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

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
9 October 2014 (09.10.2014)

WIPO | PCT

(10) **International Publication Number**
WO 2014/163819 A1

(51) **International Patent Classification**:
H04L 9/08 (2006.01) ***H04L 9/32*** (2006.01)
G06F 21/32 (2013.01)

(21) **International Application Number**:
PCT/US2014/017314

(22) **International Filing Date**:
20 February 2014 (20.02.2014)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:
61/776,551 11 March 2013 (11.03.2013) US

(71) **Applicant**: **LOCKHEED MARTIN CORPORATION** [US/US]; 6801 Rockledge Drive, Bethesda, MD 20817 (US).

(72) **Inventors**: **HRYBYK, Alexander, Gregory**; 8367 Williamstowne Drive, Millersville, MD 21108 (US). **COCKRUM, Chris, K.**; 4501 Mainfield Avenue, Baltimore, MD 21214 (US).

(74) **Agents**: **KERN, John, S.** et al.; Oblon, Spivak, McClelland, Maier & Neustadt, L.L.P, 1940 Duke Street, Alexandria, VA 22314 (US).

(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, LT, 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, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, 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).

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

[Continued on next page]

(54) **Title**: BIOMETRIC TEMPLATE PROTECTION USING ERROR CORRECTION CODING

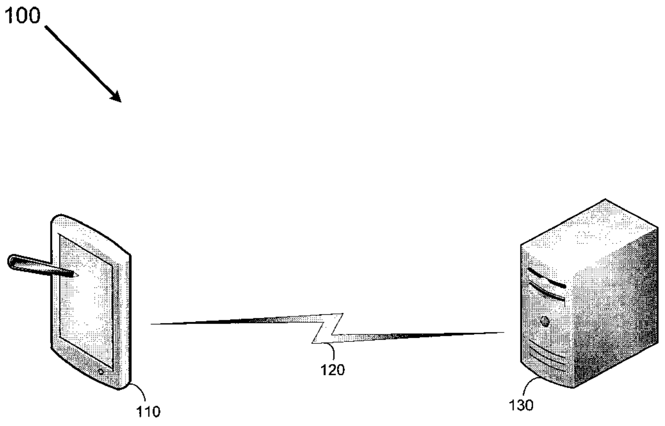

FIG. 1

(57) **Abstract**: Methods and systems for providing gesture-based security are disclosed. For example, a method for establishing secure communications can include receiving one or more human gestures using a sensor on a first device, quantizing the one or more human gestures so as to create a metric of the one or more human gestures, performing an error correction operation on the metric using error correction information derived from a template of the metric to create a corrected metric, performing a hashing operation on the corrected metric to create a metric hash, and comparing the metric hash to a hash of the template to verify that the one or more human gestures sufficiently conform to the template.

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

BIOMETRIC TEMPLATE PROTECTION USING ERROR CORRECTION CODING

INCORPORATION BY REFERENCE

[0001] This application claims the benefit of U.S. Provisional Application No. 61/776,551 entitled "Gesture-initiated Encryption Algorithm using Forward Error Correction" filed on March 11, 2013, the content of which is incorporated herein by reference in its entirety.

BACKGROUND

[0002] The background description provided herein is for the purpose of generally presenting the context of the disclosure. Work of the presently named inventors, to the extent the work is described in this background section, as well as aspects of the description that may not otherwise qualify as prior art at the time of filing, are neither expressly nor impliedly admitted as prior art against the present disclosure.

[0003] A password is a commonly used starting point for an encryption key. Since a password is typically familiar to a user and will not change in the immediate future, it can be hashed and stored on a medium to essentially hide it in plain sight. The amount of entropy in a password can be very low if the password is not of significant complexity and length. While one can simply increase the length and complexity of a password to increase its entropy, the tradeoff is that longer and more complex passwords are harder to remember. Hence, people typically choose simpler passwords which are easily cracked.

SUMMARY

[0004] Various aspects and embodiments of the invention are described in further detail below.

[0005] In an embodiment, a method for establishing secure communications includes receiving one or more human gestures using a sensor on a first device, quantizing the one or more human gestures so as to create a metric of the one or more human gestures, performing an error correction operation on the metric using error correction information derived from a template of the metric to create a corrected metric, performing a hashing operation on the corrected metric to create a metric hash, and comparing the metric hash to a hash of the template to verify that the one or more human gestures sufficiently conform to the template.

[0006] In another embodiment, a method for creating a password includes receiving a set of one or more human gestures using a sensor on a first device a plurality of times to create a plurality of entries, wherein for each entry the one or more human gestures generally conform with one another, quantizing each entry to create a plurality of metric entries, and deriving a template using the plurality of metric entries such that the template is a statistical amalgam of the plurality of metric entries.

[0007] In yet another embodiment, a device for establishing secure communications includes quantizing circuitry configured to quantize one or more human gestures so as to create a metric of the one or more human gestures, error correction circuitry configured to perform an error correction operation on the metric using error correction information derived from a template of the metric to create a corrected metric, hashing circuitry configured to perform a hashing operation on the corrected metric to create a metric hash, and verification circuitry configured to compare the metric hash to a hash of the template to verify that the one or more human gestures sufficiently conform to the template.

[0008] In yet another embodiment, a device for creating a password includes a sensor capable of deriving a set of one or more human gestures a plurality of times to create a plurality of entries, wherein for each entry the one or more human gestures generally conform with one another, quantizing circuitry configured to quantize each entry so as to create a plurality of metric entries, and template circuitry configured to derive a template using the plurality of metric entries such that the template is a statistical amalgam of the plurality of metric entries.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] Various embodiments of this disclosure that are proposed as examples will be described in detail with reference to the following figures, wherein like numerals reference like elements, and wherein:

[0010] FIG. 1 is a wireless system capable of providing a secure log-in using a graphic-based password system.

[0011] FIGs. 2A and 2B depict different hashes that result from minor variances of similar hand-drawn gestures.

[0012] FIG. 3 is a block diagram of a user terminal capable of deriving a gesture-based password, and for securely logging onto a system using human-based gestures.

[0013] FIG. 4 is a block diagram of a server capable of receiving and verifying a gesture-based password.

[0014] FIG. 5 is a flowchart for creating an invariant password from variant gestures.

[0015] FIG. 6 is a flowchart for securing access to a system using a gesture-based password.

[0016] FIG. 7 depicts an analysis of false positives using gesture-based passwords.

[0017] FIG. 8 depicts an analysis of false negatives using gesture-based passwords.

[0018] FIG. 9 depicts a performance analysis of gesture-based passwords.

DETAILED DESCRIPTION OF EMBODIMENTS

[0019] The disclosed methods and systems below may be described generally, as well as in terms of specific examples and/or specific embodiments. For instances where references are made to detailed examples and/or embodiments, it is noted that any of the underlying principles described are not to be limited to a single embodiment, but may be expanded for use with any of the other methods and systems described herein as will be understood by one of ordinary skill in the art unless otherwise stated specifically.

[0020] FIG. 1 depicts a communication system 100 usable to provide secure communications using a gesture-based password. As shown in FIG. 1, the communication system 100 includes a user terminal 110 coupled to a server 130 via an electronic communications link 120. While the user terminal 110 depicted in Fig. 1 is a tablet computer having a wireless interface, it is to be appreciated that the communication device 110 can take a large number of forms, including any of a large number of smart phones, tablets, laptop computers and other computers as long as such forms include an appropriate set of sensors, such as a touch screen, capable of sensing/measuring human gestures.

[0021] While the communication system 100 of FIG. 1 is depicted as a two-part system, in various embodiments the techniques described below can be applied so as to provide passwords for the user terminal 110 alone such that a user can secure access to his tablet computer, smart phone or other device.

[0022] FIGs. 2A and 2B depict different hashes that result from minor variances of similar hand-drawn gestures. Hashing is a well-known technique for storing passwords while minimizing the probability that individual passwords will be exposed to theft. As shown on the left-hand sides of both FIGs. 2A and 2B, a hand-drawn letter "A" is provided with small differences between the two. As also shown in FIGs. 2A and 2B, quantizing and hashing each entry of the letter "A" results in completely different hash values, thereby making hand-drawn gestures an unlikely candidate for passwords given that humans can rarely, if ever, exactly reproduce a drawn gesture. However, in order to form an invariant hash, the information extracted from the gesture must be 100% exact. To address the reproducibility issue, as will be explained below, a Forward Error Correction (FEC) algorithm can be used to correct small amounts of error in feature vectors extracted from a gesture to produce an invariant key/password that can be used for encryption and/or access.

