(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 January 2016 (07.01.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/001657 A1

(51) International Patent Classification:
*H04L 29/06* (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/GB2015/051915

(22) International Filing Date:
30 June 2015 (30.06.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1411824.4 2 July 2014 (02.07.2014) GB

(71) Applicant: **VALIDSOFT UK LIMITED** [GB/GB]; 35 New Broad Street, London EC2M 1NH (GB).

(72) Inventors: **THORNHILL, Daniel**; c/o Validsoft UK Limited, 9 Devonshire Square, London, Greater London EC2M 4YF (GB). **PETERSEN, John**; c/o Validsoft UK Limited, 9 Devonshire Square, London, Greater London EC2M 4YF (GB). **CARROLL, Patrick**; c/o Validsoft UK Limited, 9 Devonshire Square, London, Greater London EC2M 4YF (GB).

(74) Agent: **HGF LIMITED**; Document Handling - (HGF) York, Belgrave Hall, Belgrave Street, Leeds Yorkshire LS2 8DD (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,

*[Continued on next page]*

(54) Title: BIOMETRIC AUTHENTICATION METHOD AND SERVER

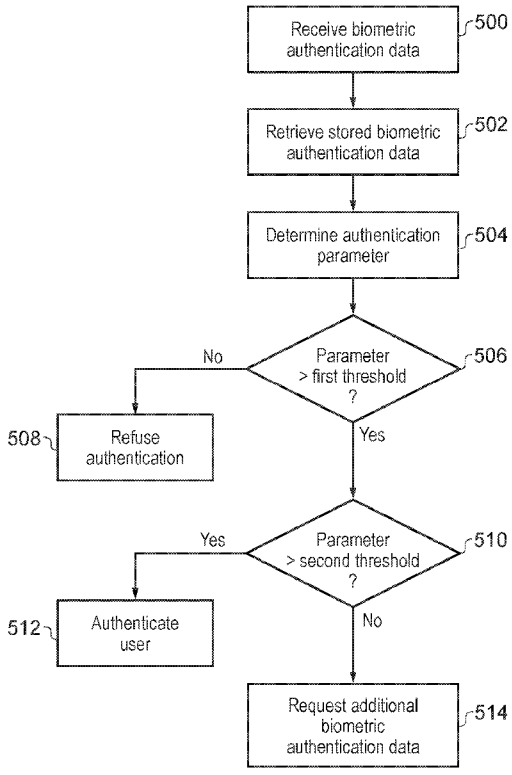


FIG. 5

(57) Abstract: A biometric authentication method. The method comprises receiving biometric authentication data from a user via a communication channel and determining an authentication parameter by comparing the biometric authentication data to stored biometric authentication data. The authentication parameter is compared to first and second thresholds. Based on the result of the comparison it is determined whether to refuse to authenticate the user, to authenticate the user, or to request additional authentication data from the user. An authentication server arranged to implement the method is also disclosed.

WO 2016/001657 A1

TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

**Declarations under Rule 4.17**:

— *of inventorship (Rule 4.17(iv))*

**Published**:

— *with international search report (Art. 21(3))*

# BIOMETRIC AUTHENTICATION METHOD AND SERVER

**[0001]** This invention relates to biometric authentication method and an authentication server for implementing the biometric authentication method.

## BACKGROUND

**[0002]** Biometric authentication systems and methods are used in many areas of modern life. In particular, systems where sensitive or personal data is involved, securing transactions which are considered high risk, or other scenarios where security is a concern, biometric authentication is frequently used. These methods may be employed when a participant in such a system needs to transmit or receive sensitive or personal data to another participant. In this situation, one or both participants may need to be authenticated to ensure their identity is satisfactory to the other participant. Often it may just be the participant who wishes to be sent data who requires authenticating. This may be due to the other party being implicitly authenticated through their possession of the data.

**[0003]** An example of such a system is that involving a financial institution, such as a bank, and a client or user of the financial institution.

**[0004]** When the user wishes to make a transaction relating to an account, the bank may require that user to prove that they are a person who is authorised to make transactions for the account. Historically, such proof could occur through the user visiting a location of the bank and providing a signature or proof of identification which would match details that the bank possessed regarding the authorized person. Alternatively, the user could write a letter to the bank, again providing a signature or proof of identification.

**[0005]** In recent times it has become common to interact with banks using modern communication techniques. Access to bank accounts may now be provided over the internet, where many traditional actions (such as money transfers or personal detail changes) may be performed once a user has logged in to a designated account service provided by the bank. Authenticating a user attempting to perform a transaction or log-in to an account service is still a major concern subject to fraudulent misuse.

**[0006]** Typically, authentication methods can be classified into one of three different types. The first type involves authenticating a user through some apparatus or object possessed by the user. For example, a bank may provide a user with a “card reader” as an authentication apparatus. This device acts as a one-time pin generation pad, which is a well-known form of encryption. A one-time pad allows a user, through the use of a banking card (such as a credit or debit card), to obtain a specific code required to authorize a

transaction (that is, to authorize the user attempting the transaction). The code may be generated based on the specific banking card (or associated bank account) details of the user. The code may further be generated based on the date and time of the attempted transactions, or the details for the transaction. For example, the destination account details involved in the transaction in the case of transferring funds. The user can then provide this code to the bank when attempting the transaction. The bank is in possession of similar means to identify or generate a code associated with the transaction. If the code the bank generates is the same as that received from the user (within a tolerance range), the transaction may be authorized. That is, the bank believes the user is legitimate due to being able to provide the correct code.

**[0007]** This type of authentication is disadvantageous due to the requirement for the user to be in possession of the authentication apparatus whenever they wish to be authenticated. Failure of the apparatus (through damage etc.), loss of the apparatus, or lack of access to the apparatus could all prevent a user from being able to authenticate themselves and so perform transactions. This can greatly inconvenience a user. The very requirement of being in possession of the apparatus may also inconvenience a user.

**[0008]** The second type of authentication method involves authenticating a user through the use of something known to the user, such as a password or other authentication information. An example of this type would be an internet banking service which requires a user name, password, memorable information or other information ideally known only to the user.

**[0009]** This type of authentication may be problematic due to the requirement that the user remembers the authentication information. There may exist a large number of services which require passwords from a user, and it may often be difficult for the user to remember separate authentication information for all of the services. In this situation, a user may typically re-use the same authentication information for several of the services. This can compromise the security of each service. This security method also assumes the user “secret” information has not been compromised, which may no longer be true in modern society.

