishing a communication channel with the portable device 110 (step 637). The verification server prompts the user to enter her access identifier into the portable device 110 (step 640). For example, if the portable device 110 is a cellular telephone, the verification server 125 may prompt the user by playing a recorded message. Once the connection is established, then subsequent transmission to and from the portable device 110 will rely on transmission through the data connector 306. For example, transmitted information through an analog data connector 306 may include audible frequency shift or phase shift keyed analog modem signals. In this case, the user of the portable device 110 may be required to initiate a connection to an analog modem at the verification server. Transmitted information through a digital data connector 306 is binary in form and presented in serial data packets. Once the connection is established, the verification system takes over operation of the portable device 110.

In another implementation in which the portable device 110 transmits digital information, the verification system of the portable device 110 may be able to initiate the call directly at step 635 using cellular digital packet data (CDPD) protocol over an analog or digital cellular network (or using GSM digital protocol outside the United States). In any case, the amount of information that will be carried through the established communication channel is about 1 kilobyte (kB). Even at moderate data transmission speeds (for example, 9600 bps) that typically characterize wireless communication, the 1 kB payload may be uploaded in about less than 10 seconds of data transmission time.

The portable device 110 receives the access identifier from the user (who has entered the access identifier) and forwards this access identifier to the verification server 125 over the established communication channel (step 645). Upon receipt of the access identifier (step 650), the verification server 125 determines if the received access identifier is valid (step 655). If the access identifier is not valid (step 655), the verification server 125 may continue to prompt the user to enter a correct access identifier for a predetermined number of times (step 640). If the access identifier is valid (step 655), the verification server 125 forwards a signal through the established communication channel to the portable device 110 to prompt the user to verify her identity (step 660).

Next, the portable device 110 receives user verification input (step 662) and subsequently performs a verification procedure (step 665). As shown in Fig. 7, if the identity verification is fingerprint verification, the portable device 110 may perform a procedure 665 for verification. Initially, the portable device fingerprint reader images the finger (step 700). The portable device may then emit an acknowledgement tone to indicate a satisfactory image grab and extraction. Next, the fingerprint reader of the portable device converts the finger image into a verification signal such as a biometric template (step 705). The fingerprint reader then prepares the verification signal for subsequent transmission by, for example, compressing and encrypting the verification signal to reduce the likelihood of interception during transmission (step 710).

After the verification procedure is complete (step 665), the portable device 110 transmits the verification signal to the verification server 125 over the established communication channel (step 670). The verification server 125 receives and processes the verification signal (step 675). For example, if the verification signal has been compressed and/or encrypted by the portable device 110, the verification server 125 decompresses and/or decrypts the verification signal at step 675.

The verification server 125 determines if the verification signal is a valid signal by comparing the verification signal against a pre-established enrollment template for that particular user (step 680). If the verification signal is valid (step 680), then the user's identity has been successfully verified and the verification server 125 may notify the user as such (step 685). For example, notification may include the verification server 125 disconnecting its direct connection with the portable device 110. Otherwise, if the verification signal is not valid (step 680), the verification server 125 prompts the user to try again (step 660) until a predetermined retry limit is exhausted.

The verification server 125 sends an acknowledgement of positive verification of the user's identity for that access identifier to the transaction server 115 (step 690). When the transaction server 115 receives the positive verification acknowledgement, the transaction server 115 grants to the user access of the transaction (step 695). For example, if the transaction server is a host server of a web site, the user would be able to login to and access that web site.

A number of embodiments of the invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention.

The identity verification may include other forms of biometric verification such as, for example, speech recognition, which would require no modification to the portable device. In this case, all of the modifications would be programmed at the verification server of the system 100. Another form of biometric identification that may be implemented is a cornea or iris scan.

Fingerprint identity verification may be used to surreptitiously indicate duress. For example, the verification server may include several templates for a user, each template indicating a user's intentions. One of those templates may correspond to an alternate finger that a user would only use when faced with an emergency. In this way, the verification server may record the duress transaction and/or place an emergency call to proper authorities. This feature would provide added security, safety, and peace of mind for the user.

A duress indicator may not be as easy to implement using speech recognition. However, a duress indicator may be implemented through a user modification of the user's PIN or a user modification of an access identifier. For example, the user may add an extra digit (that may be predefined) to one of these identifiers to indicate duress.

In some transactions, such as credit card or telephone transactions, the transaction server may be implemented as an operator associated with the transaction device 105, which may be a telephone. The operator performs many of the operations of the transaction server 115, including requesting an access identifier from the verification server 125. The operator communicates with the user who is requesting a transaction from the portable device 110. The operator at the transaction device may open up an extra line using a conference mode of the telephone to dial in to the verification server 125 simultaneously with communication with the user. The verification server 125 answers as if the user had initiated the call and performs an audio dialogue. When the verification server requests the identity verification to be performed, the user presses their finger against the finger print reader, activating the mobile identity verification function. The portable device captures the fingerprint image, extracts the template, encodes the data (using an encryption scheme), establishes a modem link to the verification server (which is awaiting the modem's communication), and transmits the template. The verification server reports sucessful verification or requests a retry. If successful, the verification server forwards verification to the transaction server. The operator breaks the connection to the conference, hanging up on the verification server line, while remaining connected to the user. In this way, the user performs a verification transaction while still online with the assisting operator.

The adapted battery component 410 may be designed to provide space for marketing information so that the user of a mobile identity verification device 110 is simultaneously promoting the product to others. The adapted battery component 410 may be migrated to other cellular telephones of the same style and type as the original cellular telephone that was upgraded. Therefore, the user need not purchase a new adapted battery component every time she buys a new cellular telephone.

Accordingly, other embodiments are within the scope of the following claims.

What is claimed is:

1. A method performed at a verification server of verifying an identity of a user attempting to access a transaction hosted by a transaction server, the method comprising:

receiving a biometric signal from a verification system that is housed in a portable device and that is separate from the transaction server and the verification server;

validating the received biometric signal; and

sending acknowledgement of validation to the transaction server;

wherein the received biometric signal includes information relating to the user's identity that was obtained using biometric verification.

2. The method of claim 1 further comprising receiving a user identifier from the transaction server and generating an access identifier in response to the received user identifier.

3. The method of claim 2 further comprising sending the access identifier to the transaction server for presentation to the user and prompting a user to enter the access identifier.

4. The method of claim 3 further comprising:

receiving the access identifier from the user;

validating the received access identifier; and

prompting the user to produce the biometric signal by performing a verification action.

5. The method of claim 4 wherein validating the received access identifier includes determining if the received access identifier corresponds to the generated access identifier.

6. The method of claim 1 wherein validating the received biometric signal includes determining if the received biometric signal corresponds to a predetermined biometric template for the user.

7. The method of claim 1 wherein receiving a biometric signal includes receiving a biometric signal transmitted through a wireless channel.

8. The method of claim 1 wherein receiving a biometric signal includes receiving information relating to a physical feature of the user.

9. The method of claim 1 wherein the portable device is a cellular telephone.

10. The method of claim 1 wherein the portable device is a personal digital assistant.

11. A system for verifying an identity of a user attempting to access a transaction hosted by a transaction server, the system comprising:

a device separate from the transaction server and carried by the user, the device including a verification system;

a verification server separate from the transaction server and the device, the verification server comprising:

a processor having a communication link that transmits content to and from the user device and to and from the transaction server; and

memory storing instructions performed by the processor (i) to receive a biometric signal from the verification system; (ii) to validate the received biometric signal; and (iii) to send acknowledgement of validation to the transaction server;

wherein the received biometric signal includes information relating to the user's identity that was obtained using biometric verification.

12. The system of claim 11 wherein the verification system comprises:

an imager,

a processor, and

memory that stores instructions performed by the verification system processor (i) to image a finger; (ii) to convert the finger image into a biometric template; and (iii) to prepare the biometric template for subsequent transmission.

13. The system of claim 11 wherein the transaction server comprises:

a processor having a communication link that transmits content to and from the user device and to and from the verification server;

memory storing instructions performed by the transaction server processor (i) to receive a user request to access the transaction; (ii) to receive a user identifier; (iii) to send the user identifier to the verification server; (iv) to receive an access identifier from the verification server; (v) to present the access identifier to the portable device; (vi) to receive acknowledgement verifying the user identity from the verification server; and (vii) to grant the user access to the transaction.

14. A system for converting a portable device into a portable verification device, the system comprising:

a body that houses components needed to perform a first function of the portable device;

a compartment in the body of the portable device to store an energy source to power the housed components of the portable device; and

an adapted compartment into which a fingerprint reader is encapsulated;

wherein the adapted compartment fits in the compartment of the portable device to convert the portable device into a portable verification device that performs the first function and a second verification function.

15. The system of claim 14 wherein the portable device is a cellular telephone.

16. The system of claim 14 wherein the compartment includes a battery pack.

17. The system of claim 14 wherein the adapted compartment includes a battery pack.

18. The system of claim 14 wherein the fingerprint reader includes:

an imager,

a processor, and

memory that stores instructions performed by the processor (i) to image a finger, (ii) to convert the finger image into a biometric template, and (iii) to prepare the biometric template for transmission.

19. A method of converting a portable device into a portable verification device, the method comprising:

forming a mold cavity shaped like a compartment in a body of the portable device to store an energy source to power elements needed to perform a first function of of the portable device;

inserting a fingerprint reader into the mold cavity;

injecting a material into the mold cavity to encapsulate the fingerprint reader;

permitting the injected material to solidify to form an adapted compartment; and

attaching the adapted compartment to the portable device to convert the portable device into a portable verification device that performs the first function and a verification function.

20. The method of claim 19 wherein the portable device is a cellular telephone and the compartment includes a battery pack.

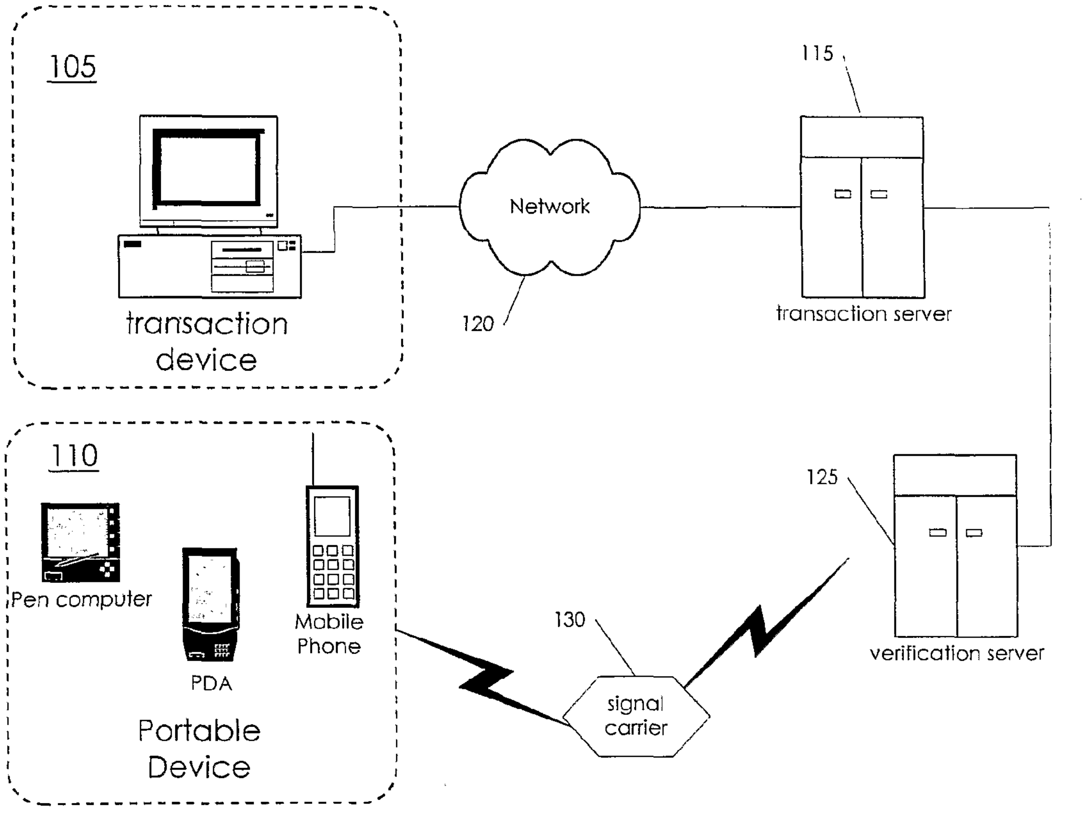

105
transaction device
Network
120
115
transaction server
110
Pen computer
PDA
Mobile Phone
Portable Device
130
signal carrier
125
verification server