[0023] FIG. 3 is a block diagram of the user terminal 110 of FIG. 1 capable of securely accessing data using human-drawn gestures. As shown in FIG. 3, the user terminal 110 includes a processor 310, a memory 320, a sensor 330, quantizing circuitry 340, training circuitry 350, template circuitry 360, error coding circuitry 370, error correction circuitry 380, hashing circuitry 382, verification circuitry 384 and input/output circuitry 390.

[0024] Although the user terminal 110 of Fig. 3 uses a bussed architecture, it should be appreciated that any other architecture may be used as is well known to those of ordinary skill in the art. For example, in various embodiments, the various components 310-390 can take the form of separate electronic components coupled together via a series of separate busses. Still further, in other embodiments, one or more of the various components 310-390 can take form of separate processing systems coupled together via one or more networks. Additionally, it should be appreciated that each of components 310-390 advantageously can be realized using multiple computing devices employed in a cooperative fashion.

[0025] It also should be appreciated that some of the above-listed components 340-380 can take the form of software/firmware routines residing in memory 320 and be capable of being executed by the processor 310, or even software/firmware routines residing in separate memories in separate computing systems being executed by different controllers. Still further, it is to be appreciated that some of the above-listed components 340-380 can reside on a completely different platform, such as the server 130 of FIG. 1 or some other device.

[0026] In a first series of operations, the user terminal 110 can be used to create a gesture-based password than can be variant from user-entry to user-entry, yet for each user entry an invariant password and hash will be created. Under control of the processor 310, the sensor 330 can measure/receive one or more hand-drawn gestures of a user. Since a gesture's coordinates will likely vary slightly each time the user draws it, the gesture must first be quantized into discrete components to be manipulated.

[0027] Accordingly, the quantizing circuitry 340 is used to quantize gestures measured/received by the sensor 330. One possible approach to characterizing a gesture, which involves interpolation and discrete angle quantization, is provided below. However, the example below is just one of many possible quantization approaches, and therefore to be considered a non-limiting example.

[0028] A gesture, G, with N points can be described according to Eq. (1) below:

$$G = [x_i, y_i, t_i], \qquad i = [0, 1, 2, \ldots N\text{-}1]; \qquad \text{Eq.(1)}$$

where x_i and y_i are Cartesian coordinates for a point I, and t_i is a relative time occurrence for point i.

[0029] A given gesture can be interpolated to have a very large constant number of points, M >> N.

$$\hat{G} = [\hat{x}_j, \hat{y}_j, \hat{t}_j] \qquad j = [0, 1, 2, \ldots M\text{-}1]; \qquad \text{Eq.(2)}$$

[0030] The new interpolated gesture on M points can then be evenly grouped into a constant number (D) of secti$\hat{S}$ns such that:

$$\hat{S}_k = [\hat{x}_m, \hat{y}_m, \hat{t}_m] \qquad \text{Eq.(3)}$$

$$m = \lfloor kM/D, kM/D+1, kM/D+2, kM/D+n\ldots, kM/D+M/D-1 \rfloor \ \text{Eq.(4)}$$

$$k = [0,1,2,\ldots,D-1] \qquad \text{Eq.(5)}$$

$$n = [0,1,2,\ldots,M/D-1]$$

where $\hat{y}_j, \hat{x}_j, \hat{t}_j$ are averages of y_j, x_j and t_j for a pluralitiy of gesture entries.

[0031] For the purposes of this document, the set of sections developed by equations (1)-(5) are referred to as a “metric” of a gesture.

[0032] The angle $\theta_{k,m}$ between two points {m,m+*1*} in sections *k* is determined according to Eq.(6) below:

$$\theta_{k,m} = \tan^{-1}\left(\frac{\hat{S}_k[y_{m+1}] - \hat{S}_k[y_m]}{\hat{S}_k[x_{m+1}] - \hat{S}_k[x_m]}\right) \qquad \text{Eq.(6)}$$

[0033] Returning to FIG. 1, assuming that a user wishes to create a new gesture-based password, the training circuitry 350 first determines whether the pictogram created by a user is a suitable candidate for a password or encryption key. The criteria for such a determination can vary, but such criteria may include, for example, whether there pictogram is too simple, e.g., a single vertical line; whether the pictogram is too complex; and so on. Assuming that an acceptable pictogram is selected, the user can re-enter the pictogram N times so that the training circuitry can determine whether the pictogram can be reliably re-created by the user. The particular criteria for determining consistency can include, for example, whether angles between points consistently fall within an acceptable error range, whether a total angular error for all points is acceptable, and so on.

[0034] Assuming that the training circuitry 350 determines that a pictogram is acceptable and can be reliably reproduced, the template circuitry 360 creates a template of the metrics of the gestures used to create the desired pictogram. To do this, the training circuitry 350 can employ some statistical amalgam of the metrics, such as use average angles between points, use median angles between points, or use any other statistical data capable of embodying a likely representation of some idealized or likely metric of the gestures.

[0035] Assuming that average angles are used, the average angle Θ for each section *k* of equations (5)-(6) is determined according to Eq.(7) below:

$$\Theta = [\theta_k] = \frac{1}{M/D} \sum_{m=0}^{M/D-1} \theta_{k,m} \qquad \text{Eq.(7)}$$

[0036] Once determined, the average angles are quantized into the appropriate level given a quantization level count, L, according to Eq.(8) below:

$$\hat{\Theta} = floor([\theta_k]/L) \qquad \text{Eq.(8)}$$

[0037] The compilation all of the average angle metrics forms the template, which may be used as the basis of a password or encryption key.

[0038] To better protect the template, the hashing circuitry 382 can perform a hashing operation on the template to create a template hash. The template hash can then be stored in the memory 320 or the memory of another device, such as the server 130 of FIG. 1.

[0039] Next, the error coding circuitry 370 encodes the template using any number of error coding techniques, such as Reed-Solomon block coding, which will create a set of error detection and correction bits that, when applied to gestures that resemble the template, will enable a device to transform individual gesture entries into the template.

[0040] One can view the problem of recognizing a gesture as analogous to correcting distorted data that has passed through a non-ideal data channel. The template is considered an error-free message. However, when the error-free message is sent through a channel (e.g., the touch screen of a tablet), the error-free message is subjected to error/distortion. Error coding allows a designer to redundantly encode data so that the error-free data can be reproduced. The Reed-Solomon technique, which is commonly used to correct errors in scanning bar codes, as well as reading CD and DVD media, provides one non-limiting example of redundant coding. Reed-Solomon uses block codes; meaning, the message to be transmitted is divided up into separate blocks of data. Each block then has error correction information added to it to form a self-contained code word. For each two bits of error correction information added, one symbol can be corrected in the template.

[0041] The error correction information can then be stored in the memory 320 or within some other device for later use. When this error correction information is applied to a gesture closely resembling the template, the gesture will be transformed to resemble the template. The amount of difference between a given gesture and a template that can be tolerated depends on the number of error correction bits. The more error correction bits allocated, the greater the variation among gestures that can be tolerated.

[0042] Once the template hash and the respective template error correction information have been determined, the user can then employ the user terminal 110 to recognize gesture-based passwords and encryption keys. In such an exemplary operation, the sensor 330 measures/receives a hand-drawn set of one or more gestures from a user, which are then quantized by the quantizing circuitry 340.

[0043] Once quantized, the error coding circuitry 370 can create data blocks using the quantized gestures and the error correction information previously derived using the template. The data blocks can then be transmitted to a remote device if desired, or the error-correction circuitry 380 can then perform an error correction operation on the quantized gesture data in order to attempt to re-create the template.

[0044] Once the error correction operation is performed, the hashing circuitry 382 can them perform a hashing operation on the "corrected" data to create a hash of the gesture. The verification circuitry 384 can compare the gesture hash to the template hash. If there is a match, then the verification circuitry 384 can provide the appropriate access to the user.