**[0010]** The third type of authentication method involves biometric information. Biometric authentication systems involve the identification of humans by their characteristic traits. Biometric identifiers are the distinctive, measureable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological or behavioural characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition, retina and odour/scent. Behavioural characteristics

are related to the pattern of behaviour of a person, including but not limited to: typing rhythm, gait, and voice. It will be appreciated that behavioural characteristics are determined partly by physiological characteristics and partly by learned behaviour. These characteristics are typically detected using some biometric scanning apparatus, such as: a scanner for detecting fingerprints; a microphone for detecting vocal patterns or other characteristics; or a camera for detecting iris, retina or other eye-related characteristics. One or more of these characteristics may be used as the basis for an authentication process.

**[0011]** Advantageously, biometric authentication methods do not require the user to be in possession of an authentication apparatus or to remember authentication information and so can be particularly attractive to users and service providers such as banks.

**[0012]** As one example, a user may provide a record of their voice to a bank when they open an account or set up an online service to interact with the account. The voice record may be a vocalization associated with a specific phrase, or some other audible sound. This initial sample may well be accompanied by some more traditional method of authentication to verify that the voice record provided belongs to the legitimate user (to prevent tampering). Once a record of the legitimate user's voice record is held by the bank, the user can authorize future actions by providing a voice sample when prompted, such that the bank can compare this to the sample they hold. This can be readily achieved for telephone banking services, and for internet banking services (assuming that the users internet enabled device includes a microphone). It is, however, necessary that the microphone or telephone is capable of reading a voice provided by a user to the standards required by the authentication process. Said standards may relate to the degree of correlation required by the bank between the voice record on file and the voice provided by the user when attempting to authorize and action.

**[0013]** Voice authentication may also be referred to as speaker verification when a user seeks to positively confirm that they are who they say they are, and the authentication process comprises comparing a speech sample against a stored voice sample (or a template extracted from such a stored sample) obtained at the time of enrolling a user into the authentication system. Voice authentication may either be text dependent where the same text must be spoken for enrolment and verification or text independent. Both scenarios are based on the recognition that acoustic features of speech vary between individuals as a result of anatomy and learned behavioural patterns. Text dependent voice authentication has the advantage that the chance of successful authentication is increased due to an increased likelihood that the acoustic features of speech will match. That is, text dependent voice authentication has a reduced rate of false negative outcomes to

authentication. Varies techniques may be used to compare a voice sample submitted by a user and a stored voice sample. However, each result in a numerical authentication parameter corresponding to a degree of correlation between the samples. The authentication parameter may be scaled according to a normalised scale. This degree of correlation may be compared to a predetermined threshold. Based on the results of this comparison, the user is either authenticated or not authenticated. Although the example of voice authentication has been discussed in detail, it will be appreciated that alternative forms of biometric authentication also result in the establishment of a degree of correlation to determine an authentication parameter that can be compared to a threshold. Adjusting the threshold allows the security of such a biometric process to be controlled. A high threshold may correspond to a high degree of correlation and so a more-secure system, while a low threshold may correspond to a low degree of correlation and so a less-secure system. Due to the fact that biometric authentication is a probabilistic form of authentication, a voice sample provided by a legitimate user when authorizing an action is very unlikely to perfectly match the voice sample held by the bank as external and physical factors will influence the scoring algorithms. The degree to which the two may differ can vary, and as such it is entirely possible for a false-negative situation to occur in which a legitimate user fails to authenticate themselves due to the degree of correlation not exceeding the threshold set by the bank. This can be frustrating for the legitimate user. Similarly, either by accident or for fraudulent reasons, the voice sample of an illegitimate user may match the voice sample of the legitimate user held by the bank such that the illegitimate user is incorrectly authenticated. This occurrence is described as a false-positive, and typically results in fraud perpetrated against the bank.

**[0014]** The rate at which false positives and false negatives occur is dependent, at least in part, on the threshold for authentication. A lower threshold (or one which requires a lower degree of correlation) reduces the number of false-negatives but increases the amount of false-positives. As such, while legitimate user frustration is decreased, fraud is increased. Contrastingly, a higher threshold (requiring a higher degree of correlation) increases the number of false-negatives but decreases the number of false-positives. As such, while legitimate user frustration is increased, fraud is decreased.

**[0015]** For a given authentication system there may be a point (that is, a specific threshold value) where the number or regularity of false-positives is equals to that of false-negatives. This is known as an Equal Error Rate (EER). A common practice is to set the threshold for the authentication method equal according to the EER of the authentication system, such that frustration and fraud are balanced. The EER may be determined through simulations, for instance using repeated voice samples from a large pool of test subjects to

discover the number of false-positives and false-negatives that occur for any given threshold. The results of a typical simulation are shown in Figure 1.

**[0016]** In Figure 1 the X axis represents the authentication correlation threshold represented on a normalised scale, and the Y axis represents an error rate. An EER 110 is shown for a false-negative curve 120, corresponding to the number of false-negatives which occur or are predicted to occur for the given threshold value, and a false-positive curve (130), corresponding to the number of false-positives which occur or are predicted to occur for the given threshold value. If the location of the EER 110 is also set as the threshold value when implementing the authentication method, there is defined a frustration area 125 and a fraud area 135. Therefore, in Figure 1, the frustration area 125 is the area under the false-negative curve 120 to the left of the threshold, and the fraud area 135 is the area under the false-positive curve 130 to the right of the threshold. The frustration area 125 relates to the legitimate users of the biometric system who are unable to authenticate themselves. The fraud area 135 relates to fraudulent or illegitimate persons who are able to imitate legitimate users (victims). It should be apparent that to shift the threshold away from the EER 110 to higher values would increase the size of the frustration area 125 while decreasing the size of the fraud area 135. Similarly, shifting the threshold away from the EER 110 to lower values would decrease the size of the frustration area 125 while increasing the size of the fraud area 135.

**[0017]** In some systems a low threshold may correspond to a high degree of correlation while a high threshold corresponds to a low degree of correlation. In such a system, the curves and areas of Figure 1 would be reversed. That is, the false-negative curve becomes the false-positive curve, the false-positive curve becomes the false-negative curve, the frustration area becomes the fraud area and the fraud area becomes the frustration area. Similarly, in some systems the false-negative curve 120 may be substantially different from the false-positive curve 130 (that is, the curves may not be symmetric about the EER). The EER 110 may not occur at some average threshold value such as may be implied in Figure 1.

**[0018]** As apparent from the above, the existence of the EER creates a dilemma for organisations wishing to deploy a biometric system, especially in financial services. They will want to avoid fraud caused by impersonation attacks, but will also not want to jeopardise the system through high volumes of false rejections. Even at very low false-negative rates, when multiplied by user-bases measured in millions, when performing high volumes of transaction, a high volume of false rejections can occur which result in cost, reputation damage and potentially render the biometric system unworkable.