Fig. 1

100

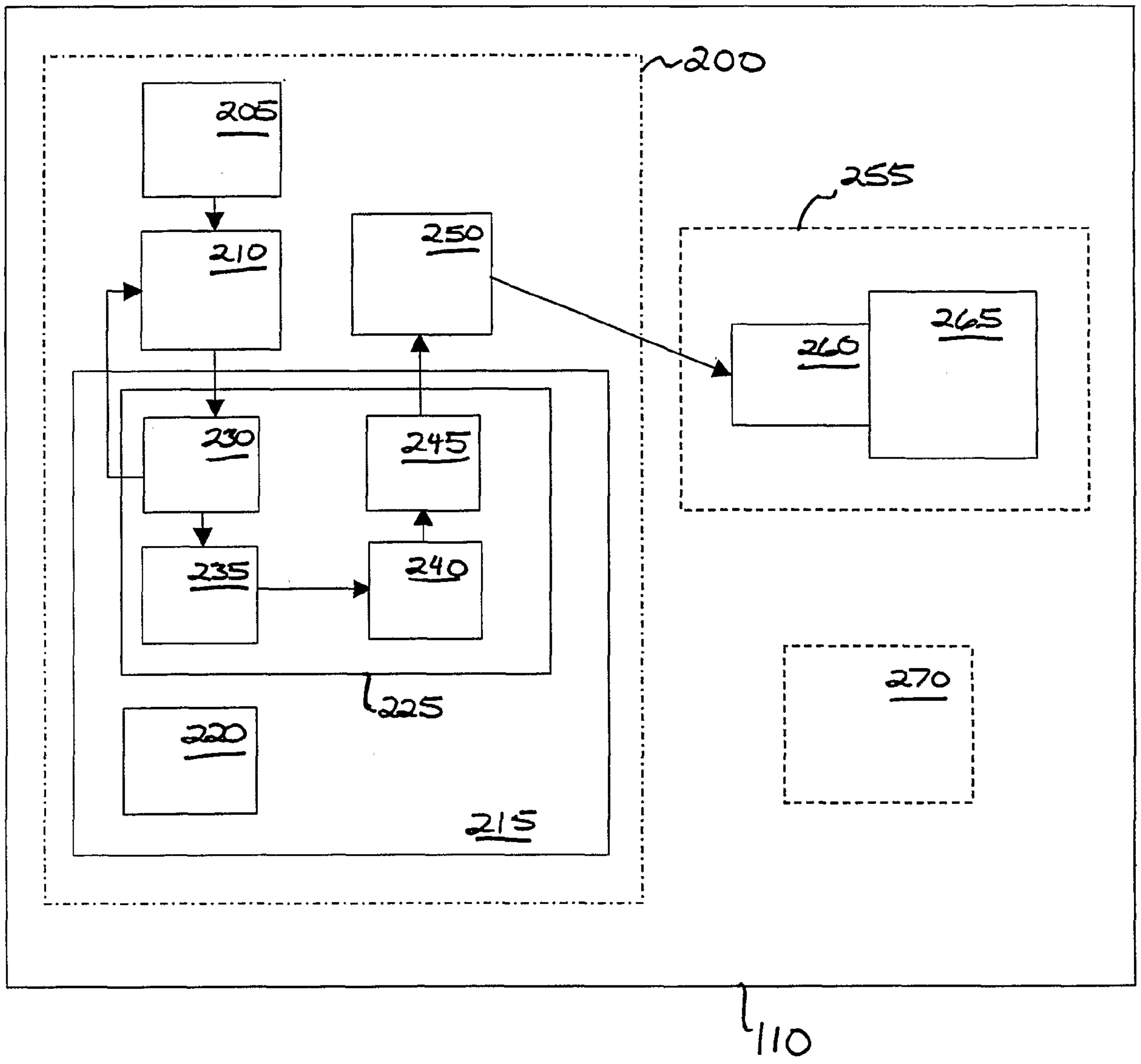


Fig. 2

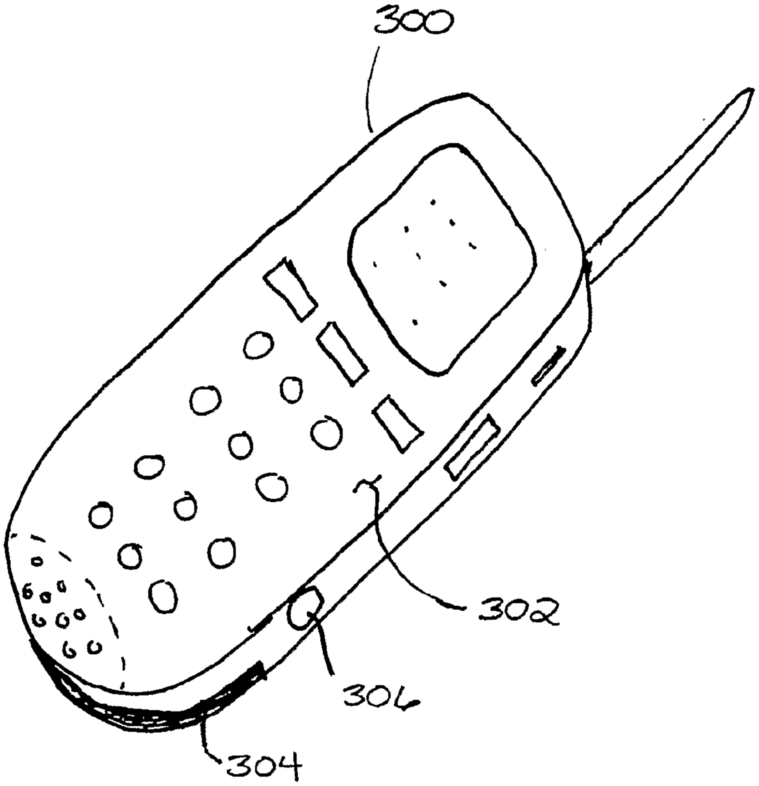


Fig. 3

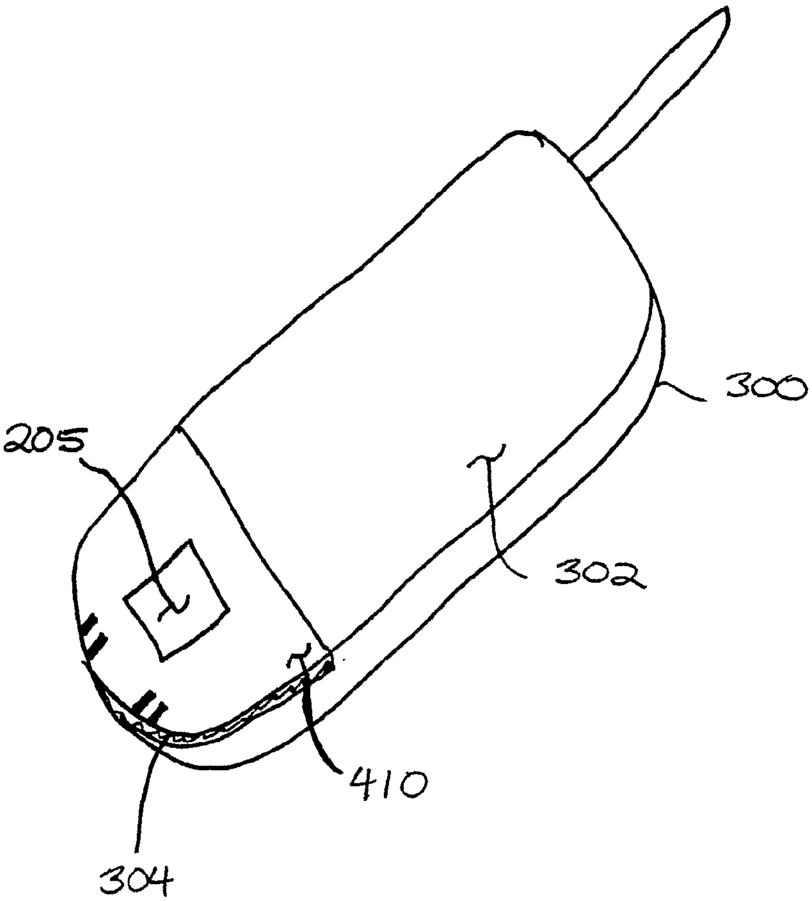


Fig. 4

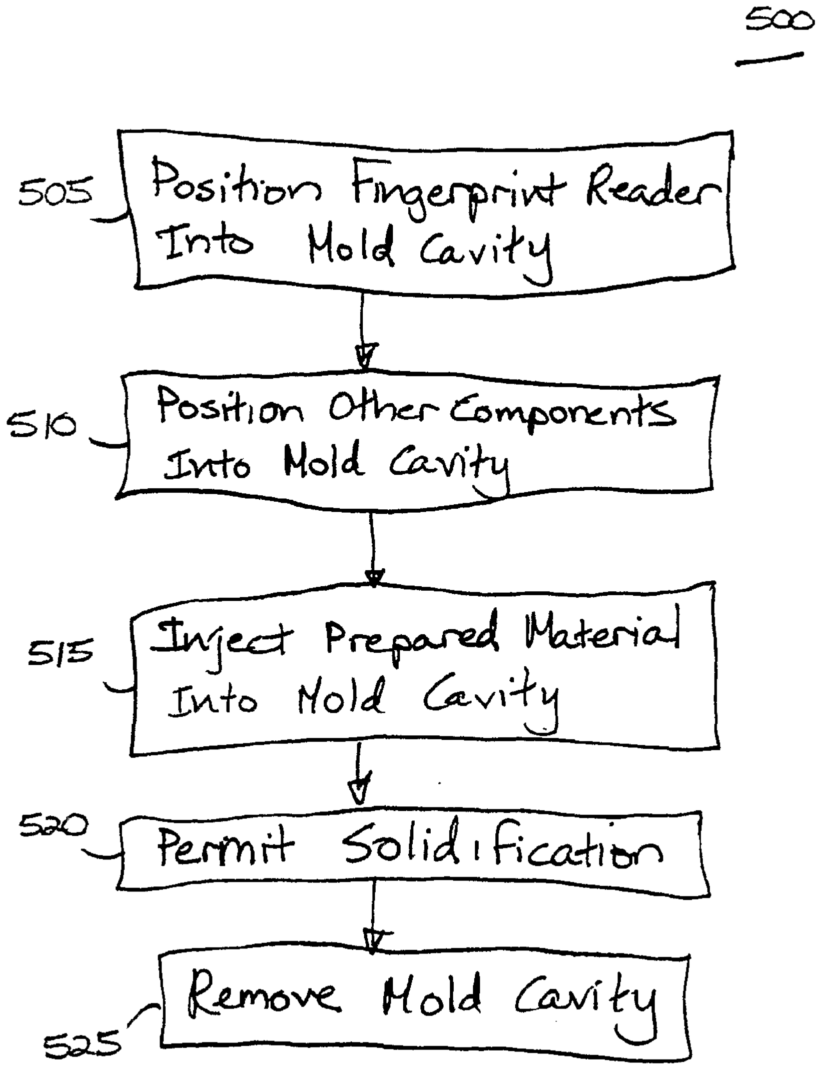

500
505
Position Fingerprint Reader Into Mold Cavity
510
Position Other Components Into Mold Cavity
515
Inject Prepared Material Into Mold Cavity
520
Permit Solidification
525
Remove Mold Cavity

Fig. 5

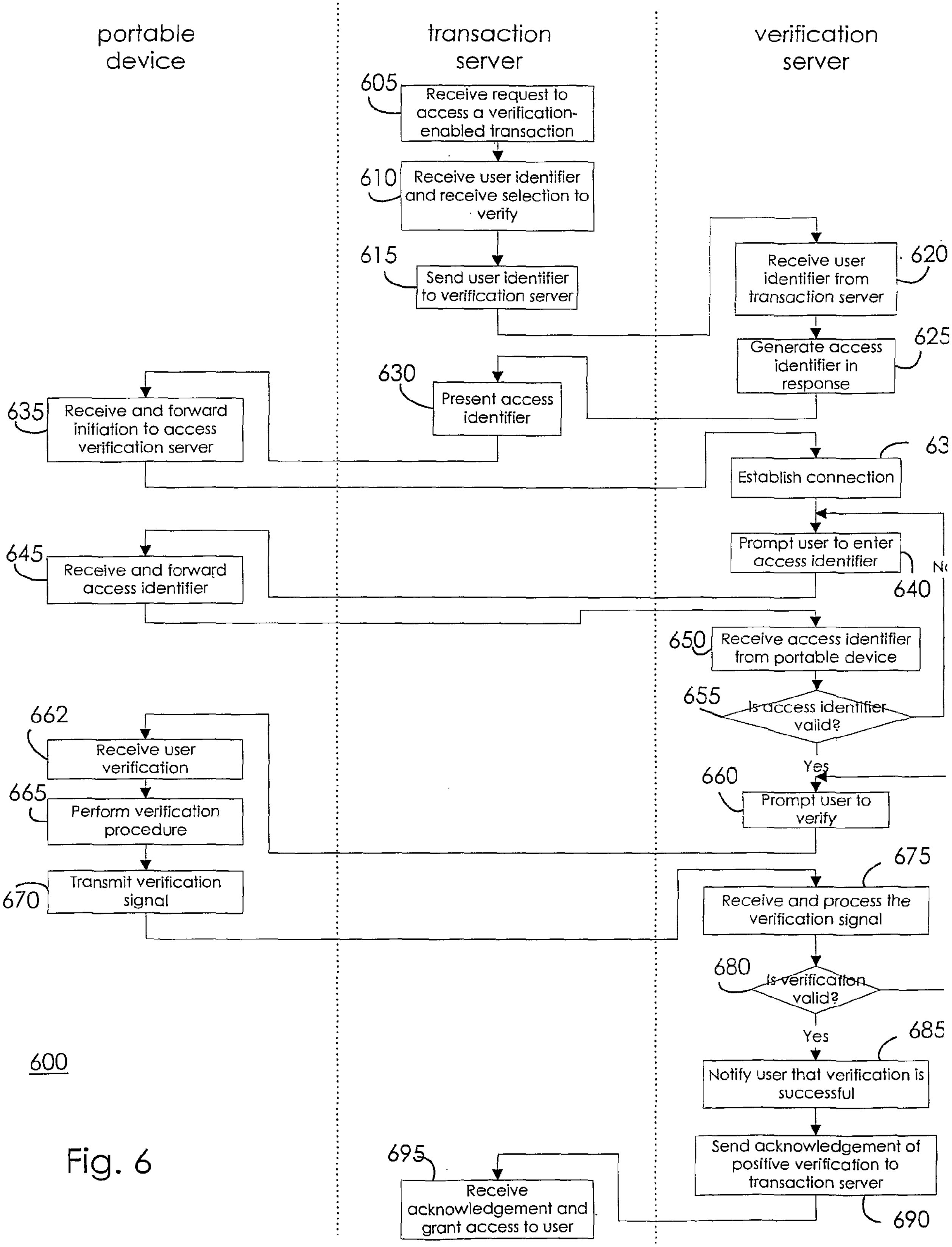

portable device
transaction server
verification server
605
Receive request to access a verification-enabled transaction
610
Receive user identifier and receive selection to verify
615
Send user identifier to verification server
620
Receive user identifier from transaction server
625
Generate access identifier in response
630
Present access identifier
635
Receive and forward initiation to access verification server
63
Establish connection
Prompt user to enter access identifier
640
No
645
Receive and forward access identifier
650
Receive access identifier from portable device
655
Is access identifier valid?
Yes
660
Prompt user to verify
662
Receive user verification
665
Perform verification procedure
670
Transmit verification signal
675
Receive and process the verification signal
680
Is verification valid?
Yes
685
Notify user that verification is successful
Send acknowledgement of positive verification to transaction server
690
695
Receive acknowledgement and grant access to user
600

Fig. 6

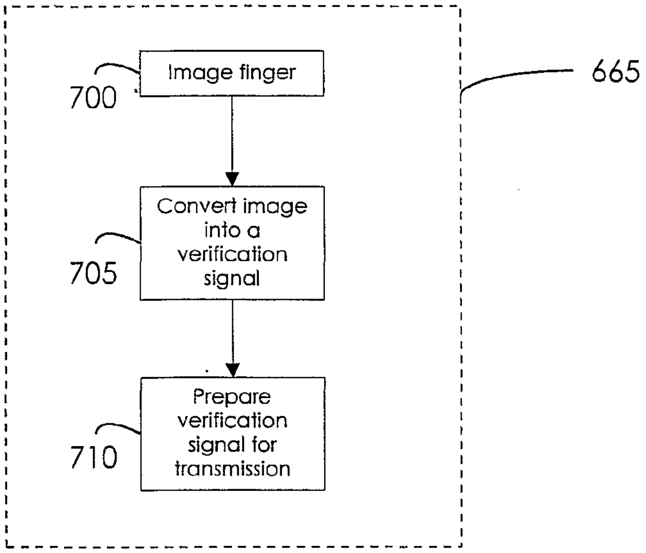


Image finger
700
Convert image into a verification signal
705
Prepare verification signal for transmission
710
665

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/15843

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :GO6F 11/30
US CL :713/201, 200, 202
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/201, 200, 202

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST - JPO, EPO, DERWENT, USPATFULL, IBMTBD terms: biometric, verification, remote, authentic$, authoriz$.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,915,973 A (HOEHN-SARIC ET AL) 29 June 1999, entire document.	1-10
Y	US 6,040,783 A (HOUVENER et al.) 21 March 2000, entire document.	1-10

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:
"A"	document defining the general state of the art which is not considered to be of particular relevance
"E"	earlier document published on or after the international filing date
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O"	document referring to an oral disclosure, use, exhibition or other means
"P"	document published prior to the international filing date but later than the priority date claimed
"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&"	document member of the same patent family

Date of the actual completion of the international search

01 JULY 2002

Date of mailing of the international search report

24 JUL 2002

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

NORMAN M. WRIGHT

Telephone No. (703) 305-3900

Electronic Acknowledgement Receipt

EFS ID:	22360404
Application Number:	13572166
International Application Number:	
Confirmation Number:	9752
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Correspondence Address:	Michael E. Milz Brinks Hofer Gilson & Lione P.O. Box 10395 - Chicago IL 60610 US 3123214200 -
Filer:	E. Brandon Nykiel/Alice Thoennes
Filer Authorized By:	E. Brandon Nykiel
Attorney Docket Number:	12838/8
Receipt Date:	15-MAY-2015
Filing Date:	10-AUG-2012
Time Stamp:	16:03:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		12838_IDSBFiling_051515.pdf	203458 ec6aa908b303d03f2d8769d8b4a8d6f0e99ed61f	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Miscellaneous Incoming Letter	1	1
	Information Disclosure Statement (IDS) Form (SB08)	2	3

Warnings:

Information:

2	Foreign Reference	B3.pdf	1948009 5904b6c603f13fc41457566657c1c0a37e675204	no	26

Warnings:

Information:

3	Other Reference-Patent/App/Search documents	B4.pdf	237718 fb540695a9be649f7981d4fe6e76e1cd8fd98342	no	6

Warnings:

Information:

4	Other Reference-Patent/App/Search documents	B5.pdf	204930 8bb21812af041937f9737cc6c1140307064dbcef	no	3

Warnings:

Information:

Total Files Size (in bytes):	2594115

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS pursuant to 37 CFR §1.8 on the below date:

Date: May 15, 2015 Name: E. Brandon Nykiel Signature: /E. Brandon Nykiel/

BRINKS
GILSON
& LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: Christopher John Burke
Appln. No.: 13/572,166
Filed: August 10, 2012
For: REMOTE ENTRY SYSTEM
Attorney Docket No.: 12838/8

Examiner: Rahman, Mohammad L.
Art Unit: 2438
Conf. No.: 9752

TRANSMITTAL

Mail Stop Amendment
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Attached is/are:

☒ Supplemental Information Disclosure Statement; and References B3-B5.