[0045] FIG. 4 is a block diagram of the server 130 of FIG. 1 capable of providing securely access based on human-based gestures. FIG. 4 demonstrates that servers and like devices need only minor modifications to hardware or software in order to accommodate the disclosed security techniques. As shown in FIG. 4, the server 130 includes a processor 410, a memory 420, error correction circuitry 430, hashing circuitry 440, verification circuitry 45 and input/output circuitry 990. The memory 420 contains a template hash 422 for a user-drawn set of gestures.

[0046] As with the user terminal 110 of Fig. 3, the server 130 of FIG. 4 may be constructed using a large variety of architectures, and some or all of the components 430-450 may take the form of software/firmware routines residing in memory 420.

[0047] In operation, one or more blocks of data containing quantized gesture-based data and error correction information/bits from a respective template are received by the input/output circuitry 490 and delivered to the error correction circuitry 430.

[0048] The error correction circuitry 430 then performs the appropriate error correction operations, e.g., a Reed-Solomon type error correction, to produce corrected gesture data.

[0049] The hashing circuitry 440 can them perform a hashing operation on the corrected data to create a hash of the gesture where after the verification circuitry 450 can compare the gesture hash to the template hash 422 in the memory 420. If there is a match, then the verification circuitry 450 can provide the appropriate access to the user.

[0050] FIG. 5 is a flowchart outlining a set of exemplary operations usable for creating an invariant password from human-variant gestures. While the below-described operations are described as occurring in a particular sequence for convenience, it is noted that the order of various operations may be changed from embodiment to embodiment. It is further noted that various operations may occur simultaneously or may be made to occur in an overlapping fashion.

[0051] The process starts in at S502 where a human-drawn trial gesture is measured/received using a sensor, and quantized. As discussed above, while gestures can be quantized according to the equations (1)-(6) outlined above so as to embody angular information, other quantization techniques/approaches may be used in other embodiments. Next, at S510, a determination is made as to whether the received gesture is suitable as a password, e.g., it has an appropriate complexity and not previously used. If the received gesture is not suitable, control jumps back to S502 where another trial gesture may be entered; otherwise, control continues to S512.

[0052] At S512, the trial gesture of S502 is repeatedly received and quantized for user training to determine whether the user can reliably recreate the gesture. At S520, if the user has not consistently reproduce the desired gesture, control jumps back to S512 where the gesture may be re-entered; otherwise, control continues to S522.

[0053] At S522, using the repeatedly entered sets of gestures of S512 and/or using another set of user-supplied gesture entries, a template of the gestures is created, along with the appropriate error correction information usable to transform variant gestures to resemble the invariant template. At S524, a hash of the template is created and stored. Control continues to S526.

[0054] At S526, the trial gesture is re-entered by the user M times, and at S528 each gesture entry is quantized and encoded using the error correction information of S522. At S530, error correction and hashing is performed for each of the M entries, and at S540 a determination is made as to whether each gesture hash matches the template hash of S524. If each of the gesture hashes match the template hash, then it is determined that a suitable gesture-based password/key has been found; otherwise, control jumps back to S502.

[0055] FIG. 6 is a flowchart outlining a set of exemplary operations usable for securing access to a system using a gesture-based password. As with FIG. 5, while the below-described operations are described as occurring in a particular sequence for convenience, it is noted that the order of various operations may be changed from embodiment to embodiment. It is further noted that various operations may occur simultaneously or may be made to occur in an overlapping fashion.

[0056] The process starts in at S602 where a human-drawn gesture is received and quantized. Again, as discussed above, while gestures can be quantized according to the equations (1)-(6) outlined above so as to embody angular information, other quantization techniques/approaches may be used in other embodiments. Next, at S604, the quantized gesture is error-coded using the appropriate error correction information derived from a respective template. Control continues to S606.

[0057] At S606, the encoded gesture is sent to a server or other remote device, and at S610 the encoded gesture is received. In a variety of embodiments, operations S606 and S610 may be eliminated assuming that the desired access may be had on the device used to receive and quantize the gestures. Control continues to S612.

[0058] At S612, error correction and hashing is performed on the gesture to produce a gesture hash. At S614, the gesture hash is compared to a hash of the template, and at S620 a determination is made as to whether the gesture hash matches the template hash. If the gesture hashes match the template hash, then control continues to S622 where access is provided to the user; otherwise, control jumps back to S602.

[0059] FIGs. 7 and 8 depict an error analysis using gesture-based passwords. In a set of experiments, a group of users drew custom, personalized symbols using a tablet computer. The users then trained the system by drawing their symbol ten times, and gesture templates were created and error-coded. After this, subsequent gestures were quantized and error-coded using the error-correction information for the appropriate template. The distribution of error values were analyzed under two classes.

[0060] The first class, shown in graph 700 of FIG. 7, represents the condition that two gesture were drawn by the same person, $p(e \mid H_0)$, and should reflect a correct match. The second class, shown in graph 800 of FIG. 8, represents the condition that two gestures were drawn by different people, $p(e \mid H_0)$, and should reflect an incorrect match.

[0061] FIG. 9 depicts a receiver operating characteristic (ROC) curve of gesture-based passwords, which depicts how the false rejection rate (FRR) changes given a false acceptance rate (FAR), i.e., the percent of incorrect outcomes that were mistakenly labeled correct. Using a sample set of data from thirty people, a FRR of 0.1% was achieved with 0% FAR. If the error metric was a perfect classifier for the two classes, the two distribution curves in FIGs. 7 and 8 would be completely separated along the x-axis with no overlap, which would yield an area under the ROC equal to 1. In the empirical data there is very little overlap, leading the ROC curve of FIG. 9 to show a high classification accuracy. Setting a false acceptance rate of 0% results in a false rejection rate of 0.1%.

[0062] While the invention has been described in conjunction with the specific embodiments thereof that are proposed as examples, it is evident that many alternatives, modifications, and variations will be apparent to those skilled in the art. Accordingly, embodiments of the invention as set forth herein are intended to be illustrative, not limiting. There are changes that may be made without departing from the scope of the invention.

WHAT IS CLAIMED IS:

1. A method for establishing secure communications, comprising:

receiving one or more human gestures using a sensor on a first device;

quantizing the one or more human gestures so as to create a metric of the one or more human gestures; and

performing an error correction operation on the metric using error correction information derived from a template of the metric to create a corrected metric.

2. The method of claim 1, further comprising:

performing a hashing operation on the corrected metric to create a metric hash.

3. The method of claim 2, further comprising:

comparing the metric hash to a hash of the template to verify that the one or more human gestures sufficiently conform to the template.

4. The method of claim 2, further comprising:

using the metric hash as an encryption key.

5. The method of claim 1, further comprising:

encoding the metric using the template error correction information to create an error-coded metric; and

communicating the error-coded metric to a second device; wherein

the error correction operation, the hashing operation and the comparing operation are performed on the second device.

6. The method of claim 1, wherein the one or more human gestures are measured by a touch screen incorporated into the first device.

7. The method of claim 1, wherein the metric includes angular information between discrete locations of the one or more human gestures so as to make the one or more human gestures size invariant.

8. The method of claim 1, further comprising:

deriving the template using a plurality of gesture entries such that the template is a statistical amalgam of the plurality of gesture entries.

9. A method for creating a password, comprising:

receiving a set of one or more human gestures using a sensor on a first device a plurality of times to create a plurality of entries, wherein for each entry the one or more human gestures generally conform with one another;

quantizing each entry to create a plurality of metric entries; and

deriving a template using the plurality of metric entries such that the template is a statistical amalgam of the plurality of metric entries.

10. The method of claim 9, further comprising:

error-coding the template to derive error-correction information that, when applied to each of the plurality of metric entries, the error-correction information will cause each of the metric entries to transform into the template.

11. The method of claim 9, further comprising:

before creating the template, determining whether the one or more human gestures are suitable as a hand-drawn password.

12. The method of claim 11, further comprising:

before creating the template, performing a training routine so as to determining whether the one or more human gestures can be drawn consistently by a user.

13. The method of claim 9, wherein each metric entry includes angular information between discrete gesture locations so as to make the one or more human gestures size invariant.

14. The method of claim 9, wherein the template includes mean angles of the plurality of metric entries.

15. A device for establishing secure communications, comprising:

quantizing circuitry configured to quantize one or more human gestures so as to create a metric of the one or more human gestures; and

error correction circuitry configured to perform an error correction operation on the metric using error correction information derived from a template of the metric to create a corrected metric.