**[0019]** While this method of setting the threshold may be suitable in certain cases, it still allows for a certain degree of both false-positives and false-negatives due to the described compromise. Additionally, setting the threshold more arbitrarily leads to the problems described above or increasing either frustration or fraud. There is a need to provide a better system which reduces both the number of false-positives and the number of false-negatives.

## BRIEF SUMMARY OF THE DISCLOSURE

**[0020]** It is an aim of certain embodiments of the present invention to provide an authentication method that reduces the rate of false negatives without unacceptably increasing the false positive rate.

**[0021]** According to a first aspect of the present invention there is provided a biometric authentication method, the method comprising: receiving biometric authentication data from a user via a communication channel; determining an authentication parameter by comparing the biometric authentication data to stored biometric authentication data; comparing the authentication parameter to first and second thresholds; and determining, based on the result of the comparison, whether to refuse to authenticate the user, to authenticate the user, or to request additional authentication data from the user.

**[0022]** Advantageously, the present invention reduces the false negative rate by comparing authentication data to first and second thresholds, which produces a third result of the authentication method in which further authentication data is requested.

**[0023]** Requesting additional authentication data may comprise requesting additional biometric authentication data.

**[0024]** The method may further comprise: receiving additional biometric authentication data from a user via a communication channel; determining a second authentication parameter by comparing the biometric authentication data to stored biometric authentication data; comparing the second authentication parameter to the first and second thresholds; and determining, based on the comparison, whether to refuse to authenticate the user or to authenticate the user.

**[0025]** The biometric authentication data or the additional biometric authentication data may comprise voice biometric data or face-recognition biometric data

**[0026]** The method may further comprise determining to request additional authentication data from the user if the authentication parameter is between the values of the first and second thresholds.

**[0027]** Requesting additional authentication data may comprise requesting at least one of: requesting and receiving the same authentication data through the same communication channel; requesting and receiving the same authentication data through a different communication channel; requesting and receiving different authentication data through the same communication channel; and requesting and receiving different authentication data through a different communication channel.

**[0028]** Received or stored biometric authentication data may comprise processed data extracted from or a function of biometric authentication data.

**[0029]** The processed data may comprise biometric authentication data that has been encrypted or subjected to a cryptographic hash function.

**[0030]** In accordance with certain embodiments of the present invention, the method further comprises setting at least one of the first and second thresholds according to a determined false error rate or a determined false positive rate.

**[0031]** The false negative rate may indicate a rate at which it is determined, in error, to refuse to authenticate a user. The false positive rate may indicate a rate at which it is determined, in error, not to refuse to authenticate a user.

**[0032]** According to a second aspect of the present invention there is provided an authentication server arranged to: receive biometric authentication data from a user via a communication channel; determine an authentication parameter by comparing the biometric authentication data to stored biometric authentication data; compare the authentication parameter to first and second thresholds; and determine, based on the result of the comparison, whether to refuse to authenticate the user, to authenticate the user, or to request additional authentication data from the user.

**[0033]** The authentication server may be further arranged to implement the above method.

**[0034]** There is also disclosed a biometric authentication method, the method comprising: receiving biometric authentication data from a user via a communication channel; determining an authentication parameter by comparing the biometric authentication data to stored biometric authentication data; determining a first threshold and a second threshold; comparing the authentication parameter to the first and second thresholds; and determining, based on the result of the comparison, whether to refuse to authenticate the user, to authenticate the user, or to request additional authentication data from the user; wherein determining the first and second threshold comprises setting one of the first and second thresholds according to one of a currently recorded false negative rate and a currently recorded false positive rate.

**[0035]** Setting one of the first and second thresholds according to one of a currently recorded false negative and a currently recorded false positive rate may comprise obtaining information regarding a number of false negatives (or false positives) associated with the current first and second thresholds; and adjusting at least one of the current first and second thresholds based on the obtained information.

**[0036]** Setting one of the first and second thresholds may further comprise adjusting at least one of the current first and second thresholds based on information regarding a number of false negatives (or false positives) associated with previously-used first and second thresholds.

**[0037]** The information may be obtained by recording information regarding previous performances of the authentication method where a false error or a false positive occurred for the associated first and second thresholds.

**[0038]** There is also disclosed an authentication server arranged to implement this further biometric authentication method.

**[0039]** Another aspect of the invention provides a computer program comprising instructions arranged, when executed, to implement a method in accordance with any one of the above-described aspects. A further aspect provides machine-readable storage storing such a program.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0040]** Embodiments of the invention are further described hereinafter with reference to the accompanying drawings, in which:

Figure 1 graphically shows the proportion of authentication attempts which result in a false-negative or false-positive result for a certain threshold value in a simulated authentication system;

Figure 2 shows how ranges of threshold values may be allocated to certain zones defined by a first and second threshold in accordance with an embodiment of the present invention;

Figure 3 shows graphically how a first and second threshold can be used to partition off ranges of thresholds and so modify the proportion of false-negative results for certain threshold values in accordance with an embodiment of the present invention;

Figure 4 schematically illustrates an authentication system in accordance with an embodiment of the present invention; and

Figure 5 is a flowchart illustrating a method of performing authentication according to an embodiment of the present invention.

## DETAILED DESCRIPTION

**[0041]** In the following, the result of an authentication attempt is defined as a degree of correlation or a "score", each of which may be represented by a single value. This value relates to a measure of success of an authentication attempt, where success results in authentication into the authentication system.

**[0042]** Embodiments of the present invention intend to decrease or mitigate the rate and volume of false-negatives through application of a technique which may be referred to as "Grey Zone Logic" (GZL).

**[0043]** In typical authentication systems the use of a threshold creates a binary system in which the result of an authentication attempt either passes of fails. The application of GZL creates a third outcome wherein an authentication attempt does not pass or fail outright, but prompts a further authentication attempt. In certain embodiments, GZL is applied by designating a range of threshold values (or indicators of a degree of correlation, or score values) as a grey zone. This grey zone may be described as non-deterministic, in that an authentication attempt does not pass or fail if the authentication result (or its related degree of correlation or score) corresponds to a score value within the grey zone (that is, the authentication result corresponds to the grey zone). A score value within the grey zone, if subjected to conventional authentication processing, may correspond to a pass or a fail: it may fall either side of a single threshold, as shown in Figure 1.

**[0044]** When an authentication result provided in a first authentication method falls within the grey zone, GZL is instigated based on predefined contingency rules. The rules may be designed to invoke other methods of authentication that replace the first authentication method, or they may invoke other methods of strong authentication that augment the first authentication method, or they may involve repeated application of the first authentication method.