Fee calculation:

☒ No additional fee is required.

☒ Per 37 CFR §1.27, ☒ Applicant is small entity □ Applicant is micro entity.

□ An extension fee in an amount of $_____ for a _____-month extension of time under 37 CFR § 1.136(a).

□ A petition or processing fee in an amount of $_____ under 37 CFR § 1.20(_____).

□ An additional filing fee has been calculated as shown below:

					Fee		Small Entity Fee		Micro Entity Fee	
	Claims Remaining After Amendment		Highest No. Previously Paid	Present Extra	Rate	Add'l Fee	Rate	Add'l Fee	Rate	Add'l Fee
Total	68	Minus	67	1	x $ 80 =	$	1x $ 40 =	$40	x $20 =	$
Independent		Minus			x $420 =	$	x $210 =	$	x $105 =	$
First Presentation of Multiple Dep. Claim					+ $780 =	$	+ $390 =	$	+ $195 =	$
					Total	$	Total	$40	Total	$

Fee payment:

□ Please charge Deposit Account No. 23-1925 in the amount of $_____ for ____________________.

□ Payment by credit card in the amount of $_____ (Form PTO-2038 is attached).
WARNING: Information on this form may become public. **Credit card information should not be included on this form.**

☒ The Director is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925.

Respectfully submitted,

May 15, 2015
Date

/E. Brandon Nykiel/
E. Brandon Nykiel (Reg. No. 62,972)

PTO/SB/122 (09-04)
Approved for use through 07/31/2006. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

CHANGE OF CORRESPONDENCE ADDRESS
Application

Address to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	13/572,166
Filing Date	August 10, 2012
First Named Inventor	Christopher John Burke
Art Unit	2438
Examiner Name	Mohammad L. Rahman
Attorney Docket Number	12838/8

Please change the Correspondence Address for the above-identified patent application to:

☑ The address associated with Customer Number: **00757**

OR

□ Firm or Individual Name

Address

City | State | Zip

Country

Telephone | Fax

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

I am the:

□ Applicant/Inventor

□ Assignee of record of the entire interest.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

☑ Attorney or agent of record. Registration Number 34,880.

□ Registered practitioner named in the application transmittal letter in an application without an executed oath or declaration. See 37 CFR 1.33(a)(1). Registration Number____________________.

Signature			
Typed or Printed Name	Michael E. Milz		
Date	May 20, 2015	Telephone	312-321-4200

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	22397514
Application Number:	13572166
International Application Number:	
Confirmation Number:	9752
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Correspondence Address:	Michael E. Milz Brinks Hofer Gilson & Lione P.O. Box 10395 - Chicago IL 60610 US 3123214200 -
Filer:	Michael Edward Milz/Alice Thoennes
Filer Authorized By:	Michael Edward Milz
Attorney Docket Number:	12838/8
Receipt Date:	20-MAY-2015
Filing Date:	10-AUG-2012
Time Stamp:	14:57:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		12838-8-ChangeCorresp.pdf	124623 2fbaf4a750711cd7573ebb477ea44123c051a038	yes	2

Multipart Description/PDF files in .zip description

Document Description	Start	End
Transmittal Letter	1	1
Change of Address	2	2

Warnings:

Information:

Total Files Size (in bytes):	124623

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS pursuant to 37 CFR §1.8 on the below date:

Date: May 20, 2015 Name: Michael E. Milz, Reg. No. 34,880 Signature:

BRINKS
GILSON
& LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: Christopher John Burke
Appln. No.: 13/572,166
Filed: August 10, 2012
For: REMOTE ENTRY SYSTEM
Attorney Docket No.: 12838/8

Examiner: Rahman, Mohammad L.
Art Unit: 2438
Conf. No.: 9752

TRANSMITTAL

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Attached is/are:

☒ Change of Correspodence Address - Application.

Fee calculation:

☒ No additional fee is required.

□ Per 37 CFR §1.27, □ Applicant is small entity □ Applicant is micro entity.

□ An extension fee in an amount of $_____ for a _____-month extension of time under 37 CFR § 1.136(a).

□ A petition or processing fee in an amount of $_____ under 37 CFR § 1.17(_____).

□ An additional filing fee has been calculated as shown below:

					Fee		Small Entity Fee		Micro Entity Fee	
	Claims Remaining After Amendment		Highest No. Previously Paid	Present Extra	Rate	Add'l Fee	Rate	Add'l Fee	Rate	Add'l Fee
Total		Minus			x $ 80 =	$	x $ 40 =	$	x $20 =	$
Independent		Minus			x $420 =	$	x $210 =	$	x $105 =	$
First Presentation of Multiple Dep. Claim					+ $780 =	$	+ $390 =	$	+ $195 =	$
					Total	$	Total	$	Total	$

Fee payment:

□ Please charge Deposit Account No. 23-1925 in the amount of $_____ for _____.

□ Payment by credit card in the amount of $_____ (Form PTO-2038 is attached).
WARNING: Information on this form may become public. **Credit card information should not be included on this form.**

☒ The Director is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925.

Respectfully submitted,

May 20, 2015
Date

Michael E. Milz (Reg. No. 34,880)

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being filed electronically with the U.S. Patent and Trademark Office on

Date: July 27, 2015 Name: E. Brandon Nykiel (Reg. No. 62,972) Signature: /E. Brandon Nykiel/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: Christopher John Burke

Appln. No.: 13/572,166

Filed: August 10, 2012

For: REMOTE ENTRY SYSTEM

Attorney Docket No: 12838/8

Examiner: Rahman, Mohammad L.

Art Unit: 2438

Confirmation No. 9752

AMENDMENT AND RESPONSE TO NON-FINAL OFFICE ACTION MAILED APRIL 27, 2014

MAIL STOP - Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir or Madam:

In response to the non-final Office Action mailed April 27, 2015, please enter the following amendments and consider the following remarks.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 7 of this paper.

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of the Claims:

What is claimed is:

1-68. (Cancelled)

69. (New) A system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute; and

a receiver sub-system comprising:

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information, wherein the transmitter sub-system further comprises means for populating the data base of biometric signatures, the population means comprising:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for populating the data base according to the instruction.

70. (New) The system according to claim 69, further comprising:

means for providing a signal for directing input of the series of entries of the biometric signal;

means for incorporating into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database; and

means for constructing an audit trail of biometric signals provided to the biometric sensor for the purpose of accessing the controlled item.

71. (New) The system according to claim 69, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class, the accessibility attribute preferably comprising:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

72. (New) The system according to claim 69, wherein the controlled item is one of:

a locking mechanism of a door; and

an electronic lock on a Personal Computer (PC).

73. (New) The system according to claim 69, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration, and/or the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

74. (New) The system according to claim 69, wherein said conditional access comprises one of:

provision of access to the controlled item if the accessibility attribute comprises an access attribute:

provision of access to the controlled item and sounding of an alert if the accessibility attribute comprises a duress attribute; and

denial of access to the controlled item and sounding of an alert if the accessibility attribute comprises an alert attribute.

75. (New) The system as claimed in claim 69, wherein:

the biometric sensor is for authenticating the identity of a user;

the means for emitting comprises a transmitter for transmitting information capable of granting more than two types of access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and

the system further comprising a control panel for receiving the information and for providing the secure access requested.

76. (New) The system according to claim 75, wherein the control panel includes a converter for receiving the secure wireless signal and for outputting the information, and/or the biometric sensor authenticates the identity of the user by comparing a biometric input from the user with a biometric signature for the user in a biometric database, and/or the biometric sensor, the biometric database, and the transmitter are located in a remote fob.

77. (New) The system according to claim 76, wherein the secure wireless signal comprises an RF carrier and a rolling code, and the converter preferably converts the rolling code to the Wiegand protocol.

78. (New) A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and

means for emitting a secure access signal conveying said information dependent upon said accessibility attribute;

wherein the transmitter sub-system further comprises means for populating the database of biometric signatures, the populating means comprising:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for populating the database according to the instruction.

79. (New) A method for providing secure access to a controlled item in a system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal capable of granting more than two types of access to the controlled item, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon information in said secure access signal, the method comprising the steps of:

populating the database of biometric signatures by:

receiving a series of entries of the biometric signal;

determining at least one of the number of said entries and a duration of each said entry;

mapping said series into an instruction; and

populating the database according to the instruction;

receiving a biometric signal;

matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;

emitting a secure access signal conveying information dependent upon said accessibility attribute; and

providing conditional access to the controlled item dependent upon said information.

80. (New) The method according to claim 79, wherein the step of populating the database of biometric signatures further comprises the step of enrolling a biometric signature into the database of biometric signatures comprising the steps of:

receiving a biometric signal; and

enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty.

81. (New) The method according to claim 80, wherein the step of enrolling the biometric signature further comprises receiving another biometric signal to confirm the enrolling of the biometric signal as an administrator signature, and is preferably performed dependent upon generation of a feedback signal adapted to direct provision of at least one of the biometric signal and the other biometric signal.

82. (New) A non-transitory computer readable storage medium for storing a computer program comprising instructions, which when executed by processors causes the processors to perform the steps of the method of claim 79.

Remarks

I. Introduction

Claims 69-82 are pending. In this Amendment and Response, Claims 45-68 are cancelled. Claims 69-82 are added. No new matter is added. Applicant respectfully requests reconsideration in view of the amendments and the following remarks.

II. Claim Objections

Now cancelled dependent claims 47-56, 59-61, 64, and 66-68 were objected to for reciting "A method" or "A system." Cancellation of these claims obviates the objection. Additionally, Applicant notes that in the currently pending claims, "The" is used instead of "A" in order to avoid similar claim objections.

Now cancelled claims 46 and 57 were objected to for reciting "operable for;" on grounds that such use is an incomplete sentence. In addition to these claims being cancelled, these claim terms are not used in the currently pending claims, which obviates the objection.

III. Claim Rejections Under 35 U.S.C. § 112

In the Office Action, claims 45-46, 48, 53, 57, 58, 63, and 65 were rejected under 35 U.S.C. § 112, second paragraph on grounds that the term "operable for" is a statement of intended use and does not impose any positive limitation on the scope of the claims. In addition, claims 46, 57, 58, 63, and 65 were rejected under 35 U.S.C. § 112, second paragraph on grounds that the terms "appropriate number" and "appropriate duration" are relative terms that render the claims indefinite. The currently pending claims do not use these terms, which obviates the rejection.

IV. Claim Rejections Under 35 U.S.C. § 101

Claims 45-68 were rejected under 35 U.S.C. § 101 on grounds that they were directed to an abstract idea without significantly more. Applicants do not agree with the § 101 rejections as to claims 45-68, and their cancellation should in no way be construed as acquiescing to the rejections. In addition, Applicant provides the following reasons why currently pending claims 69-82 are directed to statutory subject matter and should not be rejected under § 101.

A. Federal Register Interim Guidance

The Federal Register Notice: 2014 Interim Guidance on Patent Subject Matter Eligibility states that "In accordance with the existing two-step analysis for patent subject matter eligibility under 35 U.S.C. 101 explained in MPEP 2106, the claimed invention:

- (Step 1) ''must be directed to one of the four statutory categories'' and
- (Step 2) 'must not be wholly directed to subject matter encompassing a judicially recognized exception"

The Interim Guidance states further that a claim to a process, machine, manufacture or composition of matter (Step 1: YES) that is not directed to any judicial exceptions (Step 2A: NO) is eligible and needs no further eligibility analysis.

Step 2A (Part 1 Mayo Test) involves determining whether the claim is directed to a law of nature, a natural phenomenon, or an abstract idea (judicial exceptions).

B. The Office Action

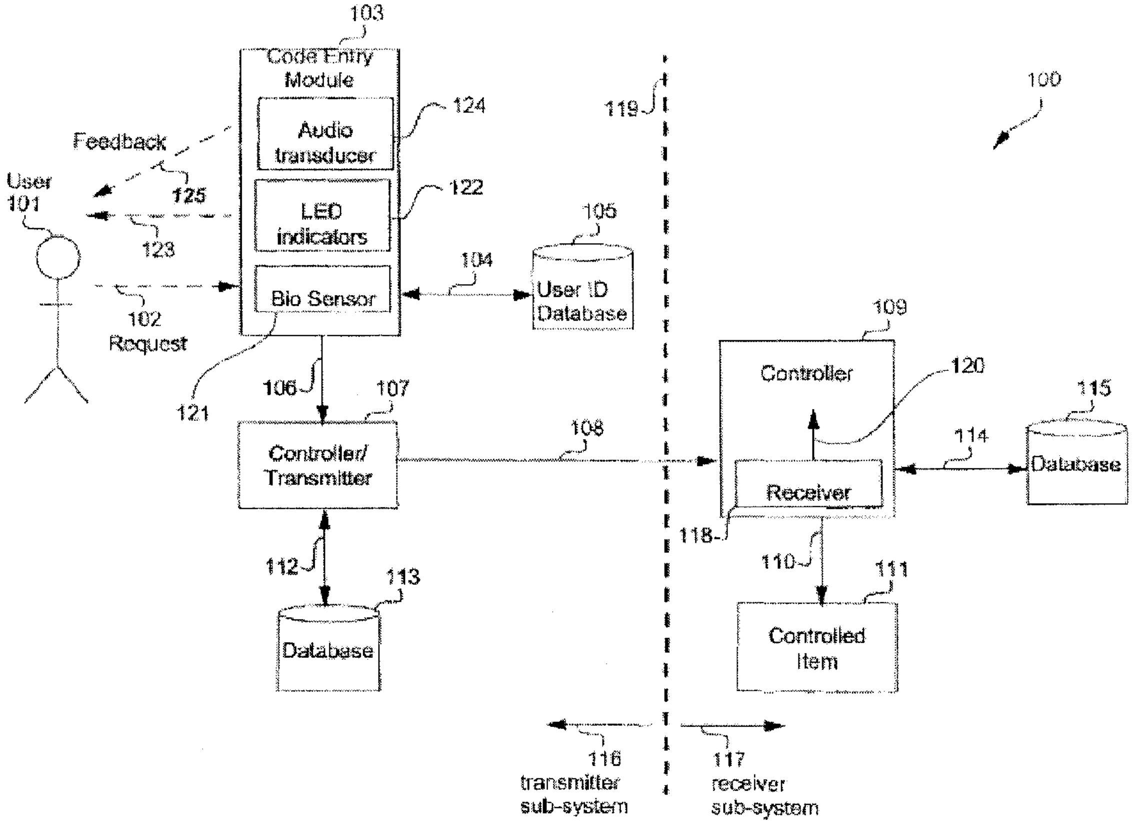
The Office Action states that the "Claims are directed towards performing a simple biometric authentication. The underlying invention is merely a simple biometric matching operation to access a controlled item".