16. The circuit of claim 15, further comprising:

hashing circuitry configured to perform a hashing operation on the corrected metric to create a metric hash.

17. The circuit of claim 16, further comprising:

verification circuitry configured to compare the metric hash to a hash of the template to verify that the one or more human gestures conform to the template.

18. The circuit of claim 15, further comprising:

encoding circuitry configured to encode the metric using the template error correction information to create an error-coded metric; and

input/output circuitry to send the error-coded metric to a second device.

19. The circuit of claim 15, further comprising a sensor, wherein the one or more human gestures are derived using the sensor.

20. The circuit of claim 15, wherein the metric includes angular information between discrete locations of the one or more human gestures so as to make the one or more human gestures size invariant.

21. The circuit of claim 15, wherein the template is a statistical amalgam of a plurality of gesture entries.

22. A device for creating a password, comprising:

a sensor capable of deriving a set of one or more human gestures a plurality of times to create a plurality of entries, wherein for each entry the one or more human gestures generally conform with one another;

quantizing circuitry configured to quantize each entry so as to create a plurality of metric entries; and

template circuitry configured to derive a template using the plurality of metric entries such that the template is a statistical amalgam of the plurality of metric entries.

23. The device of claim 22, further comprising:

error-coding circuitry encode the template to derive error-correction information that, when applied to each of the plurality of metric entries, will enable the metric entries to create a hash that is identical to a hash of the template.

24. The device of claim 22, further comprising:

hashing circuitry to create a hash of the template.

25. The device of claim 22, further comprising:

training circuitry configured to enable a user to perform a training routine so as to determining whether the one or more human gestures can be drawn consistently by the user.

26. The device of claim 22, wherein each metric entry includes angular information between discrete locations of a respective set of gestures so as to make the one or more human gestures size invariant.

27. The device of claim 26, wherein the template is a statistical amalgam of the plurality of metric entries.

28. The device of claim 27, wherein the template includes mean angles of the plurality of metric entries.

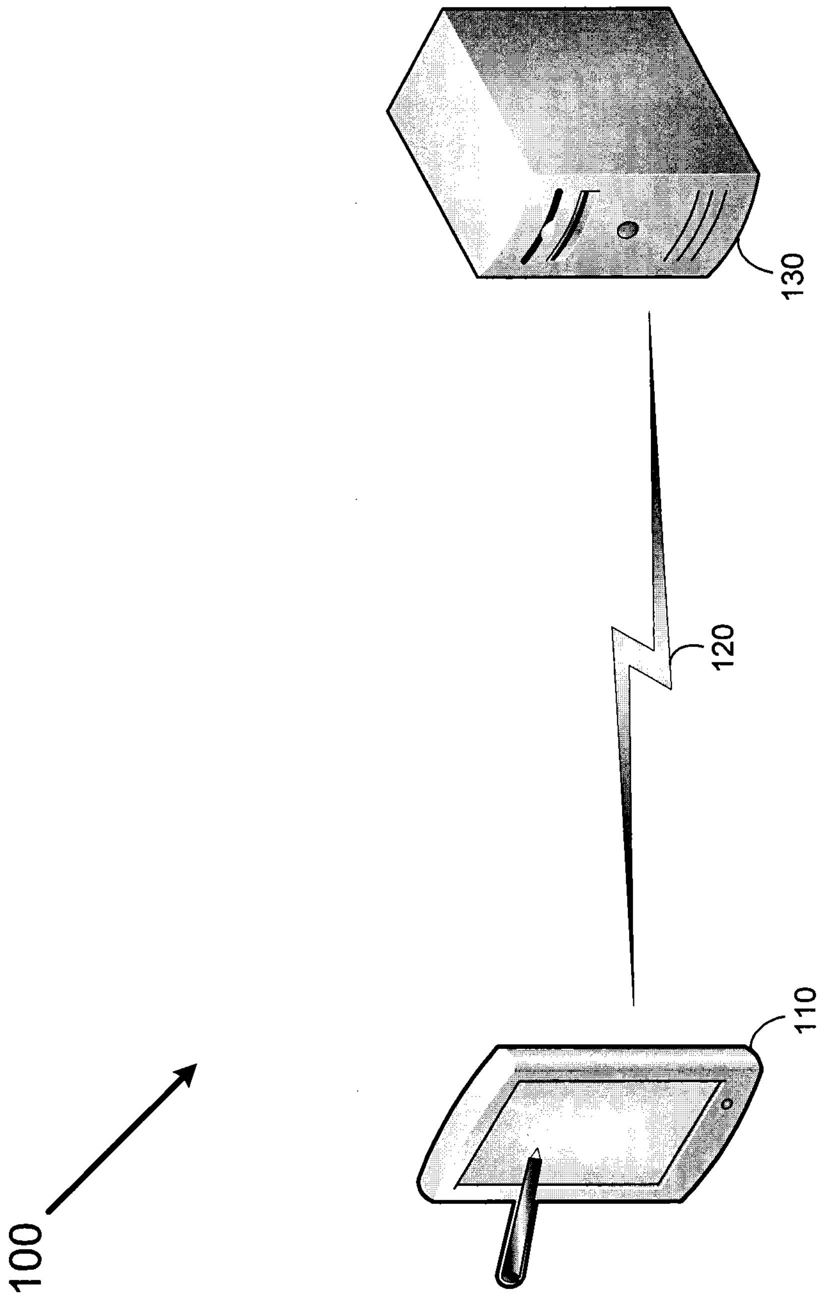

FIG. 1

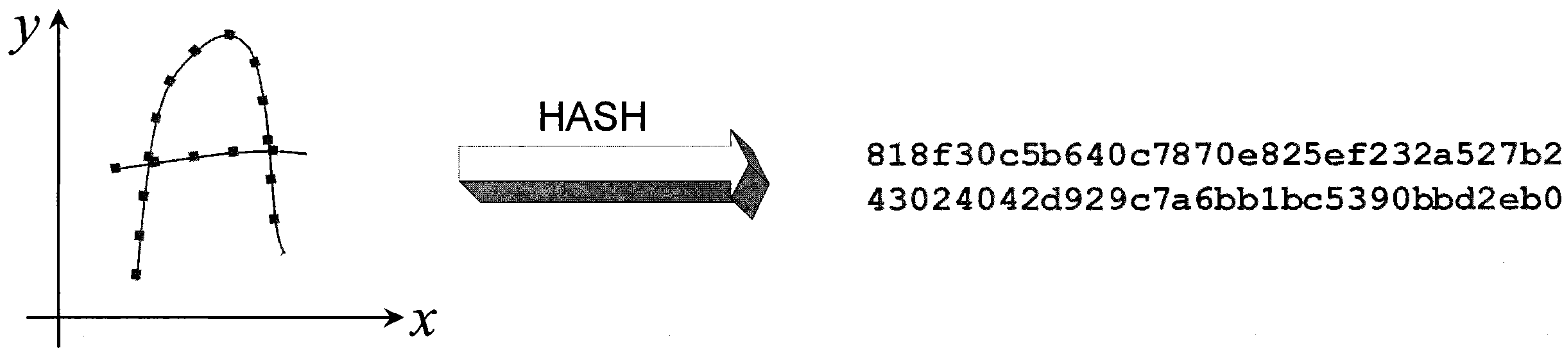
y
x
HASH
818f30c5b640c7870e825ef232a527b2
43024042d929c7a6bb1bc5390bbd2eb0