**[0045]** Figure 2 shows how a grey zone may be implemented in an example authentication system.

**[0046]** In Figure 2, a false-negative curve 220 and a false-positive curve 230 are shown. Note that there is no requirement as to which curve is which, as evidenced by the lack of axis labels or quantities on the axes of the figure, and so they may be switched. A first threshold 245 and a second threshold 255 are defined, represented in Figure 2 as vertical lines. The first threshold has the effect of defining a first area 240, which encompasses the area to the left of the first threshold 245 of Figure 2. The second threshold has the effect of defining a second area 160, which encompasses the area to the right of the second threshold 255 Figure 2. Between the two thresholds is defined a third area known hereafter

as the grey zone 250. The existence of the grey zone 250 relies on the first threshold 245 being distinct from the second threshold 255.

**[0047]** The designation between the first threshold 245 and the second threshold 255 is not strict and the terms could easily be swapped between the two vertical lines in Figure 2. That is, noting the EER 210 of Figure 2, there is no requirement for the first threshold 245 to be located to the left of the EER 210 and there is no requirement for the second threshold 255 to be located to the right of the EER 210. The same considerations apply to the designated first area 240 and second area 260.

**[0048]** In the system represented in Figure 2, the first area 240 may be used to define a fail zone. The first area 240 would therefore span a range of score values which are considered to correspond to failed authentication attempts. That is, if an authentication result score corresponds to a score value within the first area 240, then the associated authentication attempt has failed.

**[0049]** The second area 260 may therefore be used to define a pass zone. The second area 260 would therefore span another range of score values which are considered to correspond to passed authentication attempts. That is, if an authentication result score corresponds to a score value within the second area 260, then the associated authentication attempt has passed.

**[0050]** In the example of Figure 2 the first area 240 and the second area 260 are defined as the fail zone and pass zone respectively. However in other embodiments the first area 240 may be defined as the pass zone and the second area 260 may be defined as the fail zone instead. In such as embodiment it may be that the false-negative curve 220 and the false-positive curve 230 are defined differently to the above.

**[0051]** In Figure 2, the first threshold 245 and the second threshold 255 have been defined such that the grey zone 250 is located about the EER 210. It should be noted that this is merely one disposition of the grey zone 250 and that there is no requirement for the grey zone 250 to relate to the position of the EER 210 or even to either of or both of the false-negative curve 220 and false-positive curve 230. That is, a grey zone may be defined independently of other factors in the authentication system, or the disposition of the grey zone may rely on one or more factors in the authentication system. The location of a singular threshold and the grey zone will now be discussed with reference to Figure 3 and Figure 4.

**[0052]** Referring back to Figure 1, as discussed above it can be seen that there exist threshold scores where the error caused by either false-negatives or false-positives is

essentially 100%. As may be expected, these threshold scores also correspond to essentially 0% error caused by false-positives or false-negatives respectively.

**[0053]** A single threshold 110 is defined in Figure 1 and is located at the EER of the authentication system. At this point, the errors caused by false-negatives and false-positives is approximately 6% each, resulting in a total error of approximately 12%. For the specific authentication system giving rise to the results shown in Figure 1, this can be viewed as providing the most efficient system. That is, adjusting the threshold 110 to the left or to the right will not decrease the total amount of error to lower than 12%. For example, shifting the threshold 110 to a threshold value of '0.4' would result in a combined error of approximately 22%. Figure 1 therefore demonstrates the limitations of a system utilizing only a single threshold.

**[0054]** Referring now to Figure 3, this is a graphical representation of an embodiment of the present invention wherein a first threshold 310 and a second threshold 320 have been defined for an authentication system similar to that giving rise to the results of Figure 1.

**[0055]** In Figure 3, the first threshold 310 has been defined near the threshold value of '0.2'. This is located to the left of the EER value shown in Figure 1, which was located at a threshold value of approximately '0.3'. The second threshold 320 has been defined near the threshold value of approximately '0.575'. This is located to the right of the EER value shown in Figure 1. This defines a grey zone 330 that is therefore similar to that shown in Figure 2 where the grey zone 250 was defined around the EER 210. However, note that in Figure 3 the grey zone 330 extends around the EER to different extents than that shown in Figure 2, demonstrating the configurability of the present invention.

**[0056]** The first threshold 310 and the second threshold 320 also serve to define a fail zone and a pass zone. In the embodiment represented in Figure 3, the area to the left of the first threshold 310 may be defined as the fail zone, and the area to the right of the second threshold 320 may be defined as the pass zone. Authentication attempts corresponding to authentication results which fall into the fail zone or pass zone are, respectively, failed or passed.

**[0057]** The definition of the grey zone 330 in Figure 3 has been made according to a technique in accordance with an embodiment of the present invention, which may be referred to as "Dynamic Contingency Processing" (DCP). DCP determines where the first threshold 310 and the second threshold 320 are located.

**[0058]** With DCP, the first threshold 310 (or the low-boundary of the grey zone 330) is located at the point (threshold score value) where the error related to false-negatives is approximately zero, or just begins to exceed zero (or just before it begins to exceed zero).

This means that all authentication results which would previously have resulted in a false-negative – were a singular threshold to have been defined at the location of the first threshold 310 – will now trigger a contingency rule. Said contingency rule may require further authentication from a user, using a separate of the same authentication system. In this manner, a genuine or legitimate user may be authenticated while a fraudulent or illegitimate user is not authenticated.

**[0059]** As seen in Figure 3, the false-negative curve is truncated at the second threshold 410 to reflect that false-negatives are now unlikely to occur in this system. However it should be apparent that a legitimate user may still not be authenticated if they perform an authentication attempt where the authentication result corresponds to a very low threshold score, that is, one that does not exceed even the first threshold 310. Such an authentication result may occur if, to use the example of a voice-based system, the user making the authentication attempt is unwell or if there is a fault with the voice detection apparatus. Certain embodiments of the present may completely eliminate the problem of false-negatives in authentication systems, though the present invention is not limited to complete elimination. While shifting the first threshold 4310 to a lower threshold score (and so diverging from the DCP model) will enable these very low score legitimate authentication attempts to correspond to the grey zone 330, this will reduce the efficiency of the method by increasing the number of additional or secondary authentication attempts. Were the grey zone for an authentication system made large enough, it should be obvious that the authentication system becomes effectively redundant as most or all authentication attempts would result in an additional or secondary authentication attempt.

**[0060]** With DCP, the second threshold 320 (or the high-boundary of the grey zone 330) may be located at the point where the error related to false-positives is approximately zero, or begins to exceed zero. By setting the second threshold 320 in this way, the method aims to pass as many legitimate user authentication attempts as possible without passing any illegitimate users. That is, by identifying a threshold score value above which it is unlikely that a false-positive will occur, the second threshold 320 can be set such that all authentication results corresponding to scores above this value are passed.

**[0061]** In the above, the skilled person would appreciate that which is intended by locating a threshold at a point where a false-negative error rate or a false-positive error rate is approximately zero. That is, this may involve identification of a threshold setting which corresponds to a particular value (for example: 1%, 2%, 5% etc.) representing an acceptable (or, at least, tolerated) proportion of authentication attempts which result in a false negative or false positive situation. This threshold setting or value may be identified

through simulations of similar authentication systems which do not employ DCP, or from other recorded data.

**[0062]** However, it should be apparent that an illegitimate user may still be authenticated if they make an authentication attempt where the authentication result is above the second threshold 320. These occurrences may be further mitigated by moving the second threshold 320 to a higher threshold score value; however this will have the effect of increasing the number of additional or secondary authentication attempts and so reduce the efficiency of the authentication system.

**[0063]** However, it should be noted that only one of the first threshold 310 or the second threshold 320 may be defined as described above when using DCP. That is, DCP may be used to define only one of the two thresholds, allowing the other threshold to be defined separately in another manner. This would allow, to use an example as described above, the second threshold 320 to be set at an even higher value resulting in a stricter system in which fewer authentication attempts will be located in the pass zone and more in the grey zone.

**[0064]** Alternatively, at least one of the thresholds could be defined in a dynamic manner. For example, if the authentication system is configured to record data corresponding to the number of false-positives and false-negatives that occur (this may be a real authentication system which is in use as opposed to further simulations) then this data could be incorporated into deciding where the thresholds are located. This data may additionally take into account times of day, amount of user authentication attempt, location of a user making an authentication attempt etc. Additionally, this data may be used in combination with DCP such that the first threshold and the second threshold are dynamically set according to the number of false-negatives and false-positives recorded by the authentication system. In such an authentication system and using DCP as described above, this may be accomplished by requiring the system to lower the first threshold whenever a false-negative is recorded and raise the threshold whenever a false-positive is recorded (to use the example of Figure 1 where higher threshold values reflect larger proportions of false-negatives).

**[0065]** Setting one of the first and second thresholds in this manner may comprise obtaining recorded data for false negative or false positive rates for a current first threshold and second threshold (that is, the currently-defined grey zone), and adjusting one of the current first threshold and second threshold according to the obtained recorded data.

**[0066]** Alternatively or additionally, setting one of the first and second thresholds may also comprise taking into account data which was previously recorded for other first and second thresholds (that is, previously-defined grey zones).

**[0067]** Dynamically setting at least one of the first and second thresholds in combination with DCP may thereby allow dynamic modification of the extent of the grey zone. That is, the upper and lower boundaries of the grey zone may be adjusted according to the numbers of false negative and/or false positives occurring certain first and second thresholds. This tuning of the grey zone – which may occur continuously (that is, the dynamic setting may occur in the background by monitoring for any new false positive or false negative occurrences and altering a threshold as appropriate) – can allow for control of the number of additional or secondary authentication attempts which may result from authentication parameters from otherwise-legitimate or otherwise-fraudulent authentication attempts falling within the grey zone. That is, the burden on the system resulting from these additional authentication attempts may be relieved, albeit in a manner which still aims to reduce at least one of the false negative rate and the false positive rate.

**[0068]** The recorded data may be from known instances where a false negative is determined to have occurred. For example, a false negative may be determined to have occurred if additional authentication data is requested from a user, and it is determined to authenticate the user on the basis of this additional authentication data. That is, in this instance, the user, although being legitimate according to the additional authentication data, was not authenticated on the basis of the authentication data they initially provided, indicating that the relevant threshold may have been set too high. Alternatively, an occurrence of a false negative may be recorded as a result of feedback from a legitimate user.

**[0069]** Similarly, the recorded data may also be from known instances where a false positive has occurred. For example, a false positive may be determined to have occurred if it is determined that fraudulent activity occurred in association with a successful authentication attempt. The skilled person will appreciate how fraudulent activity may be determined to occur, whether by manual reporting on the part of a legitimate user, automatic detection by a monitoring system, or some other suitable means.

**[0070]** Alternatively, the recording of a certain number of false-negatives or false-positives may be required before any changes to the first threshold or second threshold occur.

**[0071]** Referring now to Figure 4, this schematically illustrates an authentication system in accordance with an embodiment of the present invention. The authentication system may comprise an authentication server 400 and a user 402. In order to authenticate the user 402 to the authentication server 400 the user sends biometric authentication data to the authentication server 400 across a first communication channel 404. The server 400 is arranged to compare the received authentication data to stored authentication data and to

determine a degree of correlation, which is then compared to first and second thresholds as discussed above. As a result of the comparison, the authentication server 400 may determine that additional authentication data is required, and may send a request to the user for additional information either across the first communication channel 404 or across a second communication channel 406. Alternatively, a message indicating successful or unsuccessful authentication may be sent. In accordance with other embodiments of the invention the user's biometric authentication data may be transmitted indirectly from the user to the server. For instance, where biometric authentication is used to secure access to a financial transactions server the user may communicate only with the financial transactions server which may forward biometric authentication data to the authentication server. The authentication server may in return send the result of the authentication or any request for additional authentication data via the financial services server.

**[0072]** Referring now to Figure 5, this illustrates in the form of a flowchart a method of performing authentication according to an embodiment of the present invention as described above. At step 500 the server receives biometric authentication data from a user. At step 502 the server retrieves stored biometric authentication data. This may be locally stored or it may be retrieved from another server (not shown in Figure 4). In accordance with certain embodiments of the present invention the received and stored biometric authentication data may comprise raw authentication data. For the example of voice authentication this may comprise raw audio recordings. However, in preferred embodiments the raw authentication data is not stored. Instead, a processed version of the authentication is stored, which may take the form of a voice print in which data which uniquely characterises a user's voice is retained. Furthermore, in certain embodiments of the present invention voice print data may be stored in an encrypted form or subjected to a one way hash to avoid the risk of a user's voice print being compromised. For the received biometric authentication data the processing to generate characterising data and/or encrypting or hashing may be performed before transmission to the server.

**[0073]** At step 504 the received biometric authentication data and the stored biometric authentication data are compared to determine an authentication parameter. At step 506 the authentication parameter is compared to a first threshold, and if the authentication parameter is below the first threshold then the authentication is refused at step 508. Alternatively, if the authentication parameter is above the first threshold then at step 510 the authentication parameter is compared to a second threshold. If the authentication parameter is above the second threshold then the user is authenticated at step 512. Otherwise at step 514 additional authentication data is requested from the user.

**[0074]** It will be appreciated that where additional authentication data is requested from the user, this may comprise the same type of biometric authentication data as the original authentication data, or it may be any other type of authentication data. For the example of voice authentication, it may be that the user is requested to provide another sample of the same word or phrase, or a different word or phrase. In some embodiments increased security is achieved by requesting additional authentication data across a different channel to the originally used channel.

**[0075]** Throughout the description and claims of this specification, the words "comprise" and "contain" and variations of them mean "including but not limited to", and they are not intended to (and do not) exclude other components, integers or steps. Throughout the description and claims of this specification, the singular encompasses the plural unless the context otherwise requires. In particular, where the indefinite article is used, the specification is to be understood as contemplating plurality as well as singularity, unless the context requires otherwise.

**[0076]** Features, integers or characteristics described in conjunction with a particular aspect, embodiment or example of the invention are to be understood to be applicable to any other aspect, embodiment or example described herein unless incompatible therewith.

**[0077]** It will be also be appreciated that, throughout the description and claims of this specification, language in the general form of "X for Y" (where Y is some action, activity or step and X is some means for carrying out that action, activity or step) encompasses means X adapted or arranged specifically, but not exclusively, to do Y.

**[0078]** Features, integers or described in conjunction with a particular aspect, embodiment or example of the invention are to be understood to be applicable to any other aspect, embodiment or example described herein unless incompatible therewith. All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive. The invention is not restricted to the details of any foregoing embodiments. The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.

The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

**CLAIMS:**

1. A biometric authentication method, the method comprising:

receiving biometric authentication data from a user via a communication channel;

determining an authentication parameter by comparing the biometric authentication data to stored biometric authentication data;

comparing the authentication parameter to first and second thresholds; and

determining, based on the result of the comparison, whether to refuse to authenticate the user, to authenticate the user, or to request additional authentication data from the user.

2. The method of claim 1, wherein the requesting additional authentication data comprises requesting additional biometric authentication data.

3. The method of claim 2, further comprising:

receiving additional biometric authentication data from a user via a communication channel;

determining a second authentication parameter by comparing the biometric authentication data to stored biometric authentication data;

comparing the second authentication parameter to the first and second thresholds; and

determining, based on the comparison, whether to refuse to authenticate the user or to authenticate the user.

4. The method of any preceding claim, wherein the biometric authentication data or the additional biometric authentication data comprises voice biometric data or face-recognition biometric data

5. The method of any preceding claim, further comprising determining to request additional authentication data from the user if the authentication parameter is between the values of the first and second thresholds.

6. The method of any preceding claim, wherein requesting additional authentication data comprises requesting at least one of:

requesting and receiving the same authentication data through the same communication channel;

requesting and receiving the same authentication data through a different communication channel;

requesting and receiving different authentication data through the same communication channel; and

requesting and receiving different authentication data through a different communication channel.

7. The method of any preceding claim, wherein received or stored biometric authentication data comprises processed data extracted from or a function of biometric authentication data.

8. The method of claim 7, wherein the processed data is comprises biometric authentication data that has been encrypted or subjected to a cryptographic hash function.

9. An authentication server arranged to:

receive biometric authentication data from a user via a communication channel;

determine an authentication parameter by comparing the biometric authentication data to stored biometric authentication data;

compare the authentication parameter to first and second thresholds; and

determine, based on the result of the comparison, whether to refuse to authenticate the user, to authenticate the user, or to request additional authentication data from the user.

10. An authentication server according to claim 9, wherein the authentication server is further arranged to implement the method of any one of claims 2 to 8.

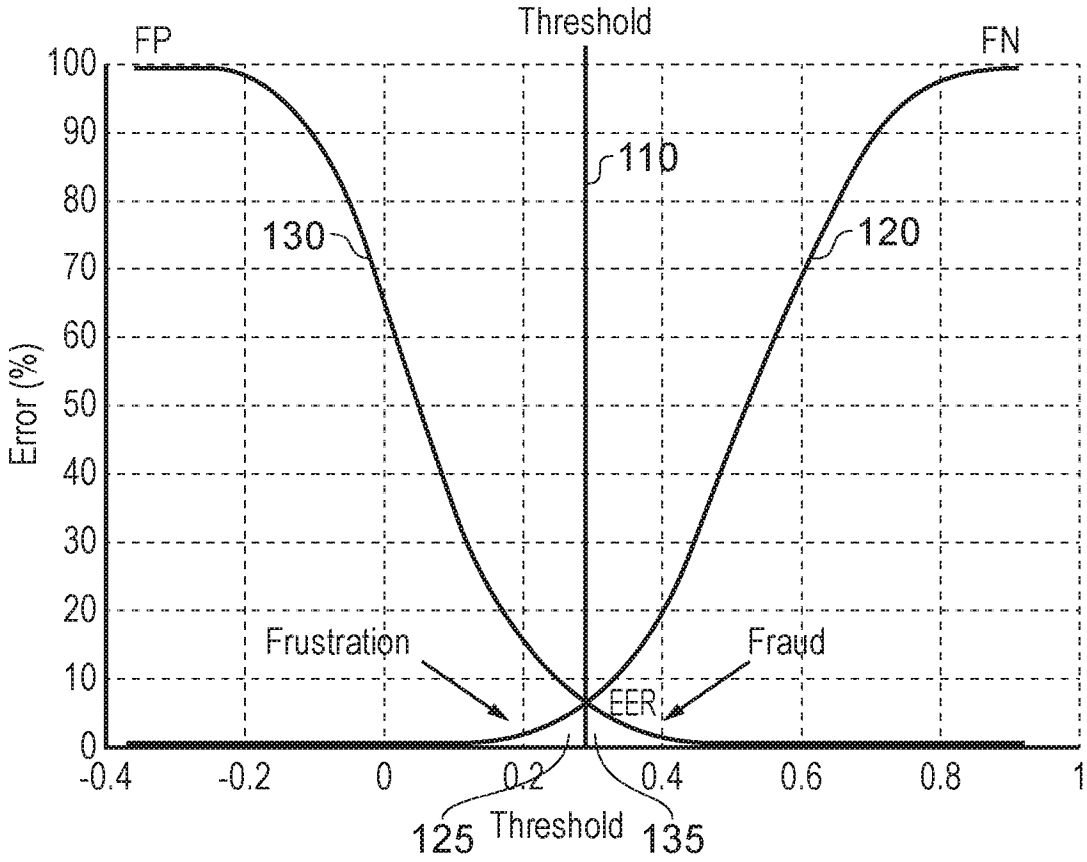
FP
Threshold
FN
100
90
80
70
60
50
40
30
20
10
0
Error (%)
110
130
120
Frustration
Fraud
EER
-0.4
-0.2
0
0.2
0.4
0.6
0.8
1
125
Threshold
135

FIG. 1

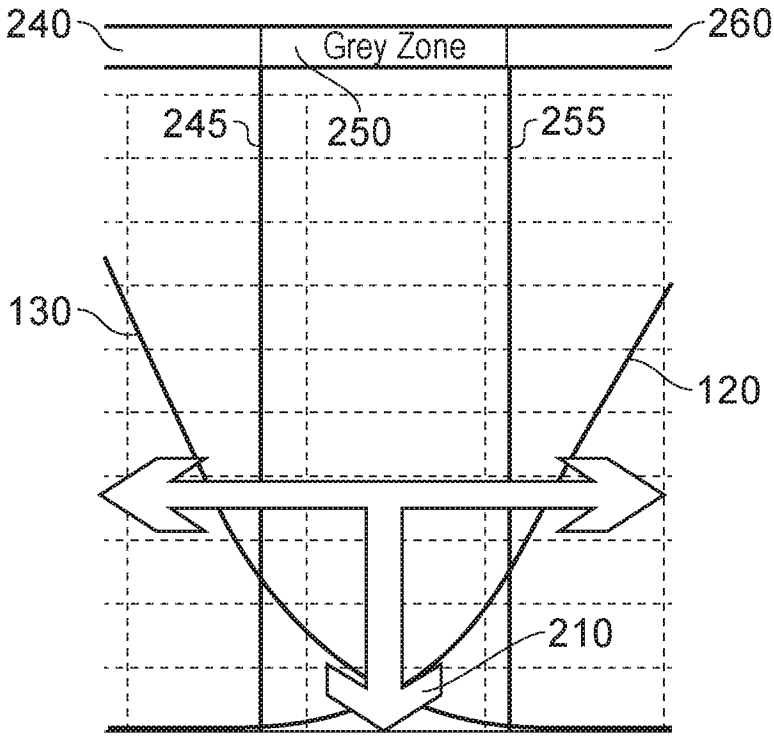
240
260
Grey Zone
245
250
255
130
120
210

FIG. 2

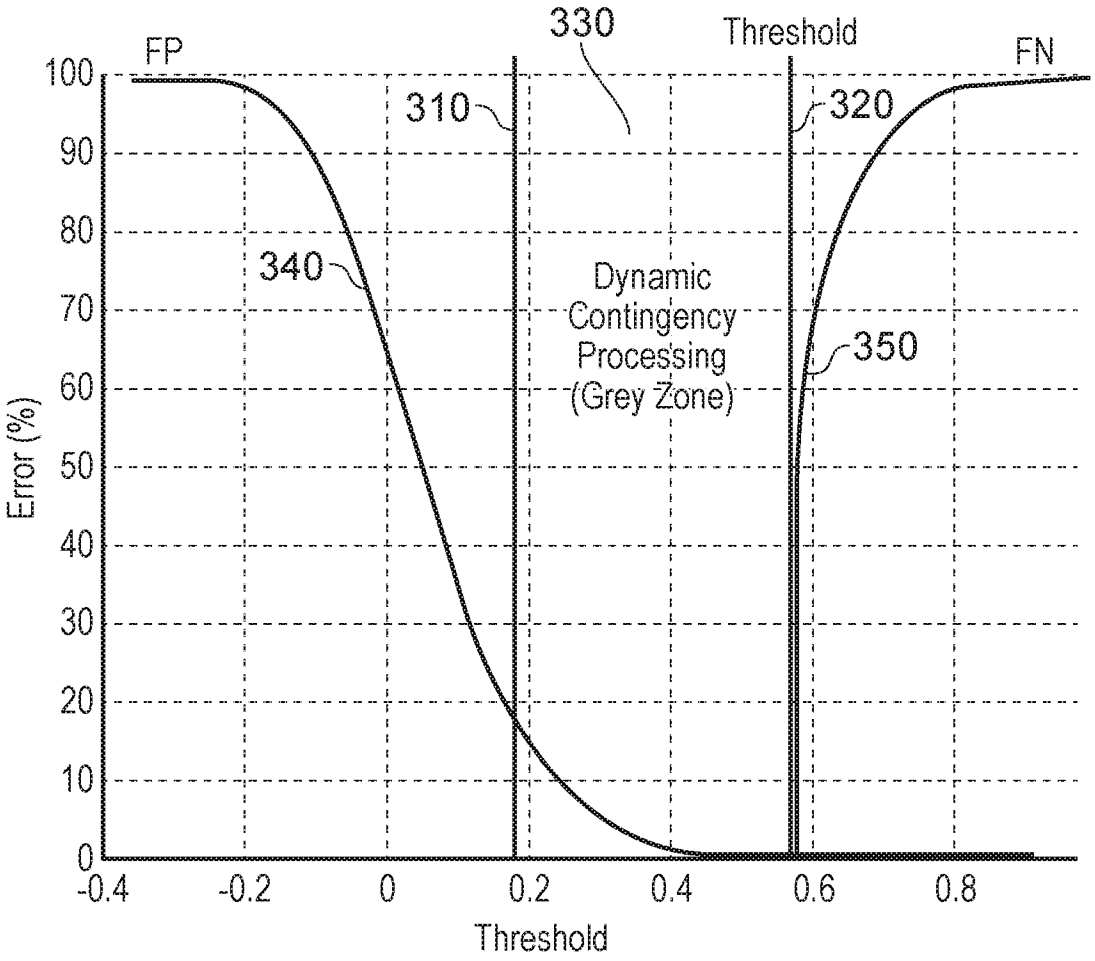
FP
330
Threshold
FN
310
320
340
Dynamic
Contingency
Processing
(Grey Zone)
350
Error (%)
100
90
80
70
60
50
40
30
20
10
0
-0.4
-0.2
0
0.2
0.4
0.6
0.8
Threshold

FIG. 3

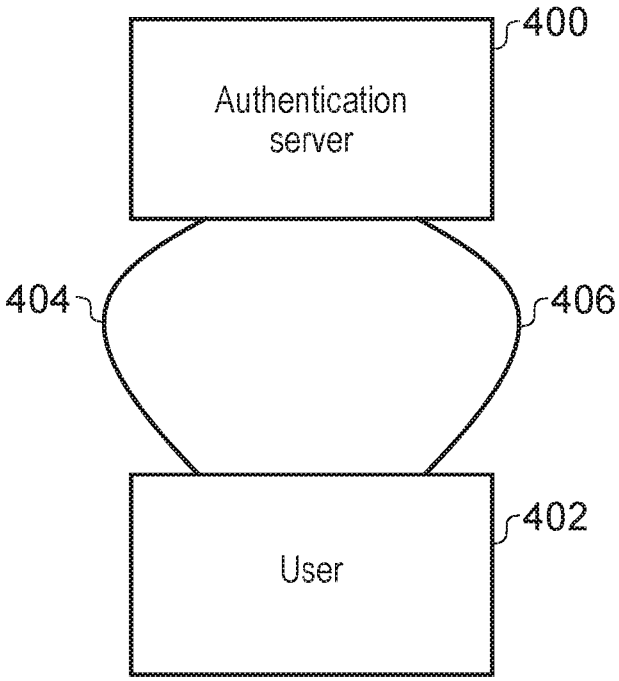


FIG. 4

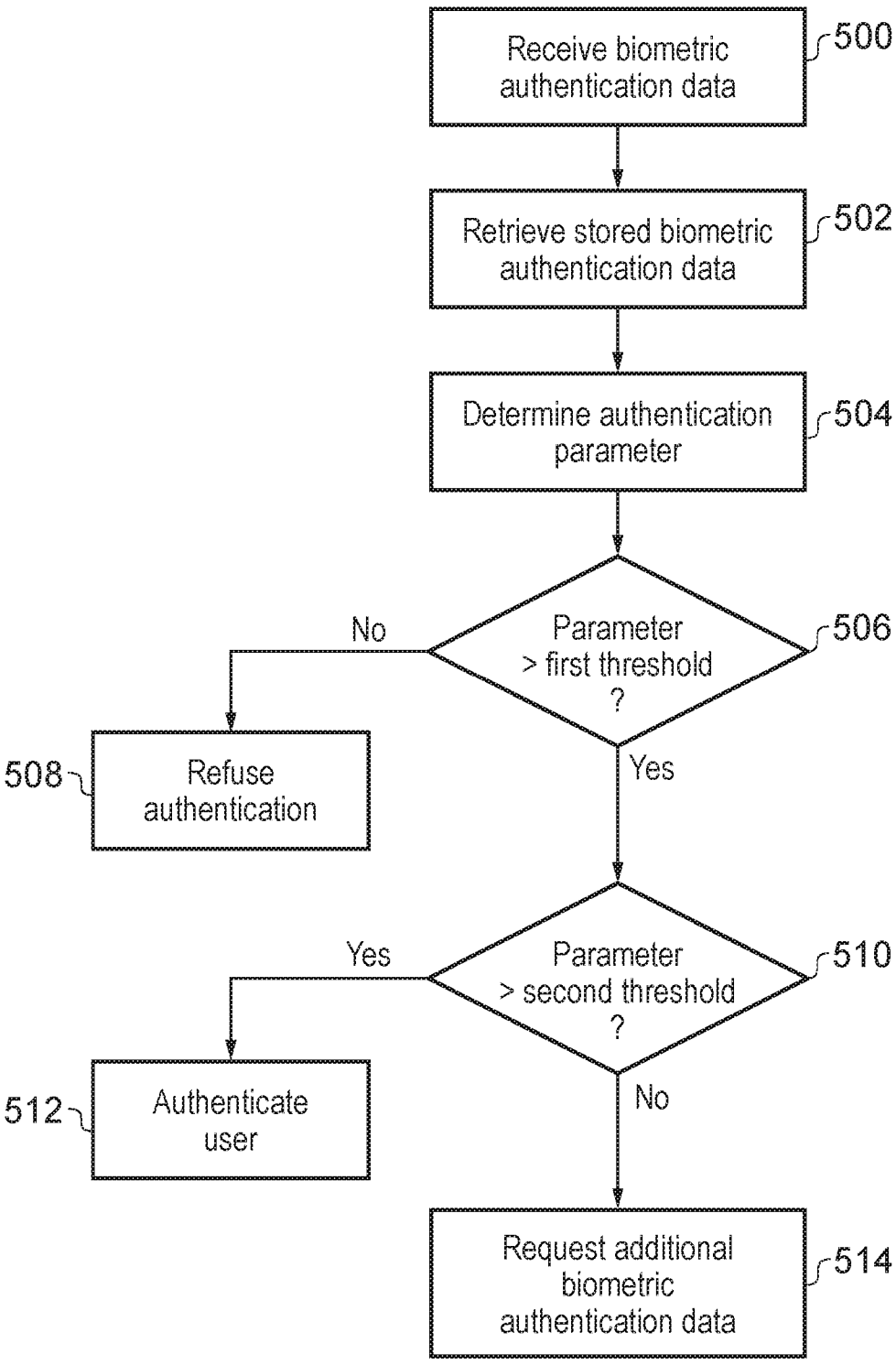
Receive biometric authentication data
500
Retrieve stored biometric authentication data
502
Determine authentication parameter
504
Parameter > first threshold ?
506
No
Yes
508
Refuse authentication
Parameter > second threshold ?
510
Yes
No
512
Authenticate user
Request additional biometric authentication data
514

FIG. 5

# INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2015/051915

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L9/32
ADD.

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)
H04L

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)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | US 7 007 298 B1 (SHINZAKI TAKASHI [JP] ET AL) 28 February 2006 (2006-02-28)<br>column 6, line 59 - column 7, line 5<br>column 10, line 34 - line 54<br>column 17, line 18 - line 20 | 1,2,4,<br>7-10 |
| Y | EP 1 645 990 A2 (FUJITSU LTD [JP])<br>12 April 2006 (2006-04-12)<br>paragraph [0080]<br>paragraph [0085] | 1,2,4,<br>7-10 |
| Y | US 2008/209227 A1 (VENKATESAN RAMARATHNAM [US] ET AL) 28 August 2008 (2008-08-28)<br>paragraph [0026] | 8 |
| A | US 2007/136792 A1 (TING DAVID M [US] ET AL) 14 June 2007 (2007-06-14)<br>paragraph [0033]<br>paragraph [0039] | 1,4,9,10 |

☐ 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 application or patent but 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 | Date of mailing of the international search report |
|---|---|
| 7 October 2015 | 16/10/2015 |

| Name and mailing address of the ISA/ | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016 | Tenbieg, Christoph |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2015/051915

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 7007298 B1 | 28-02-2006 | JP 2000259278 A | 22-09-2000 |
| | | US 7007298 B1 | 28-02-2006 |
| EP 1645990 A2 | 12-04-2006 | EP 1645990 A2 | 12-04-2006 |
| | | JP 4340618 B2 | 07-10-2009 |
| | | JP 2006107340 A | 20-04-2006 |
| | | KR 20060046619 A | 17-05-2006 |
| | | US 2006078177 A1 | 13-04-2006 |
| US 2008209227 A1 | 28-08-2008 | TW 200843445 A | 01-11-2008 |
| | | US 2008209227 A1 | 28-08-2008 |
| | | WO 2008106336 A1 | 04-09-2008 |
| US 2007136792 A1 | 14-06-2007 | NONE | |