The Office Action asserts that "The claim(s) does/do not include additional elements that are sufficient to amount to significantly more than the judicial exception because the additional element(s) or combination of elements in the claim(s) other than the abstract idea per se amount(s) to no more than recitation of generic computer structure" (this relates to Step 2 of the Interim Guidance process.

C. The Claimed Invention

New system claim 69 is directed to providing secure access to a controlled item by matching a received biometric signal against members of a database of biometric signatures, and providing conditional access to the controlled item dependent upon the success or otherwise of the matching operation. The controlled item 111 can be a door locking mechanism on a secure door, or an electronic key circuit in a personal computer (PC) that is to be accessed by the user 101 [0080].

New claim 69 is clearly directed to a machine (the statutory categories are process, machine, manufacture or composition of matter). The claimed invention is illustrated, in one example, in Fig. 2 of the present specification, reproduced below for convenience.



The operation of the claimed invention is provided at [0078] - [0080] which states (paraphrased) A user 101 makes a request 102 to a biometric sensor 121 in a code entry module 103 which interrogates a user identity database 105. If the identity of the user 101 is authenticated, then the code entry module 103 sends a signal 106 to a controller/transmitter 107 which checks a current rolling code in a database 113. If the incoming rolling code is legitimate, then the controller 109 sends a command 110 to a controlled item 111. The controlled item 111 can be a door locking mechanism on a secure door, or an electronic key circuit in a personal computer (PC) that is to be accessed by the user 101.

Clearly the invention operates to provide the access (e.g., by opening the door), and does not merely generate information.

The Interim Guidance states that a claim to a machine that is not directed to any judicial exceptions (Step 2A: NO) is eligible and needs no further eligibility analysis.

It is respectfully submitted that the Office Action erred in characterising the claims as being directed to a judicial exception, being an abstract idea.

The Abstract Idea Examples referred to in the Office Action describe the following patent-eligible examples:

i. Isolating and Removing Malicious Code from Electronic Messages;

ii. E-Commerce Outsourcing System/Generating a Composite Web Page;

iii. Digital Image Processing;

iv. Global Positioning System.

The following patent-ineligible examples are also described:

v. Digital Image Processing;

vi. The Game of Bingo;

vii. E-Commerce providing Transaction Performance Guaranty;

viii. Distribution of Products over the Internet.

It is apparent that <u>none</u> of the above examples involve an apparatus or a method in which an actual physical effect flows from practicing the invention, such as opening a door, or enabling physical access to a PC.

It is submitted that new claim 69 is not directed towards performing a simple biometric authentication, but rather is directed towards using biometric authentication to either produce or prevent physical access to a controlled item.

Accordingly, the claim to the machine is not directed to any judicial exceptions, is therefore eligible and needs no further eligibility analysis.

Accordingly, for at least the reasons noted above, it is submitted that new claim 69 is eligible under 35 USC 101, and the rejection should be set aside.

The other claims recite, either explicitly or by dependence, the same or equivalent features to those referred to in regard to new claim 69. Accordingly, for at least the reasons noted above, it is submitted that new claims 69-82 are eligible under 35 USC 101, and the rejection should be set aside.

V. Claim Rejections Under 35 U.S.C. § 102

The Office Action at page 5 rejects now cancelled claim 45 (directed to a transmitter sub-system) under pre-AIA 35 U.S.C. 102(e/a) as being anticipated by Hoffman et al (US 7,152,045).

New claim 78 is directed to a transmitter sub-system and recites, among other features:

i. wherein the transmitter sub-system further comprises means for populating the database of biometric signatures, the populating means comprising:

ii. means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

iii. means for mapping said series into an instruction; and

iv. means for populating the database according to the instruction.

Hoffman does not disclose or suggest any of the above-noted features.

For at least this reason, new claim 78 is novel over Hoffman.

VI. Claim Rejections Under 35 U.S.C. § 103

The Office Action at page 7 rejects now cancelled claims 46-58, 60-63, and 67-68 under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hoffman in view of lgaki et al. (US 5,109,428) hereinafter "lgaki" and in further view of Pu et al. (US 6,229,906) hereinafter "Pu".

Now cancelled claim 46 is directed to a system for providing secure access to a controlled item, as is new claim 69.

New claim 69 recites, among other features, the following:

i. wherein the transmitter sub-system further comprises means for populating the database of biometric signatures, the populating means comprising:

ii. means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

iii. means for mapping said series into an instruction; and

iv. means for populating the database according to the instruction.

The Office Action states the following:

v. Hoffman-lgaki combination is silent on but the analogous art Pu teaches said succession being characterized according to at least one of the number of said entries and a duration of each said entry;

vi. the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration.

The Office Action then asserts that one of ordinary skilled artisan would have been motivated to modify the combined system of Hoffman & lgaki with the idea of succession being characterized according to at least one of the number of said entries and a duration of each said entry, the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration as taught by Pu because the use of Pu could provide the Biometric Input Device of Hoffman the ability to include at least one of the number of said entries and a duration of each said entry, the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration to implement high security of the system by using secret sequence codes formed by body parts.

In order to address this rejection, the operation of claim 69 is firstly described as follows: the claimed system populates the signature database using series of entries from a user such as the administrator. In particular (see [0109] – [0111]) [0109] an administrator can provide control information to the code entry module by providing a succession of finger presses to the biometric sensor 121, providing that these successive presses are of the appropriate duration, the appropriate quantity, and are input within a predetermined time. In one arrangement, the control information is encoded by either or both (a) the number of finger presses and (b) the relative duration of the finger presses. If the successive finger presses are provided within this predetermined time, then the controller 107 accepts the presses as potential control information and checks the input information against a stored set of legal control signals. One example of a legal control signal can be expressed as follows: "Enrol an ordinary user"->dit, dit, dit, dah

Accordingly, (a) the series of entries of the biometric signal is generated by the administrator, and (b) the information contained by the series of entries defines, in the above example, enrolment of an ordinary user.

In contrast, Igaki receives only a single fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate (Abstract). Igaki then processes the single biometric signal to form a sequence of image data. The object of Igaki (col. 1, lines 41-52) is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad (emphasis added) on a sensor. The alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary, and the troublesome process of the repeated fingerpad pressing down operations is eliminated.

In Igaki the sequence of image data is generated as follows (col. 6, lines 1-17) A fingerpad of the person to be registered is pressed on the plate of the fingerprint sensor. The pressure of the fingerpad is increased from an initial low value gradually to higher values to reach a predetermined constant high value. During this increase of the pressure, the fingerprint image is optically picked up every 1/30 second. The optically picked up fingerprint image is analog-to-digitally converted into digital data. The converted digital data is supplied to the binarization circuit where the binarization of the converted digital data is carried out. The binarized data is stored into the first frame memory.

Igaki thus receives only a single finger press from a user, and generates a sequence of image data from that single finger press. Igaki intends, by this process, "to ensure the correctness of the registered fingerprint data in which minutiae (characteristic points) having a high frequency of appearance are adopted as the registered data" while avoiding the problems of the prior art being " … it is troublesome for the person whose fingerprint is being picked up to carry out such a plurality of picking-up operations, and further, it is necessary to carry out an alignment between minutiae because the location of the second operation of pressing down of the fingerprint after the lifting of the fingerprint after the first operation of pressing down of the fingerprint does not usually coincide with the location of the fingerprint in the first pressing down operation." (col. 1, lines 14-17, 30-39).

Combining Hoffman and Igaki would appear to improve the accuracy of Hoffman when receiving a biometric signal (col. 13, lines 2-8).

However, the proposal to combine Pu with Hoffman – Igaki is problematic for the following reasons.

The Office Action makes reference to the following passages from Pu:

vii. characterized according to at least one of the number of said entries (Pu, col. 2, lines 18-22; 5, lines 25-46)

viii. a duration of each said entry (Pu, col. 5, lines 50-55);

ix. the number of said entries is the appropriate number of entries, and the duration of each said entry is of the appropriate duration (Pu, col. 2, lines 40-43; col. 4, lines 30-33, 40-67; col. 5, lines 50-55).

Pu is concerned with an identification system using biometric information of human body parts and a secret sequence code. In particular, biometric information of human body parts is used to form the secret sequence code. Specifically, a combination entry device recognizes user's fingerprints which are entered as a sequence. While the sensor can be fooled for any one fingerprint, the use of a plurality of different fingerprints improves the identification capability. In particular, the combination of fingerprints in the proper order is necessary to undo the lock. (Abstract)

It is submitted that there is no logical manner in which Pu can be combined with Hoffman – Igaki without the impermissible use of hindsight, and even then the combination will not operate in the same manner as the claimed invention.

Firstly, as noted above Hoffman – Igaki specifically uses a single finger-press in order to overcome the limitations of the prior art requirements for multiple finger presses in order to ensure the correctness of the registered fingerprint data in which minutiae having a high frequency of appearance are adopted as the registered data. Pu on the other hand uses a plurality of different fingerprints in order to generate a code, which teaches away from the single finger-press basis of Hoffman – Igaki.

Secondly, as noted the use of a plurality of different fingerprints in Pu improves the identification capability. In particular, the combination of fingerprints in the proper order is necessary to undo the lock. (Abstract) Accordingly, Pu is concerned with accuracy of identification capability, not with enrolment of users.

Finally, the Office Action itself states, at page 11, 1st paragraph, that the motivation for combining Pu with Hoffman – Igaki is *to implement high security of the system* by using secret sequence codes formed by body parts. This would clearly not disclose or suggest *wherein the transmitter sub-system further comprises means for populating the database of biometric signatures, the populating means comprising: means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of* *the number of said entries and a duration of each said entry; means for mapping said series into an instruction; and means for populating the database according to the instruction.*

For at least the reasons noted above, it is submitted that new claim 69 is patentable over Hoffman, Igaki and Pu whether these documents are considered alone or in combination.

The other claims recite, either explicitly or by dependence, the same or equivalent features to those referred to in regard to new claim 69. Accordingly, for at least the reasons noted above, it is submitted that new claims 69-82 are patentable over Hoffman, Igaki and Pu whether these documents are considered alone or in combination.

The Office Action at page 22 rejects pending claim 66 under pre-AIA 35 U.S.C. 103(a) as being unpatentable over lgaki in view of Pu and further in further view of Koo et al (WO 2002/12660).

The Office Action concedes that lgaki is silent on but the analogous art Koo teaches enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty.

However, the Applicant is of the opinion that Koo does not remedy the deficiency of Igaki and Pu as noted above, and that combining Igaki, Pu, and Koo would not disclose or suggest *wherein the transmitter sub-system further comprises means for populating the database of biometric signatures, the populating means comprising: means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry; means for mapping said series into an instruction; and means for populating the database according to the instruction.*

For at least the reasons noted above, it is submitted that the new claims 69-82 are patentable over Igaki, Pu, and Koo whether these documents are considered alone or in combination.

VII. Conclusion

With this amendment and response, the present pending claims of this application are allowable, and Applicants respectfully request the Examiner to issue a Notice of Allowance for this application. Should the Examiner deem a telephone conference to be beneficial in expediting allowance/examination of this application, the Examiner is invited to call the undersigned attorney at the telephone number listed below.

Respectfully submitted,

/E. Brandon Nykiel/

E. Brandon Nykiel/
Attorney Reg. No. 62,972
Attorney for Applicant

Date: July 27, 2015

BRINKS GILSON & LIONE
P.O. Box 10395
Chicago, Illinois 60610
(312) 321-4200

Electronic Acknowledgement Receipt

EFS ID:	23031858
Application Number:	13572166
International Application Number:	
Confirmation Number:	9752
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Customer Number:	757
Filer:	E. Brandon Nykiel/Maggie Krause
Filer Authorized By:	E. Brandon Nykiel
Attorney Docket Number:	12838/8
Receipt Date:	27-JUL-2015
Filing Date:	10-AUG-2012
Time Stamp:	15:58:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		12838_8_ResponseFiling_072715.pdf	897989 9c935201c890eeea5698c609ad506e45888cf850	yes	18

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Miscellaneous Incoming Letter	1	1
	Amendment/Req. Reconsideration-After Non-Final Reject	2	2
	Claims	3	7
	Applicant Arguments/Remarks Made in an Amendment	8	18

Warnings:

Information:

Total Files Size (in bytes):	897989

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS pursuant to 37 CFR §1.8 on the below date:

Date: July 27, 2015 Name: E. Brandon Nykiel Signature: /E. Brandon Nykiel/

BRINKS
GILSON
& LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: Christopher John Burke
Appln. No.: 13/572,166
Filed: August 10, 2012
For: REMOTE ENTRY SYSTEM
Attorney Docket No.: 12838/8

Examiner: Rahman, Mohammad L.
Art Unit: 2438
Conf. No.: 9752

TRANSMITTAL

Mail Stop Amendment
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Attached is/are:

☒ Amendment and Response to Non-Final Office Action Mailed April 27, 2015.

Fee calculation:

☒ No additional fee is required.

☒ Per 37 CFR §1.27, ☒ Applicant is small entity ☐ Applicant is micro entity.

☐ An extension fee in an amount of $_____ for a _____-month extension of time under 37 CFR § 1.136(a).

☐ A petition or processing fee in an amount of $_____ under 37 CFR § 1.20(_____).

☐ An additional filing fee has been calculated as shown below:

					Fee		Small Entity Fee		Micro Entity Fee	
	Claims Remaining After Amendment		Highest No. Previously Paid	Present Extra	Rate	Add'l Fee	Rate	Add'l Fee	Rate	Add'l Fee
Total	68	Minus	67	1	x $ 80 =	$	1x $ 40 =	$40	x $20 =	$
Independent		Minus			x $420 =	$	x $210 =	$	x $105 =	$
First Presentation of Multiple Dep. Claim					+ $780 =	$	+ $390 =	$	+ $195 =	$
					Total	$	Total	$40	Total	$

Fee payment:

☐ Please charge Deposit Account No. 23-1925 in the amount of $_____ for ___________________.