FIG. 2A

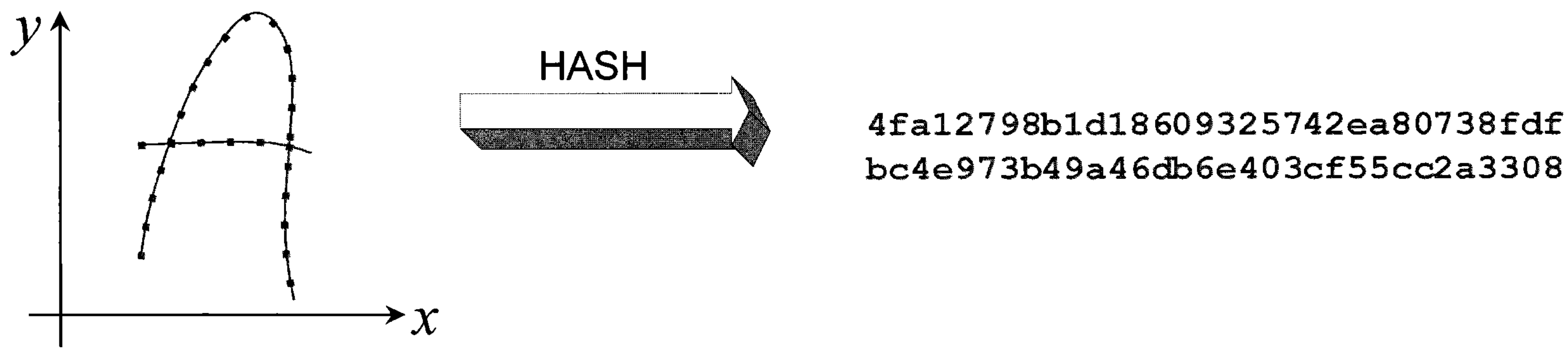
y
x
HASH
4fa12798b1d18609325742ea80738fdf
bc4e973b49a46db6e403cf55cc2a3308

FIG. 2B

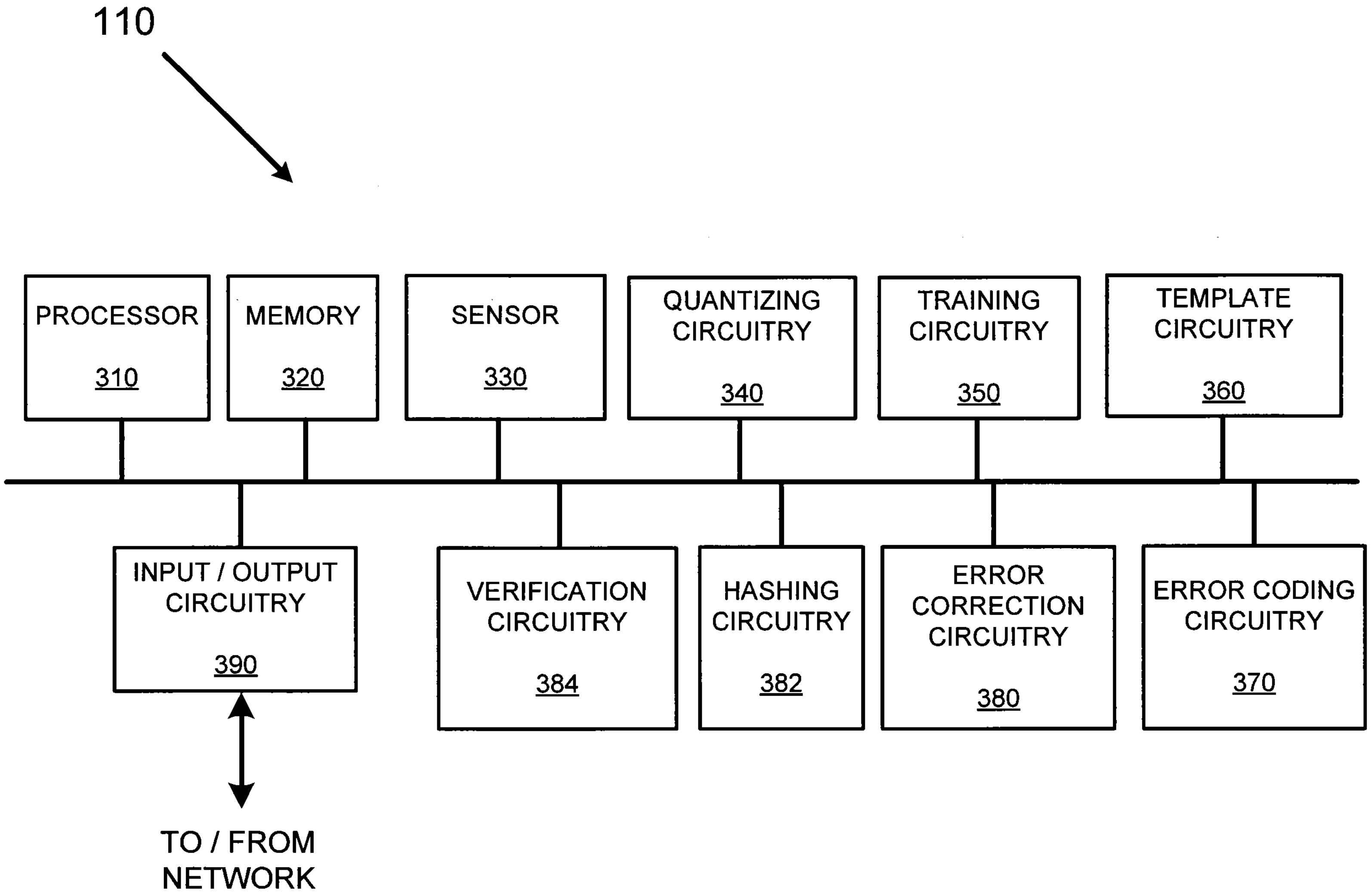
110
PROCESSOR 310
MEMORY 320
SENSOR 330
QUANTIZING CIRCUITRY 340
TRAINING CIRCUITRY 350
TEMPLATE CIRCUITRY 360
INPUT / OUTPUT CIRCUITRY 390
VERIFICATION CIRCUITRY 384
HASHING CIRCUITRY 382
ERROR CORRECTION CIRCUITRY 380
ERROR CODING CIRCUITRY 370
TO / FROM NETWORK

FIG. 3

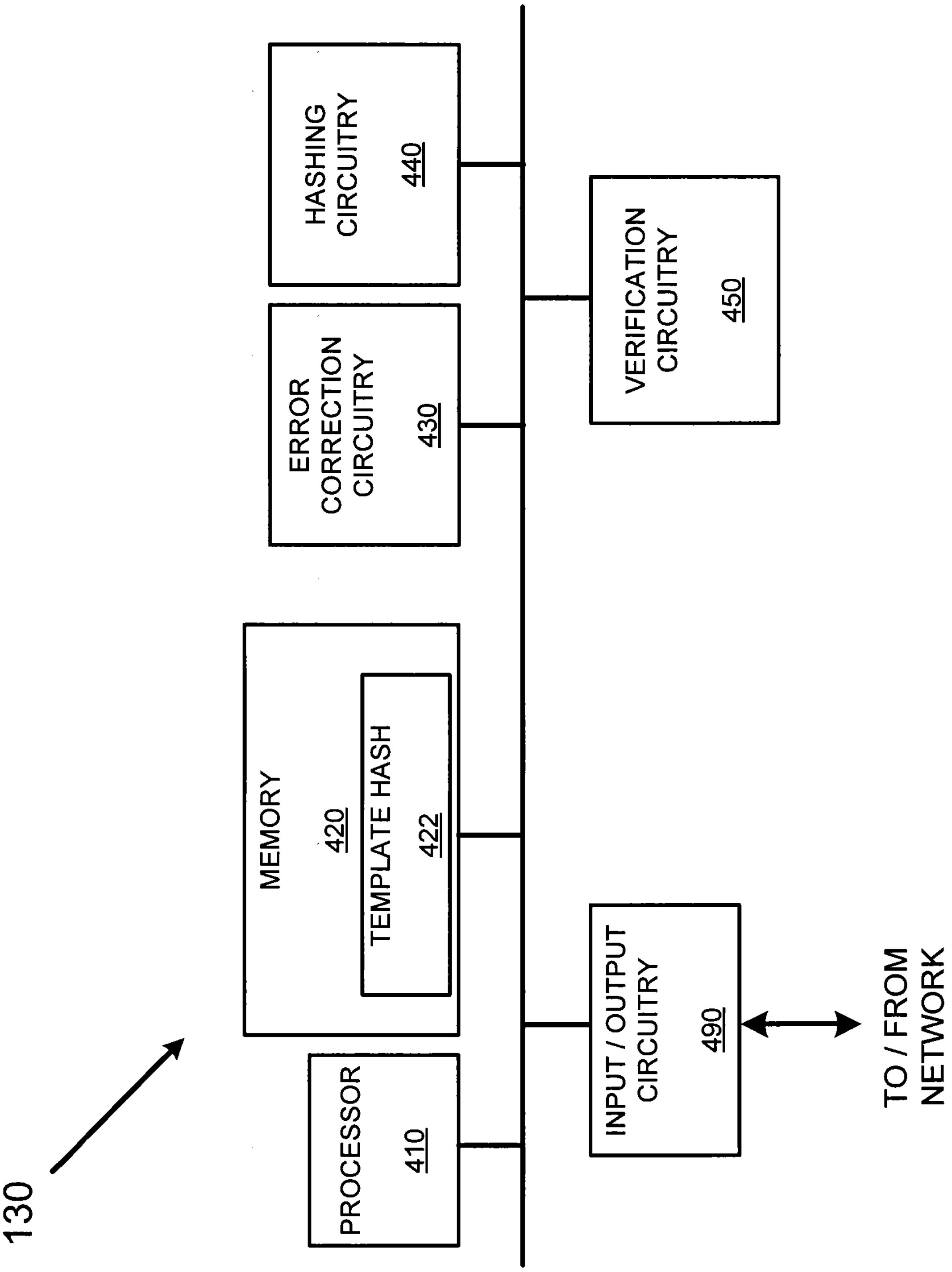
130
PROCESSOR
410
MEMORY
420
TEMPLATE HASH
422
ERROR CORRECTION CIRCUITRY
430
HASHING CIRCUITRY
440
VERIFICATION CIRCUITRY
450
INPUT / OUTPUT CIRCUITRY
490
TO / FROM NETWORK

FIG. 4

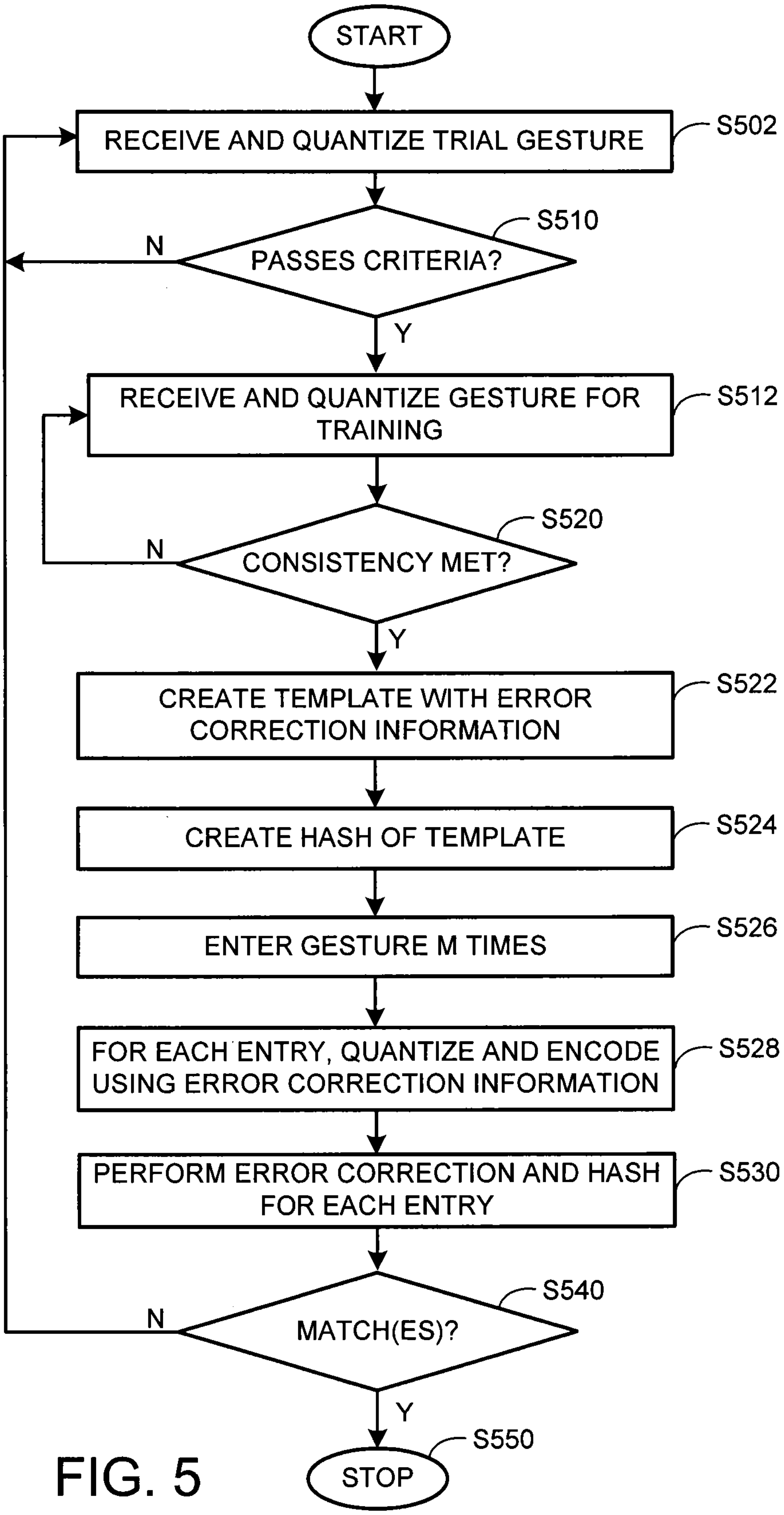
START
RECEIVE AND QUANTIZE TRIAL GESTURE
S502
PASSES CRITERIA?
S510
N
Y
RECEIVE AND QUANTIZE GESTURE FOR TRAINING
S512
CONSISTENCY MET?
S520
N
Y
CREATE TEMPLATE WITH ERROR CORRECTION INFORMATION
S522
CREATE HASH OF TEMPLATE
S524
ENTER GESTURE M TIMES
S526
FOR EACH ENTRY, QUANTIZE AND ENCODE USING ERROR CORRECTION INFORMATION
S528
PERFORM ERROR CORRECTION AND HASH FOR EACH ENTRY
S530
MATCH(ES)?
S540
N
Y
STOP
S550

FIG. 5

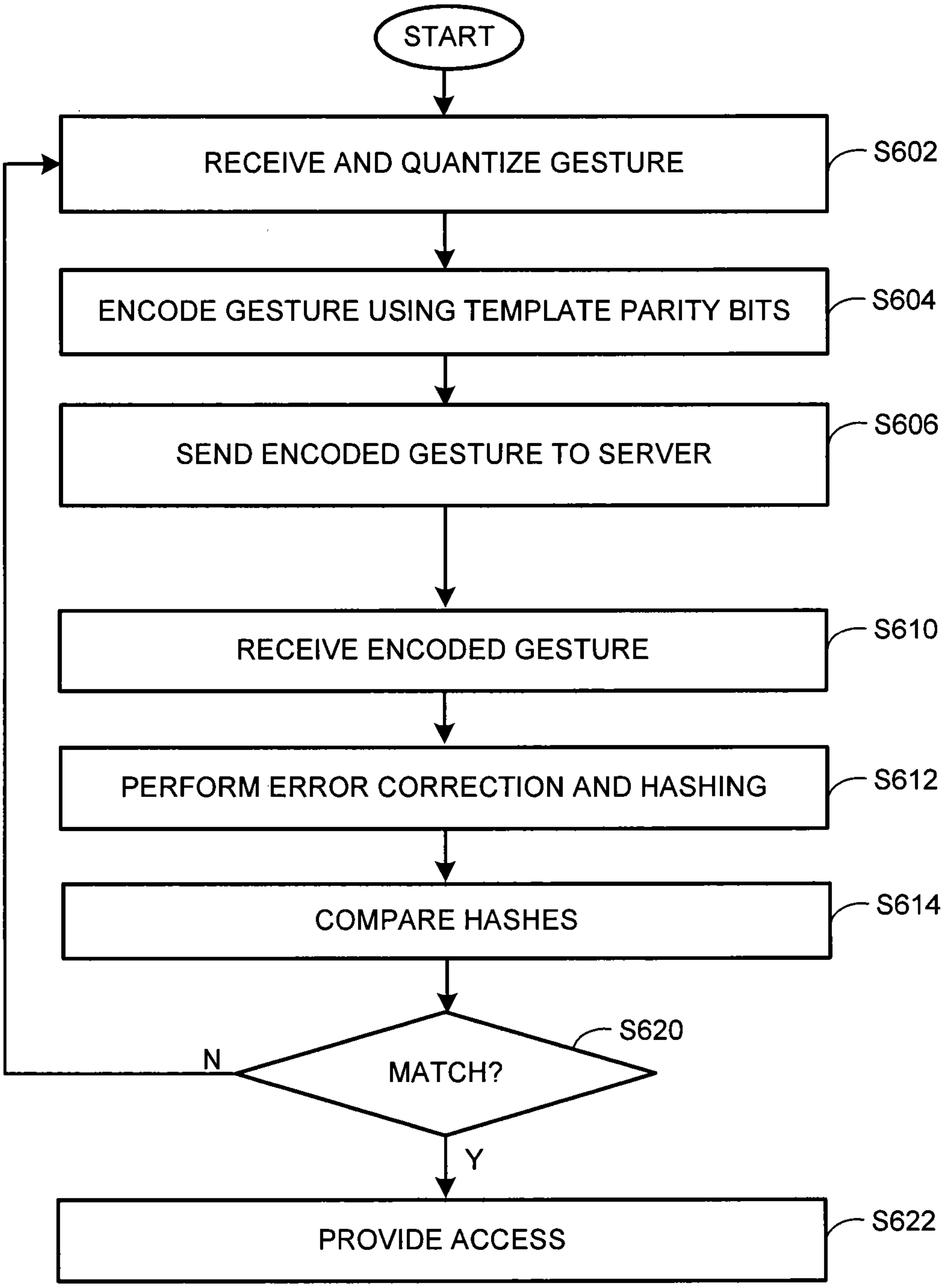
START
RECEIVE AND QUANTIZE GESTURE
S602
ENCODE GESTURE USING TEMPLATE PARITY BITS
S604
SEND ENCODED GESTURE TO SERVER
S606
RECEIVE ENCODED GESTURE
S610
PERFORM ERROR CORRECTION AND HASHING
S612
COMPARE HASHES
S614
MATCH?
S620
N
Y
PROVIDE ACCESS
S622

FIG. 6

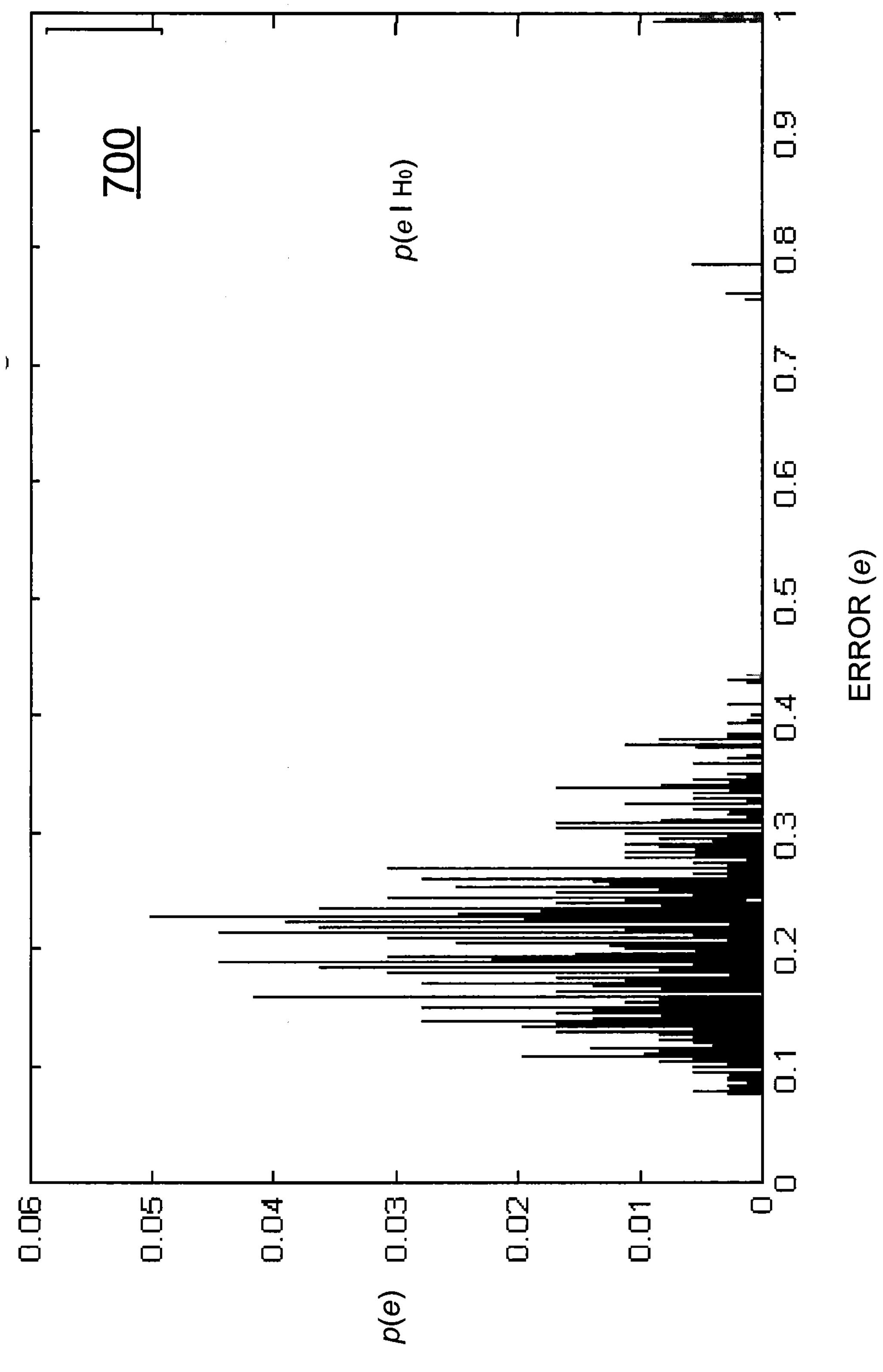
700
p(e | H₀)
p(e)
0.06
0.05
0.04
0.03
0.02
0.01
0
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
ERROR (e)

FIG. 7

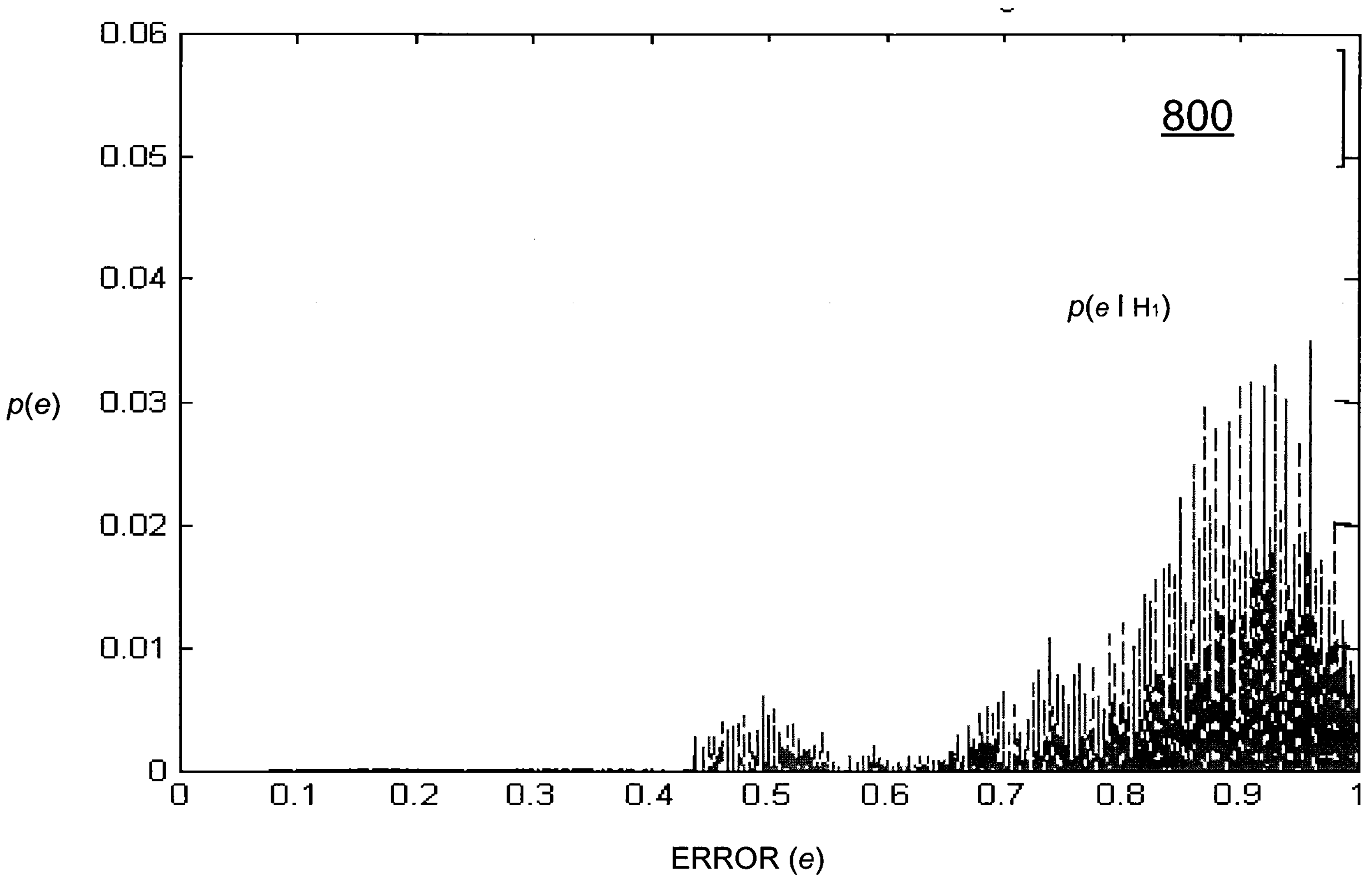
800
$p(e \mid H_1)$
$p(e)$
0.06
0.05
0.04
0.03
0.02
0.01
0
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
ERROR (e)

FIG. 8

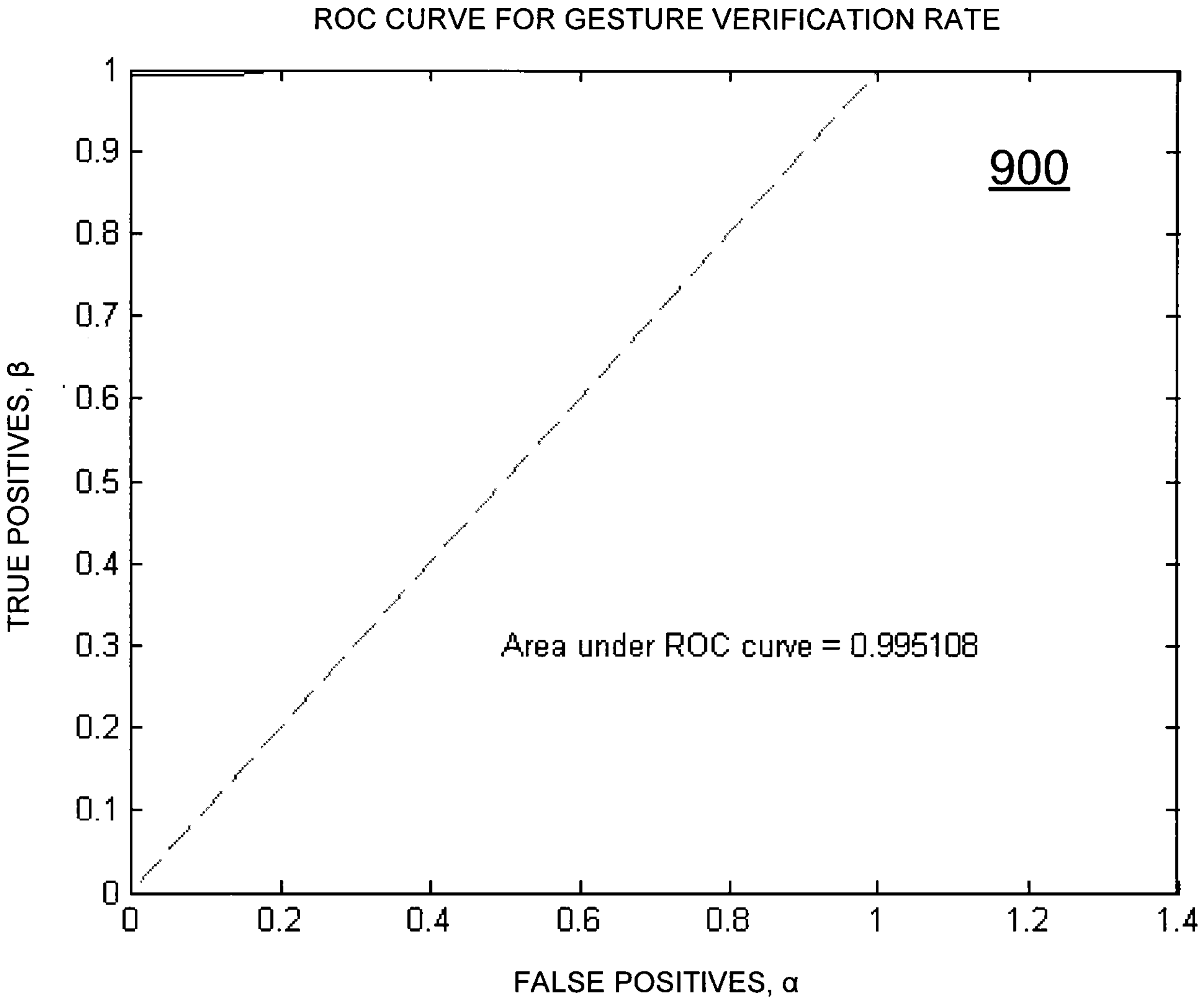
ROC CURVE FOR GESTURE VERIFICATION RATE
900
Area under ROC curve = 0.995108
TRUE POSITIVES, β
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
0.2
0.4
0.6
0.8
1
1.2
1.4
FALSE POSITIVES, α

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/017314

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 G06F21/32 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 G06F

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, PAJ, WPI Data, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EMANUELE MAIORANA: "User adaptive fuzzy commitment for signature template protection and renewability", JOURNAL OF ELECTRONIC IMAGING, vol. 17, no. 1, 1 March 2008 (2008-03-01), page 011011, XP055129893, ISSN: 1017-9909, DOI: 10.1117/1.2885239	1-6, 8-12, 15-20, 22-24
Y	paragraph [01.2] paragraph [0002] figure 3 ----- -/--	7,13,14, 20,25-28

☒ 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 18 July 2014	Date of mailing of the international search report 28/07/2014
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Bec, Thierry

1

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CHIARA ERCOLE; PATRIZIO CAMPISI; ALESSANDRO NERI: "Iris-based authentication system with template protection and renewability", SPIE, PO BOX 10 BELLINGHAM WA 98227-0010 USA, 8 October 2007 (2007-10-08), XP040246931, Proc. SPIE 6741, Optics and Photonics for Counterterrorism and Crime Fighting III paragraphs [0003] - [0004] figure 3 -----	1-5, 8-10, 15-19, 21-24
Y	DAVID GONZALEZ MARTINEZ ET AL: "Secure crypto-biometric system for cloud computing", SECURING SERVICES ON THE CLOUD (IWSSC), 2011 1ST INTERNATIONAL WORKSHOP ON, IEEE, 6 September 2011 (2011-09-06), pages 38-45, XP032063713, DOI: 10.1109/IWSSCLOUD.2011.6049023 ISBN: 978-1-4577-1185-5 paragraph [0III] - paragraph [00IV] -----	7,13,14, 20,25-28
A	US 2011/231667 A1 (KINDARJI BRUNO [FR] ET AL) 22 September 2011 (2011-09-22) the whole document -----	1-28

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2014/017314

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011231667 A1	22-09-2011	CA 2743954 A1	17-06-2010
		CN 102273128 A	07-12-2011
		EP 2356773 A1	17-08-2011
		FR 2939583 A1	11-06-2010
		JP 2012511202 A	17-05-2012
		KR 20110104934 A	23-09-2011
		US 2011231667 A1	22-09-2011
		WO 2010066992 A1	17-06-2010