☐ Payment by credit card in the amount of $_____ (Form PTO-2038 is attached).
WARNING: Information on this form may become public. **Credit card information should not be included on this form.**

☒ The Director is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925.

Respectfully submitted,

July 27, 2015
Date

/E. Brandon Nykiel/
E. Brandon Nykiel (Reg. No. 62,972)

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/572,166	Filing Date 08/10/2012	□ To be Mailed

ENTITY: □ LARGE ☒ SMALL □ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
□ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
□APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
□ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter “0” in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT	**07/27/2015**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 14	Minus	** 44	= 0	x $40 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***10	= 0	x $210 =	0
	□ Application Size Fee (37 CFR 1.16(s))						
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD’L FEE	**0**

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))						
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD’L FEE	

* If the entry in column 1 is less than the entry in column 2, write “0” in column 3.

** If the “Highest Number Previously Paid For” IN THIS SPACE is less than 20, enter “20”.

*** If the “Highest Number Previously Paid For” IN THIS SPACE is less than 3, enter “3”.

The “Highest Number Previously Paid For” (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/LASHAWN MORGAN/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

757 7590 10/16/2015

BGL
P.O. BOX 10395
CHICAGO, IL 60610

EXAMINER	
RAHMAN, MOHAMMAD L	
ART UNIT	**PAPER NUMBER**
2438	

DATE MAILED: 10/16/2015

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/572,166	08/10/2012	Christopher John Burke	12838/8	9752

TITLE OF INVENTION: REMOTE ENTRY SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	01/19/2016

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

757 7590 10/16/2015
BGL
P.O. BOX 10395
CHICAGO, IL 60610

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/572,166	08/10/2012	Christopher John Burke	12838/8	9752

TITLE OF INVENTION: REMOTE ENTRY SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	01/19/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
RAHMAN, MOHAMMAD L	2438	726-007000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 ____________________

2 ____________________

3 ____________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual □ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:

□ Issue Fee

□ Publication Fee (No small entity discount permitted)

□ Advance Order - # of Copies ____________________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.

□ Payment by credit card. Form PTO-2038 is attached.

□ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number ____________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

□ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

□ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature ______________________ Date ______________________

Typed or printed name ______________________ Registration No. ______________________

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/572,166	08/10/2012	Christopher John Burke	12838/8	9752

757 7590 10/16/2015

BGL
P.O. BOX 10395
CHICAGO, IL 60610

EXAMINER	
RAHMAN, MOHAMMAD L	
ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 10/16/2015

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	**Application No.** 13/572,166	**Applicant(s)** BURKE, CHRISTOPHER JOHN	
	Examiner MOHAMMAD L. RAHMAN	**Art Unit** 2438	**AIA (First Inventor to File) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *See Continuation Sheet*.

   □ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on______.

2. □ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are *69-71 and 73-82*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☒ All b) □ Some *c) □ None of the:

   1. ☒ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. ______ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 5/15/2015
3. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *9/30/2015* .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. □ Other _____.

/MOHAMMAD L RAHMAN/
Primary Examiner, Art Unit 2438

Continuation of Item 1. This communication is responsive to : examiner initiated interview on 9/30/2015 and communication filed 7/27/2015.

DETAILED ACTION

1. The present application is being examined under the pre-AIA first to invent provisions.

2. This notice of allowance is in response to examiner initiated interview on 9/30/2015 and applicant's arguments/amendments filed 07/27/2015.

3. The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior office action. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

4. Claims 69, 78, and 79 have been amended.

Claims 1-68 and 72 have been canceled.

Claims 69-71 and 73-82 are now renumbered as claims 1-13 are pending.

EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

6. Authorization for this examiner's amendment was given in a telephone interview with applicants' representative *Nykiel Brandon, Registration No. 62,972* on September 30, 2015 and via email on September 30, 2015.

Please Enter the following claim amendments:

Please replace claim 69 with the following:

69. (Currently amended) A system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute; and

a receiver sub-system comprising:

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information,

wherein the transmitter sub-system further comprises means for populating the data base of biometric signatures, the population means comprising:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for populating the data base according to the instruction**,**

wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

Please replace claim 78 with the following:

78. (Currently amended) A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and

means for emitting a secure access signal conveying said information dependent upon said accessibility attribute;

wherein the transmitter sub-system further comprises means for populating the database of biometric signatures, the populating means comprising:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for populating the database according to the instruction,

wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

Please replace claim 79 with the following:

79. (Currently amended) A method for providing secure access to a controlled item in a system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal capable of granting more than two types of access to the controlled item, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon information in said secure access signal, the method comprising the steps of:

populating the database of biometric signatures by:

receiving a series of entries of the biometric signal;

determining at least one of the number of said entries and a duration of each said entry;

mapping said series into an instruction; and

populating the database according to the instruction;

receiving a biometric signal;

matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;

emitting a secure access signal conveying information dependent upon said accessibility attribute; and

providing conditional access to the controlled item dependent upon said information,

wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

RESPONSE TO ARGUMENTS

7. The terminal disclaimer filed on 03/10/2015 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of any patent granted on US patent # 8,266,442 has/have been reviewed and accepted. The terminal disclaimer has been recorded.

8. In view of examiner's amendments to independent claims 69, 78 and 79 and applicants' persuasive arguments (see pp. 7-11 in remarks) filed 07/27/2015, claims 69-71, and 73-82 are statutory under 35 USC § 101.

9. 35 USC § 112 ¶6th Interpretation:

Claim 69

In claim 69, each of the "means for" features are recited as being included with a "transmitter sub-system or a "receiver sub-system." The Specification shows and describes each of the transmitter sub-system and the receiver sub-system as including sufficient structure. For example, Fig. 2 shows a transmitter sub-system 116 as including a controller/transmitter 107, an audio transducer 124, LED indicators 122, a biometric sensor 121, a user ID database 105, and a database 113, all of which are structural elements. Fig. 10 further shows that the controller/transmitter 107 includes a processor 1005, memory 1004, an audio-video interface 1007, a communication interface 1008, an interconnected bus 1004, and an input/output (I/O) interface, which are structural elements. Fig. 2 and 10 also show the receiver sub-system as including a controller 109, a database 115, and a receiver 118, which are structural elements.

In addition to the structural elements shown in Figs. 2 and 10, methods of operation (i.e., acts) associated with the transmitter sub-system 116 and the receiver sub-system 117 are described with reference to flow charts in Figs. 3, 4, and 6-9. The Specification ties the acts described with reference to these figures to the structural elements disclosed in Figs. 2 and 10. For example, in paragraph [0134], the Specification states:

> FIG. 10 is a schematic block diagram of the system in FIG. 2. The disclosed secure access methods are preferably practiced using a computer system arrangement 100', such as that shown in FIG. 10 wherein the processes of FIGS. 3-4, and 6-9 may be implemented as software, such as application program modules executing within the computer system 100'. In particular, the method steps for providing secure access are effected by instructions in the software that are carried out under direction of the respective processor modules 107 and 109 in the transmitter and receiver sub-systems 116 and 117. The instructions may be formed as one or more code modules, each for performing one or more particular tasks. The software may also be divided into two separate parts, in which a first part performs the provision of secure access methods and a second part manages a user interface between the first part and the user. The software may be stored in a computer readable medium, including the storage devices described

> below, for example. The software is loaded into the transmitter and receiver sub-systems 116 and 117 from the computer readable medium, and then executed under direction of the respective processor modules 1 07 and 109. A computer readable medium having such software or computer program recorded on it is a computer program product. The use of the computer program product in the computer preferably effects an advantageous apparatus for provision of secure access.

Further support in the Specification, referencing Fig. 2 and/or the methods of Figs. 3-4, 6-9, is provided for each of the means for limitations in claim 69 as follows:

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute

> Block 202 in Fig. 3 and [0092]: The received biometric signal 102 is compared with information in the biometric signature database 105.

means for emitting a secure access signal conveying information dependent upon said accessibility attribute

> Block 205 in Fig. 3 and [0093]: The controller 107 sends the appropriate access signal 108 to the controller 109.

means for receiving the transmitted secure access signal

> [0096]: Fig. 4 shows the method of operation of the control sub-system 117 of FIG. 2. The method 300 commences with a testing step 301 which continuously checks whether the access signal 108 has been received from 107. The step 301 is performed by the controller 109. When the access signal 108 is received, the process 300 is directed from the step 301 by means of a YES arrow to a step 302.

means for providing conditional access to the controlled item dependent upon said information

> [0096]: In the step 302, the controller 109 compares the rolling code received by means of the access signal 108 with a reference code in the database 115. A subsequent testing step 303 is performed by the controller 109. In the step 303 if the code received on the access signal 108 is successfully matched against the reference code in the database 115 then the process 300 is directed in accordance with a YES arrow to a step 304. [0097] In the step 304 the controller 109 sends the control signal 110 to the controlled item 111 (for example opening the secured door).

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry

> [0109]: The first administrator can provide control information to the code entry module by providing a succession of finger presses to the biometric sensor 121; [0104]: FIG. 6 shows a process 700 that determines if a biometric signal has been received by the biometric sensor 121 in the code entry module in FIG. 2; [0105]: If the database 105 is empty, then the process 700 is directed to 706 in FIG. 8, which depicts a process 800 dealing with the enrolment or the administration function for loading relevant signatures into the database 105.

means for mapping said series into an instruction

> [0109]: The first administrator can provide control information to the code entry module by providing a succession of finger presses to the biometric sensor 121, providing that these successive presses are of the appropriate duration, the appropriate quantity, and are input within

a predetermined time. In one arrangement, the control information is encoded by either or both (a) the number of finger presses and (b) the relative duration of the finger presses. If the successive finger presses are provided within this predetermined time, then the controller 107 accepts the presses as potential control information and checks the input information against a stored set of legal control signals;

means for populating the data base according to the instruction

[0110]: One example of a legal control signal can be expressed as follows: [0111] "Enrol an ordinary user"->dit, dit, dit, dah

Claim 70

In claim 70, support for the "means for" language for purposes of § 112, second paragraph even if § 112, paragraph 6 is invoked is as follows:

means for providing a signal for directing input of the series of entries of the biometric signal

This feature is about assisting the user to input a series of entries of the biometric signal. For example, see [0081] The code entry module 103 also incorporates at least one mechanism for providing feedback to the user 101. This mechanism can, for example, take the form or one or more Light Emitting Diodes (LEDs) 122 Which can provide visual feedback, depicted by an arrow 123 to the user 101. Alternately or in addition the mechanism can take the form of an audio signal provided by an audio transducer 124 providing audio feedback 125. ***Also***, [0110] One example of a legal control signal can be expressed as follows: [0111] "Enrol an ordinary user"->dit, dit, dit, dah Where "dit" is a finger press of one second's duration (provided by the user 101 in response to the feedback provided by the Amber LED as described below), and "dah" is a finger press of two second's duration;

means for incorporating into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database;

This feature is optionally used when, for example, a user provides a biometric signal to the step 201 in Fig. 3, and their biometric signal is matched against signatures in the database in the steps 202 and 203 in Fig. 3. [0079] states that if the identity of the user 101 is authenticated successfully, then the code entry module 103 sends a signal 106 to a controller/transmitter 107 which sends an access signal, as depicted by an arrow 108 to a controller 109. If the incoming rolling code forming the access signal 108 is found to be legitimate, then the controller 109 sends a command, as depicted by an arrow 110, to a controlled item 111. The controlled item 111 can be a door locking mechanism on a secure door, or an electronic key circuit in a personal computer (PC) that is to be accessed by the user 101. The fact that the user presently providing the biometric signal provides a legitimate signal is sufficient to open the controlled door, or access the controlled PC without that user having to identify themselves further. Eg if "John" provides a biometric signal which matches a signature in the database, then John is able to access the controlled item without his name "John" being inserted into the access signal 108. If however it is desired to construct an audit trail, then as well as providing John with access to the controlled item, it is also necessary to record the fact that it is John who is doing the accessing. This is the object of the "incorporation of the identification field into the secure access signal", and this is clearly only done if the user is a legitimate user and has a matching biometric signal in the database.

means for constructing an audit trail of biometric signals provided to the biometric sensor for the purpose of accessing the controlled item

> see [0121]: An optional additional step (not shown) can prepare an identification field for insertion into the access signal 108. This sends, to the receiver sub-system 117, ID information that the receiver sub-system can use to construct an audit trail listing Which users, having signatures in the database 105, have been provided with access to the controlled item 111

Claim 78

The "means for" language recited in this claim is supported by the Specification for purposes of § 112, paragraph 2 even if § 112, paragraph 6 is invoked at least for the reasons set forth above for claim 69.

10. In view of examiner's amendments to independent claims 69, 78 and 79 and applicants' persuasive arguments (see pp. 11-16 in remarks) filed 07/27/2015, claims 69-71, and 73-82 are in condition for allowance over prior arts of record.

ALLOWABLE SUBJECT MATTER

11. **Claims 69-71 and 73-82** are allowed over prior art of record.

EXAMINER'S STATEMENT OF REASONS FOR ALLOWANCE

12. Regarding the claimed terms, the Examiner notes that a "general term must be understood in the context in which the inventor presents it." In re Glaug 283 F.3d 1335, 1340, 62 USPQ2d 1151, 1154 (Fed. Cir. 2002). Therefore the Examiner must interpret the claimed terms as found on the specification of the instant application. Clearly almost all the general terms in the claims may have multiple meanings. So where a claim term "is susceptible to various meanings,...the inventor's lexicography must prevail.... " Id. Using these definitions for the claims, the claimed invention was not reasonably found in the prior art.

13. This communication warrants No Examiner's Reason for Allowance, Applicant's reply make evident the reasons for allowance, satisfying the "record as a whole" proviso of the rule 37 CFR 1.104(e). Specifically, amended independent claims 69, 78, and 79 in view of examiner's amendment and the substance of applicant's persuasive arguments, see pp. 11-16 in remarks filed 07/27/2015 from the record and no statement is deemed necessary (see MPEP 1302.14).

None of the prior art of record taken by itself or in any combination, would have anticipated or made obvious the claimed invention of the present application at or before the time it was filed.

Examiner performed updated search and additional search does not yield other specific references that reasonably, either singularly or in combination with cited references, would result a proper rejection that would have anticipated or made obvious all the steps disclosed in the independent claims 69, 78, and 79 with proper motivation at or before the time it was effectively filed.

14. Any comments considered necessary by applicant must be submitted no later than payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance."

CONCLUSION

15. Prior arts made of record, not relied upon:

US 5,933,515 (Pu et al.), US 2004/0042642 (Bolle et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MOHAMMAD L. RAHMAN whose telephone number is (571)270-7471. The examiner can normally be reached on Monday to Friday: 9:00 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, TAGHI T. ARANI can be reached on 5712723787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MOHAMMAD L RAHMAN/
Primary Examiner, Art Unit 2438

Examiner-Initiated Interview Summary	**Application No.** 13/572,166	**Applicant(s)** BURKE, CHRISTOPHER JOHN	
	Examiner MOHAMMAD L. RAHMAN	**Art Unit** 2438	

All participants (applicant, applicant's representative, PTO personnel):

(1) *MOHAMMAD L. RAHMAN*. (3)_____.

(2) *BRANDON NYKIEL*. (4)_____.

Date of Interview: *30 September 2015*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *69,78 and 79*.

Identification of prior art discussed: *None*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

To expedite prosecution, the Examiner telephoned and spoke with Attorney of Record Mr. Brandon Nykiel who authorized the Examiner to amend Claims 69, 78, and 79 and to cancel Claims 72 to place the claimed invention in condition for allowance.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/MOHAMMAD L RAHMAN/
Primary Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 13/572,166	Applicant(s)/Patent Under Reexamination BURKE, CHRISTOPHER JOHN	
	Examiner MOHAMMAD L. RAHMAN	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5,933,515 A	08-1999	Pu; Allen	G06K9/00006	340/5.53
*	B	US-2004/0042642 A1	03-2004	Bolle, Rudolf Maarten	G07C9/00134	382/115
	C	US-				
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	56	(duration (time near5 (period length span))) and ((series sequence$1) near5 (biometric fingerprint (retina near2 scan)) near5 entr$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/10/01 13:36
L3	23	L2 AND (G07C9/00158 or G06F21/35 or H04W12/08 or H04L63/0861 or G06F21/32 or H04W84/18 or H04W84/12).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/10/01 13:36
L4	12	L2 and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/10/01 13:37
L5	108	((series sequence$1) near5 (biometric fingerprint (retina near2 scan)) near5 entr$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/10/01 14:41
L6	23	L3 AND (G07C9/00158 or G06F21/35 or H04W12/08 or H04L63/0861 or G06F21/32 or H04W84/18 or H04W84/12).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/10/01 14:42
L7	20	L5 and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/10/01 14:43
L8	46	L5 AND (G07C9/00158 or G06F21/35 or H04W12/08 or H04L63/0861 or G06F21/32 or H04W84/18 or H04W84/12).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/10/01 14:43
S1	656	(biometric fingerprint) with (key near fob)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:45
S2	275	(biometric fingerprint) with (key near fob) and (audit$ examin$3	US-PGPUB; USPAT;	OR	ON	2014/03/18 12:47

		investigat$3)	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S3	49	(biometric fingerprint) with (key near fob) and (audit$ examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20040813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:48
S4	43	(biometric fingerprint) with (key near fob) and (audit$ examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:51
S5	0	(biometric fingerprint) with (remote near key near fob) and (audit$ examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:52
S6	0	(biometric fingerprint) with (remote near2 key near fob) and (audit$ examin$3 investigat$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/18 12:53
S7	2	("8266442").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:36
S8	2	"20120278863"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:42
S9	2	"20120311346"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:43
S10	2	"20120311343"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 12:43
S11	29	((Christopher) near2 (Burke)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/19 15:33
S12	16349	(713/182-186,168).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	OFF	2014/03/19 15:34

			IBM_TDB			

S13	23869	(726/2,7,26-30).CCLS.	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2014/03/19
						15:34

S14	33433	(709/224-225).CCLS.	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2014/03/19
						15:35

S15	738	biometric with identif$7 same (access near2 (right privilege control)) and (((unconditional unlimited) near2 access) duress alert telemetry)	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/03/19
						15:35

S16	33	(enroll$3 register$3) with (((biometric adj image) biometric (fingrprint adj image) fingerprint) near (sequence array))	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/03/19
						15:35

S17	4829	assign$3 with (access near (right privilege))	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/03/19
						15:35

S18	1377	(access near (right privilege)) same ((biometric adj image) biometric (fingrprint adj image) fingerprint)	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/03/19
						15:36

S19	174	S17 and S18	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/03/19
						15:36

S20	26	S12 and S19	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/03/19
						15:36

S21	24	S13 and S19	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2014/03/19
						15:37

S22	4	S14 and S19	US-PGPUB;
			USPAT;
			USOCR; FPRS;
			EPO; JPO;
			DERWENT;
				OR	ON	2014/03/19
						15:37

			IBM_TDB			
S23	23	S15 and S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S24	65	S12 and S15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S25	41	S13 and S15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S26	11	S14 and S15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S27	27	S15 and S17	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S28	165	S15 and S18	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:37
S29	1377	(access near (right privilege)) same ((biometric adj image) biometric (fingrprint adj image) fingerprint)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:38
S30	131	(assign$3 provid$3) with (access adj (right privilege)) same (biometric fingerprint)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/03/19 15:38
S31	94	(biometric fingerprint) with ((multiple plural consecutive sequential successive) near2 entr$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/11/06 13:34
S32	33	(biometric fingerprint) with ((multiple plural consecutive sequential successive) near2 entr$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2014/11/06 13:34

			IBM_TDB			
S33	18809	(713/182-186,168).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/11/06 13:35
S34	2	S33 and S32	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/11/06 13:35
S35	29312	(726/2,7,26-30).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/11/06 13:35
S36	0	S35 and S32	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/11/06 13:35
S37	39035	(709/224-225).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/11/06 13:35
S38	0	S37 and S32	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/11/06 13:35
S39	36	((Christopher) near2 (Burke)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2014/11/06 13:35
S40	0	S39 and S31	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/11/06 13:35
S41	10	(biometric fingerprint) with ((consecutive sequential successive) near2 entr$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/11/06 13:36
S42	17	(calculat$3 detect$3 identify$3) with (number near5 (biometric near2 entr$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/20 21:40
S43	0	(calculat$3 detect$3 identify$3) with (duration near5 (biometric near2	US-PGPUB; USPAT;	OR	ON	2015/04/20 21:40

		entr$3))	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S44	1	(calculat$3 detect$3 identify$3) with ((duration period time) near5 (biometric near2 entr$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/20 21:40
S45	1	(calculat$3 detect$3 identify$3) with ((duration period time length span) near5 (biometric near2 entr$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/20 21:41
S46	14	((duration period time length span) near5 (biometric near2 entr$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/21 10:42
S47	0	(duration (time near2 (period length span))) with ((each multiple plural) near5 (biometric near2 entr$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/21 10:47
S48	0	(duration (time near5 (period length span))) with ((each multiple plural) near5 (biometric near2 entr$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/21 10:47
S49	23	(duration (time near5 (period length span))) with (biometric near2 entr$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/21 10:47
S50	8	(biometric fingerprint) SAME ((consecutive sequential successive) near2 entr$3) SAME ((number count$3) near5 entr$3) AND (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/21 11:15
S51	13	(biometric fingerprint) SAME ((consecutive sequential successive) near2 entr$3) AND ((number count$3) near5 entr$3) AND (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/21 11:16
S52	55	(duration (time near5 (period length span))) with ((biometric fingerprint (retina near2 scan)) near5 entr$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/21 11:25
S53	19	(duration (time near5 (period length span))) with ((biometric fingerprint	US-PGPUB; USPAT;	OR	ON	2015/04/21 11:25

		(retina near2 scan)) near5 entr$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S54	161	"5109428"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/21 12:15
S55	4	"5109428".PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/21 12:15
S56	3	(biometric fingerprint) same ((consecutive successive) near2 entr$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/21 12:20
S57	43	(biometric fingerprint) same ((consecutive successive multiple) near2 entr$3) and (@ad OR @pd OR @rlad OR @ptad) < "20030813"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/21 12:22
S58	2	"6195447 ".PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/21 13:12
S59	2	"6229906".PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/21 13:41
S60	93012	(G07C9/00158 or G06F21/35 or H04W12/08 or H04L63/0861 or G06F21/32 or H04W84/18 or H04W84/12).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/22 21:24
S61	55	(duration (time near5 (period length span))) with ((biometric fingerprint (retina near2 scan)) near5 entr$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/22 21:25
S62	17	S60 and S61	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/04/22 21:25
S63	56	(duration (time near5 (period length span))) and ((series sequence$1)	US-PGPUB; USPAT;	OR	ON	2015/09/09 11:55

		near5 (biometric fingerprint (retina near2 scan)) near5 entr$3)	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S64	56	(duration (time near5 (period length span))) and ((series sequence$1) near5 (biometric fingerprint (retina near2 scan)) near5 entr$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/09/09 13:14

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	4	((duration (time near5 (period length span))) and ((series sequence$1) near5 (biometric fingerprint (retina near2 scan)) near5 entr$3) and (map$4 match$3) and database).CLM.	US-PGPUB; USPAT; UPAD	OR	ON	2015/10/01 13:28

10/1/2015 2:43:47 PM
C:\Users\mrahman3\Documents\EAST\Workspaces\13572166_First.wsp

Proposed Examiner's Amendment

69. (Currently amended) A system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute; and

a receiver sub-system comprising:

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information,

wherein the transmitter sub-system further comprises means for populating the data base of biometric signatures, the population means comprising:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for populating the data base according to the instruction,

wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

70. (Previously presented) The system according to claim 69, further comprising:

means for providing a signal for directing input of the series of entries of the biometric signal;

means for incorporating into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database; and

means for constructing an audit trail of biometric signals provided to the biometric sensor for the purpose of accessing the controlled item.

71. (Previously presented) The system according to claim 69, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class, the accessibility attribute preferably comprising:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

72. (Cancelled)

73. (Previously presented) The system according to claim 69, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration, and/or the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

74. (Previously presented) The system according to claim 69, wherein said conditional access comprises one of:

provision of access to the controlled item if the accessibility attribute comprises an access attribute:

provision of access to the controlled item and sounding of an alert if the accessibility attribute comprises a duress attribute; and

denial of access to the controlled item and sounding of an alert if the accessibility attribute comprises an alert attribute.

75. (Previously presented) The system as claimed in claim 69, wherein:

the biometric sensor is for authenticating the identity of a user;

the means for emitting comprises a transmitter for transmitting information capable of granting more than two types of access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and

the system further comprising a control panel for receiving the information and for providing the secure access requested.

76. (Previously presented) The system according to claim 75, wherein the control panel includes a converter for receiving the secure wireless signal and for outputting the information, and/or the biometric sensor authenticates the identity of the user by comparing a biometric input from the user with a biometric signature for the user in a biometric database, and/or the biometric sensor, the biometric database, and the transmitter are located in a remote fob.

77. (Previously presented) The system according to claim 76, wherein the secure wireless signal comprises an RF carrier and a rolling code, and the converter preferably converts the rolling code to the Wiegand protocol.

78. (Currently amended) A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and

means for emitting a secure access signal conveying said information dependent upon said accessibility attribute;

wherein the transmitter sub-system further comprises means for populating the database of biometric signatures, the populating means comprising:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for populating the database according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

79. (Currently amended) A method for providing secure access to a controlled item in a system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal capable of granting more than two types of access to the controlled item, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon information in said secure access signal, the method comprising the steps of:

populating the database of biometric signatures by:

receiving a series of entries of the biometric signal;

determining at least one of the number of said entries and a duration of each said entry;

mapping said series into an instruction; and

populating the database according to the instruction;

receiving a biometric signal;

matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;

emitting a secure access signal conveying information dependent upon said accessibility attribute; and

providing conditional access to the controlled item dependent upon said information,

wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

80. (Previously presented) The method according to claim 79, wherein the step of populating the database of biometric signatures further comprises the step of enrolling a biometric signature into the database of biometric signatures comprising the steps of:

receiving a biometric signal; and

enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty.

81. (Previously presented) The method according to claim 80, wherein the step of enrolling the biometric signature further comprises receiving another biometric signal to confirm the enrolling of the biometric signal as an administrator signature, and is preferably performed dependent upon generation of a feedback signal adapted to direct provision of at least one of the biometric signal and the other biometric signal.

82. (Previously presented) A non-transitory computer readable storage medium for storing a computer program comprising instructions, which when executed by processors causes the processors to perform the steps of the method of claim 79.

Sufficient Support for "means for" Language in the Claims

The MPEP states that "the broadest reasonable interpretation of a claim limitation that invokes 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph is the structure, material or act described in the specification as performing the entire claimed function and equivalents to the disclosed structure, material or act. *See* MPEP 2181.

Even if the "means for" language in the claims is interpreted as invoking § 112, para. 6, § 112, paragraph 2 is satisfied for the following reasons:

Claim 69

In claim 69, each of the "means for" features are recited as being included with a "transmitter sub-system or a "receiver sub-system." The Specification shows and describes each of the transmitter sub-system and the receiver sub-system as including sufficient structure. For example, Fig. 2 shows a transmitter sub-system 116 as including a controller/transmitter 107, an audio transducer 124, LED indicators 122, a biometric sensor 121, a user ID database 105, and a database 113, all of which are structural elements. Fig. 10 further shows that the controller/transmitter 107 includes a processor 1005, memory 1004, an audio-video interface 1007, a communication interface 1008, an interconnected bus 1004, and an input/output (I/O) interface, which are structural elements. Fig. 2 and 10 also show the receiver sub-system as including a controller 109, a database 115, and a receiver 118, which are structural elements.

In addition to the structural elements shown in Figs. 2 and 10, methods of operation (i.e., acts) associated with the transmitter sub-system 116 and the receiver sub-system 117 are described with reference to flow charts in Figs. 3, 4, and 6-9. The Specification ties the acts described with reference to these figures to the structural elements disclosed in Figs. 2 and 10. For example, in paragraph [0134], the Specification states:

> FIG. 10 is a schematic block diagram of the system in FIG. 2. The disclosed secure access methods are preferably practiced using a computer system arrangement 100', such as that shown in FIG. 10 wherein the processes of FIGS. 3-4, and 6-9 may be implemented as software, such as application program modules executing within the computer system 100'. In particular, the method steps for providing secure access are effected by instructions in the software that are carried out under direction of the respective processor modules 107 and 109 in the transmitter and receiver sub-systems 116 and 117. The instructions may be formed as one or more code modules, each for performing one or more particular tasks. The software may also be divided into two separate parts, in which a first part performs the provision of secure access methods and a second part manages a user interface between the first part and the user. The software may be stored in a computer readable medium, including the storage devices described below, for example. The software is loaded into the transmitter and receiver sub-systems 116 and 117 from the computer readable medium, and then executed under direction of the respective processor modules 1 07 and 109. A computer readable medium having such software or computer program recorded on it is a computer program

> product. The use of the computer program product in the computer preferably effects an advantageous apparatus for provision of secure access.

Further support in the Specification, referencing Fig. 2 and/or the methods of Figs. 3-4, 6-9, is provided for each of the means for limitations in claim 69 as follows:

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute

> Block 202 in Fig. 3 and [0092]: The received biometric signal 102 is compared with information in the biometric signature database 105.

means for emitting a secure access signal conveying information dependent upon said accessibility attribute

> Block 205 in Fig. 3 and [0093]: The controller 107 sends the appropriate access signal 108 to the controller 109.

means for receiving the transmitted secure access signal

> [0096]: Fig. 4 shows the method of operation of the control sub-system 117 of FIG. 2. The method 300 commences with a testing step 301 which continuously checks whether the access signal 108 has been received from 107. The step 301 is performed by the controller 109. When the access signal 108 is received, the process 300 is directed from the step 301 by means of a YES arrow to a step 302.

means for providing conditional access to the controlled item dependent upon said information

> [0096]: In the step 302, the controller 109 compares the rolling code received by means of the access signal 108 with a reference code in the database 115. A subsequent testing step 303 is performed by the controller 109. In the step 303 if the code received on the access signal 108 is successfully matched against the reference code in the database 115 then the process 300 is directed in accordance with a YES arrow to a step 304. [0097] In the step 304 the controller 109 sends the control signal 110 to the controlled item 111 (for example opening the secured door).

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry

> [0109]: The first administrator can provide control information to the code entry module by providing a succession of finger presses to the biometric sensor 121; [0104]: FIG. 6 shows a process 700 that determines if a biometric signal has been received by the biometric sensor 121 in the code entry module in FIG. 2; [0105]: If the database 105 is empty, then the process 700 is directed to 706 in FIG. 8, which depicts a process 800

dealing with the enrolment or the administration function for loading relevant signatures into the database 105.

means for mapping said series into an instruction

[0109]: The first administrator can provide control information to the code entry module by providing a succession of finger presses to the biometric sensor 121, providing that these successive presses are of the appropriate duration, the appropriate quantity, and are input within a predetermined time. In one arrangement, the control information is encoded by either or both (a) the number of finger presses and (b) the relative duration of the finger presses. If the successive finger presses are provided within this predetermined time, then the controller 107 accepts the presses as potential control information and checks the input information against a stored set of legal control signals;

means for populating the data base according to the instruction

[0110]: One example of a legal control signal can be expressed as follows: [0111] "Enrol an ordinary user"->dit, dit, dit, dah

<u>Claim 70</u>

In claim 70, support for the "means for" language for purposes of § 112, second paragraph even if § 112, paragraph 6 is invoked is as follows:

means for providing a signal for directing input of the series of entries of the biometric signal

This feature is about assisting the user to input a series of entries of the biometric signal. For example, see [0081] The code entry module 103 also incorporates at least one mechanism for providing feedback to the user 101. This mechanism can, for example, take the form or one or more Light Emitting Diodes (LEDs) 122 Which can provide visual feedback, depicted by an arrow 123 to the user 101. Alternately or in addition the mechanism can take the form of an audio signal provided by an audio transducer 124 providing audio feedback 125. ***<u>Also</u>***, [0110] One example of a legal control signal can be expressed as follows: [0111] "Enrol an ordinary user"->dit, dit, dit, dah Where "dit" is a finger press of one second's duration (provided by the user 101 in response to the feedback provided by the Amber LED as described below), and "dah" is a finger press of two second's duration;

means for incorporating into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database;

This feature is optionally used when, for example, a user provides a biometric signal to the step 201 in Fig. 3, and their biometric signal is matched against signatures in the database in the steps 202 and 203 in Fig. 3. [0079] states that if the identity of the user 101 is authenticated successfully, then the code entry module 103 sends a signal 106 to a controller/transmitter 107 which sends an access signal, as depicted by an arrow 108 to a controller 109. If the incoming rolling code forming the access signal 108 is found to be

> legitimate, then the controller 109 sends a command, as depicted by an arrow 110, to a controlled item 111. The controlled item 111 can be a door locking mechanism on a secure door, or an electronic key circuit in a personal computer (PC) that is to be accessed by the user 101. The fact that the user presently providing the biometric signal provides a legitimate signal is sufficient to open the controlled door, or access the controlled PC without that user having to identify themselves further. Eg if "John" provides a biometric signal which matches a signature in the database, then John is able to access the controlled item without his name "John" being inserted into the access signal 108. If however it is desired to construct an audit trail, then as well as providing John with access to the controlled item, it is also necessary to record the fact that it is John who is doing the accessing. This is the object of the "incorporation of the identification field into the secure access signal", and this is clearly only done if the user is a legitimate user and has a matching biometric signal in the database.

means for constructing an audit trail of biometric signals provided to the biometric sensor for the purpose of accessing the controlled item

> see [0121]: An optional additional step (not shown) can prepare an identification field for insertion into the access signal 108. This sends, to the receiver sub-system 117, ID information that the receiver sub-system can use to construct an audit trail listing Which users, having signatures in the database 105, have been provided with access to the controlled item 111

Claim 78

The "means for" language recited in this claim is supported by the Specification for purposes of § 112, paragraph 2 even if § 112, paragraph 6 is invoked at least for the reasons set forth above for claim 69.

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS on the below date:

Date: May 15, 2015 Name: E. Brandon Nykiel Signature: /E. Brandon Nykiel/

BRINKS
GILSON
&LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of:	Christopher John Burke		
Appln. No.:	13/572,166	Examiner:	Rahman, Mohammad L.
Filed:	August 10, 2012	Art Unit:	2438
For:	REMONTE ENTRY SYSTEM	Conf. No.:	9752
Attorney Docket No.:	12838-8		

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

In accordance with the duty of disclosure, Applicant(s) hereby cites the following references:

US PATENT REFERENCES

EXAMINER INITIAL		DOCUMENT NUMBER Number-Kind Code (if known)	DATE	NAME
	B1	2002/0038818 A1	04-04-2002	Zingher et al.
	B2	2003/0126439 A1	07-03-2003	Wheeler et al.

FOREIGN PATENT REFERENCES

EXAMINER INITIAL		DOCUMENT NUMBER Number-Kind Code (if known)	DATE	COUNTRY	TRANSLATION YES OR NO
	B3	WO 02/095589 A1	11-28-2002	PCT	N/A

OTHER ART – NON PATENT LITERATURE DOCUMENTS

EXAMINER INITIAL	Include name of author, title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	B4	Extended European Search Report for corresponding EP application number 14188004 dated April 22, 2015
	B5	Office Action for corresponding Canadian application number 2,535,434 dated March 27, 2015

Examiner Signature	/Mohammad Rahman/	Date Considered	10/01/2015

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.L.R./

1. PRIORITY INFORMATION:

☐ This application claims priority under 35 USC §120 to the following United States patent application(s):. In accordance with 37 CFR §1.98(d), copies of the references cited herein which were submitted to, or cited by, the office, in compliance with 37 CFR §1.98(a)-(c) in the earlier application are not provided herewith. The Examiner is directed to those references cited in all Information Disclosure Statements filed in the priority United States patent application(s) cited above in addition to the references cited herein.

2. CERTIFICATIONS: (CHECK ALL THAT APPLY)

☐ For purposes of 37 CFR §1.704(d)(i), Applicant hereby certifies that each item of information contained in this Information Disclosure Statement was first cited in any communication from a patent office in a counterpart foreign or international application or from the Office, and that this communication was not received by any individual designated in 37 CFR §1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement.

☐ For purposes of 37 CFR §1.704(d)(ii), Applicant hereby certifies that each item of information contained in this Information Disclosure Statement is a communication that was issued by a patent office in a counterpart foreign or international application or by the Office, and that this communication was not received by any individual designated in 37 CFR §1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement.

☒ Applicant hereby certifies pursuant to 37 CFR §1.97(e)(1) that each item of information in this Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

☐ Applicant hereby certifies pursuant to 37 CFR §1.97(e)(2) that no item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated in 37 CFR §1.56(c), more than three months prior to the filing of this Information Disclosure Statement.

3. FEE INFORMATION: (CHECK IF FEE REQUIRED)

☐ Applicant has calculated a processing fee in the amount of _________ to be due under 37 CFR §1.17(p) in connection with the filing of this Information Disclosure Statement. Applicant authorizes charging the fee to Deposit Account ________.

☒ The Director is hereby authorized to charge any fee deficiency associated with the filing of this Information Disclosure Statement to Deposit Account 23-1925.

Pursuant to the undersigned attorney's obligation and duties under 37 CFR §§ 1.56 and 1.98(a)(3) and (c), either English language abstracts, partial translations, or full translations are included for patent documents which are not in English for the express purpose of providing a concise explanation of the references to the Patent and Trademark Office with the opportunity to evaluate the same. Applicant respectfully requests the Examiner's consideration of the above reference(s) and entry thereof into the record of this application.

By submitting this Statement, Applicant is attempting to fully comply with the duty of candor and good faith mandated by 37 CFR §1.56. As such, this Statement is not intended to constitute an admission that any of the enclosed references, or other information referred to therein, constitutes "prior art" or is otherwise "material to patentability," as that phrase is defined in 37 CFR §1.56(a).

Respectfully submitted,

May 15, 2015
Date

/E. Brandon Nykiel/
E. Brandon Nykiel (Reg. No. 62,972)

xaminer Signature	/Mohammad Rahman/	Date Considered	10/01/2015

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R./

Technique using order and timing for enhancing **fingerprint** authentication system effectiveness
C Hekimian - US Patent App. 10/741,087, 2003 - Google Patents
... The timer or "clock" begins **counting** in fixed increments of perhaps a quarter of a second, from **...** A clock local to the sensing station **counts** in fixed increments starting from this first fingertip closure **...** If the send command is detected the clock **count** is saved to the buffer and the buffer **...**
Cited by 8 Related articles All 2 versions Cite Save

Fingerprint matching using transformation parameter clustering
RS Germain, A Califano, S Colville - Computing in Science and ..., 1997 - computer.org
... drawn be- tween each pair of minutiae, the number of ridges crossed by this line can be **counted**, as shown in Figure 4. This ridge-**counting** procedure repeats **...** The full index consists of nine components: the length of each side, the ridge **count** between each pair, and the **...**
Cited by 241 Related articles All 10 versions Cite Save

Minutia data extraction in **fingerprint** identification
S Igaki, T Shinzaki, F Yamagishi, H Ikeda... - US Patent ..., 1992 - Google Patents
... on a sensor the alignment between **successive fingerprint** image data produced in **successive**, multiple **fingerprint ...** for the content of the storage for minutia data is carried out thereby to **count** the number **...** number of the minutia data from the highest result of the **counting** is stored **...**
Cited by 115 Related articles All 2 versions Cite Save

Duplicate Data Elimination in a SAN File System.
B Hong, D Plantenberg, DDE Long, M Sivan-Zimet - MSST, 2004 - Citeseer
... Because block reference **counts** are crucial to data integrity, any up- date on them should be **...** A **fingerprint** is valid only if its block reference **count** is no less than 1 **...** The linear structure makes **consecutive fingerprint** comparisons efficient because all related **entries** are in memory. **...**
Cited by 66 Related articles All 24 versions Cite Save More

Audio **fingerprinting**: Combining computer vision & data stream processing
S Baluja, M Covell - Acoustics, Speech and Signal Processing, ..., 2007 - ieeexplore.ieee.org
... When we look at the wavelets for **successive** images for two songs, we see easily **...** Figure 1. The representation for two songs -4 **consecutive** spectrogram images shown for each, skipping **...** The similarity ofthe bit vectors iscomputed by **counting** the exact matches in the p- length **...**
Cited by 72 Related articles All 8 versions Cite Save

Fingerprint verification method employing plural correlation judgement levels and sequential judgement stages
T Kamiya, K Kawasaki, K Kawai, M Nagura... - US Patent ..., 1991 - Google Patents
... stepping operation described above, whereupon the degree of correlation is measured by **counting** the number **...** of mutually non-corresponding pixels for the secondary window region c are **counted**, to obtain **...** if the input **fingerprint** image is of poor quality, then the **count** value N **...**
Cited by 71 Related articles All 2 versions Cite Save

The STCN **Fingerprint**
PCA Vriesema - Studies in bibliography, 1986 - JSTOR
... If a signature falls under only a part of one character or under parts of two **successive** characters, these parts **count** as whole **...** A space, regardless of length, **counts** as one character and is represented as a $. The characters are tran- scribed in accordance with the relevant **...**
Cited by 11 Related articles All 2 versions Cite Save More

System and method for **fingerprint** data verification
PC Ross - US Patent 6,195,447, 2001 - Google Patents
... minutia include particular types of irregularities, the scanning angle, the ridge **count**, and the **...** Again taking into account the phenomena that **successive** detected **fingerprint** image minutia from the **...** Jun 2, 2010, Dec 30, 2010, Craig Stephen Etchegoyen, Use of **Fingerprint** with an **...**
Cited by 46 Related articles All 2 versions Cite Save

Fingerprint recognition and retrieval system
MK Sparrow - US Patent 4,747,147, 1988 - Google Patents
... θ) of said ridge scan line from a predetermined first angular orientation,. means for **counting** the number of **...** the predetermined point on the line for the purpose of measuring said ridge **counts** (R), and **...** are scanned can be determined for the entire **fingerprint** and ridge **count** data (R **...**
Cited by 116 Related articles All 2 versions Cite Save

Method and apparatus for **fingerprint** matching using transformation parameter clustering based on local feature correspondences

A Califano, SE Colville, RS Germain - US Patent 6,041,133, 2000 - Google Patents

... associated with the given triplet of feature points including, for example, the ridge **counts**, local direction **...** in step 801 by initializing a variable N e that represents the a **count** of eligible **...** largest of the three sides associated with the triplet, and then enumerating **successive** sides by **...**

Cited by 40 Related articles All 2 versions Cite Save

Fingerprinting to identify repeated sound events in long-**duration** personal audio recordings

JP Ogle, DPW Ellis - Acoustics, Speech and Signal Processing, ..., 2007 - ieeexplore.ieee.org

... proposed a system to identify repeating multimedia segments from long **duration** streams using vector quantized low-level feature vec- tors [8]. Herley outlined a **...** The linear search algorithm must scan the file in order check- ing each **fingerprint entry** to identify potential matches. **...**

Cited by 39 Related articles All 8 versions Cite Save

Fingerprint image **entry** device of electrostatic capacitance sensing type

I Fujieda - US Patent 6,055,324, 2000 - Google Patents

... 7) for consecutively making the signal generating electrodes serving as the scanning signal leads in each row to generate signals having an active **duration** which overlaps in **...** FIG. 1 is a perspective view showing a first embodiment of a **fingerprint** image **entry** device of **...**

Cited by 15 Related articles All 2 versions Cite Save

Fingerprint apparatus and method

T Higuchi - US Patent 6,950,540, 2005 - Google Patents

... This registration is temporary for the **duration** of the guest's stay at the hotel **... fingerprint**, the apparatus communicates with the hotel server 1302 to determine if the input **fingerprint** matches the **fingerprint** data on **...** If it does, the lock mechanism of the door is released allowing **entry**. **...**

Cited by 38 Related articles All 4 versions Cite Save

Acquiring a 2D rolled equivalent **fingerprint** image from a non-contact 3D finger scan

A Fatehpuria, DL Lau... - Defense and ..., 2006 - proceedings.spiedigitallibrary.org

... The advantages of the proposed system are: • Automated **Fingerprint Entry**: As proposed, the hand is scanned while rested with the palm down. **...** We can also control the flash **duration** to match the acquisition window of all the cameras. **...**

Cited by 18 Related articles All 4 versions Cite Save

Biometric sequence codes

A Pu, D Psaltis - US Patent 6,229,906, 2001 - Google Patents

... By removing and placing the user's **fingerprint** on the input device for a plurality of times with different **duration**, a **fingerprint** Morse Code is generated and then **...** For example, one **fingerprint** can be used to form a code by rotating the finger 90° at one sequential **entry** relative to **...**

Cited by 15 Related articles All 2 versions Cite Save

Dual technology door **entry** person authentication

S Huseth, B Anderson - US Patent App. 10/728,564, 2003 - Google Patents

... Dual technology door **entry** person authentication US 20050122210 A1. Abstract. A security system reader receives a signal containing an **...** activates the power supply 50 to generate power in a sufficient amount and for a sufficient **duration** to power the **fingerprint** reader 46 **...**

Cited by 1 Related articles All 2 versions Cite Save

Fingerprint based authentication system with keystroke dynamics for realistic user

GV Kumar, K Prasanth, SG Raj... - Current Trends in ..., 2014 - ieeexplore.ieee.org

... key (See Figure 3 (c)) • Up to up time is the time **duration** in between **...** We presented a novel approach for authentication of the user based on **fingerprint**, login credential and login according to the biometric characteristics based on keystrokes of the password **entry**. **...**

Related articles Cite Save

Method and system of deduplication-based **fingerprint** index caching

W Wu, V Janakiraman - US Patent 8,392,384, 2013 - Google Patents

... It may also increase the **duration** of a restore operation, such that a client may have to wait for an unacceptably long period of **...** Then, content router 130 may search cached **fingerprint** index 135 and/or persistent **fingerprint** index 145 to locate the **fingerprint entry** containing the **...**

Cited by 3 Related articles All 3 versions Cite Save

Method and system for authenticating a user of a computer system

J McKeeth - US Patent 6,766,456, 2004 - Google Patents

... a particular geometric pattern under the condition that the user performs such pattern concurrently with, or after a predetermined **duration** from, scanning his/her **fingerprint**. In performing the passive act, the user may wait a predetermined time intervals between **entry** of various **...**

Cited by 33 Related articles All 2 versions Cite Save

Modeling of indoor positioning systems based on location fingerprinting

K Kaemarungsi, P Krishnamurthy - INFOCOM 2004. Twenty- ..., 2004 - ieeexplore.ieee.org

... position. This sample vector is compared with all li existing entries in the database. The **fingerprint entry** that has the closest match to the user's sample of RSS is used by the system as the estimate of the user's current location. This **...**
Cited by 475 Related articles All 8 versions Cite Save

Issue Classification	**Application/Control No.** 13572166	**Applicant(s)/Patent Under Reexamination** BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	**Art Unit** 2438

CPC						
Symbol					**Type**	**Version**
G07C		9	/	00158	F	2013-01-01
G06F		21	/	32	I	2013-01-01
G06F		21	/	35	I	2013-01-01
H04L		63	/	0861	I	2013-01-01
H04W		12	/	08	I	2013-01-01
H04W		84	/	12	A	2013-01-01
H04W		84	/	18	A	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

(Assistant Examiner)	(Date)	**Total Claims Allowed:** 13	
/MOHAMMAD L RAHMAN/ Primary Examiner.Art Unit 2438 (Primary Examiner)	10/01/2015 (Date)	O.G. Print Claim(s) 69	O.G. Print Figure 2

Issue Classification	**Application/Control No.** 13572166	**Applicant(s)/Patent Under Reexamination** BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	**Art Unit** 2438

US ORIGINAL CLASSIFICATION

CLASS	SUBCLASS

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				

INTERNATIONAL CLASSIFICATION

CLAIMED					NON-CLAIMED				
H	0	4	L	29 / 06 (2006.01.01)					

(Assistant Examiner)	(Date)	**Total Claims Allowed:** 13	
/MOHAMMAD L RAHMAN/ Primary Examiner.Art Unit 2438 (Primary Examiner)	10/01/2015 (Date)	O.G. Print Claim(s) 69	O.G. Print Figure 2

Issue Classification	**Application/Control No.** 13572166	**Applicant(s)/Patent Under Reexamination** BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	**Art Unit** 2438

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** ☒ **T.D.** □ **R.1.47**

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		17		33		49		65	12	81				
	2		18		34		50		66	13	82				
	3		19		35		51		67						
	4		20		36		52		68						
	5		21		37		53	1	69						
	6		22		38		54	2	70						
	7		23		39		55	3	71						
	8		24		40		56		72						
	9		25		41		57	4	73						
	10		26		42		58	5	74						
	11		27		43		59	6	75						
	12		28		44		60	7	76						
	13		29		45		61	8	77						
	14		30		46		62	9	78						
	15		31		47		63	10	79						
	16		32		48		64	11	80						

(Assistant Examiner)	(Date)	**Total Claims Allowed:** 13	
/MOHAMMAD L RAHMAN/ Primary Examiner.Art Unit 2438 (Primary Examiner)	10/01/2015 (Date)	O.G. Print Claim(s) 69	O.G. Print Figure 2

Index of Claims	**Application/Control No.** 13572166	**Applicant(s)/Patent Under Reexamination** BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	**Art Unit** 2438

✓	**Rejected**	**-**	**Cancelled**	**N**	**Non-Elected**	**A**	**Appeal**
=	**Allowed**	**÷**	**Restricted**	**I**	**Interference**	**O**	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** ☒ **T.D.** □ **R.1.47**

CLAIM		**DATE**								
Final	Original	03/19/2014	11/06/2014	04/22/2015	10/01/2015					
	1	✓	-	-	-					
	2	✓	-	-	-					
	3	✓	-	-	-					
	4	✓	-	-	-					
	5	✓	-	-	-					
	6	✓	-	-	-					
	7	✓	-	-	-					
	8	✓	-	-	-					
	9	✓	-	-	-					
	10	✓	-	-	-					
	11	✓	-	-	-					
	12	✓	-	-	-					
	13	✓	-	-	-					
	14	✓	-	-	-					
	15	✓	-	-	-					
	16	✓	-	-	-					
	17	✓	-	-	-					
	18	✓	-	-	-					
	19	✓	-	-	-					
	20	✓	-	-	-					
	21	✓	-	-	-					
	22	✓	-	-	-					
	23	✓	-	-	-					
	24	✓	-	-	-					
	25	✓	-	-	-					
	26	✓	-	-	-					
	27	✓	-	-	-					
	28	✓	-	-	-					
	29	✓	-	-	-					
	30	✓	-	-	-					
	31	✓	-	-	-					
	32	✓	-	-	-					
	33	✓	-	-	-					
	34	✓	-	-	-					
	35	✓	-	-	-					
	36	✓	-	-	-					

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13572166	BURKE, CHRISTOPHER JOHN
	Examiner	**Art Unit**
	MOHAMMAD L RAHMAN	2438

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

☐ **Claims renumbered in the same order as presented by applicant** ☐ **CPA** ☒ **T.D.** ☐ **R.1.47**

CLAIM		DATE								
Final	Original	03/19/2014	11/06/2014	04/22/2015	10/01/2015					
	37	✓	-	-	-					
	38	✓	-	-	-					
	39	✓	-	-	-					
	40	✓	-	-	-					
	41	✓	-	-	-					
	42	✓	-	-	-					
	43	✓	-	-	-					
	44	✓	-	-	-					
	45		✓	✓	-					
	46		✓	✓	-					
	47		✓	✓	-					
	48		✓	✓	-					
	49		✓	✓	-					
	50		✓	✓	-					
	51		✓	✓	-					
	52		✓	✓	-					
	53		✓	✓	-					
	54		✓	✓	-					
	55		✓	✓	-					
	56		✓	✓	-					
	57		✓	✓	-					
	58		✓	✓	-					
	59		✓	✓	-					
	60		✓	✓	-					
	61		✓	✓	-					
	62		✓	✓	-					
	63		✓	✓	-					
	64		✓	✓	-					
	65		✓	✓	-					
	66		✓	✓	-					
	67		✓	✓	-					
	68			✓	-					
1	69				=					
2	70				=					
3	71				=					
	72				-					

Index of Claims	**Application/Control No.** 13572166	**Applicant(s)/Patent Under Reexamination** BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	**Art Unit** 2438

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** ☒ **T.D.** □ **R.1.47**

CLAIM		DATE								
Final	Original	03/19/2014	11/06/2014	04/22/2015	10/01/2015					
4	73				=					
5	74				=					
6	75				=					
7	76				=					
8	77				=					
9	78				=					
10	79				=					
11	80				=					
12	81				=					
13	82				=					

Search Notes	**Application/Control No.** 13572166	**Applicant(s)/Patent Under Reexamination** BURKE, CHRISTOPHER JOHN
	Examiner MOHAMMAD L RAHMAN	**Art Unit** 2438

CPC- SEARCHED

Symbol	Date	Examiner
H04L63/0861	4/22/2015	MLR
G06F21/32	4/22/2015	MLR

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
713	186	03/19/2014	MLR
Updated Search			
713	186	11/6/2014	MLR

SEARCH NOTES

Search Notes	Date	Examiner
Combined text search with classes/sub-classes (see EAST)	3/19/2014	MLR
Inventor name, Assigee	3/19/2014	MLR
NPL Search - Google Scholar IEEE ACM WIPO	3/19/2014	MLR
Updated Search		
Updated keywords combined with classes/sub-classes	11/6/2014	MLR
Inventor name, Assignee	11/6/2014	MLR
NPL Search - Google Scholar IEEE ACM WIPO	11/6/2014	MLR
Updated Text search combined with CPC symbols (see EAST)	4/22/2015	MLR
Inventor name, Assignee	4/22/2015	MLR
NPL Search - Google Scholar IEEE ACM WIPO	4/22/2015	MLR
Updated text search combined with CPC symbols (G07C9/00158 or G06F21/35 or H04W12/08 or H04L63/0861 or G06F21/32 or H04W84/18 or H04W84/12).cpc.	10/1/2015	MLR
Google Scholar, IEEE, ACM	10/1/2015	MLR
Inventor name, Assignee	10/1/2015	MLR

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
DOT claim search	((duration (time near5 (period length span))) and ((series sequence$1) near5 (biometric fingerprint (retina near2 scan)) near5 entr$3) and (map$4 match$3) and database).CLM.	10/1/2015	MLR

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

757 7590 10/16/2015
BGL
P.O. BOX 10395
CHICAGO, IL 60610

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Electronic Filing

I hereby certify that this Fee(s) Transmittal is being electronically transmitted to the United States Patent and Trademark Office via the EFS pursuant to 37 CFR §1.8, on the date indicated below.

E. Brandon Nykiel	(Depositor's name)
/E. Brandon Nykiel/	(Signature)
January 15, 2016	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/572,166	08/10/2012	Christopher John Burke	12838/8	9752

TITLE OF INVENTION: REMOTE ENTRY SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	01/19/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
RAHMAN, MOHAMMAD L	2438	726-007000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Brinks Gilson & Lione
2 ____________
3 ____________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: SECURICOM (NSW) PTY LTD

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Ramsgate, Australia

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual ☒ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:

☒ Issue Fee
□ Publication Fee (No small entity discount permitted)
□ Advance Order - # of Copies ____________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.
□ Payment by credit card. Form PTO-2038 is attached.
☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 23-1925 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

□ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

□ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /E. Brandon Nykiel/ Date January 15, 2016

Typed or printed name E. Brandon Nykiel Registration No. 62,972

Electronic Patent Application Fee Transmittal

Application Number:	13572166
Filing Date:	10-Aug-2012
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Filer:	E. Brandon Nykiel/Patricia Chiovari
Attorney Docket Number:	12838/8

Filed as Small Entity

Filing Fees for **Utility under 35 USC 111(a)**

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
	Total in USD ($)			**480**

Electronic Acknowledgement Receipt

EFS ID:	24638893
Application Number:	13572166
International Application Number:	
Confirmation Number:	9752
Title of Invention:	REMOTE ENTRY SYSTEM
First Named Inventor/Applicant Name:	Christopher John Burke
Customer Number:	757
Filer:	E. Brandon Nykiel/Jesus Rodriguez
Filer Authorized By:	E. Brandon Nykiel
Attorney Docket Number:	12838/8
Receipt Date:	15-JAN-2016
Filing Date:	10-AUG-2012
Time Stamp:	15:59:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$480
RAM confirmation Number	2620
Deposit Account	231925
Authorized User	NYKIEL, BRANDON

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		12838_8_IssueFeeFiling_011516.pdf	167914 5d18e848cff250d0ce6acde84c6dfce1c1fc9045	yes	2
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Miscellaneous Incoming Letter		1	1	
	Issue Fee Payment (PTO-85B)		2	2	
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30479 fa1eb2980cc68fb1e3ed0c7309d52811c5802e14	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	198393		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS pursuant to 37 CFR §1.8 on the below date:

Date: January 15, 2016 Name: E. Brandon Nykiel Signature: /E. Brandon Nykiel/

BRINKS
GILSON
& LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: Christopher John Burke

Appln. No.: 13/572,166

Filed: August 10, 2012

For: REMOTE ENTRY SYSTEM

Attorney Docket No.: 12838/8

Examiner: Rahman, Shawnchoy

Art Unit: 2438

Conf. No.: 9752

TRANSMITTAL

Mail Stop Issue Fee
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Attached is/are:

☒ Part B – Fee(s) Transmittal.

Fee calculation:

☐ No additional fee is required.

☒ Per 37 CFR §1.27, ☒ Applicant is small entity ☐ Applicant is micro entity.

☐ An extension fee in an amount of $_____ for a _____-month extension of time under 37 CFR § 1.136(a).

☐ A petition or processing fee in an amount of $_____ under 37 CFR § 1.20(_____).

☐ An additional filing fee has been calculated as shown below:

					Fee		Small Entity Fee		Micro Entity Fee	
	Claims Remaining After Amendment		Highest No. Previously Paid	Present Extra	Rate	Add'l Fee	Rate	Add'l Fee	Rate	Add'l Fee
Total		Minus			x $ 80 =	$	1x $ 40 =	$40	x $20 =	$
Independent		Minus			x $420 =	$	x $210 =	$	x $105 =	$
First Presentation of Multiple Dep. Claim					+ $780 =	$	+ $390 =	$	+ $195 =	$
					Total	$	Total	$40	Total	$

Fee payment:

☒ Please charge Deposit Account No. 23-1925 in the amount of $480 for Issue Fee.

☐ Payment by credit card in the amount of $_____ (Form PTO-2038 is attached).
WARNING: Information on this form may become public. **Credit card information should not be included on this form.**

☒ The Director is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925.

Respectfully submitted,

January 15, 2016
Date

/E. Brandon Nykiel/
E. Brandon Nykiel (Reg. No. 62,972)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/572,166	02/23/2016	9269208	12838/8	9752

757 7590 02/03/2016

BGL
P.O. BOX 10395
CHICAGO, IL 60610

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 78 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Christopher John Burke, Ramsgate, AUSTRALIA;

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas, Waco Divison on the following

□ Trademarks or ☑ Patents. (□ the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 6:21-cv-00165	DATE FILED 2/23/2021	U.S. DISTRICT COURT Western District of Texas, Waco Divison
PLAINTIFF CPC Patent Technologies Pty Ltd.		DEFENDANT Apple Inc.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 US 8,620,039	12/31/2013	CPC Patent Technologies Pty Ltd. by assignment
2 US 9,269,208	2/23/2016	CPC Patent Technologies Pty Ltd. by assignment
3 US 9,665,705	5/30/2017	CPC Patent Technologies Pty Ltd. by assignment
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY □ Amendment □ Answer □ Cross Bill □ Other Pleading

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas, Waco Divison on the following

□ Trademarks or ☑ Patents. (□ the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 6:21-cv-00166	DATE FILED 2/23/2021	U.S. DISTRICT COURT Western District of Texas, Waco Divison

PLAINTIFF CPC Patent Technologies Pty Ltd.	DEFENDANT HMD Global OY

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 US 9,269,208	2/23/2016	CPC Patent Technologies Pty Ltd. by assignment
2 US 9,665,705	5/30/2017	CPC Patent Technologies Pty Ltd. by assignment
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY □ Amendment □ Answer □ Cross Bill □ Other Pleading

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy