ALAN SEGE (CA BAR NO. 177350)
ALAN SEGE ESQ., PC
13323 Washington Blvd, Suite 302
Los Angeles, CA 90066
Telephone: (310) 957-3301
alan@alansege.com

RYAN E. HATCH (CA Bar No. 235577)
ADAM J. REIS (CA Bar No. 354712)
HATCH LAW PC
13323 Washington Blvd, Suite 302
Los Angeles, CA 90066
(310) 279-5076 Telephone
(310) 693-5328 Facsimile
ryan@hatchlaw.com

Attorneys for Intervenor iProov Ltd

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

FACETEC, INC., a Delaware corporation, Plaintiff, v. JUMIO CORPORATION, a Delaware corporation, Defendant, and IPROOV, LTD, a United Kingdom limited company, Intervenor.	Case No. 3:24-3623-RFL **INTERVENOR IPROOV LTD'S PRELIMINARY INVALIDITY CONTENTIONS PURSUANT TO PATENT L.R. 3-3**

FACETEC EXHIBIT 2011
JUMIO v. FACETEC
IPR2025-00106

TABLE OF CONTENTS

Table of Contents **2**

I. Invalidity Contentions [Patent L.R. 3-3] **4**

a. Priority Date **7**

b. Claim Construction **9**

c. Identification of Prior Art [Patent L.R. 3-3(a)] **10**

i. Prior Art Patents and Patent Application Publications 10

ii. Prior Art Publications 11

iii. Prior Art Sales/Public Uses 13

d. Grounds for Invalidity [Patent L.R. 3-3(b)] **13**

i. Primary References 14

1. U.S. Patent No. 8,798,336 ("Nechyba") 14
2. U.S. Patent No. 9.230,158 ("Ramaswamy") 14
3. U.S. Patent Pub. No. 2011/0299741 ("Zhang") 15
4. U.S. Patent No. 8,977,010 ("Frischholz") 15
5. U.S. Patent Application Pub. No. 2008/0192980 ("Park") 16
6. U.S. Patent No. 10,755,084 ("Ganong") 16
7. U.S. Patent No. 9,412,169 ("Bud") 17
8. Moving Face Spoofing Detection via 3D Projective Invariants ("Marsico") 17
9. U.S. Patent No. 9,330,322 ("Ferren") 18

ii. Additional References 18

1. U.S. Patent Pub. No. 2008/0304716 ("Hirose") 19
2. U.S. Patent No. 9,690,998 ("Negi") 22
3. U.S. Patent No. 9,524,421 ("Ross") 28
4. U.S. Patent No. 8,290,220 ("Uchida") 31
5. Face Liveness Detection Using 3D Structure Recovered from a Single Camera ("Wang") 34
6. U.S. Patent No. 9,408,076 ("Chen") 36
7. U.S. Patent No. 2007/0009139 ("Landschaft") 40
8. U.S. Patent No. 8,970,348 ("Evans") 44
9. U.S. Patent Pub. No. 2019/0342329 ("Turgeman") 47
10. U.S. Patent No. 9,510,196 ("Sensharma") 53
11. U.S. Patent Pub. No. 2014/0310764("Tippett") 58
12. U.S. Patent No. 10,169,672 ("Langley") 62
13. U.S. Patent No. 9,652,663 ("Lau") 67
14. U.S. Patent No. 8,984,622 ("Baldwin '622") 72
15. U.S. Patent No. 9,607,138 ("Baldwin '138") 77
16. U.S. Patent No. 9,600,649 ("Parry") 82
17. U.S. Patent No. 8,705,812 ("Karakotsios") 87
18. U.S. Patent No. 8,630,493 ("Gokturk") 90
19. U.S. Patent No. 8,966,613 ("Horvitz") 94
20. U.S. Patent No. 10,049,287 ("Holz") 98
21. U.S. Patent No. 8,856,541 ("Chaudhury") 101
22. Non-intrusive Liveness Detection by Face Images ("Kollreider") 105
23. U.S. Patent No. 2014/0366113 ("LeCun") 108
24. U.S. Patent No. 7,840,034 ("Takahashi") 110
25. U.S. Patent Pub. No. US 2014/0309880 ("Ricci") 112
26. Securing Sensitive Data Stored on Smartphones ("Wilson") 114
27. U.S. Patent No. 10,042,993 ("Beigi") 116
28. A liveness detection method for face recognition based on optical flow field ("Bao") 125
29. Face liveness detection using variable focusing ("Kim") 125

30. Liveness Measurements Using Optical Flow for Biometric Person Authentication ("Smiatacz") ... 126
31. U.S. Patent Pub. No. US 2002/0113884 ("Tanii") ... 127
32. U.S. Patent No. US 8,437,513 ("Derakhshani") ... 128
33. U.S. Patent Pub. No. 2010/0014720 ("Hoyos") ... 133
iii. State of the Art and Obviousness ... 136
iv. Motivations for Making Combinations of Prior Art ... 137
v. State of the Art and Motivations to Combine ... 140
vi. Specific Motivations ... 141
vii. Groups of References ... 142
1. Camera-Based 3D Authentication ... 142
2. Multiple Images ... 145
3. Biometric Data ... 148
4. Changing Camera Location ... 151
5. Comparing Images ... 153
6. Authentication Based on Image Differences ... 157
7. User Prompts ... 161
8. Oval Prompts ... 164
9. Hand-Held Devices ... 165
10. Movement of Devices ... 168
11. Laptop or Desktop Computer Devices ... 170
12. User Image ... 172
13. Server-Based Solutions ... 174
14. Fish-Eye Distortion/Ear Tracking ... 177
15. Compare With Enrollment Image ... 178
16. Examining Third Image (Interpolating Data) ... 179
17. Reflection Detection ... 181
viii. Motivations based on admitted prior art ... 182
ix. Secondary Considerations ... 182
e. Invalidity Charts [Patent L.R. 3-3(c)] ... 183
f. Section 101 and 112 Defenses [Patent L.R. 3-3(d)] ... 184
i. Indefiniteness ... 185
ii. Lack of Written Description and/or Enablement ... 187
iii. Means Plus Function Claims ... 191
iv. Ineligibility under 35 U.S.C. § 101 ... 192
II. Document Production [Patent L.R. 3-4] ... 192
III. Additional Contentions and Disclosures Incorporated by Reference ... 192

Pursuant to Patent L.R. 3-3, intervenor iProov Ltd. ("iProov") hereby makes the following disclosures of preliminary invalidity contentions to Plaintiff FaceTec, Inc. ("FaceTec") based on the information presently available. iProov reserves the right to modify, amend, or supplement this disclosure, as provided by the Federal Rules of Civil Procedure and local rules, as additional information becomes available.

Based on FaceTec's Disclosure of Asserted Claims and Infringement Contentions ("Infringement Contentions"), served on November 12, 2024, iProov understands that FaceTec is alleging infringement of U.S. Patent Nos. 10,776,471 ("the '471 Patent"), 11,157,606 ("the '606 Patent"), 11,693,938 ("the '938 Patent"), and 11,874,910 ("the '910 Patent") (collectively "the FaceTec Asserted Patents") and in particular, claims 10-20 of the '471 Patent, claims 1-9 and 19-20 of the '606 Patent, claims 1-24 of the '938 Patent, and claims 10-21 of the '910 Patent (collectively "the FaceTec Asserted Claims"). For purposes of these contentions, iProov addresses only the FaceTec Asserted Claims. iProov reserves the right to amend or supplement this disclosure as necessary in view of any changes or amendments made, for any reason, to Plaintiff's infringement theories, infringement contentions, or FaceTec Asserted Claims, including to Plaintiff's asserted priority and/or invention date(s).

I. INVALIDITY CONTENTIONS [PATENT L.R. 3-3]

These Preliminary Invalidity Contentions are based on iProov's current knowledge and understanding of the Facetec Asserted Patents and the prior art, along with iProov's understanding of Plaintiff's infringement allegations and apparent claim interpretations based on those allegations, as set forth in Facetec's Infringement Contentions. iProov provides these Preliminary Invalidity Contentions despite the deficiencies in Plaintiff's Infringement Contentions. These Preliminary Invalidity Contentions should not be construed as a waiver by iProov of any objections to Plaintiff's Infringement Contentions or as an admission that the Infringement Contentions were adequate or that Plaintiff's apparent claim interpretations therein are correct, have merit, or should be adopted. Additionally, and as further explained below, where these Preliminary Invalidity Contentions disclose that a prior art reference meets a claim limitation, such position may be based on Plaintiff's

apparent claim interpretations in its Infringement Contentions; iProov does not necessarily agree that such interpretations are correct, have merit, or should be adopted.

iProov's investigation of the FaceTec Asserted Patents, their file histories, and the prior art is ongoing, and iProov expressly reserves the right to supplement these Preliminary Invalidity Contentions based on further discovery and in a manner consistent with the Federal Rules of Civil Procedure, and the Local Rules, or otherwise in accordance with any order or direction of this Court or agreement of the parties. iProov's ongoing investigation includes, but is not limited to, serving subpoenas on prior artists, publishers, inventors, assignees, and owners regarding prior art, seeking additional information related to the references and prior art systems disclosed in these Preliminary Invalidity Contentions, and seeking additional information regarding Plaintiff's Infringement Contentions and the products and services accused of infringing therein. Additionally, iProov has not yet had the benefit of taking the deposition of the named inventors or those that worked with the named inventors, or of the named inventors, authors, and entities listed on any references or systems identified in these Preliminary Invalidity Contentions.

iProov reserves the right to rely on additional prior art; further analysis of prior art; application of prior art to new or different claims; depositions and discovery from prior art sources and authors; analysis of prior art products; combinations of references; expert opinion and/or testimony; evidence supporting invalidity of any asserted claim; and any additional relevant information that may result from its further investigation and discovery. Additionally, iProov reserves the right to rely on additional information, testimony, and/or analysis concerning operation of prior art systems. Moreover, iProov reserves the right to revise its ultimate contentions concerning the invalidity of the FaceTec Asserted Claims, which may change depending upon the Court's construction of the FaceTec Asserted Claims, any findings as to the priority or invention date of the FaceTec Asserted Claims, and/or positions that Plaintiff or its expert witness(es) may take concerning claim construction, infringement, and/or invalidity issues.

Prior art not included in this disclosure, whether known or unknown to iProov, may become relevant. In particular, iProov is currently unaware of the extent, if any, to which Plaintiff will

contend that limitations of the FaceTec Asserted Claims are not disclosed in the prior art identified by iProov, or will contend that any of the identified references do not qualify as prior art.

Further, Plaintiff has not produced prior art known to it, including regarding any known prior art products. As discovery in this action provides iProov with additional information, iProov may serve subpoenas on third parties believed to have knowledge, documentation, and/or corroborating evidence relating to invalidity and/or prior art. It is therefore likely that iProov will discover additional prior art pertinent to the invalidity of the FaceTec Asserted Claims and iProov reserves the right to supplement these contentions after becoming aware of additional prior art or information. iProov further reserves the right to introduce and use such supplemental materials at trial.

iProov's claim charts in Exhibits 471-A through 471-I, 606-A through 606-I, 938-A through 938-I, and 910-A through 910-I cite particular teachings and disclosures of the prior art as applied to features of the FaceTec Asserted Claims. However, persons having ordinary skill in the art may view an item of prior art generally in the context of other publications, literature, products, and understanding. Accordingly, the cited portions are only exemplary, and iProov reserves the right to rely on uncited portions of the prior art references and on other publications and expert testimony as aids in understanding and interpreting the cited portions, as providing context thereto, and as additional evidence that a claim limitation is known or disclosed. Citations to figures are inclusive of all discussion of those figures. iProov further reserves the right to rely on uncited portions of the prior art references, other publications, documents explicitly or implicitly incorporated by reference, and testimony, to establish bases for combinations of certain cited references that render the FaceTec Asserted Claims obvious. Further, for any combination, iProov reserves the right to rely additionally on information generally known to those skilled in the art and/or common sense.

The references discussed herein and in the claim charts in Exhibits 471-A through 471-I, 606-A through 606-I, 938-A through 938-I, and 910-A through 910-I, or elsewhere identified, may disclose the elements of the FaceTec Asserted Claims explicitly and/or inherently, and/or they may be relied upon to show the state of the art in the relevant timeframe. The exemplary obviousness

combinations are provided in the alternative to iProov's anticipation contentions and are not to be construed to suggest that any reference included in the combinations is not itself anticipatory.

iProov further intends to rely on inventor admissions concerning the scope of the FaceTec Asserted Claims or of the prior art relevant to the FaceTec Asserted Claims found in, inter alia: the patent prosecution history and/or reexamination history for the Asserted Patent and related patents and/or patent applications; any deposition testimony of a named inventor of the Asserted Patent; and the papers filed and any evidence submitted by Plaintiff in conjunction with this litigation. iProov reserves the right to contend that the FaceTec Asserted Claims are invalid for failure to name the correct inventor(s), and/or to contend that Plaintiff lacks standing to bring this litigation with respect to such patents.

Depending on the Court's construction of the FaceTec Asserted Claims, and/or positions that Plaintiff or its expert witness(es) may take concerning claim interpretation, infringement, and/or invalidity issues, the charted prior art references in Exhibits 471-A through 471-I, 606-A through 606-I, 938-A through 938-I, and 910-A through 910-I or otherwise identified herein, may be of greater or lesser relevance, and different combinations of these references may be implicated. Given this uncertainty, the charts may reflect alternative applications of the prior art against the FaceTec Asserted Claims. Nothing stated herein shall be construed as an admission or a waiver of any particular construction of any claim term.

In addition to these Preliminary Invalidity Contentions and prior art identified herein, iProov hereby relies on and incorporates by reference in their entirety and expressly reserves the right to rely upon invalidity expert reports, including all invalidity positions, invalidity charts and all prior art cited therein, as well as invalidity contentions presented by any present or former defendant in any of Plaintiff's or its predecessors' lawsuits or by potential or actual licensees to the FaceTec Asserted Patents, including any reexamination or other post-grant review including PTAB and foreign proceedings, involving the FaceTec Asserted Patents, any patents that claim priority to, claim priority from, or are the basis for a claim of priority in the FaceTec Asserted Patents, or any foreign counterparts (collectively, "related patents").

a. PRIORITY DATE

In its Infringement Contentions, Plaintiff asserts that each FaceTec Asserted Claim is entitled to a priority date of at least July 3, 2015. Reference to an "asserted priority date" should not be construed to mean that iProov agrees that the FaceTec Asserted Claims are in fact entitled to such priority date, or that Plaintiff has provided proper notice as to its contentions for a priority date.

For a patent to gain the benefit of the filing date of an earlier application, "each application in the chain leading back to the earlier application must comply with the written description requirement of 35 U.S.C. 112." *Zenon Environmental, Inc. v. U.S. Filter Corp.*, 506 F.3d 1370, 1378 (Fed. Cir. 2007). iProov reserves the right to challenge the priority date depending on how FaceTec seeks to interpret its claims in applying them for infringement and distinguishing prior art for invalidity. iProov reserves the right to challenge the priority date based on the new material added to the FaceTec Asserted Patents and related parent applications. FaceTec's interpretation of the FaceTec Asserted Claims may result in additional flaws in FaceTec's priority date should FaceTec attempt to capture subject matter that was not disclosed until a later date. Thus, iProov reserves the right to challenge the priority date of the FaceTec Asserted Claims.

To the extent Plaintiff later alleges that any activities occurred before July 3, 2015 for the FaceTec Asserted Claims, including any belated reliance on the filing of provisional applications, iProov reserves the right to supplement these Preliminary Invalidity Contentions to address any such contention, including by identifying and/or charting additional prior art that may become relevant in view of such assertion. Likewise, to the extent Plaintiff successfully establishes an invention date before any of the prior art references relied on by iProov, then those references serve as evidence of secondary considerations of obviousness, particularly, contemporaneous invention by others. To the extent Plaintiff alleges that any prior art relied on in these Preliminary Invalidity Contentions does not actually qualify as prior art to the FaceTec Asserted Patents, iProov reserves the right to rebut those allegations (*e.g.*, by demonstrating an earlier critical date for the challenged prior art and/or a later priority date and/or date of invention for a particular FaceTec Asserted Claim). iProov also reserves the right to rely on additional documents, information, and evidence to demonstrate public availability by a certain date of a prior art reference or to rebut any efforts by

Plaintiff to allege any reference was not publicly available by a certain date or otherwise available as prior art.

b. CLAIM CONSTRUCTION

To the extent that these Preliminary Invalidity Contentions rely on or otherwise embody particular constructions of terms or phrases in the FaceTec Asserted Claims, iProov is not conceding to any such constructions as proper constructions of those terms or phrases at this time. The Court has established separate deadlines for the parties' proposed claim constructions in this litigation, and iProov will disclose its proposed constructions accordingly. For purposes of these Preliminary Invalidity Contentions, iProov may adopt alternative claim construction positions. In particular, portions of these Preliminary Invalidity Contentions, including the claim charts attached as exhibits, may be based on the underlying claim constructions and/or interpretations in Plaintiff's Infringement Contentions, to the extent such constructions and/or interpretations are understood by iProov. iProov does not concede that any such constructions or interpretations by Plaintiff are proper, and expressly reserves the right to contest any such constructions.

Throughout the attached Exhibits, iProov provides examples of where references disclose subject matter recited in preambles, without regard to whether the preambles are properly considered to be limitations of the FaceTec Asserted Claims. iProov reserves the right to argue, at the appropriate stage of this case, that the preambles are or are not limitations. Further, the fact that iProov provides examples of any limitation does not mean that iProov believes that the limitation is defined, or otherwise enabled, or comports with the requirements of the patent statute, including, but not limited to, 35 U.S.C. § 112.

Nothing disclosed herein is an admission or acknowledgement that any of iProov's products or services infringes any of the FaceTec Asserted Claims. iProov reserves the right to supplement, modify, or otherwise amend these Preliminary Invalidity Contentions, including based on the Court's claim construction rulings or opinions or the parties' positions or arguments taken in connection with the claim construction process. Moreover, iProov reserves the right to rely on any disclosures in the accompanying production as it believes necessary in view of positions Plaintiff may take with respect to the scope and meaning of the FaceTec Asserted Claims.

c. IDENTIFICATION OF PRIOR ART [PATENT L.R. 3-3(A)][1]

In addition to the references cited on the face of the FaceTec Asserted Patents and related patents, the admitted prior art references in the specifications of the FaceTec Asserted Patents and related patents, the prosecution histories of the FaceTec Asserted Patents and related patents, the references cited in any reexaminations, reissue proceedings, or other post-grant proceedings in the U.S. Patent Office of the FaceTec Asserted Patents and related patents, and the references cited in any invalidity contentions or expert reports submitted in any action or proceedings involving the FaceTec Asserted Patents or related patents, iProov below identifies the following prior art that anticipates each asserted claim and/or renders it obvious. The identification of any patent or patent publication shall be deemed to include any counterpart patent or application filed, published, or issued anywhere in the world.

iProov has set forth in detail in the accompanying claim charts and discussion below the particular claims that are anticipated under 35 U.S.C. § 102 and/or rendered obvious under 35 U.S.C. § 103 by the particular reference.

i. PRIOR ART PATENTS AND PATENT APPLICATION PUBLICATIONS

Patent / Publication No.	Origin	Date of Issue / Publication[2]
7,840,034	United States	11/23/2010
8,280,120	United States	10/02/2012
8,290,220	United States	10/16/2012
8,437,513	United States	05/07/2013
8,630,493	United States	01/14/2014
8,705,812	United States	04/22/2014
8,798,336	United States	08/05/2014
8,856,541	United States	10/07/2014
8,966,613	United States	02/24/2015

[1] iProov also hereby identifies any systems or products that embody the technology described in any patent or publication identified in these Preliminary Invalidity Contentions. iProov reserves the right to rely on any documents or other evidence regarding any such systems.

[2] The dates in this column are the latest dates on which the patents or publications were publicly available. iProov reserves the right to rely on the U.S. patents and publications in this list under 35 U.S.C. § 102(a) based on their earlier filing dates. iProov reserves the right to identify earlier dates for any references in this list should such dates be ascertained through discovery.

Patent / Publication No.	Origin	Date of Issue / Publication[2]
8,970,348	United States	03/03/2015
8,977,010	United States	03/10/2015
8,984,622	United States	03/17/2015
9,075,975	United States	07/07/2015
9,230,158	United States	01/05/2016
9,330,322	United States	05/03/2016
9,408,076	United States	08/02/2016
9.412,169	United States	08/09/2016
9,510,196	United States	11/29/2016
9,524,421	United States	12/20/2016
9,600,649	United States	03/21/2017
9,607,138	United States	03/28/2017
9,652,663	United States	05/16/2017
9,690,998	United States	06/27/2017
9,971,920	United States	05/15/2018
10,049,287	United States	08/14/2018
10,042,993	United States	08/07/2018
10,169,672	United States	01/01/2019
10,755,084	United States	08/25/2020
2002/0113884 A1	United States	08/22/2002
2007/0009139 A1	United States	01/11/2007
2008/0192980 A1	United States	08/14/2008
2008/0304716 A1	United States	12/11/2008
2010/0014720 A1	United States	01/21/2010
2011/0299741 A1	United States	12/08/2011
2014/0310764 A1	United States	10/16/2014
2014/0309880 A1	United States	10/16/2014
2014/0366113 A1	United States	12/11/2014
2019/0342329 A1	United States	11/07/2019

ii. PRIOR ART PUBLICATIONS

Title, Author(s), and Publisher	Date of Publication[3][4]
A Matter of Perspective, John Cornicello, Cornicello Photography, www.cornicello.com	05/08/2007
An Efficient Algorithm for Motion Detection Based Facial Expression Recognition Using Optical Flow, Ahmad R. Naghsh-Nilchi, and Mohammad Roshanzamir, World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering	2008
Face Distortion is Not Due to Lens Distortion, Daniel H. Baker, Daniel's Visionarium A blog about visual perception	05/05/2022
Impact of Focal Length on Portraits, Bill Waldman, www.ontakingpictures.com	08/09/2010
Perspective in Portraits, Nathan Yan, Digital Photography DeCal	2007
Evaluating Liveness by Face Images and the Structure Tensor, Klaus Kollreider, Hartwig Fronthaler and Josef Bigun, Institute or Electrical and Electronic Engineers (IEEE)	2005
Moving Face Spoofing Detection via 3D Projective Invariants, Maria De Marsico, Michele Nappi, Daniel Riccio, Jean-Luc Dugelay, Institute or Electrical and Electronic Engineers (IEEE)	2012
Face Liveness Detection Using 3D Structure Recovered from a Single Camera, Tao Wang, Jianwei Yang, Zhen Lei, Shengcai Liao, Stan Z. Li, Institute or Electrical and Electronic Engineers (IEEE)	2013
Non-intrusive Liveness Detection by Face Images, Klaus Kollreider, Hartwig Fronthaler, Josef Bigun, Image and Vision Computing	05/22/2007
Securing Sensitive Data Stored on Smartphones, Mark Wilson and Lei Chen, Institute or Electrical and Electronic Engineers (IEEE)	2012
A Liveness Detection Method for Face Recognition Based on Optical Flow Field, Wei Bao, Hong Li, Nan Li, Wei Jiang, 2009 International Conference on Image Analysis and Signal Processing	06/02/2009
Face Liveness Detection Using Variable Focusing, Sooyeon Kim, Sunjin Yu, Kwangtaek Kim, Yuseok Ban, and Sangyoun Lee, Institute or Electrical and Electronic Engineers (IEEE)	2013
Liveness Measurements Using Optical Flow For Biometric Person Authentication, Maciej Smiatacz, Metrology and Measurement Systems (M&MS)	05/2012

[3] The dates in this column are the latest dates, based on iProov's current investigation, on which the publications were publicly available. iProov reserves the right to identify earlier dates should such dates be ascertained through discovery.

[4] To the extent Plaintiff disagrees with any of these identified dates of publication, iProov is available to meet and confer.

iii. PRIOR ART SALES/PUBLIC USES

iProov hereby identifies any systems or products that embody the technology described in any patent or publication identified above in Sections I.c.i and I.c.ii, including and sales or public uses by any assignee or patentee of the FaceTec Asserted Patents or the named inventors.

Additionally, iProov reserves the right to supplement its disclosure of prior art sales and public uses of the claimed invention as discovery progresses.

d. GROUNDS FOR INVALIDITY [PATENT L.R. 3-3(B)]

The primary prior art references for the FaceTec Asserted Patents on which iProov presently relies based on investigation to date are identified below. The exhibits to these Preliminary Invalidity Contentions contain claim charts for the primary prior art references. Obviousness combinations of the primary prior art references are separately identified throughout these Preliminary Invalidity Contentions.

iProov's reliance on each prior art reference identified throughout these Preliminary Invalidity Contentions (whether primary references or secondary references) includes the reference itself, anything incorporated by the reference, any system embodying the reference, and any testimony by those with knowledge of the reference, such as named authors and inventors.[5] All such documents and information shall be considered one prior art reference to the extent they describe a single prior art system or solution, or the closely related work of a single prior art author. In addition to the specific references below, iProov reserves the right to rely on all admitted prior art in the FaceTec Asserted Patents and its file history, as well as anything admitted as known in the prior art by the patent owner, or which may lead to the additional discovery of prior art. iProov reserves the right to supplement these Preliminary Invalidity Contentions as discovery reveals further information about prior use and/or prior public knowledge of products, methods, or systems that iProov has reason to believe anticipate or render obvious one or more FaceTec Asserted Claims. During discovery, iProov plans on issuing subpoenas to third parties and therefore reserves the right to identify and rely on additional prior art in the possession of such parties. iProov further

[5] For example, for each patent identified as a prior art reference in these Preliminary Invalidity Contentions, iProov reserves the right to rely on the patent itself and/or any system that practices or embodies the patent to demonstrate invalidity.

reserves the right to identify and rely on additional prior art in Plaintiff's possession, custody, or control that has not yet been produced or identified to iProov, including prior art identified and/or produced in prior litigations or in post-grant proceedings at the U.S. Patent and Trademark Office.

i. PRIMARY REFERENCES

The following primary references, alone or in combination with any other reference(s) identified in this section or elsewhere in these Preliminary Invalidity Contentions, render invalid one or more of the FaceTec Asserted Claims.

1. U.S. PATENT NO. 8,798,336 ("NECHYBA")

U.S. Patent No. 8,798,336 was filed on September 23, 2013 and granted August 5, 2014. Nechyba qualifies as prior art to the FaceTec Asserted Patents under at least 35 U.S.C. §§ 102(a)(1), 102(a)(2). Nechyba anticipates and/or renders obvious (in combination with the knowledge of a person of ordinary skill in the art) all FaceTec Asserted Claims. The claim charts attached as **Exhibits 471-A, 606-A, 910-A, and 938-A** provide representative, non-limiting examples of where Nechyba discloses, either expressly or inherently, each element, thereby anticipating those claims. To the extent Plaintiff asserts that Nechyba does not anticipate any FaceTec Asserted Claim, such FaceTec Asserted Claim would have been obvious in view of Nechyba alone and/or in view of the knowledge of a person of ordinary skill in the art. Additionally, it would have been obvious to combine or modify Nechyba with concepts from other prior art, including any of the other primary references, secondary references, and/or in view of the knowledge of a person of ordinary skill in the art, including as explained herein, to achieve the claimed inventions.

2. U.S. PATENT NO. 9.230,158 ("RAMASWAMY")

U.S. Patent No. 9.230,158 was filed on December 18, 2012, and granted January 5, 2016. Ramaswamy qualifies as prior art to the FaceTec Asserted Patents under at least 35 U.S.C. §§ 102(a)(2). Ramaswamy anticipates and/or renders obvious (in combination with the knowledge of a person of ordinary skill in the art) all FaceTec Asserted Claims. The claim charts attached as **Exhibits 471-B, 606-B, 910-B, and 938-B** provide representative, non-limiting examples of where Ramaswamy discloses, either expressly or inherently, each element, thereby anticipating those claims. To the extent Plaintiff asserts that Ramaswamy does not anticipate any FaceTec Asserted

Claim, such FaceTec Asserted Claim would have been obvious in view of Ramaswamy alone and/or in view of the knowledge of a person of ordinary skill in the art. Additionally, it would have been obvious to combine or modify Ramaswamy with concepts from other prior art, including any of the other primary references, secondary references, and/or in view of the knowledge of a person of ordinary skill in the art, including as explained herein, to achieve the claimed inventions.

3. U.S. PATENT PUB. NO. 2011/0299741 ("ZHANG")

U.S. Patent Pub. No. 2011/0299741 was filed on June 8, 2010, and published December 8, 2011. Zhang qualifies as prior art to the FaceTec Asserted Patents under at least 35 U.S.C. §§ 102(a)(1), 102(a)(2). Zhang anticipates and/or renders obvious (in combination with the knowledge of a person of ordinary skill in the art) all FaceTec Asserted Claims. The claim charts attached as **Exhibits 471-C, 606-C, 910-C, and 938-C** provide representative, non-limiting examples of where Zhang discloses, either expressly or inherently, each element, thereby anticipating those claims. To the extent Plaintiff asserts that Zhang does not anticipate any FaceTec Asserted Claim, such FaceTec Asserted Claim would have been obvious in view of Zhang alone and/or in view of the knowledge of a person of ordinary skill in the art. Additionally, it would have been obvious to combine or modify Zhang with concepts from other prior art, including any of the other primary references, secondary references, and/or in view of the knowledge of a person of ordinary skill in the art, including as explained herein, to achieve the claimed inventions.

4. U.S. PATENT NO. 8,977,010 ("FRISCHHOLZ")

U.S. Patent No. 8,977,010 was filed on October 19, 2012, and granted March 10, 2015. Frischholz qualifies as prior art to the FaceTec Asserted Patents under at least 35 U.S.C. §§ 102(a)(1), 102(a)(2). Frischholz anticipates and/or renders obvious (in combination with the knowledge of a person of ordinary skill in the art) all FaceTec Asserted Claims. The claim charts attached as **Exhibits 471-D, 606-D, 910-D, and 938-D** provide representative, non-limiting examples of where Frischholz discloses, either expressly or inherently, each element, thereby anticipating those claims. To the extent Plaintiff asserts that Frischholz does not anticipate any FaceTec Asserted Claim, such FaceTec Asserted Claim would have been obvious in view of Frischholz alone and/or in view of the knowledge of a person of ordinary skill in the art.

Additionally, it would have been obvious to combine or modify Frischholz with concepts from other prior art, including any of the other primary references, secondary references, and/or in view of the knowledge of a person of ordinary skill in the art, including as explained herein, to achieve the claimed inventions.

5. U.S. PATENT APPLICATION PUB. NO. 2008/0192980 ("PARK")

U.S. Patent Application Pub. No. 2008/0192980 was filed on August 13, 2007 and published on August 14, 2008. Park qualifies as prior art to the FaceTec Asserted Patents under at least 35 U.S.C. §§ 102(a)(1), 102(a)(2). Park anticipates and/or renders obvious (in combination with the knowledge of a person of ordinary skill in the art) all FaceTec Asserted Claims. The claim charts attached as **Exhibits 471-E, 606-E, 910-E, and 938-E** provide representative, non-limiting examples of where Park discloses, either expressly or inherently, each element, thereby anticipating those claims. To the extent Plaintiff asserts that Park does not anticipate any FaceTec Asserted Claim, such FaceTec Asserted Claim would have been obvious in view of Park alone and/or in view of the knowledge of a person of ordinary skill in the art. Additionally, it would have been obvious to combine or modify Park with concepts from other prior art, including any of the other primary references, secondary references, and/or in view of the knowledge of a person of ordinary skill in the art, including as explained herein, to achieve the claimed inventions.

6. U.S. PATENT NO. 10,755,084 ("GANONG")

U.S. Patent No. 10,755,084 was filed on November 6, 2018 and claims priority to an application filed December 31, 2007. Ganong qualifies as prior art to the FaceTec Asserted Patents under at least 35 U.S.C. §§ 102(a)(1), 102(a)(2). Ganong anticipates and/or renders obvious (in combination with the knowledge of a person of ordinary skill in the art) all FaceTec Asserted Claims. The claim charts attached as **Exhibits 471-F, 606-F, 910-F, and 938-F** provide representative, non-limiting examples of where Ganong discloses, either expressly or inherently, each element, thereby anticipating those claims. To the extent Plaintiff asserts that Ganong does not anticipate any FaceTec Asserted Claim, such FaceTec Asserted Claim would have been obvious in view of Ganong alone and/or in view of the knowledge of a person of ordinary skill in the art. Additionally, it would have been obvious to combine or modify Ganong with concepts from other

prior art, including any of the other primary references, secondary references, and/or in view of the knowledge of a person of ordinary skill in the art, including as explained herein, to achieve the claimed inventions.

7. U.S. PATENT NO. 9,412,169 ("BUD")

U.S. Patent No. 9,412,169 B2 to Bud, et al., ("'169") granted August 9, 2016, qualifies as prior art to the FaceTec Asserted Patents under at least 35 U.S.C. §§ 102(a) because it is a patent that was filed before the effective filing date of the FaceTec Asserted Patents, depending on the effective filing date proven for each of the asserted claims. The '169 Patent was (1) published May 26, 2016 (US 2016/0148384), which is before the filing date of the '606 Patent's parent application (U.S. Patent No. 10,614,204) and Provisional Application (No. 62,460,670) as well as the '471 Patent's parent application (U.S. Patent No. 10,262,126); (2) filed August 28, 2015 (which is the same date the '606 Patent's C-I-P grand-parent application and the '471 Patent's grand-parent application (U.S. Patent No. 9,953,149)); and (3) claims priority to a provisional filed November 21, 2014, which is before any relevant disclosures in the provisional applications related to the FaceTec Asserted Patents. Bud anticipates and/or renders obvious (in combination with the knowledge of a person of ordinary skill in the art) all FaceTec Asserted Claims. The claim charts attached as **Exhibits 471-G, 606-G, 910-G, and 938-G** provide representative, non-limiting examples of where Bud discloses, either expressly or inherently, each element, thereby anticipating those claims. To the extent Plaintiff asserts that Bud does not anticipate any FaceTec Asserted Claim, such FaceTec Asserted Claim would have been obvious in view of Bud alone and/or in view of the knowledge of a person of ordinary skill in the art. Additionally, it would have been obvious to combine or modify Bud with concepts from other prior art, including any of the other primary references, secondary references, and/or in view of the knowledge of a person of ordinary skill in the art, including as explained herein, to achieve the claimed inventions.

8. MOVING FACE SPOOFING DETECTION VIA 3D PROJECTIVE INVARIANTS ("MARSICO")

"Moving Face Spoofing Detection via 3D Projective Invariants" by Marsico et al. ("Marsico") qualifies as prior art under at least 35 U.S.C. § 102(a)(1) because it is a printed publication that was publicly available before the effective filing date of U.S. Patent No. 11,157,606

("the '606 Patent"). Marsico anticipates and/or renders obvious (in combination with the knowledge of a person of ordinary skill in the art) all FaceTec Asserted Claims. The claim charts attached as **Exhibits 471-H, 606-H, 910-H, and 938-H** provide representative, non-limiting examples of where Marsico discloses, either expressly or inherently, each element, thereby anticipating those claims. To the extent Plaintiff asserts that Marsico does not anticipate any FaceTec Asserted Claim, such FaceTec Asserted Claim would have been obvious in view of Marsico alone and/or in view of the knowledge of a person of ordinary skill in the art. Additionally, it would have been obvious to combine or modify Marsico with concepts from other prior art, including any of the other primary references, secondary references, and/or in view of the knowledge of a person of ordinary skill in the art, including as explained herein, to achieve the claimed inventions.

9. U.S. PATENT NO. 9,330,322 ("FERREN")

U.S. Patent No. 9,330,322 was filed on October 5, 2016, and granted May 3, 2016. Ferren qualifies as prior art to the FaceTec Asserted Patents under at least 35 U.S.C. § 102(a)(2). Ferren anticipates and/or renders obvious (in combination with the knowledge of a person of ordinary skill in the art) all FaceTec Asserted Claims. The claim charts attached as **Exhibits 471-I, 606-I, 910-I, and 938-I** provide representative, non-limiting examples of where Ferren discloses, either expressly or inherently, each element, thereby anticipating those claims. To the extent Plaintiff asserts that Ferren does not anticipate any FaceTec Asserted Claim, such FaceTec Asserted Claim would have been obvious in view of Ferren alone and/or in view of the knowledge of a person of ordinary skill in the art. Additionally, it would have been obvious to combine or modify Ferren with concepts from other prior art, including any of the other primary references, secondary references, and/or in view of the knowledge of a person of ordinary skill in the art, including as explained herein, to achieve the claimed inventions.

ii. ADDITIONAL REFERENCES

Additional prior art references ("secondary references") are relevant to the invalidity of the FaceTec Asserted Claims. To the extent a primary reference does not disclose or render obvious one or more of the elements of the FaceTec Asserted Claims, a person of ordinary skill in the art

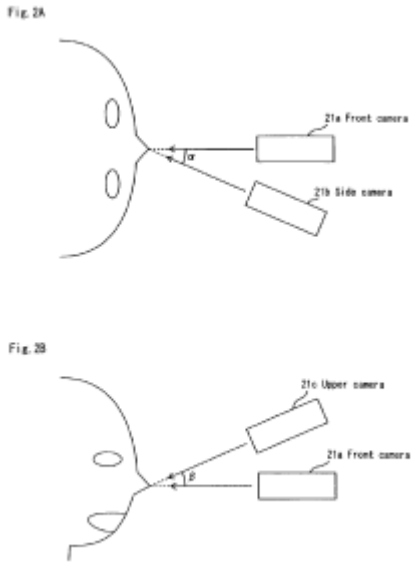
would be motivated to combine the primary reference with any other primary reference(s) that discloses that limitation or with one or more of these secondary references.

The secondary references include:

1. U.S. PATENT PUB. NO. 2008/0304716 ("HIROSE")

Hirose discloses a face recognition device that captures the face of a person from different directions and uses these images to identify the person by comparing facial data with individual identification data previously stored in the device that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Hirose include:

> "A face recognition device of the present invention comprises a plurality of imaging devices capable of simultaneously capturing the face of a person from directions different from one another, and a storage device, the device further comprising: a depression/protrusion data determination device determining data indicating difference of areas of portions in a predetermined color, as depression/protrusion data indicating facial depression/protrusion features of the person, by calculating the difference of the areas based on comparison of images including the face captured from two directions, the images being simultaneously captured using the plurality of imaging devices; and an identification device identifying the person by comparing the depression/protrusion data of the person determined by the depression/protrusion data determination device with individual identification data previously stored in the storage device to be the reference of comparison with the depression/protrusion data." [Abstract]



[Figs. 2A and 2B]

"(1) A face recognition device provided with a plurality of imaging devices capable of simultaneously capturing the face of a person from directions different from one another, and a storage device, the device comprising:

a depression/protrusion data determination device determining data indicating difference of areas of portions in a predetermined color, as depression/protrusion data indicating facial depression/protrusion features of the person, by calculating the difference of the areas based on comparison of images including the face captured from two directions, the images being simultaneously captured using the plurality of imaging devices; and

an identification device identifying the person by comparing the depression/protrusion data of the person determined by the depression/protrusion data determination device with individual identification data previously stored in the storage device to be the reference of comparison with the depression/protrusion data.

According to the invention of (1), a plurality of images indicating the face of a person simultaneously captured from directions different from one another are obtained using the plurality of imaging devices. Then, the difference of areas of the portions in the predetermined color (the shadow portions generated due to the depression/protrusion on the face) is calculated, and the data indicating the difference of areas is determined as the depression/protrusion data indicating the facial depression/protrusion of the person.

Thereafter, the determined depression/protrusion data is compared with the previously registered individual identification data to be the reference of comparison, so as to identify the person." [0016-0019]

"(3) A face recognition device comprising: a plurality of cameras capable of simultaneously capturing the face of a person from directions different from one another; an arithmetic processing device; and a storage device,

wherein
the arithmetic processing device is to execute the processing of

(A) determining data indicating difference of areas of portions in a predetermined color, as depression/protrusion data indicating facial depression/protrusion features of the person, by calculating the difference of the areas based on comparison of images including the face captured from two directions, the images being simultaneously captured using the plurality of camera, and

(B) identifying the person by comparing the depression/protrusion data of the person determined in the processing (A) with individual identification data previously stored in the storage device to be the reference of comparison with the depression/protrusion data.

According to the invention of (3), a plurality of images indicating the face of the person simultaneously captured from directions different from one another are obtained using the plurality of cameras. Then, the difference of areas of the portions

in the predetermined color (the shadow portions generated due to the depression/protrusion on the face) is calculated, and the data indicating the difference of areas is determined as the depression/protrusion data indicating the facial depression/protrusion of the person." [0033-0038]

"Further, in the invention of (3), the data stored as the individual identification data is data showing the difference of areas of the shadow portions in the case where images of the face of the person are simultaneously captured from directions different from one another and does not have a large volume as image data. Therefore, since the volume of data to be stored is small, even individual identification data of a large number of people can be stored in a small volume." [0041]

"The face recognition device according to the present embodiment is provided with three cameras which capture the face of a person from directions different from one another. It is possible to three-dimensionally recognize the facial features by capturing images of the face of the person from different directions using the plurality of cameras." [0060]

"Hereinafter, the direction from which the front camera 21 a captures images is also referred to as a "front direction". Further, the direction from which the side camera 21 b captures images is also referred to as a "lateral direction". Furthermore, the direction from which the upper camera 21 c captures images is also referred to as an "upper direction".

The lamp 22 is for applying light to the face of the person when the three cameras capture images.

In the present embodiment, the front camera 21 a, the side camera 21 b, and the upper camera 21 c capture images of the face of the person while the lamp 22 is applying light to the face of the person.

Further, the three cameras capture images at the same time.

The front camera 21 a, the side camera 21 b, and the upper camera 21 c function as the imaging devices in the present invention." [0074-0078]

"As described above, according to the face recognition device relating to the present embodiment, three images indicating the face of the person simultaneously captured from directions different from one another by the front camera 21 a, the side camera 21 b, and the upper camera 21 c. Then, the difference of areas of the portion (the shadow portion generated due to the depression/protrusion on the face) in the predetermined color is calculated; and the data indicating the difference of areas is determined as the depression/protrusion data indicating the features of the depressed/protruding parts of the face of the person.

The person is then determined by comparing the determined depression/protrusion data and the individual identification data to be the reference of comparison with the depression/protrusion data.

As described above, in the face recognition device according to the present embodiment, it is possible to promptly conduct identification without taking time in processing, since the comparatively simple processing of obtaining the difference of the predetermined areas, not the complicated processing of extracting specific facial features such as the eyes, nose, and mouth, is conducted.

Further, in the face recognition device according to the present embodiment, the data stored as the individual identification data is data showing the difference of areas of the shadow portions in the case where images of the face of the person are simultaneously captured from directions different from one another and does not have a large volume as image data. Therefore, since the volume of data to be stored is small, even individual identification data of a large number of people can be stored in a small volume.

Further, in the face recognition device according to the present embodiment, data indicating the facial depression/protrusion features is used in identification. Namely, face recognition is conducted based on the three-dimensional features of the face.

The three-dimensional features of the face indicate the irregularities of face parts, and are unique to each person. Namely, since the depression/protrusion on the face represents the facial features of a person extremely well, comparatively highly accurate identification can be realized according to the face recognition device relating to the present embodiment, even though a simple method is used therein.

Further, the depression/protrusion data in the present embodiment comprises information relating to the two types of difference of areas, namely, two types of information including information on the difference between the area of the portion in the predetermined color in the image data obtained by the front camera 21 a and the area of the portion in the predetermined color in the image data obtained by the side camera 21 b, and information on the difference between the area of the portion in the predetermined color in the image data obtained by the front camera 21 a and the area of the portion in the predetermined color in the image data obtained by the upper camera 21 c. Therefore, as compared to the case of using one type of difference of the areas, more accurate depression/protrusion data can be obtained." [0124-0130]

2. U.S. PATENT NO. 9,690,998 ("NEGI")

Negi discloses a face recognition device that captures the face of a person from different directions and uses these images to identify the person by comparing facial data with individual identification data previously stored in the device that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Negi include:

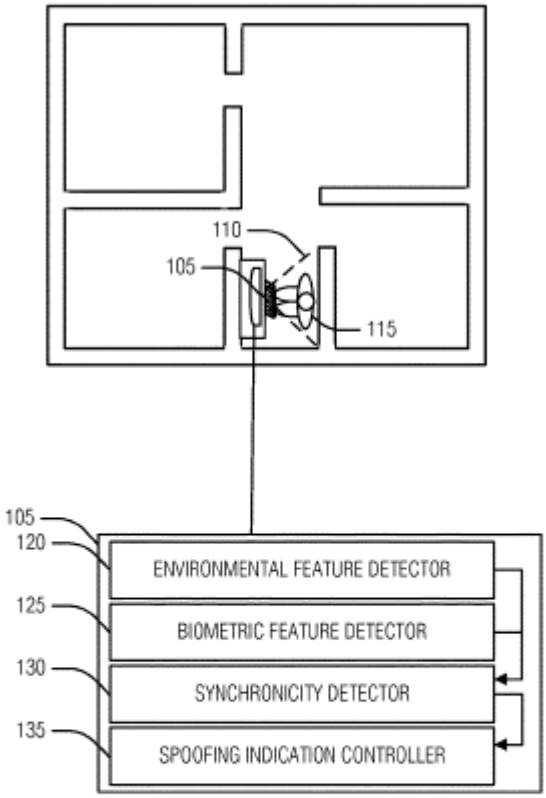
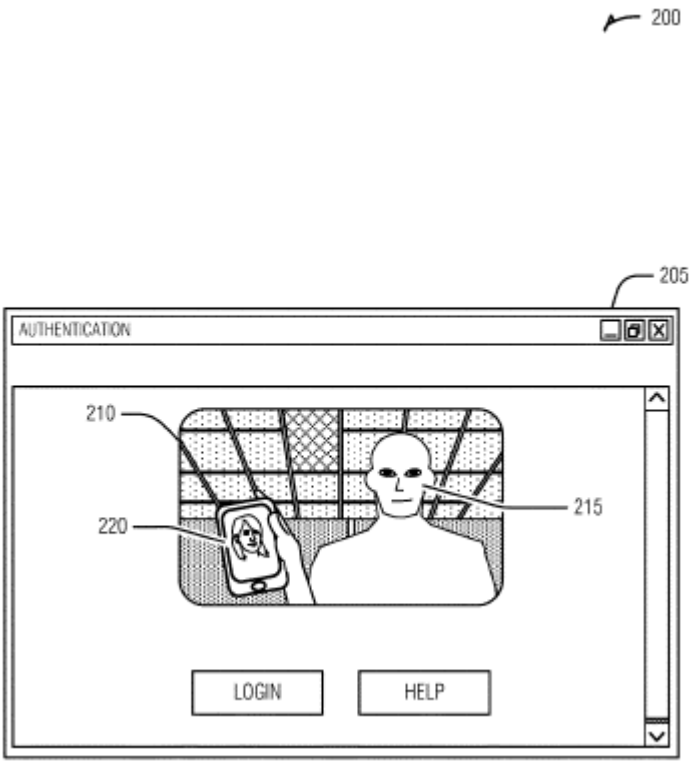

110
105
115
105
120
ENVIRONMENTAL FEATURE DETECTOR
125
BIOMETRIC FEATURE DETECTOR
130
SYNCHRONICITY DETECTOR
135
SPOOFING INDICATION CONTROLLER

FIG. 1


200
205
AUTHENTICATION
210
215
220
LOGIN
HELP

[Fig. 2]

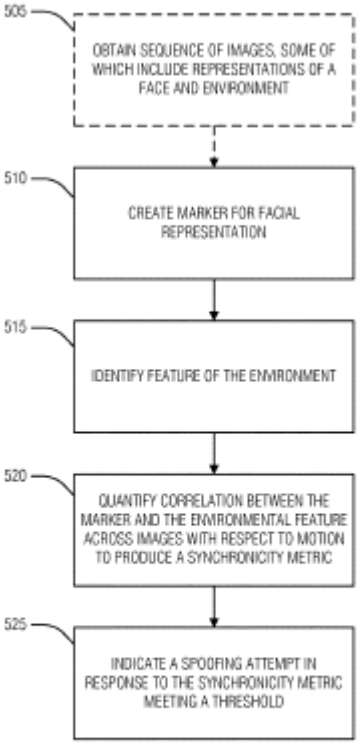

505
OBTAIN SEQUENCE OF IMAGES, SOME OF WHICH INCLUDE REPRESENTATIONS OF A FACE AND ENVIRONMENT
510
CREATE MARKER FOR FACIAL REPRESENTATION
515
IDENTIFY FEATURE OF THE ENVIRONMENT
520
QUANTIFY CORRELATION BETWEEN THE MARKER AND THE ENVIRONMENTAL FEATURE ACROSS IMAGES WITH RESPECT TO MOTION TO PRODUCE A SYNCHRONICITY METRIC
525
INDICATE A SPOOFING ATTEMPT IN RESPONSE TO THE SYNCHRONICITY METRIC MEETING A THRESHOLD

FIG. 5

"Systems and techniques for facial spoofing detection in image based biometrics are described herein. A marker may be created for a representation of a face in a first plurality of images of a sequence of images. The marker corresponds to a facial feature of the face. An environmental feature of an environment of the face may be identified across a second plurality of images of the sequence of images. A correlation between the marker and the environmental feature in the sequence of images may be quantified to produce a synchronicity metric. A spoofing attempt may be indicated in response to the synchronicity metric meeting a threshold." [Abstract]

"To prevent facial spoofing, two types of anti-spoofing techniques may be employed (alone or in combination): 1) asking users to perform certain tasks (e.g., invoking dynamic user involvement that may be hard to predict to complicate spoofing); or 2) analyzing the context (e.g., environment) of the image capture to determine whether the captured image represents a "live" user. Both techniques may distinguish between a live user and a facsimile, but merely asking for more user input may present some user experience challenges (e.g., how to represent the quest, difficulty for user's to follow the request, excessive time in performing the requests, etc.). Analyzing the context in which the image was captured, however, may avoid the user experience challenges associated with a more interactive technique." [2:9-23]

"The described components and techniques provide facial spoofing protection without involving a challenge-response user action by analyzing the facial image capture context. For example, the context of image acquisition may include analyzing relative motion of a face and environmental features (e.g., the background) across a sequence of images. Thus, if the captured representation of the face includes movements that synchronize with background features (e.g., edges of a mobile device), it may be determined that the face is a spoof attempt. Further, tell-tale contours of known device edges (e.g., the body, screen, etc.) may be determined and further implicate spoofing when, for example, the face is bounded by the edges of a digital device." [2:24-36]

"An example of facial capture context may include one or more of the following features to perform facial spoofing detection in image based biometrics." [2:37-39]

"If face is not included inside the moving frame, it could be a live user holding or using a phone (e.g., off to the side) for valid reasons (e.g., reasons other than making a spoofing attempt). However, edge movement may still be monitored to track device movement within the sequence of images. This may be beneficial when video quality is low and the edges may not be detectable in every frame. Thus, the position of the device edges may be inferred in a frame in which they are not detectable or positively detected, for example, by noting where they were last detected. In this scenario, a face appearing in an area that is within an inferred frame (e.g., because the edges aren't detected in the frame with the face) may still be called out as a spoofing attempt. As noted above, edges, or other features, that move together may be tracked to infer the position of moving entities from previous captured images to captured images where the entity cannot be found. Synchronized movement may be

tracked with respect to any of rotational, scaling, or translational movement. In an example, capturing these moving features and inferring their position in captured images in which they do not appear is referred to as capturing partial moving features." [2:60-3:22]

"The spoofing indication criteria may include the following: 1) if a face is present and inside a detected device (e.g., edge contours of known device), then indicate spoofing unless, in an example, the eyes and device edges do not all move together; 2) If the face is present but not inside the device, then determine whether face movements synchronize with other environmental features—This may allow detection of background image features when, for example, the device is held too close to the camera to view the device edges—and indicate a spoofing attempt when the eyes and detectable moving edges all move together (e.g., within a threshold); 3) If the face is not present and at least two device edges move together, then tag as the two devices edges as partial moving edges and infer a boundary of a device display in following captured image when the edges are not visible in the following captured image, and indicate spoofing if future detected face is within the inferred boundary of the device." [3:26-43]

"The sequence of images may include a first plurality of images containing a representation of the user's face, and a second plurality of images in the sequence of images including a representation of an environment of the face." [3:57-63]

"The biometric feature detector 125 may analyze the sequence of images and identify the representation of the user's face in the first plurality of images. In an example, the biometric feature detector 125 may create a marker for the representation of the face. The maker corresponds to a feature of the face—examples may include the eyes, nose, mouth, ears, or points defined by these features, such as a centroid of the eyes, a line that intersects the center of each eye, etc." [4:41-49]

"FIG. 2 illustrates an example of image capture interface 200 for facial spoofing detection in image based biometrics, according to an embodiment. The interface 200 may include a dialog 205 user interface. The dialog 205 may include the sequence of images in a viewing port 210. As shown, the viewing port 210 includes an image in the sequence of images containing a representation of the user's face 215 as well as a device 220 with another representation of a face.

FIG. 3 illustrates an example of image analysis 300 for facial spoofing detection in image based biometrics, according to an embodiment. The image illustrated in FIG. 2 may be analyzed to discern relative motion of environmental features and the representations of the faces. As illustrated, dashed lines are non-moving edges, dotted lines are curved lines in the image, and solid lines are moving edges. The analysis 300 may detect the represented faces and create the marker 305 for the live face and the maker 310 for the spoofed face. Further, the analysis 300 may determine that the edges 315 are moving together and enclose an area. Thus, from the analysis 300, it may be determined that the marker 310 is within the moving edges 315, and thus such a face is a possible spoofing attempt that should be flagged or otherwise fail to authenticate the user. In contrast, the marker 305 is not within the edges 315

and so cannot be so easily assessed as a spoofing attempt. However, if the marker 305 moves synchronously to the moving edges 315, it may be determined that everything in the image is a facsimile of the user's environment—although in the illustrated example, this is unlikely because some of the edges are not moving relative to the moving edges 315.

The example illustrated in FIG. 3 includes both live and spoofed faces. It should be noted that the detection of a spoofed face alone will result in spoofing attempt indication. Further, when both live and other faces (e.g., pictures) are present, the discrimination between the two may limit the candidate faces for authentication by simply eliminating the other faces." [5:47-6:17]

"At optional operation 505, a sequence of images from a camera may be obtained. In an example, a raw sequence of images may be obtained first. The raw sequence of images may be modified to create the sequence of images. In an example, the modification may include a change to at least one of gain, exposure, or gamma to enhance edge detection. In an example, the modification may include applying a noise filter to the sequence of raw images to produce the sequence of images. The sequence may include a first plurality of images including a representation of a face and a second plurality of images includes a representation of an environment of the face. In an example, the sequence of images may include at least thirty images." [6:55-67]

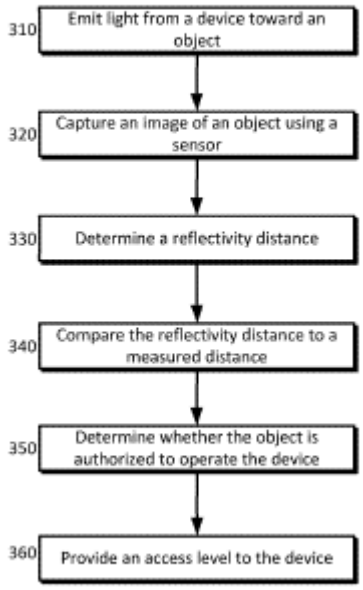
"At operation 510, a marker for the representation of the face may be created. The marker may correspond to a facial feature identifiable in the representation of the face. In an example, the marker may be selected such that changes in the marker between images in first plurality of images indicate changes in movements of the representation of the face. In an example, the marker includes a line drawn between the eyes of the facial representation." [7:1-8]

"At operation 520, a correlation between the marker and the environmental feature may be quantified with respect to motion across the sequence of images to produce a synchronicity metric. In an example, where the marker is outside the convex hull, the synchronicity metric is reduced. In an example, the first plurality of images does not include a member of the second plurality of images, the missing member precedes in time the first plurality of images and includes a determined resting spot for the moving edges that outlining an area, and the marker is within the area for an image in which the moving edges are not detected following the member, the marker is determined to be within the convex hull for the synchronicity metric. Thus, the device position is inferred from prior data and the face is determined to originate from the device even though the device (or its edges) is not detectable in the specific image in which the facial representation was found. In an example, the marker is sought within a display area of a known device, increasing the synchronicity metric if found there, and decreasing the synchronicity metric otherwise. Thus, the method 500 may discriminate between an image displayed by the device and possibly an image reflected by a case, bezel, or other non-display portion of the device." [7:31-54]

3. U.S. PATENT NO. 9,524,421 ("ROSS")

Ross discloses a face recognition device that captures the face of a person from different directions and uses these images to identify the person by comparing facial data with individual identification data previously stored in the device that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Ross include:

FIG. 3



> "Facial recognition can be used to determine whether or not a user has access privileges to a device such as a smartphone. It may be possible to spoof an authenticated user's image using a picture of the user. Implementations disclosed herein utilize time of flight and/or reflectivity measurements of an authenticated user to compare to such values obtained for an image of an object. If the time of flight distance and/or reflectivity distance for the object match a measured distance, then the person (i.e., object) may be granted access to the device." [Abstract]

> "Disclosed is an anti-spoofing technology that incorporates a light emitting source. The light may reflect off an external object and return to the device where it may be captured (e.g., by a photometric sensor) and analyzed for the time of flight of the light and reflectivity. In some configurations, the measurements for time of flight and/or reflectivity may complement a distance detected based on landmarks of a person's face. Distance measurements may be obtained for an object based on one or more of reflectivity, time of flight, and between two or more landmarks. For example, facial recognition may be used to determine that the object appears similar to the authorized user; however, one or more distance measurements based on

reflectivity, time of flight, and/or two or more landmarks may not match within a confidence interval (e.g., the distance based on reflectivity may be significantly different from the time of flight distance)." [2:52-67]

"In an implementation, an example of which is provided in FIG. 3, a profile of a first face may be obtained. For example, a profile of the first face may be generated during an enrollment process or phase. An enrollment phase may refer to when a user first associates the user's identity (e.g., user name, email, other accounts such as cloud storage, credit card, user name, password, etc.) with a device. The first face may correspond to a user authorized to operate the device. The profile may refer to one or more images corresponding to a face of an authorized user and/or a mathematical representation of the face of a user authorized to operate the device. Representations of the first face may be used subsequently as a component of facial recognition algorithms. The profile may include, for example, reflectivity data, time of flight data, and/or landmarks of the first face of a user authorized to operate the device. Reflectivity and/or time of flight data associated with the first face may be expressed as a range of values and/or in terms of a distance measurement. The profile may include measurements related to identified areas (e.g., landmarks) of the user's face, such as the distance between the user's eyes. Facial recognition software may store other features necessary to uniquely identify the user's face to the profile such as a color intensity, a histogram of gradients, or a template as described below. The profile may include time of flight data for identified features of the user's face for example." [4:14-39]

"In some configurations, a profile for the object may be generated. The object profile may include a mathematical representation of the object, reflectivity data, time of flight data, and/or landmarks identified in the object, similar to the profile obtained of a user authorized to operate a device. In some instances, facial recognition algorithms may be applied to the image captured by the device and may identify a second face in the image of the object (e.g., a face of a user other than the authorized user). A first face profile may be obtained as described earlier. The profile of the object may be compared to the profile of the first face of a user authorized to operate the device. A comparison of the object profile to the first face profile may be an initial test to determine whether or not a user is authorized to operate a device. A picture of the first face may be sufficient to fool the device into thinking that the actual user is attempting to gain access to the device. The measured distance may be determined and compared to the reflectivity distance and/or time of flight distance. The comparison at this stage may indicate a discrepancy caused by the use of a picture of the first face instead of the actual user to whom the first face belongs. Thus, the object may be denied access to the device." [6:12-33]

"In some configurations, the time of flight data may be plotted against the reflectivity for both the object and the first face (see, for example, FIG. 5). Use of a picture, for example, that contains an image of an authorized user to gain access to the device would have a distinct profile compared to that of the first face. For example, a time of flight for light reflected from a picture would be relatively uniform depending on the angle at which the picture is oriented relative toward to the light sensor. In contrast, the time of flight for light reflected from a person's face

would have a distinct profile. For example, light reflected from a person's nose would have a lower time of flight compared to light reflected from a person's ears. The reflectivity of a piece of paper containing an image of an authorized user may absorb and scatter and/or reflect light in a manner that is different from that of the user's actual face. For example, the reflectivity for one, some, or all particular points on the sheet of paper may be the same as, or within a relatively small range of that of one or more other points on the sheet of paper. In contrast, the reflectivity of a person's face may vary from one point to the next. Plotting the reflectivity versus the time of flight in the example of a sheet of paper containing an image of the first face may reveal a narrowly defined pattern whereas a person's face may have a more distributed appearance in the plot." [6:34-58]

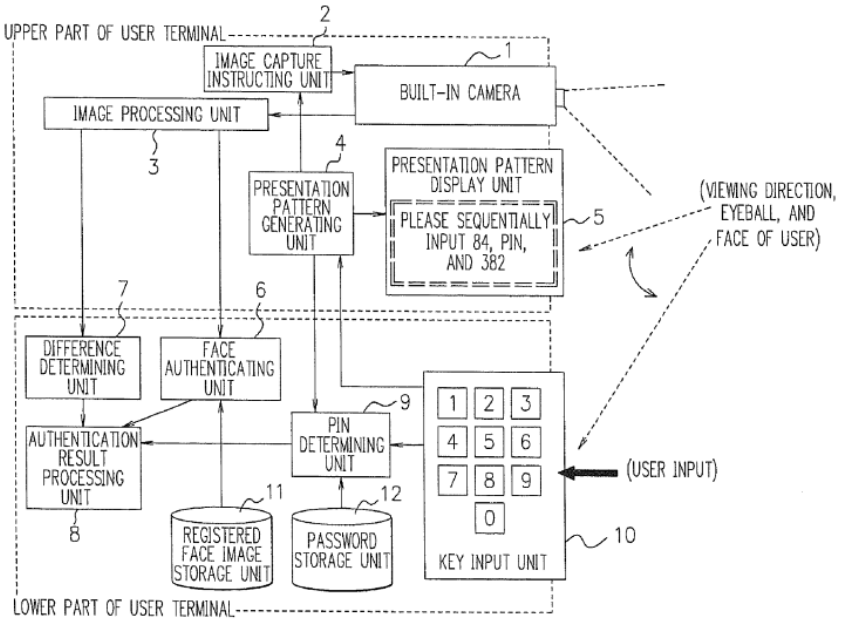
"To unlock the device using facial recognition technology, a user (such as authorized user) may provide an authentication image that represents at least a portion of his/her face. In some examples, the user may actively cause a camera of the device to capture the authentication image. The device may then compare the captured authentication image with the enrollment image, and determine whether or not the images are sufficiently similar to each other for facial recognition purposes. For example, the device may utilize one or more facial recognition programs to compare metrics associated with the authentication image to metrics associated with the enrollment image. Some examples of metrics may include distances between facial elements (pupil-to-pupil, mouth width, etc.), contours of various facial features, pixilation corresponding to skin tone or texture, hair and/or eye color, and many others. Facial recognition programs running on computing device may perform the comparison using one or more well-known recognition algorithms, such as geometric and/or photometric approaches, three-dimensional (3D) modeling and recognition techniques, principal component analysis using Eigenfaces, linear discriminate analysis, elastic bunch graph matching, pattern matching, and dynamic link matching, to name just a few. Based on comparison-based values, such as pre-programmed acceptable margins of error, facial recognition programs running on the device may determine whether or not the authentication image and the enrollment image are sufficiently similar to one another for facial recognition. In instances where the facial recognition programs grant a match, the user may successfully unlock the device. Conversely, if the facial recognition programs deny a match, the user may be unable to unlock the device and the device may continue to operate in locked mode." [7:49-8:14]

"The device may identify areas of the image that are associated with the eyes of the authorized user as landmarks. The greater the number of pixels between the eyes, the closer the object maybe positioned to the device such as where a person has positioned a picture of a user in front of a camera in an attempt to spoof an authorized user's face. The device may compare the distance between the object and the device to an expected distance, and reject the unlock attempt if the detected distance and the expected distance do not match. For example, when the device detects that the number of pixels between the eyes exceeds a preprogrammed threshold (e.g., 10 centimeters), the device may identify this as an attempt to "fool" the facial recognition programs running on the device by obtaining access to the device based

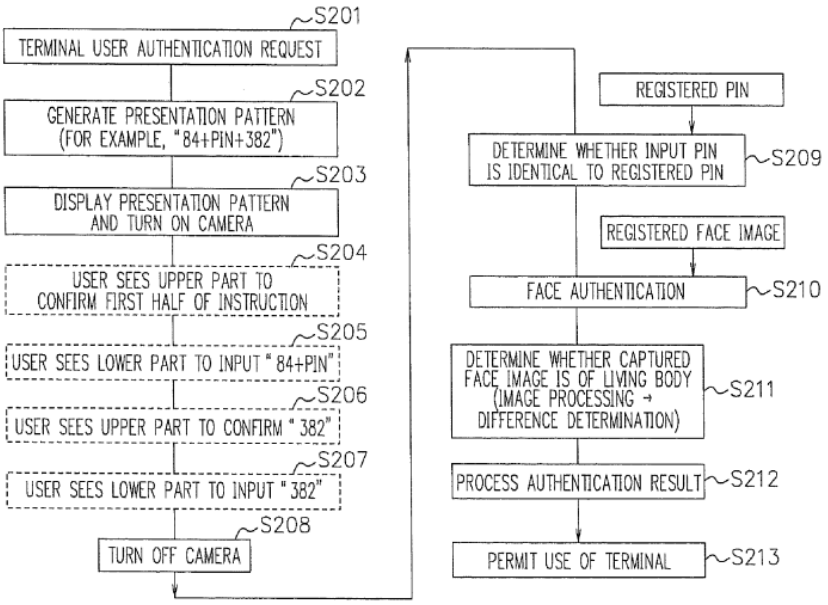
upon an image of an authorized user's face instead of the user's actual face." [8:23-38]

4. U.S. PATENT NO. 8,290,220 ("UCHIDA")

Uchida discloses a face authentication device that captures the face of a user as the user moves their face to difference positions and uses these images to determine if the captured images are of a live person that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Uchida include:



[Fig. 1]



[Fig. 2]

"The present invention relates to a face authentication technique for identifying a user using personal information equipment, such as a mobile phone." [1:7-9]

"In an example of authentication method using biometric features, such as a face of an authenticated user, a face pattern of an authorized user is captured by a camera of a terminal beforehand, and then registered in the terminal. At user authentication, the face of the user who attempts to use the terminal is captured by the camera. When similarity between the captured face image and the registered face image is sufficiently high, the user is determined as an authorized user, and the user authentication succeeds." [1:32-40]

"In order to achieve the exemplary object, according to an exemplary of the invention, a face authenticating apparatus includes: allowing a presentation pattern display unit that is provided at a different position from a key input unit to display an instruction for a user to input a key pattern during face authentication; allowing an image capturing unit to capture a face of a user and/or a movement of a portion of the face of the user during a portion of or the entire time from when the presentation pattern display unit displays the instruction to when the key input is completed; and determining whether the captured face image is of a living body." [2:26-36]

"The image capture instructing unit 2 controls the built-in camera 1 to capture a moving picture of the user's face in the view during the time from when the instruction is displayed on the presentation pattern display unit 5 to when the user completes the input of information to the key input unit 10, and then the image processing unit 3 processes the captured image. In this process, the moving picture is divided into a plurality of frames captured in the temporal direction, and a portion of or the entire frame image group is used for face authentication and the biometric verification of the face." [3:25-34]

"When the similarity between the captured face image and the registered face image is higher than a threshold value, the face authentication succeeds, and the result is notified to the authentication result processing unit 8.

In a biometric verification process of the difference determining unit 7, a plurality of frame images captured in the temporal direction are compared to each other, and a difference therebetween is evaluated to determine whether the face of a living body is captured, or a photograph or a planar moving picture is captured." [3:41-50]

"When the PINs are identical to each other, face authentication by the face authenticating unit succeeds, and the difference determining unit determines that the face of a living body is captured, the authentication result processing unit unlocks the user terminal to allow the use of the terminal." [3:56-60]

"The difference determining unit 7 performs a position adjustment process for compensating for the relative movement between the camera and the face on a plurality of frames of face images, cuts out a face image portion from the frame, and determines the similarity between the plurality of frames with regard to the center of the face image including the eyes, the nose, and the mouth (S211). If a cumulative value of similarity scores including detailed portions of the images between the frames, particularly, the positions of the eyeball of the eye is larger than a threshold value, it is determined that a still picture, such as a photograph, is presented. On the other hand, if the cumulative value of the similarity scores is smaller than the threshold value and it is determined that the detailed portions including, for example, the positions of the eyeball after the position adjustment process and the cut-out process are significantly different from each other, the difference determining unit 7 determines that the face of a living body is captured by the camera.

In the process of determining the face of a living body, the following method may be used: the positional relationship between a plurality of feature points in each frame that are defined by a plurality of organs, such as the outer corners and the inner corners of both eyes, the top and both sides of the nose, both ends of the mouth, and the center of the lip, is calculated, thereby calculating correlation between these feature points of the frames. When the positional relationship between the feature points in many frames has high correlation, the organs are not relatively moved, and thus it is possible to determine that a photograph is presented." [4:66-5:29]

"As described above, while the user alternately views the presentation pattern display unit 5 and the key input unit 10, the presentation pattern display unit 5 may display an instruction 'Please see built-in camera' to allow the user to face the built-in camera 1. In this way, it is possible to stably capture a full face image suitable for face authentication, and make the face of the user move in the vertical direction. As a result, it is possible to improve accuracy in determining the face of a living body." [6:7-15]

"Although the exemplary embodiments of the invention have been described above, the invention is not limited thereto, but various modifications and changes of the invention can be made without departing from the scope and spirit of the invention.

For example, an apparatus may read and execute a program for implementing the functions of the user terminals according to the above-described exemplary embodiments to perform the functions. The program may be transmitted to another computer system through a computer readable recording medium, such as a CD-ROM or a magneto-optical disk, or by carrier waves through the Internet or a telephone line, which is a transmission medium." [6:61-7:5]

"In the above-described exemplary embodiments, the system structure in which each function of the user terminal is implemented by one computer system is used, but the invention is not limited thereto. Each function of the user terminal may be implemented by a plurality of apparatuses.

The invention can be generally applied to a mobile phone or portable information communication equipment including a camera function." [7:6-13]

5. FACE LIVENESS DETECTION USING 3D STRUCTURE RECOVERED FROM A SINGLE CAMERA ("WANG")

Wang discloses a method of face liveness detection that uses facial structures over several images that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Wang include:

"In this paper, we propose a novel face liveness detection approach to counter spoofing attacks by recovering sparse 3D facial structure. Given a face video or several images captured from more than two viewpoints, we detect facial landmarks and select key frames. Then, the sparse 3D facial structure can be recovered from the selected key frames. Finally, an Support Vector Machine (SVM) classifier is trained to distinguish the genuine and fake faces. Compared with the previous works, the proposed method has the following advantages. First, it gives perfect liveness detection results, which meets the security requirement of face biometric systems. Second, it is independent on cameras or systems, which works well on different devices" [Pg. 1]

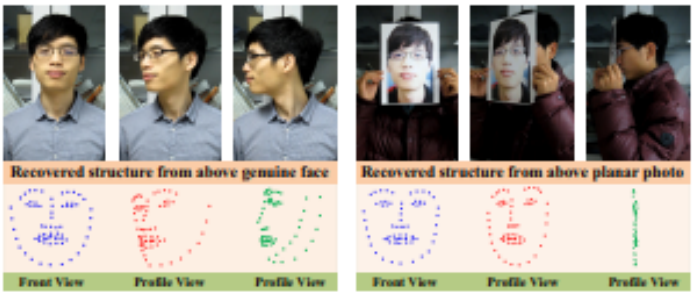


Figure 1. A comparison of recovered sparse 3D facial structures between genuine and photo face. There are significant differences between structures recovered from genuine and photo face.

[Fig. 1]

"The challenge-response is a human-computer interaction (HCI) method. The users are asked to response to the specific facial actions given by computer so that the genuine and fake faces can be classified. Eye blinking [12, 16], head rotation [2, 8], and mouth movement [8] are the most commonly used facial actions. The challenge-response methods achieve good results for face liveness detection. However, the users are asked to be highly cooperative with the system, which limits its application in practice." [Pg. 1]

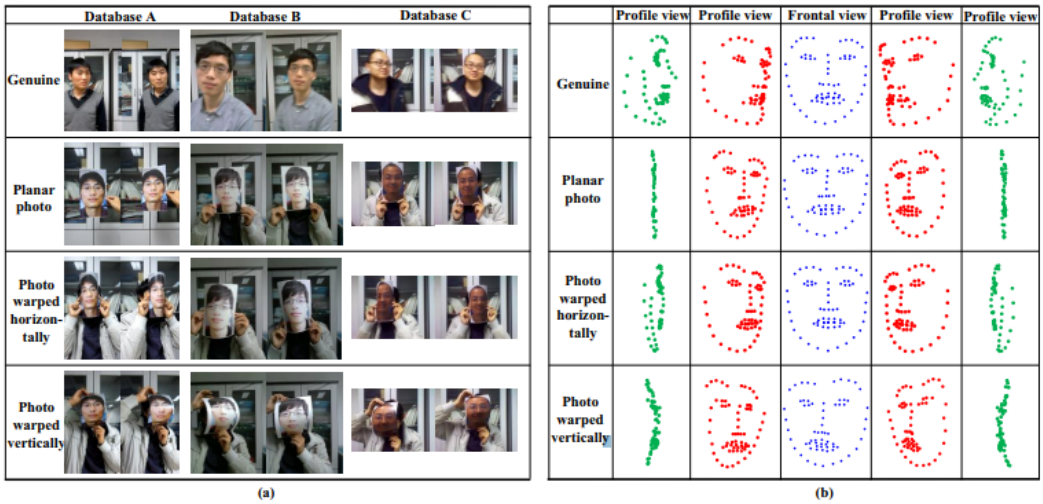
"In this paper, we propose a novel face liveness detection method by analyzing the sparse structure information in 3D space. As shown in Fig. 1, structures recovered from genuine faces usually contain sufficient 3D structure information, while structures recovered from photos are usually planar in depth. We firstly recover the sparse 3D facial structure with the input images and then an SVM classifier is trained based on the 3D structures from the genuine and fake faces. Different from the reflectance based methods, the proposed method is device independent and can work well with various inputs as long as two images from different viewpoints are provided." [Pg. 2]

"The face images with different viewpoints can be captured from a fixed camera with face moving or reversed." [Pg. 2]

"In our work, key frames are defined as those frames which are propitious to recover facial structure. We rely on graph similarity to incrementally extract key frames from an input sequence which are more likely to be those captured in various viewpoints in practice. In the case that a certain relative motion between the face and the camera happens, it is obvious that locations of facial landmarks in the image will be various along with the motion. That is, different viewpoints will lead to different distributions of facial landmarks. Based on this relation, we compute the distribution distance of landmarks to evaluate the difference of viewpoints between current frame and existing key frames in pool." [Pg. 2]

"[W]e describe our algorithm for initial facial structure recovery based on facial landmarks from two face images with different viewpoints. Let $q = \{q_1, q_2, ..., q_N\}$ be the facial landmarks in one image and $q' = \{q_1', q_2', ..., q_N'\}$ in another image, where qi denotes a 2D point in the image, N is the number of facial landmarks for a face (N=68 in our experiment)." [Pg. 2]

"After we recover the sparse 3D structure, we first align these structures and then structure features are extracted for classification. In this work, we use a predefined 3D facial structure as a reference to align a recovered structure using a coarse-to-fine way. … After alignment, the 3D coordinates of sparse structure are concatenated to form a feature vector. The SVM classifier is then trained based on the features to classify the genuine and fake face samples." [Pg. 4]



"Figure 2. (a) sample frames of a subject from database A, B and C respectively. In each database, we warp the photos horizontally and vertically. These two kind of warping approximate the real face structure much. (b) recovered structures from genuine face, planar photo, photo warped horizontally and photo warped vertically, respectively." [Fig. 2]

"In this paper, a sparse 3D structure based face liveness detection method is proposed. Given at least two face images captured from different viewpoints, the 3D sparse facial structure can be recovered. Based on this, the genuine and fake faces like printed photos can be classified. Different from the popular texture based method, the proposed method is device independent and thus more applicable in practice. Moreover, the requirements of two images from different viewpoints is easy to be met in real application and the proposed method has great potential to be deployed with the existing face recognition system." [Pg. 6]

6. U.S. PATENT NO. 9,408,076 ("CHEN")

Chen discloses a method of authentication that measures changes in facial angles across a series of images that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Chen include:

"During a technique for authenticating a user using a portable electronic device (such as a smartphone) while preventing successful 2D media attacks and virtual-camera attacks, the portable electronic device provides an instruction to a user to move the portable electronic device relative to the user's face. Then, using an imaging sensor in the portable electronic device, the portable electronic device acquires, a series of images while the portable electronic device is at different positions or orientations relative to the user's face, where the series of images include at least two images relative to a symmetry axis of the user's face (such as the midline). Moreover, the portable electronic device determines a change in a sign of a nose angle in at least the two images. Next, the portable electronic device authenticates the user based on at least one of the series of images using a facial-recognition technique." [Abstract]

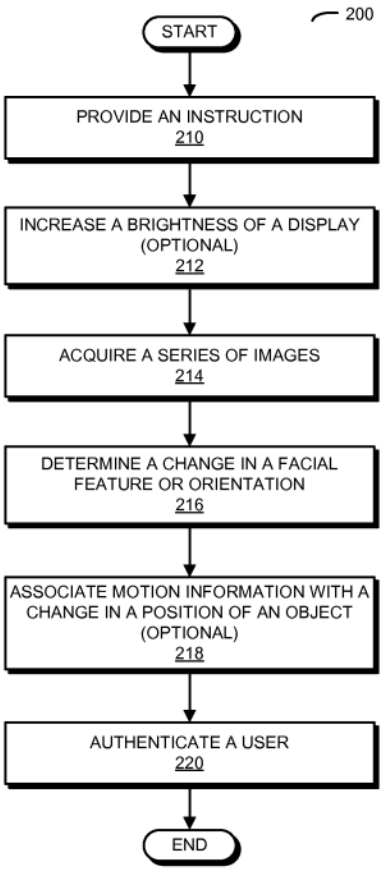

200
START
PROVIDE AN INSTRUCTION
210
INCREASE A BRIGHTNESS OF A DISPLAY
(OPTIONAL)
212
ACQUIRE A SERIES OF IMAGES
214
DETERMINE A CHANGE IN A FACIAL
FEATURE OR ORIENTATION
216
ASSOCIATE MOTION INFORMATION WITH A
CHANGE IN A POSITION OF AN OBJECT
(OPTIONAL)
218
AUTHENTICATE A USER
220
END

FIG. 2

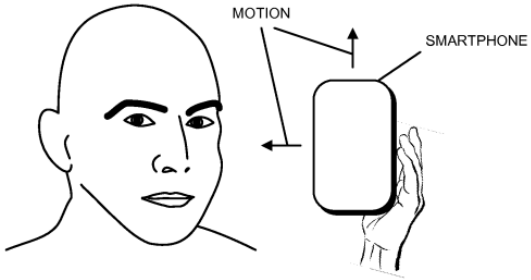

MOTION
SMARTPHONE

FIG. 3

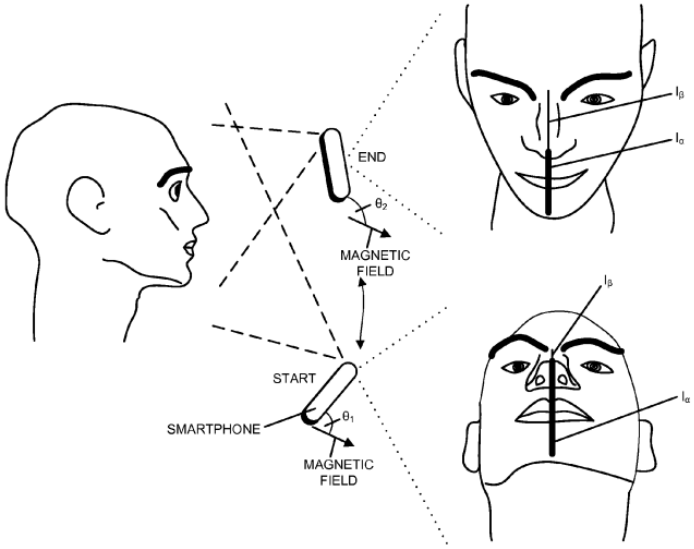


FIG. 5

"Portable electronic devices, such as smartphones and tablets, are increasingly popular computing platforms. Moreover, the ubiquity and enhanced functionality of portable electronic devices has resulted is an ever-increasing suite of applications for use with portable electronic devices, including mobile-payment applications. Consequently, securing valuable information on portable electronic devices is increasingly important." [1:24-31]

"The described embodiments relate to a portable electronic device. This portable electronic device includes: an imaging sensor (such as a front-facing camera) that acquires one or more images; a processor; and memory that stores a program module that is executed by the processor. During execution of the program module, the portable electronic device provides an instruction to a user to move the portable electronic device relative to a face of the user. Then, the portable electronic device acquires, using the imaging sensor, a series of images while the portable electronic device is at different positions relative to the face of the user, where the series of images include at least two images relative to a symmetry axis of the face of the user. Moreover, the portable electronic device determines a change in a sign of a nose angle in at least the two images. Next, the portable electronic device authenticates the user based on at least one of the series of images using a facial-recognition technique." [2:28-44]

"Furthermore, the portable electronic device may include a motion sensor (such as an accelerometer, a gyroscope, an inertial motion sensor, a compass and/or a magnetometer) that measures motion information. Prior to the authenticating, the portable electronic device may associate the motion information with a change in a position of an object in the series of images. For example, the change in the position may be based on differences in pixels in the series of images. Note that the motion information may include vibrations and rotations of the portable electronic device. In some embodiments, the associating involves correlating the motion information and the change in the position of the object." [2:45-56]

"Furthermore, the symmetry axis may include a midline of the face of the user. Consequently, the instruction to move the portable electronic device may specify at least a horizontal component of the movement." [2:62-65]

"Additionally, the determining the change in the sign of the nose angle may involve: identifying regions that include a nose in the face of the user in at least the two images; determining edges of the nose in the regions using an edge-detection technique; and calculating the nose angle based on the determined edges." [3:4-9]

"During a technique for authenticating a user using a portable electronic device (such as a smartphone) while preventing successful 2D media attacks and virtual-camera attacks, the portable electronic device provides an instruction to a user to move the portable electronic device relative to the user's face. Then, using an imaging sensor in the portable electronic device, the portable electronic device acquires, a series of images while the portable electronic device is at different positions or orientations relative to the user's face, where the series of images include at least two images relative to a symmetry axis of the user's face (such as the midline). Moreover, the portable electronic device determines a change in a sign of a nose angle in at least the two images. Next, the portable electronic device authenticates the user based on at least one of the series of images using a facial-recognition technique." [3:64-4:12]

"We now describe the authentication technique. Smartphones are typically equipped with multiple sensors, including: one or more motion sensors (such as an accelerometer, a gyroscope, an inertial motion sensor, a compass and/or a magnetometer), an imaging sensor (such as a camera) a proximity sensor, an ambient light sensor, a sound sensor (such as a microphone) and/or a 'positioning sensor' (via the Global Positioning System). Existing facial-authentication techniques use a camera to capture an image or a video of the user's face, and then compare it with one or more pre-defined templates." [4:33-43]

"FIG. 2 presents embodiments of a flow diagram illustrating method 200 for authenticating a user, which may be performed by a portable electronic device, such as electronic device 500 (FIG. 6). During operation, the portable electronic device provides an instruction to the user to move the portable electronic device (operation 210) relative to a face of the user. For example, the instruction may be displayed on a screen or a verbal command may be issued using a speaker." [5:23-30]

"Then, using an imaging sensor in the portable electronic device (such as a front-facing camera having at least a 1-2 megapixel resolution), the portable electronic device acquires a series of images (operation 214) while the portable electronic device is at different positions (or orientations) relative to the face of the user, where the series of images include at least two images (such as two photographs or a video with multiple images) relative to a symmetry axis of the face of the user." [5:31-39]

"Moreover, the portable electronic device determines a change in a facial feature or orientation (operation 216) in at least the two images, such as a change in a sign of a nose angle. For example, the determining (operation 216) may involve: identifying

regions that include a nose in the face of the user in at least the two images; determining edges of the nose in the regions using an edge-detection technique; and calculating the nose angle based on the determined edges." [5:49-56]

"Next, the portable electronic device authenticates the user (operation 220) based on at least one of the series of images using a facial-recognition technique." [5:57-59]

"In particular, as soon as the authentication starts (at time T0), the front-facing camera may begin to capture video and may perform face detection (e.g., using Haar Cascade). Once the face area is greater than or equal to a threshold (such as 40% of the area of the video frame), the front-facing camera may start recording video (at time T1). The area of the face may be approximated by the area of the face-detection output (which may be rectangular). At the same time (Ts), the authentication technique may start sampling the readings of accelerometers. If no face is detected, the authentication technique may show a prompt and ask the user to move the smartphone closer to their face." [8:5-16]

"The feature of the user's face that may be used to determine the geometry of their face may be the ratio of the distance from the center of the eye to the nose tip (lβ) and the distance from the nose tip to the chin (lα). As shown in FIG. 5, which presents a drawing illustrating a change in nose angle in two images, lα can be determined by drawing a line from the tip of the user's nose to their chin, while lβ can be found by drawing a line from the center of the user's eyes to the tip of their nose." [12:9-16]

"We now describe embodiments of an electronic device. FIG. 6 presents a block diagram illustrating an electronic device 600. This electronic device includes processing subsystem 610, memory subsystem 612, networking subsystem 614 and sensor subsystem 630. Processing subsystem 610 includes one or more devices configured to perform computational operations. For example, processing subsystem 610 can include one or more microprocessors, application-specific integrated circuits (ASICs), microcontrollers, programmable-logic devices, and/or one or more digital signal processors (DSPs)." [12:52-62]

"Electronic device 600 can be (or can be included in) any electronic device with at least one network interface. For example, electronic device 600 can be (or can be included in): a desktop computer, a laptop computer, a subnotebook/netbook, a server, a tablet computer, a smartphone, a cellular telephone, a smart watch, a consumer-electronic device, a portable computing device, and/or another electronic device." [14:10-16]

7. U.S. PATENT NO. 2007/0009139 ("LANDSCHAFT")

Landschaft discloses a method of facial recognition on a handheld electronic device using biometric data that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Landschaft include:

FIG. 2

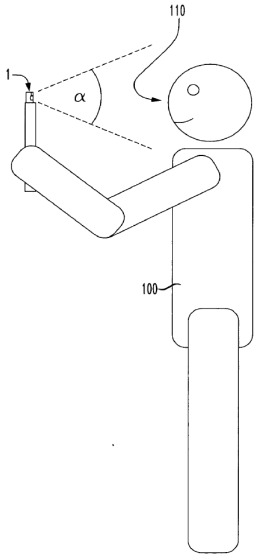


FIG. 3

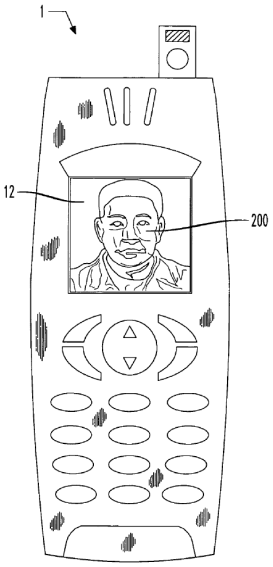


FIG. 4

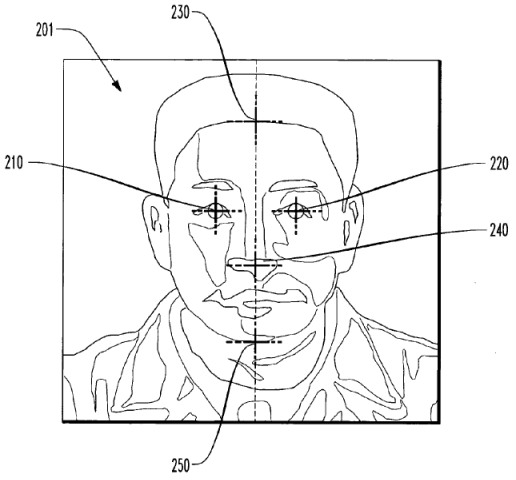
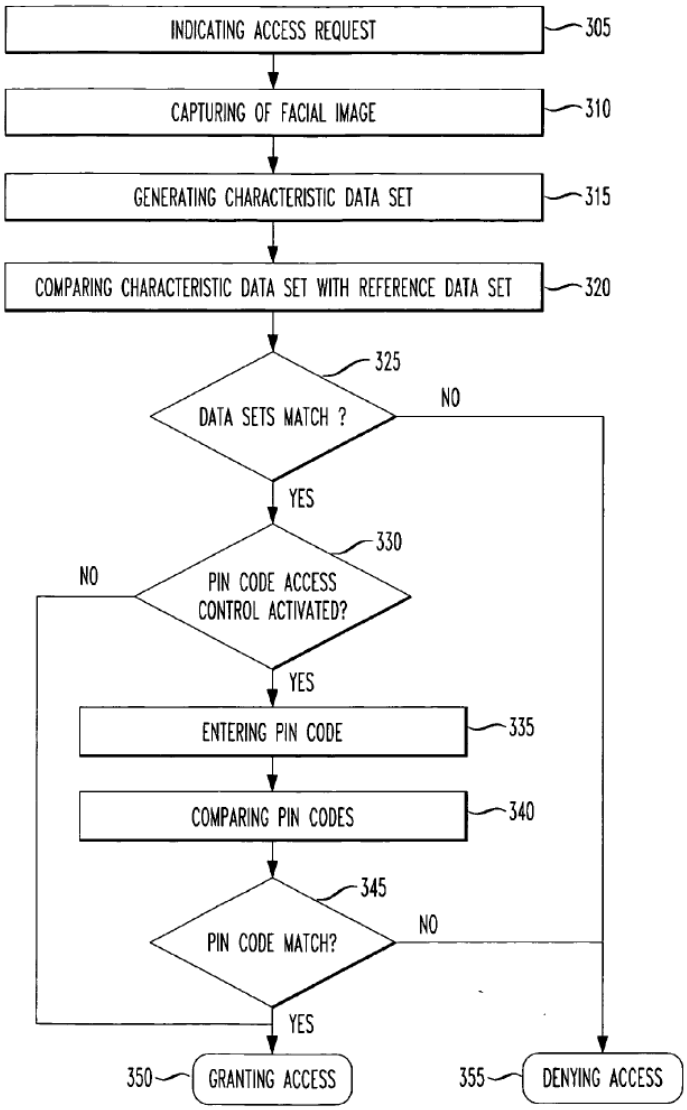

201
230
210
220
240
250

FIG. 5


INDICATING ACCESS REQUEST
305
CAPTURING OF FACIAL IMAGE
310
GENERATING CHARACTERISTIC DATA SET
315
COMPARING CHARACTERISTIC DATA SET WITH REFERENCE DATA SET
320
325
DATA SETS MATCH ?
NO
YES
330
PIN CODE ACCESS CONTROL ACTIVATED?
NO
YES
ENTERING PIN CODE
335
COMPARING PIN CODES
340
345
PIN CODE MATCH?
NO
YES
350
GRANTING ACCESS
355
DENYING ACCESS

"The present invention is directed, in general, to a security device for a handheld electronic device and, more specifically, to a facial recognition device that provides conditional user access to a handheld electronic device." [0001]

"Thus the present invention provides a method to restrict access to the functions of a handheld electronic device by comparing certain biometric functions of an authorized user with the biometric functions of a party attempting to access functions of the electronic device. This invention is particularly useful for restricting access to such devices as mobile phones, laptop and notebook computers, personal digital assistants (PDAs), as well as any other handheld electronic device to which access is limited to specific parties." [0010]

"In still another embodiment, biometric user data and biometric reference data calls for processing a facial image by determining a position or arrangement, or both together, of salient points of the facial image. Where a camera is integrated into a handheld electronic device, another embodiment provides for the device to instruct a party requesting access to repeat the capture of the biometric user data by using a different view of the facial image. This permits a greater degree of certainty in permitting access to electronic device functions by permitting redundant checks." [0013]

"The invention presents a method for restricting access to the functions of a handheld electronic device, in particular a mobile communication device such as a mobile phone. The invention provides for the provision of biometric reference data of an authorized user or authorized users, as the case may be, of a handheld electronic device. When a party requests access to the functions of such a handheld electronic device, certain biometric user data of the party requesting access is captured and compared with the biometric reference data. Access to the device can then be controlled based on such comparison. For example, in the case of a laptop computer where children have also have access, unlimited access can be provided to adults and restricted access can be provided to children." [0026]

"It is envisioned, in one embodiment of the invention, that a user of a handheld electronic device will be required to provide facial biometric user data each time the device is turned on. An advantageous embodiment of the present invention provides for a built-in camera to capture an image of the user's face to provide the biometric user data. The salient points of the user's face comprise the biometric user data that will be compared with the salient points of the user's face stored in the device as biometric reference data." [0029]

"To generate a characteristic data set based on facial characteristics that unequivocally identifies a party requesting access, in one embodiment of the invention the biometric data consists of a facial image data determining by the position or arrangement, or both, of salient points of the facial image such as the position of the eyes, ears, mouth, etc. or points on the boundary line of the face. Of course, when capturing biometric user data of a party attempting to access the device, the position and orientation of the party's face relative to the camera is important. It is possible that a comparison of the biometric user data derived from

the captured facial image in certain circumstances will not match the biometric reference data, although the party requesting access is an authorized user and the stored biometric reference data is perfectly valid. In such case, an embodiment of the present invention provides for the handheld electronic device to generate a request for the party seeking access to repeat the step of capturing his or her facial image after adjusting the position and orientation of the party's face relative to the camera." [0030]

8. U.S. PATENT NO. 8,970,348 ("EVANS")

Evans discloses a system that authenticates users with facial gestures that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Evans include:

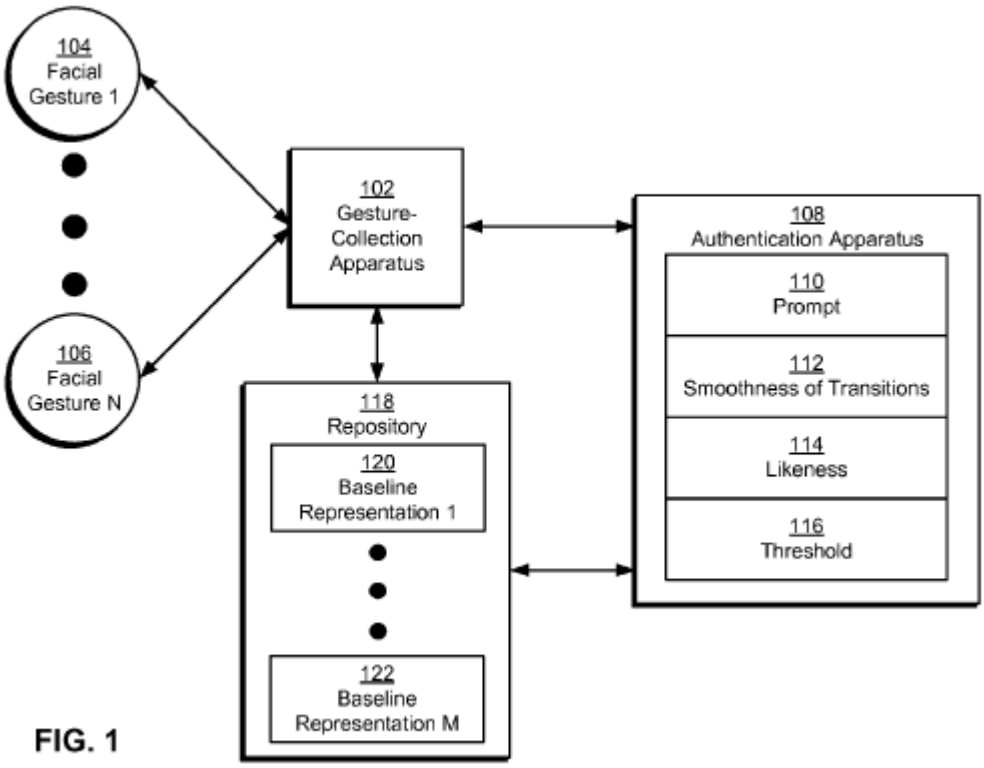


FIG. 1

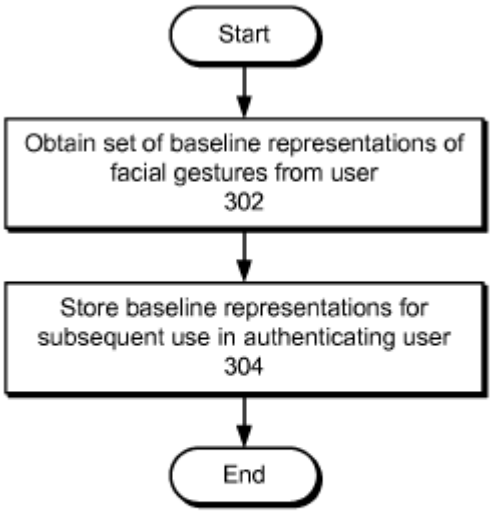

Start
Obtain set of baseline representations of facial gestures from user
302
Store baseline representations for subsequent use in authenticating user
304
End

FIG. 3

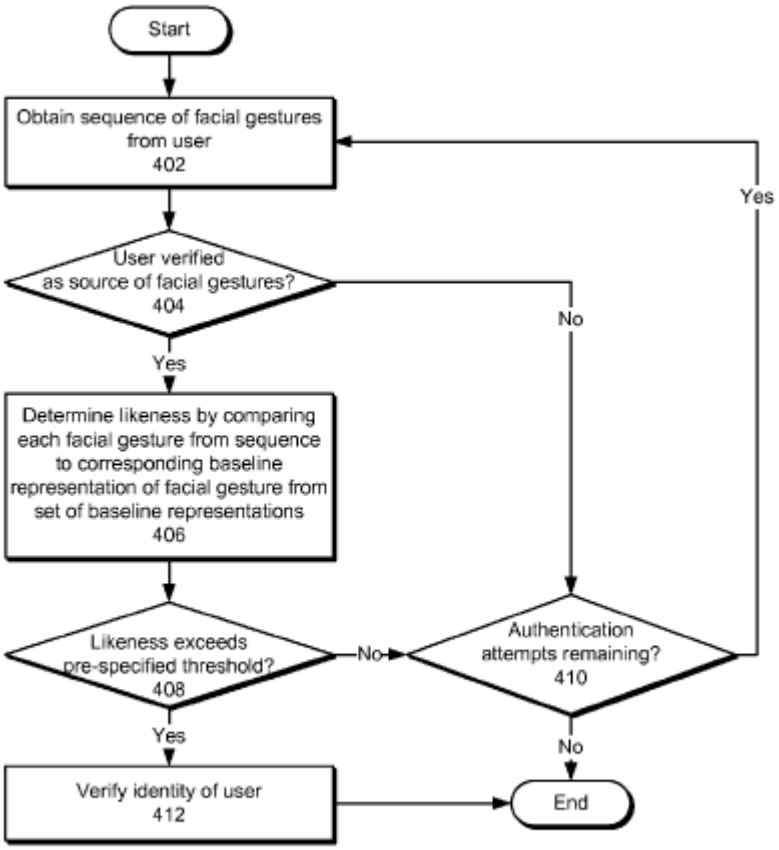

Start
Obtain sequence of facial gestures from user
402
User verified as source of facial gestures?
404
Yes
No
Determine likeness by comparing each facial gesture from sequence to corresponding baseline representation of facial gesture from set of baseline representations
406
Likeness exceeds pre-specified threshold?
408
No
Authentication attempts remaining?
410
Yes
Yes
No
Verify identity of user
412
End

FIG. 4

"In some embodiments, obtaining the sequence of facial gestures from the user involves at least one of prompting the user to provide each facial gesture from the sequence of facial gestures, and obtaining the sequence of facial gestures from the user without specifying the facial gestures in the sequence to the user." [2:4-9]

"In some embodiments, if the likeness falls below the pre-specified threshold, authenticating the user based on the likeness of the sequence to the set of baseline representations further involves attempting to verify the identity of the user using one or more new sequences of facial gestures until a limit to the number of authentication attempts for authenticating the user using the facial gestures is reached." [2:19-25]

"The disclosed embodiments provide a method and system for authenticating a user. As shown in FIG. 1, the system includes a gesture-collection apparatus 102 and an authentication apparatus 108. Gesture-collection apparatus 102 and authentication apparatus 108 may enable the authentication of a user using a sequence of facial gestures (e.g., facial gesture 1 104, facial gesture n 106) from the user, such as blank expressions, smiles, frowns, winks, blinks, grimaces, custom facial gestures, and/or facial movements (e.g., nods, head shakes, head tilts, etc.)." [3:23-32]

"In particular, gesture-collection apparatus 102 and authentication apparatus 108 may use multiple facial gestures to establish the user's identity prior to granting the user access to services, features, and/or resources associated with the user's identity. For example, the system of FIG. 1 may require authentication of the user before enabling access to a physical location (e.g., a building, a vault, etc.), a user account (e.g., email account, online banking system, social network, etc.), and/or an electronic device (e.g., mobile phone, personal computer, laptop computer, tablet computer, portable media player, etc.). To facilitate accurate and/or secure authentication of the user, the facial gestures may be accompanied by one or more other identifiers and/or authentication factors for the user and/or user account, such as a username, full name, fingerprint, voice, and/or badge. On the other hand, authentication of the user may be streamlined by requiring only the sequence of facial gestures from the user." [3:33-49]

"Authentication apparatus 108 may manage the collection of facial gestures by gesture-collection apparatus 102, as well as the authentication of the user using the facial gestures. First, authentication apparatus 108 may provide a prompt 110 for each facial gesture from the sequence of facial gestures. For example, authentication apparatus 108 may select a sequence of three random facial gestures to be provided by the user. Authentication apparatus 108 may then provide the selected facial gestures to the user (e.g., through a display and/or user interface associated with gesture-collection apparatus 102) by displaying the facial gestures within a list, or by waiting for the user to provide each facial gesture in the sequence before requesting the next facial gesture in the sequence." [4:4-18]

"In one or more embodiments, authentication apparatus 108 determines likeness 114 by comparing each facial gesture from the sequence of facial gestures to a corresponding baseline representation of the facial gesture from the baseline

representations in repository 118. For example, each baseline representation may include a set of attributes associated with the corresponding facial gesture (e.g., shape of mouth, shape of eyes, location of pupils, dimensions of nose, spacing of facial features, etc.). Likeness 114 may thus be calculated by obtaining the same attributes from each facial gesture in the sequence and determining the level of similarity between the attributes from the facial gesture and the attributes from the corresponding baseline representation. If multiple instances and/or versions of the baseline representation are available (e.g., as provided by the user during collection of the baseline representations), likeness 114 may be calculated as the level of similarity between the facial gesture and one or more relevant instances and/or versions. For example, if three versions of the baseline representation are found in repository 118, a numeric value of similarity between the facial gesture and each baseline representation may be calculated, and the numeric value that indicates the highest level of similarity between the facial gesture and the corresponding baseline representation may be used as likeness 114. Alternatively, likeness 114 may be calculated as the average of the three numeric values." [5:33-58]

"Initially, a sequence of facial gestures is obtained from the user (operation 402). The user may be prompted to provide each facial gesture from the sequence, or the sequence may be obtained from the user without specifying the facial gestures in the sequence to the user. For example, the user may be shown a description of each facial gesture (e.g., "blank expression," "smile," "frown," "blink," "grimace," "crossed eyes," "nod," "headshake," etc.) in the sequence before the user provides the facial gestures. On the other hand, the user may be prompted for a "password" containing a sequence of facial expressions that is known only to the user." [7:60-8:3]

9. U.S. PATENT PUB. NO. 2019/0342329 ("TURGEMAN")

Turgeman discloses a system, method, and device of detecting the identity and authenticating a user that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Turgeman include:

"System, method, and device of detecting identity of a user and authenticating a user; as well as detecting a possible attacker or impostor, and differentiating among users of an electronic device or of a computerized service. A mobile or portable electronic device is utilized to capture a self-taken image or video of a user, which is utilized as a user-authentication factor. The accelerometer and gyroscope or device-orientation sensor of the mobile device, sense and measure spatial and physical device properties during, before or after the submission of the self-taken image or video. Based on such spatial and physical device properties, in combination with computer-vision analysis of the content shown in the self-taken image or video, the system determines liveness of the user and freshness of the submitted self-taken image or video, and differentiates between a legitimate user and an attacker." [Abstract]

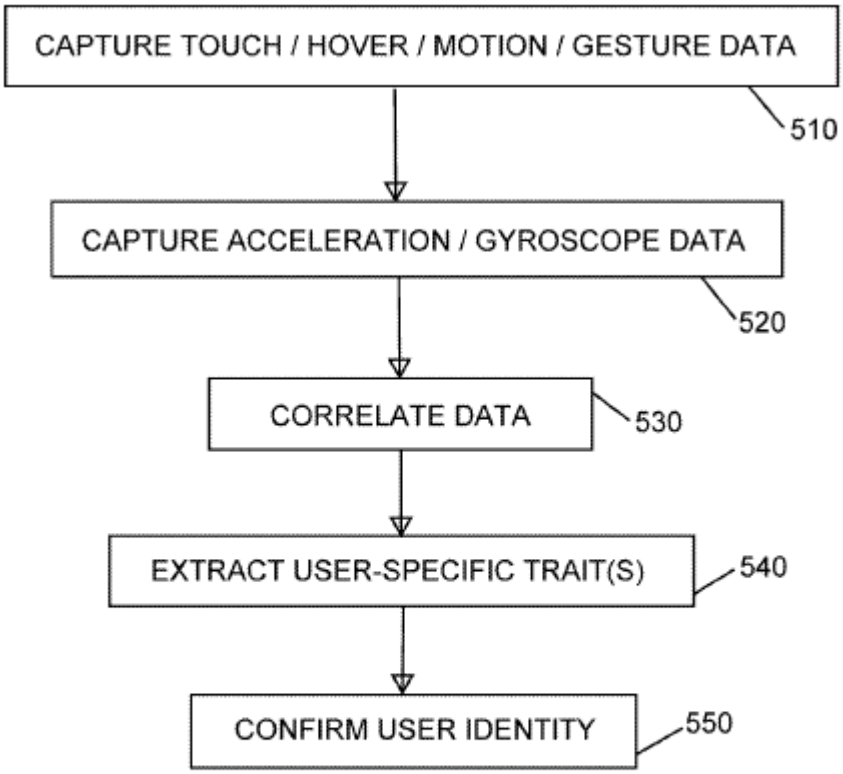


Fig. 5

"Some embodiments of the invention comprise a system, a method, and a device of detecting identity of a user and authenticating a user; as well as detecting a possible attacker or impostor, and differentiating among users of an electronic device or of a computerized service." [0034]

"For example, a mobile or portable electronic device is utilized to capture a self-taken image of a user, which is utilized as a user-authentication factor. The accelerometer and gyroscope of the mobile device, sense and measure geo-spatial device properties during, before or after the submission of the self-image authentication factor; and based on such geo-spatial device properties, the system determines liveness of the user, freshness of the submitted self-image, and possibly differentiates between a legitimate user and an attacker." [0035]

"In accordance with the present invention, for example, the method may comprise: storing a reference value of the user-specific trait, indicative of said user; in a subsequent usage session of the mobile electronic device, generating a current value of the user-specific trait correlating between touch data and acceleration data; and based on a comparison between the current value of the user-specific trait and the reference value of the user-specific trait, determining whether or not a current user

of the mobile electronic device is an authorized user of the mobile electronic device." [0045]

"In accordance with the present invention, for example, estimating the user-specific behavioral trait of said user comprises one or more of: determining that said user typically moves the mobile electronic device at a particular direction while performing a touch gesture; determining that said user typically rotates the mobile electronic device while performing a touch gesture; determining that said user typically slants the mobile electronic device at a particular angle while performing a touch gesture." [0058]

"The terms "mobile device" or "mobile electronic device" as used herein may include, for example, a smartphone, a cellular phone, a mobile phone, a tablet, a handheld device, a portable electronic device, a portable gaming device, a portable audio/video player, a smart-watch, a digital watch, a digital wrist-watch, an Augmented Reality (AR) or Virtual Reality (VR) device or glasses or helmet or headset (e.g., similar to Google Glass, or similar to Oculus Rift), a fitness band or fitness watch, a laptop computer, a tablet computer, a notebook computer, a netbook computer, an electronic device which comprises at least an accelerometer and a touch-screen, or the like." [0070]

"Some embodiments of the present invention may enable the system to ensure and/or to confirm "Liveness" of the user, of an image or video of the user, or a self-image or self-video of the user, that are submitted by a user or by an electronic device having a camera or imager, for purposes of user authentication or user identity determination, or for purposes of authorizing or blocking access of a user to a local or remote computerized service and/or to the electronic device itself; and/or to prevent, avoid, eliminate, block and/or mitigate a problem or a fraud-attempt in which an attacker or a non-legitimate user or an impostor attempts to perform "spoofing" by submitting to the system (or the electronic device itself, or to a local or remote authentication module) a non-fresh image or video, or a non-freshly-taken image or video, or a previously-recorded image or video or self-image or self-video, or a recording or a capturing of the user or of an image of the user of a video of the user, or of a play-back or a replay or a re-broadcast attempt that attempts to re-submit to the authentication module a previously-captured image or video or an attempt to submit an image or video that lack Liveness and/or that lack Freshness; as well as to provide Liveness Detection and/or Freshness Detection for such user-authentication system.

It is also clarified that although potions of the discussion herein may relate, for demonstrative purposes, to utilization of an image or an image-stream or a video-sequence for user-authentication purposes, the present invention may also be used in conjunction with user-authentication systems and methods and modules that utilize other biometric traits and/or user-specific traits, for example, user speech, user utterance, user audio sample, user audible sounds or words, a combination of audio and video, a combination of audio and an image, a combination of audio and a set of images, a fingerprint of a user, a combination of fingerprint with image

and/or video and/or audio, and/or other suitable biometric features and/or combination of biometric features." [0152-0153]

"In accordance with the present invention, a freshly-captured image or a video or a photograph of the user may be utilized for user-authentication purposes, in order to authenticate the user to a local device, a remote device, a local service and/or a remote service. For example, a system may firstly or initially capture or receive or obtain a Trusted Image of the user; for example, an image or a video of the user that the user takes in the presence of a third party (e.g., in the presence of a bank clerk, when the computerized service is a banking website or a banking application), or an image or a video of the user that the user takes upon initial creation of a user account, or upon opening a new account, or during a session that is known to be authenticated (e.g., during a usage session that was authorized via a two-step authentication process or via a two-factor authentication process). The Trusted Image, or other such "Reference Image", may be securely stored locally (e.g., in the electronic device, smartphone, tablet, laptop computer, or the like), and/or may be securely stored remotely (e.g., in a remote server, web server, application server, "cloud computing" server, or the like).

Subsequently, when the user requests to re-access that service or that electronic device, the user is requested to capture a Fresh Image of himself, via an imager or a camera of an electronic device being utilized by the user (e.g., smartphone, tablet). The Fresh Image is compared to the Trusted Image, or is analyzed in relation to it. If the two images are generally matching each other, then the user is authenticated; otherwise, the authentication attempt is blocked or rejected." [0155-0156]

"In some embodiments, the user may be required to perform one or more gestures or modifications or actions, as part of the authentication process, in order to "prove" to the authentication system that the user is indeed capturing a Fresh Image using the camera, and not, for example, pointing the camera of the device towards a previously-taken image of the user; for example, in order to stop an attacker who obtains a still image of the legitimate user, and then attempts to merely point the camera of the electronic device towards such still image. For example, the system may request the user to Blink one eye, or two eyes, or to perform a sequence of Eye Blinks, or to perform other gestures (e.g., touch his nose with one finger), in order to utilize image analysis and/or video analysis processes, to ensure that the captured image(s) or video indeed depict the required gestures or actions; thereby preventing an attacker from merely pointing the camera towards a still image, or towards a previously-captured image or video of the legitimate user." [0157]

"The present invention may strengthen the user-authentication process, by including in the authentication process also a sub-process in which the system takes into account "spatial properties" of the device, such as, accelerometer data, gyroscope data, device orientation data, device positioning data, device movement data, device tilt data (e.g., is the device generally horizontal, or generally vertical, or slanted at approximately 30 degrees), device traits that characterize the device when the user captures an image or a video, and/or user-specific traits that characterize the user when he captures an image or a video for authentication purposes; and/or the

modification or the change in values of such "spatial properties"; and/or such traits and such data (or, the change in values of such spatial properties) during a time period (e.g., 1 or 2 or 3 or 5 or 10 or K seconds) immediately prior to capturing the image or video for authentication purposes; and/or such traits and such data during a time period (e.g., 1 or 2 or 3 or 5 or 10 or K seconds) immediately after capturing the image or video for authentication purposes." [0160]

"In a second demonstrative example, the system may determine that user Adam, who from time to time authenticates by using a self-taken image of himself, typically or always captures his own image by (a) lifting his smartphone to be at approximately chest level, and (b) tilting his smartphone to be at an angle of approximately 45 degrees relative to the ground. However, in a subsequent user-authentication attempt, the system may monitor the device traits, and may determine that (A) the device is lifted to be at eye level, and/or (B) the device is capturing the image while the device is generally perpendicular to the ground. The system may determine that these fresh traits that characterize the fresh capturing of the self-image or self-video, do not match the historic or previous traits that characterized the capturing of the image or video in prior authentication sessions, or in when a Trusted or a Reference image (or video) was captured; thereby enabling the system to determine or to estimate that an attacker is attempting to authenticate, and not the legitimate user." [0163]

"In a third example, the electronic device may request the user to take a self-image, and may actually capture a stream or set of images or a video sequence (e.g., including images before, during and after the moment in which the user pushes a "snapshot" button). The electronic device may determine that the sequence of multiple frames or multiple images, does not show any "shaking movement"; whereas accelerometer data and/or gyroscope data indicate that the device was "shaken" or "shaking" during that time period or a portion thereof." [0164]

"The method and system of the present invention may be utilized with a variety of devices, and/or for authenticating a user to a variety of purposes; for example, for accessing a smartphone or tablet or smart-watch or laptop computer or desktop computer; for accessing an Internet of Things (IoT) device or appliance, or an Internet connected appliance or device; for accessing a website or a web-based service, a mobile application, an "app", a computerized service, a "cloud computing" service, a remote service, a secured service that requires authentication (e.g., email account, web-mail account, social network account, online banking account, online brokerage account); for accessing or traversing or entering or exiting a physical gate or door or entrance or exit (e.g., of a building, an office, a vehicle); for igniting or starting or driving a vehicle; and/or for other suitable tasks or systems in which user authentication is utilizes as a condition for granting or blocking access." [0172]

"Some embodiments of the present invention may perform, utilize, determine and/or estimate, for example, relation or correlation or other association between: (a) one or more behavioral parameters or traits, or one or more device-specific traits or user-specific traits that may be sensed or measured or estimated when (or during, or

before, or after) the user handles or operates the electronic device (e.g., acceleration of the electronic device, information sensed by accelerometer(s) and/or gyroscope(s) of the electronic device, slanting or tilting of the electronic device, or the like), or user-specific behavioral traits (e.g., user Adam typically lifts his smartphone vertically before capturing a self-image; user Bob typically spins his smartphone counter-clockwise immediately before or immediately after taking a self-image); and, (b) the actual content of the biometric user-identifying or user-authenticating trait, such as, self-image or image of the user, self-video or vide of the user, audio or speech or voice of the user, fingerprint of the user, or the like." [0173]

"The terms "self-taken item" or "self-taken visual item" or "self-taken camera-acquired item" or "self-taken visual acquisition item" or "self-taken visual acquisition input", as used herein, may include a self-taken image ("selfie" image) and/or a self-taken photograph and or a self-taken video ("selfie" video) and/or a self-taken batch-of-images and/or a self-taken group of video frames, or other visual or camera-based input that may be utilized for signing-in or logging-in or face-based sign in or user authentication." [0201]

"In accordance with the present invention, a user authentication unit or module or device may capture (via one or more cameras) a selfie image or a selfie video, or a set or series of selfie images or frames, which are then utilized for authenticating the user; and also for determining whether the submitted or captured image or video is a "fresh" one or a freshly-captured one or a recently-captured one, rather than being a previously-captured or previously-submitted item (e.g., captured or submitted a minute or an hour or a day or a year prior to the current authentication attempt); and also for determining Liveness, namely, that the captured image or video reflect therein a live human user, rather than (for example) being an image (or a video) of a two-dimensional printed photograph of a person." [0202]

"In a second set of examples, the user authentication unit, which may be located within the electronic device and/or may be part of a remote server, receives a submitted selfie image or selfie video. The content analyzer unit performs computer vision analysis of the content shown, and detects that the submitted four-seconds video (or, that the submitted 4 or 9 or 50 consecutive frames that were taken during the selfie acquisition) shows the user and/or its background in a manner that indicates that the capturing device was slightly shaking or moving or was instable or non-steady or non-idle, such that the submitted video (or group of images) reflects at least some shaking or movement of the hand of the user that allegedly took the video or images. For example, content analysis of the submitted video, or of the submitted set of images, shows the user's head being located at slightly different positions within the frame(s) or video or image(s); for example, an image of a "head" appears in the center frame #1, and then appears at an offset of one pixel to the right of the center in frame #2, and then appears at an offset of three pixels to the left of the center in frame #3, and so forth, reflecting some displacement from one frame to another frame. This is usual or regular in a true acquisition of a four-second selfie video; as even the most proficient human user would typically cause

some shaking or vibration or movement or instability or non-steadiness of the electronic device during the acquisition period." [0205]

10. U.S. PATENT NO. 9,510,196 ("SENSHARMA")

Sensharma discloses a method and apparatus for authenticating a user on a mobile device that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Sensharma include:

> "Disclosed is a method and apparatus for authenticating a user on a mobile device. The method may include initiating authentication of the user for access to the mobile device, where access to the mobile device is granted upon successful authentication of the user by the mobile device. The method may also include performing face recognition analysis on an image of a face of the user to determine an identity of the user. Furthermore, the method may also include determining whether a first pulse information and a second pulse information associated with the user indicate a pulse match. The method may also include authenticating the user for access to the mobile device when a pulse match is determined and the determined identity of the user has permission to access the mobile device." [Abstract]

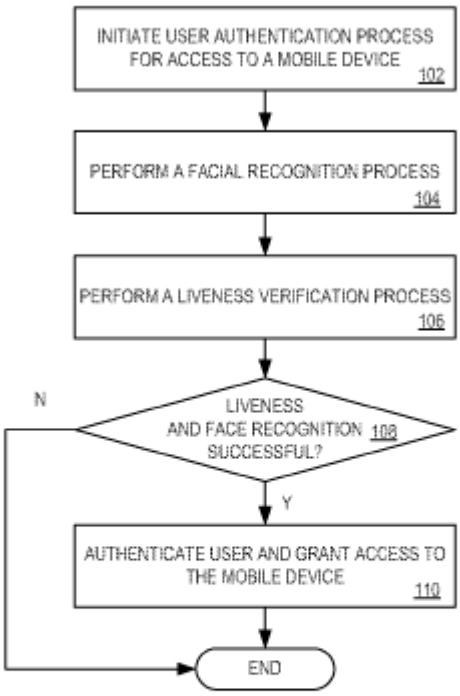

INITIATE USER AUTHENTICATION PROCESS FOR ACCESS TO A MOBILE DEVICE
102
PERFORM A FACIAL RECOGNITION PROCESS
104
PERFORM A LIVENESS VERIFICATION PROCESS
106
LIVENESS AND FACE RECOGNITION SUCCESSFUL?
108
N
Y
AUTHENTICATE USER AND GRANT ACCESS TO THE MOBILE DEVICE
110
END

FIG. 1

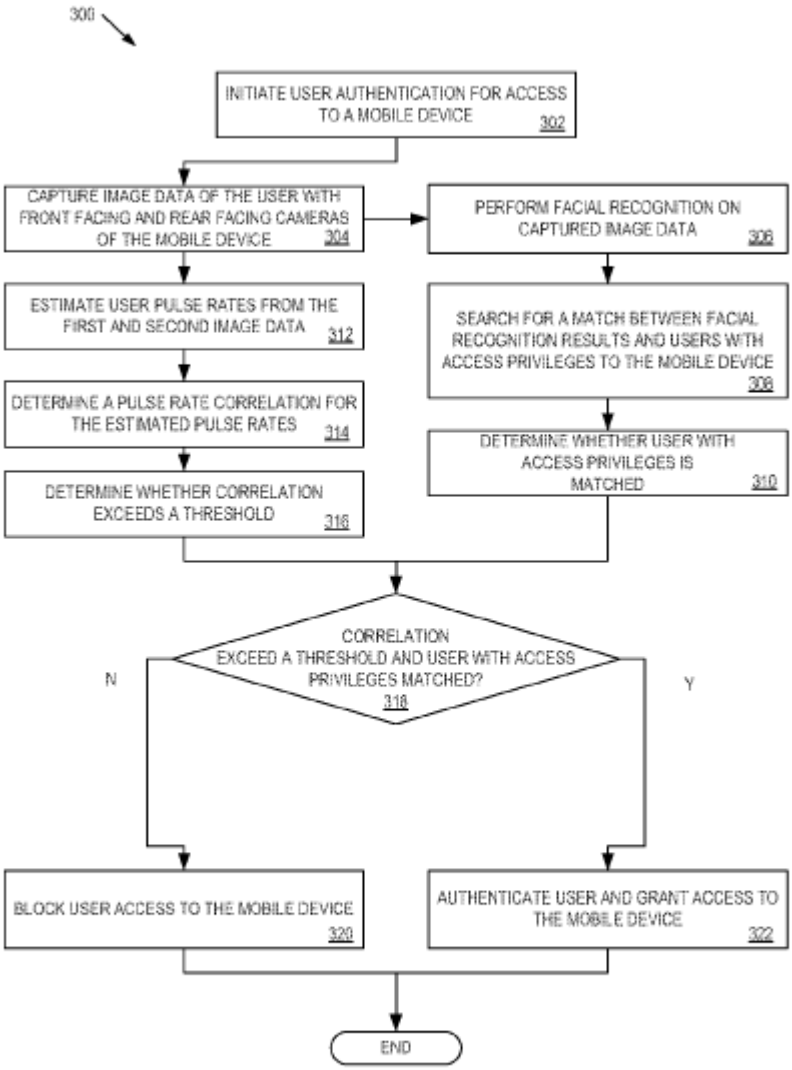

300
INITIATE USER AUTHENTICATION FOR ACCESS TO A MOBILE DEVICE 302
CAPTURE IMAGE DATA OF THE USER WITH FRONT FACING AND REAR FACING CAMERAS OF THE MOBILE DEVICE 304
PERFORM FACIAL RECOGNITION ON CAPTURED IMAGE DATA 306
ESTIMATE USER PULSE RATES FROM THE FIRST AND SECOND IMAGE DATA 312
SEARCH FOR A MATCH BETWEEN FACIAL RECOGNITION RESULTS AND USERS WITH ACCESS PRIVILEGES TO THE MOBILE DEVICE 308
DETERMINE A PULSE RATE CORRELATION FOR THE ESTIMATED PULSE RATES 314
DETERMINE WHETHER USER WITH ACCESS PRIVILEGES IS MATCHED 310
DETERMINE WHETHER CORRELATION EXCEEDS A THRESHOLD 316
CORRELATION EXCEED A THRESHOLD AND USER WITH ACCESS PRIVILEGES MATCHED? 318
N
Y
BLOCK USER ACCESS TO THE MOBILE DEVICE 320
AUTHENTICATE USER AND GRANT ACCESS TO THE MOBILE DEVICE 322
END

FIG. 3

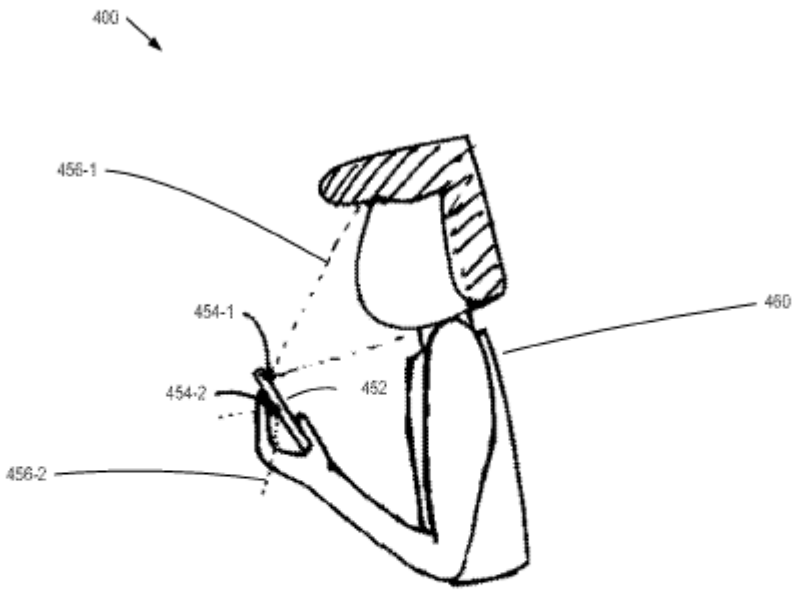


FIG. 4

"Referring to FIG. 1, processing logic begins by initiating a user authentication process for access to a mobile device (processing block 102). In one embodiment, mobile device is a mobile computing device, such as a mobile telephone, personal digital assistant, tablet computer, etc. capable of sending and receiving wireless communications over a cellular and/or wireless communication network. For example, the user authentication process is initiated when a user seeks to access a locked or protected mobile device, such as when user 460 illustrated in FIG. 4 seeks to be authenticated for purposes of accessing mobile device 452." [2:11-21]

"Processing logic performs a facial recognition process as part of user authentication to the mobile device (processing block 104). In one embodiment, in response to the user authentication process being initiated, processing logic activates one or more image capture mechanisms, such as digital cameras 454-1 and 454-2 of the mobile device 452 (see FIG. 4), for capturing digital image data. As discussed herein, digital image data may include digital video data as well as still digital video image data. In one embodiment, the image capture mechanisms may include a front-facing camera 454-1 on the mobile device as well as a rear-facing camera 454-2 on the mobile device, although additional cameras may also be utilized. The captured image data attempts to capture an image of a face 456-1 of the user 460 seeking authentication to the mobile device. Once an image of a user's face is captured,

processing logic extracts facial features from the image data, and compares those features against a facial recognition database of authorized users. When the extracted facial features match facial features of an authorized user in the database, the facial recognition process has found that the captured image data corresponds to an authorized user of the mobile device." [2:22-43]

"In one embodiment, and as discussed in greater detail below, processing logic performs the liveness verification process by estimating user pulse rates from the first and second digital video data, and attempting to correlate the pulse rates. When the pulse rates can be correlated by processing logic, then processing logic can conclude that the image captured by the front-facing camera 454-1 and the rear-facing camera 454-2 are capturing live images of the same person." [2:65-3:10]

"Further, it should be appreciated that some or all of the functions, engines or modules described herein may be performed by mobile device 210 itself and/or some or all of the functions, engines or modules described herein may be performed by another system connected through I/O controller 225 or network interface 204 (wirelessly or wired) to mobile device 210. Thus, some and/or all of the functions may be performed by another system and the results or intermediate calculations may be transferred back to mobile device 210. In some embodiments, such other device may comprise a server (not shown). In some embodiments, the other device is configured to predetermine the results, for example, based on a known configuration of the mobile device 210." [4:47-60]

"Processing logic captures image data of the user with a front-facing camera and a rear-facing camera of the mobile device (processing block 304). In one embodiment, captured image data is digital video data captured by the cameras. Processing logic performs one or more facial recognition processes on the captured image data (processing block 306). As discussed above, the facial recognition processes may include locating an image of a face depicted in the image data, and extracting visual features from the located face image. In the embodiments discussed herein, any number of facial features may be extracted, such as features corresponding to the eyes, nose, mouth, jaw, ears, cheekbones, etc., and their relative positions to one another. Processing logic then searches for a match between the facial recognition results and facial recognition features associated with users that have access privileges to the mobile device (processing block 308). The match is determined by processing logic by comparing a feature set associated with the face located in the image, with feature sets of the authorized users of the mobile device. From the comparison, processing logic determines a likelihood that the feature set associated with the face located in the image matches an authorized user's feature set to determine whether a user with access privileges is matched (processing block 310). When this likelihood exceeds a threshold likelihood, the face located in the digital video data matches an authorized user. When the likelihood does not exceed the threshold, the face is determined not to match an authorized user. In one embodiment, in the event that processing logic determines that the face does not match an authorized user (processing block 318), processing logic may proceed immediately to block 320 to block user access to the mobile device." [7:15-47]

"The teachings herein may be incorporated into (for example, implemented within or performed by) a variety of apparatuses or devices. For example, one or more aspects taught herein may be incorporated into a phone (such as a cellular phone), a personal data assistant (PDA), a tablet, a mobile computer, a laptop computer, an entertainment device (e.g., a music or video device), a headset (e.g., headphones, an earpiece, etc.), a medical device (e.g., a biometric sensor, a heart rate monitor, a pedometer, an Electrocardiography (EKG) device, etc.), a user I/O device, a computer, a server, a point-of-sale device, a set-top box, or any other suitable device." [8:40-51]

11. U.S. PATENT PUB. NO. 2014/0310764("TIPPETT")

Tippett discloses an approach for authenticating a user through gestures that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Tippett include:

"An approach is provided for authenticating and/or identifying a user through gestures. A plurality of media data sets of a user performing a sequence of gestures are captured. The media data sets are analyzed to determine the sequence of gestures. Authentication of the user is performed based on the sequence of gestures." [Abstract]

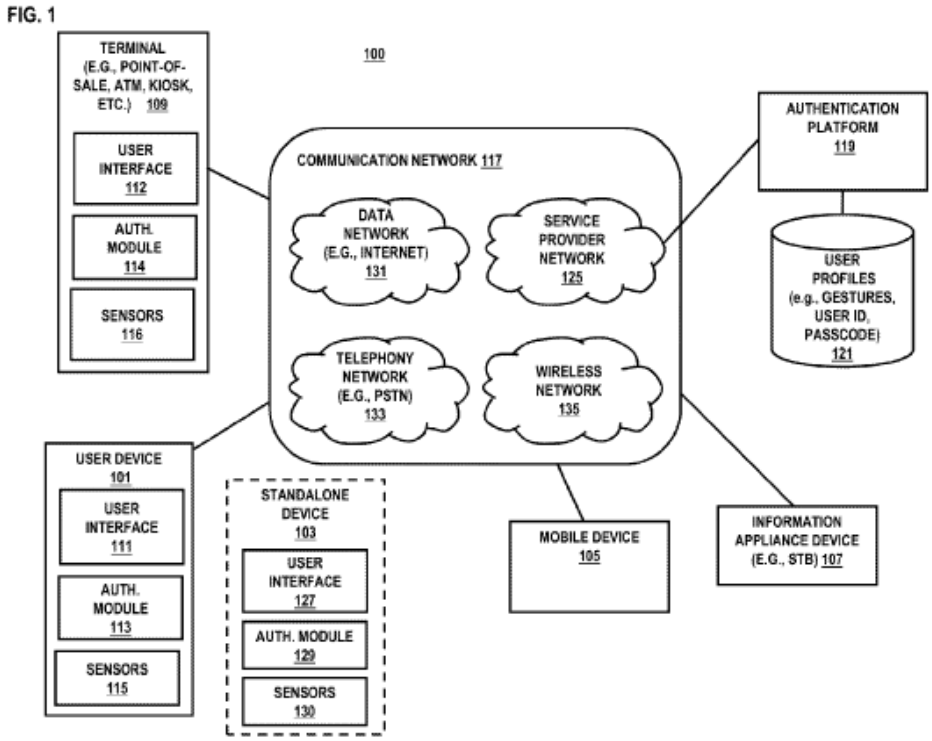


FIG. 2

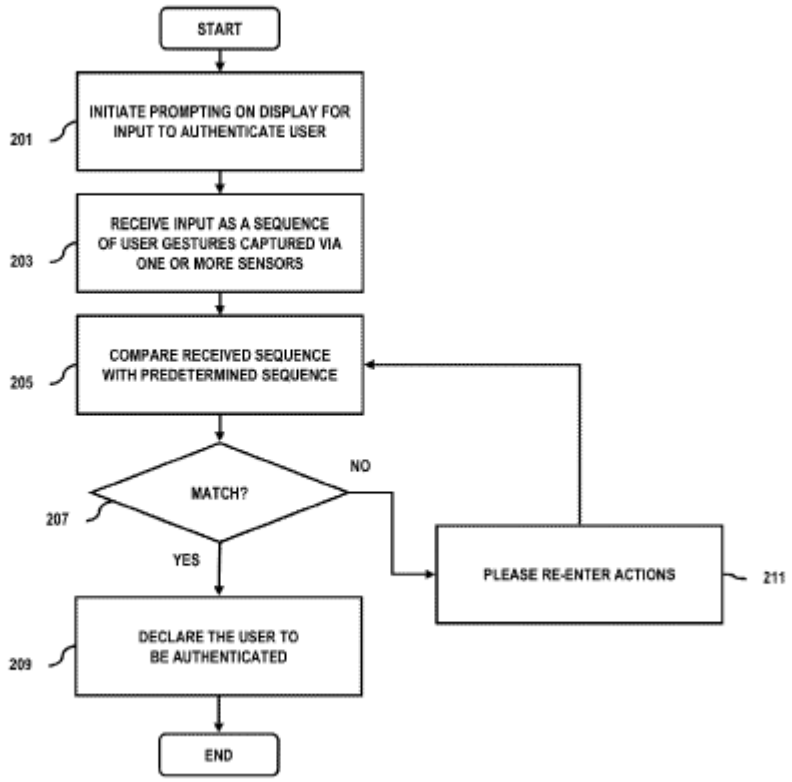

START
INITIATE PROMPTING ON DISPLAY FOR INPUT TO AUTHENTICATE USER
201
RECEIVE INPUT AS A SEQUENCE OF USER GESTURES CAPTURED VIA ONE OR MORE SENSORS
203
COMPARE RECEIVED SEQUENCE WITH PREDETERMINED SEQUENCE
205
MATCH?
207
NO
YES
PLEASE RE-ENTER ACTIONS
211
DECLARE THE USER TO BE AUTHENTICATED
209
END

FIG. 5A

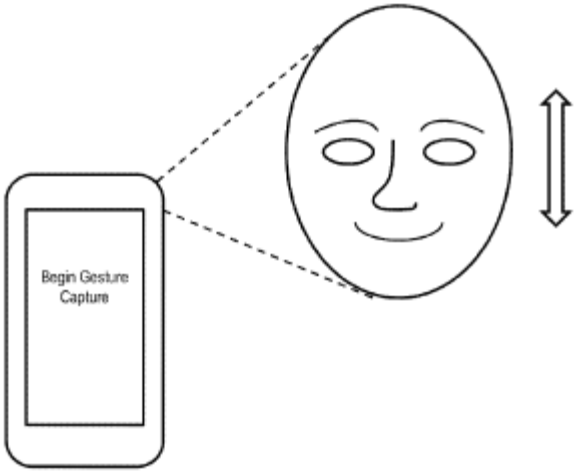

Begin Gesture Capture

FIG. 5B

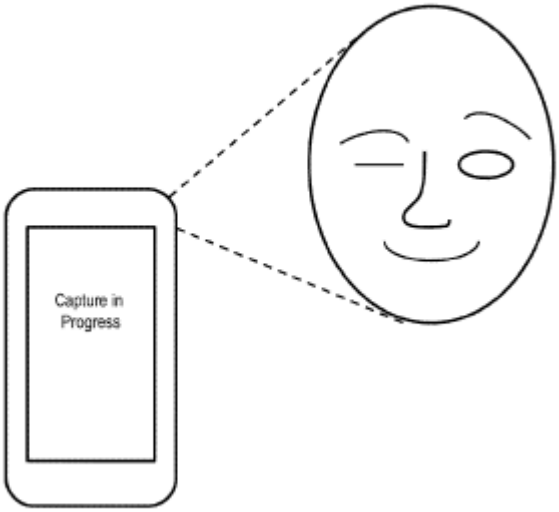


FIG. 5C

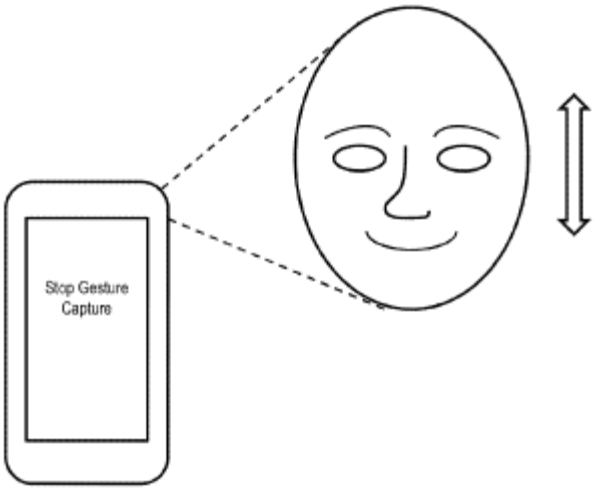


FIG. 5D

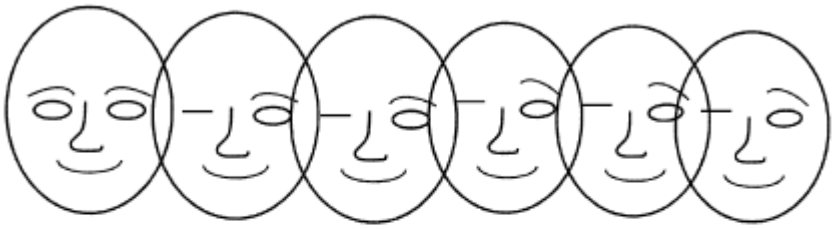
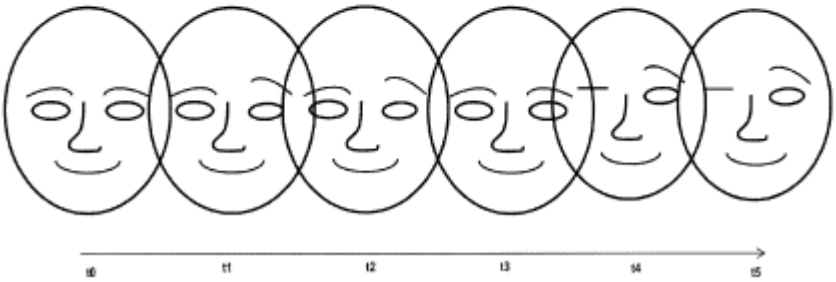


FIG. 5E



"Gestures can include movement of the hands, face, eyes, lips, nose, arms, shoulders, legs, feet, hip, or other parts of the body." [0018]

"The sensors 115 can be independent devices or incorporated into the user device 101. The sensors 115 may include an accelerometer, a gyroscope, a compass, a GPS device, microphones, touch screens, light sensors, or combinations thereof. The sensors 115 can be a head/ear phone, a wrist device, a pointing device, or a head mounted display. By way of example, the user wears a head mounted display with sensors to determine the position, the orientation and movement of the user's head. The user can wear a device around a belt, a wrist, a knee, an angle, etc., to determine the position, the orientation and movement of the user's hip, hand, leg, foot, etc. The device gives an indication of the direction and movement of a subject of interest in a 3D space.

The authentication platform 119 maintains a user profile database 121 that is configured to store user-specific gestures along with the user identification (ID) of subscribers to the authentication service, according to one embodiment. Users may establish one or more sub-profiles including reference gestures as well as other authentication credentials such as usernames, passwords, codes, personal identification numbers (PINs), and etc. relating to user authentication as well as user accounts and preferences. While user profiles repository 121 is depicted as an extension of service provider network 125, it is contemplated that user profiles repository 121 can be integrated into, collocated at, or otherwise in communication with any of the components or facilities of system 100." [0034-0035]

"In step 201, a prompt is provided on the display of the user device 101 indicating to the user that gesture authentication is needed. For example, the request may be prompted when a user attempts to log into a system. On presenting the prompt, the user device 101 can activate its camera (e.g., a front-facing camera) to begin

capturing images of the user. The user device 101 then receives the authentication input as a sequence of images or video of the user making one or more gestures (e.g., facial gestures) (step 203).” [0042]

12. U.S. PATENT NO. 10,169,672 (“LANGLEY”)

Langley discloses a method of verifying the validity of biometric data that involves directing lighting and illumination that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Langley include:

> “A method of host-directed illumination for verifying the validity of biometric data of a user is provided that includes capturing biometric data from a user with an authentication device during authentication and directing illumination of the biometric data from a host authentication system during the capturing operation. Moreover, the method includes comparing illumination characteristics of the captured biometric data against illumination characteristics expected to result from the directing operation, and determining that the user is a live user when the illumination characteristics of the captured biometric data match the illumination characteristics expected to result from the directing operation.” [Abstract]

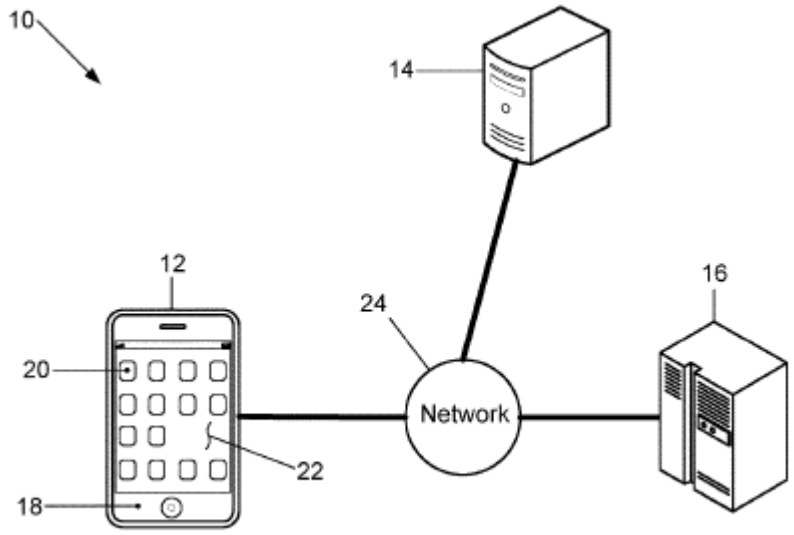


FIG. 1

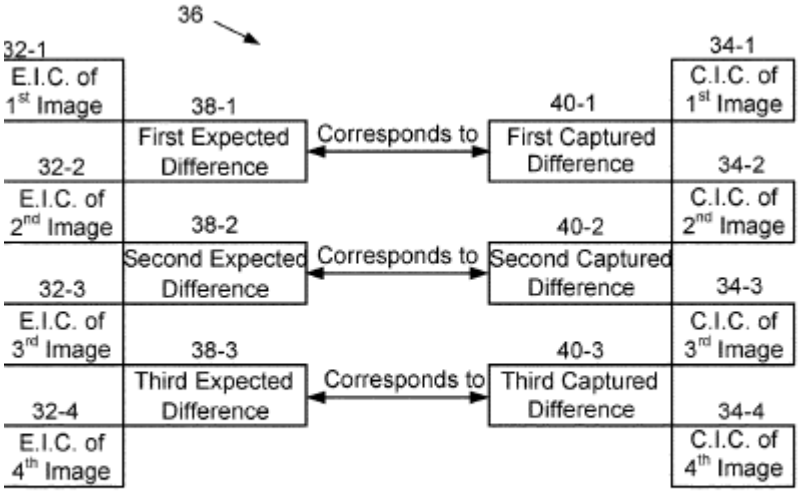


FIG. 4

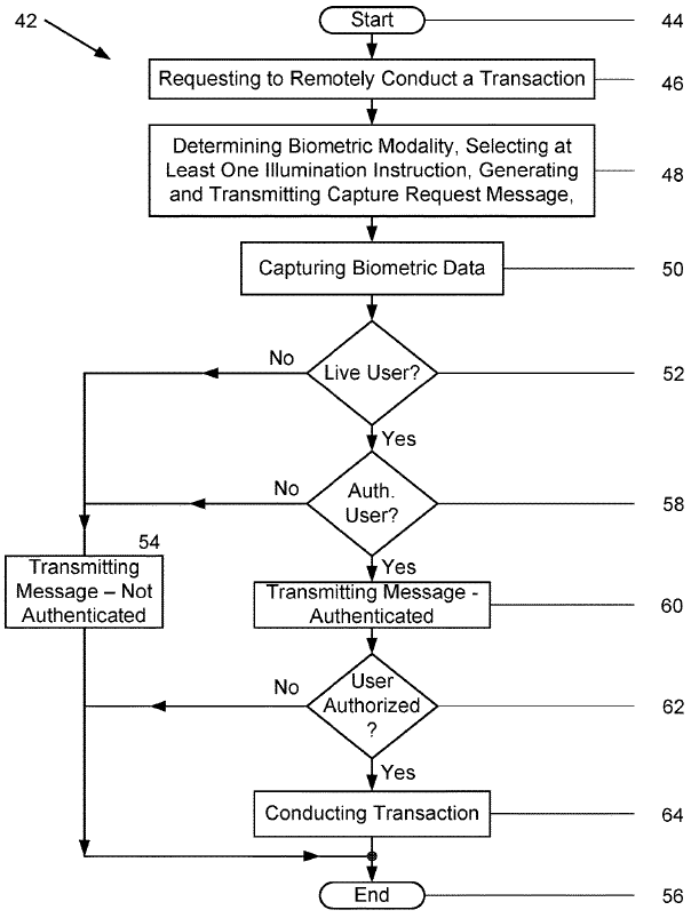


FIG. 5

"In one aspect, a method of host-directed illumination for verifying the validity of biometric data of a user is provided that includes capturing biometric data from a user with an authentication device during authentication, and directing illumination of the biometric data during the capturing operation from a host authentication

system. Moreover, the method includes comparing illumination characteristics of the captured biometric data against illumination characteristics expected to result from the directing operation, and determining that the user is a live user when the illumination characteristics of the captured biometric data match the illumination characteristics expected to result from the directing operation." [2:18-30]

"In another aspect, a computer system for verifying the validity of biometric data presented by a user during authentication transactions is provided. The computer system includes a service provider system associated with a business engaged in controlling access to resources and that contains a data base. The service provider system is configured to control access to resources relating to users enrolled therein and to conduct transactions. Moreover, the computer system includes a host authentication system that includes an authentication database. The host authentication system is configured to communicate with the service provider system over a network, to randomly select instructions stored therein to be executed while capturing biometric data, to store at least enrollment biometric data of a plurality of users, to determine the liveness of a user requesting to conduct a transaction requiring access to the resources stored in the service provider system, and to authenticate users determined to be live users." [2:31-48]

"The biometric data is captured as a sequence of photographic images that each include a captured biometric data component and captured illumination characteristics. Furthermore, the computer program causes the authentication computer system to transmit the captured biometric data to the host authentication system, and to compare each of the captured illumination characteristics against corresponding expected illumination characteristics. When the captured illumination characteristics match the corresponding expected illumination characteristic the computer program causes the authentication computer system to determine that the user is a live user." [3:8-20]

"FIG. 1 is an expanded block diagram of an exemplary embodiment of a system architecture of an Authentication Computer (AC) System 10 for verifying the validity of biometric data presented by a user during authentication transactions. More specifically, the AC system 10 includes a Remote Authentication (RA) Device 12, a Service Provider (SP) System 14, and a Host Authentication Computer (HAC) System 16.

The RA device 12 is a smart phone that at least stores applications therein, displays at least one of text and images, receives and executes specific instructions regarding illumination during authentication, and captures authentication data from a user." [3:45-56]

"Although the RA device 12 is a smart phone, the RA device 12 may alternatively be any device capable of at least displaying at least one of text and images, and capturing and transmitting data. Such other devices include, but are not limited to, a portable cellular phone, a tablet computer, a laptop computer, any type of portable communications device having wireless capabilities such as a personal digital assistant (PDA), and a personal computer." [4:20-27]

"The RA device 12 is configured to communicate with at least the SP system 14 and the HAC system 16 over a communications network 24. The communications network 24 is a 3G communications network. Alternatively, the communications network 24 may be any wireless network including, but not limited to, Wi-Fi, Global System for Mobile (GSM), Enhanced Data for GSM Evolution (EDGE), and any combination of a local area network (LAN), a wide area network (WAN) and the Internet. … The SP system 14 is a computer including components such as, but not limited to, a database server, an application server, a directory server, a web server, and a disk storage unit that may be used to store any kind of data." [4:28-54]

"The SP system 14 is a computer including components such as, but not limited to, a database server, an application server, a directory server, a web server, and a disk storage unit that may be used to store any kind of data. The disk storage unit may store at least one database. The SP system 14 is configured to at least communicate with the RA device 12 and the HAC system 16 over the network 24, and control access to resources. Resources as described herein include anything that may be protected against access by unauthorized users." [4:51-60]

"The HAC system 16 includes components such as, but not limited to, a web server, a database server, an application server, a directory server and a disk storage unit that may be used to store any kind of data. The disk storage unit may store at least one database such as, but not limited to, an authentication database. The HAC system 16 also includes a database management server and an authentication server. The database management server may be used to facilitate transferring data to and from the disk storage device. The authentication server performs matching of any feature or information associated with individuals to authenticate the identity of individuals as described herein.

The HAC system 16 is configured to communicate with the RA device 12 and the SP system 14 over the network 24." [6:15-32]

"The authentication data is biometric data that corresponds to any biometric modality desired to be used as the basis of authenticating a user requesting authentication. Such biometric modalities include, but are not limited to, face, finger, iris, and palm, and any combination of face, finger, iris and palm. The biometric data may take any form such as, but not limited to, photographic images. The enrollment data record of each authorized user stored in the HAC system 16 includes at least enrollment biometric data, a unique user identifier, and the service provider user identifier of the respective authorized user. Enrollment biometric data is biometric data obtained from the user during enrollment. The unique user identifier and service provider user identifier are alphanumeric text strings of any length and are different. By virtue of being stored in the same enrollment data record, the enrollment biometric data, the unique user identifier, and the service provider user identifier of each authorized user are associated with each other. Alternatively, such data may be stored in separate records with links to each other. Biographic data may also be included in the enrollment data records." [6:30-50]

"The HAC system 16 may also perform functions such as, but not limited to, storing a plurality of illumination instructions and expected illumination characteristics, and randomly selecting illumination instructions to be executed while capturing biometric data during authentication transactions. The randomly selected illumination instructions each require executing an action during authentication that effects illumination characteristics of the biometric modality presented for capture as a photographic image. Because each illumination instruction is randomly selected, illumination of the biometric modality during authentication is not known in advance to an imposter and thus appears unpredictable." [6:51-63]

"Moreover, the HAC system 16 may perform functions such as, but not limited to, generating illumination characteristics, and recognizing a distinctive pattern of an illumination characteristic generated as a result of executing any of the illumination instructions. An illumination instruction executed while capturing biometric data during authentication generates a captured illumination characteristic (CIC), and an illumination instruction executed while collecting the enrollment biometric data generates an expected illumination characteristic (EIC). The expected illumination characteristic (EIC) is the illumination characteristic expected to be generated as a result of executing the selected illumination instructions while capturing biometric data during authentication." [7:3-16]

"The HAC system 16 may also use differences in illumination characteristics to determine the liveness of a user. For example, the HAC system 16 may determine the CICs and EICs of captured biometric data, and compare the CICs against the EICs to determine whether they match. When the CICs and the EICs match, a user is determined to be live. Alternatively, the HAC system 16 may determine the difference between sequential CICs and the difference between sequential EICs, and compare corresponding differences of the CICs and EICs to ensure that temporal changes of the CICs agree with those of the EICs. Thus, it should be understood that the HAC system 16 may compare temporal changes in the CICs against temporal changes in the EICs to ensure that temporal changes of the CICs agree with those of the EICs. When the temporal changes of the CICs agree with those of the EICs, a user is determined to be live. It should be appreciated that the HAC system 16 may determine the illumination characteristics in any manner and may compare the illumination characteristics in any manner that facilitates determining the liveness of a user." [7:58-8:10]

"Additionally, the listing 26 includes a fourth instruction 28 for altering the orientation of the presented biometric modality. Such an instruction is an indirect method of changing the illumination of the biometric modality being captured, as it alters the relative position of the biometric modality and incidental sources of ambient illumination that may be present during authentication. For example, instructions that require altering an orientation of a presented biometric modality over time may require the user to alter his facial orientation in each photographic image while biometric data of his face is captured in a sequence of photographic images. Such facial orientations include voluntary movements such as, but not limited to, turning the head to the right, turning the head to the left, looking up, and looking down. Alternatively, the fourth instruction may require altering the

> orientation of the presented biometric modality by moving the presented biometric modality data relative to the at least one illumination device. For example, the presented biometric modality data may be moved from a first to a second position relative to the at least one illumination device." [9:55-10:8]

> "FIG. 3 is a diagram 30 illustrating EICs 32-1 to 32-4 and corresponding CICs 34-1 to 34-4 for a sequence of four photographic images captured over time during authentication. Corresponding illumination characteristics of each photographic image may be compared to determine the liveness of a user. For example, the EIC 32-1 for a first photographic image may be compared against the CIC 34-1 of the first photographic image. When a difference between the corresponding illumination characteristics 32-1 and 34-1 is within an acceptable tolerance, the EIC 32-1 is considered to match the CIC 34-1. When the corresponding illumination for each image in the sequence matches within an acceptable tolerance the user is determined to be live. Alternatively the corresponding illumination characteristics CIC, EIC of any number of images may be required to match in order to determine that a user is live. For example, the corresponding illumination characteristics CIC, EIC of three out of four images may be required to match within the expected tolerance to determine that a user is live." [11:1-20]

13. U.S. PATENT NO. 9,652,663 ("LAU")

Lau discloses a method and system for authenticating a user to a computing device using facial data and components extracted from captured images that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Lau include:

> "Exemplary methods, apparatus, and systems are disclosed for authenticating a user to computing device. In one exemplary embodiment, an indication of a request by a user to unlock a mobile device in a locked state is received. One or more images of the face of the user are captured. Facial components of the user from the one or more captured images are extracted. A determination is made as to whether the user is an authorized user or a non-authorized user based at least in part on a comparison of the facial components of the user extracted from the one or more captured images to facial components of the authorized user from one or more authentication images of the authorized stored on the mobile device. If the user is determined to be the authorized user, the mobile device unlocked; otherwise, the mobile device is maintained in its locked state." [Abstract]

FIG. 3A

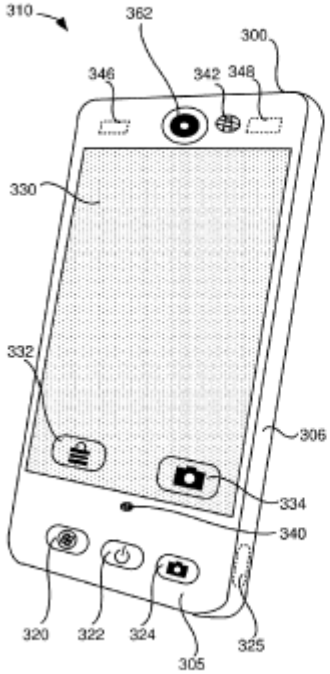


FIG. 3B

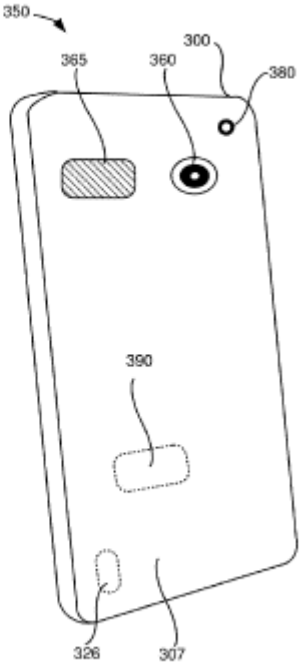


FIG. 5

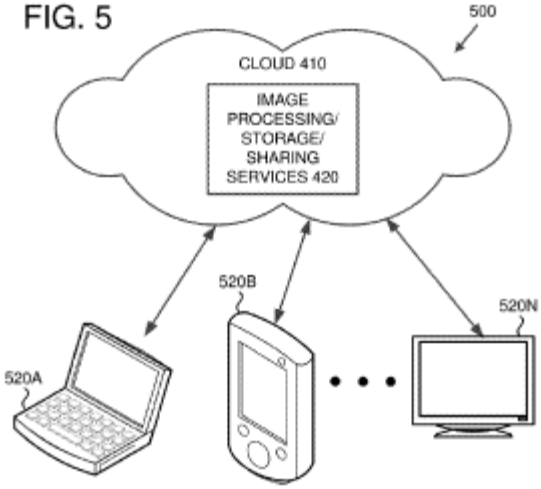


FIG. 6

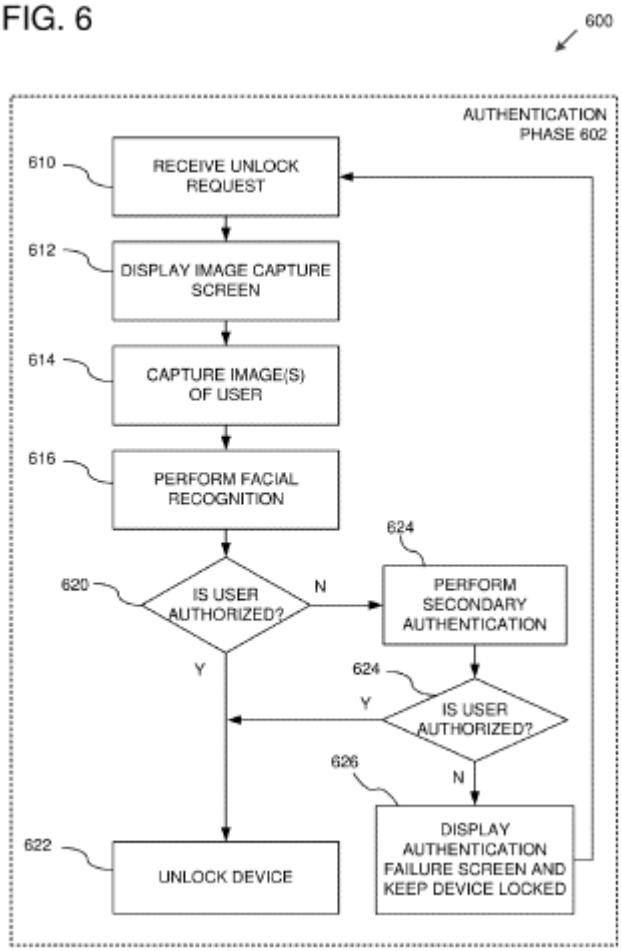

600
AUTHENTICATION PHASE 602
610
RECEIVE UNLOCK REQUEST
612
DISPLAY IMAGE CAPTURE SCREEN
614
CAPTURE IMAGE(S) OF USER
616
PERFORM FACIAL RECOGNITION
620
IS USER AUTHORIZED?
N
Y
624
PERFORM SECONDARY AUTHENTICATION
624
IS USER AUTHORIZED?
Y
N
626
DISPLAY AUTHENTICATION FAILURE SCREEN AND KEEP DEVICE LOCKED
622
UNLOCK DEVICE

FIG. 7

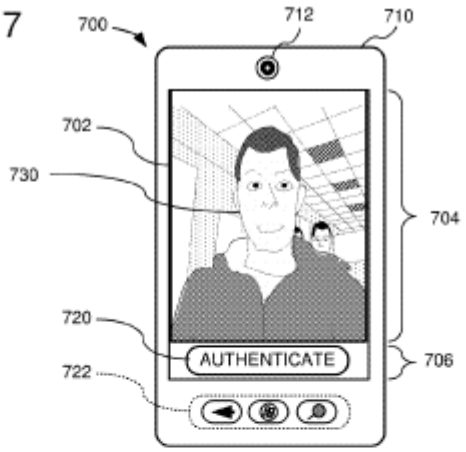

700
712
710
702
730
704
720
AUTHENTICATE
706
722

FIG. 8

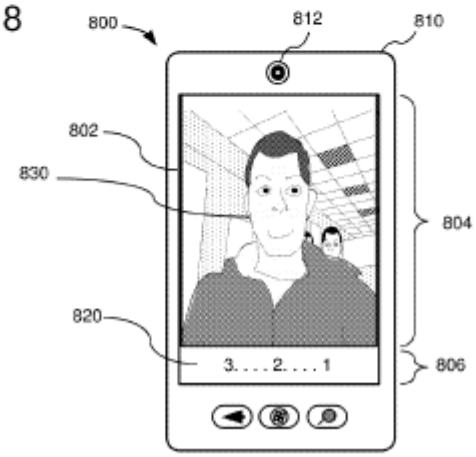

800
812
810
802
830
804
820
3. . . . 2. . . . 1
806

FIG. 9A

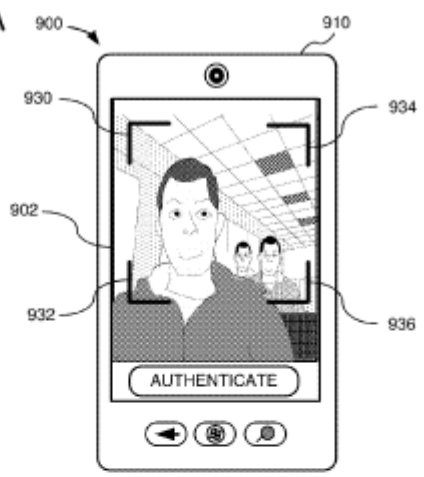
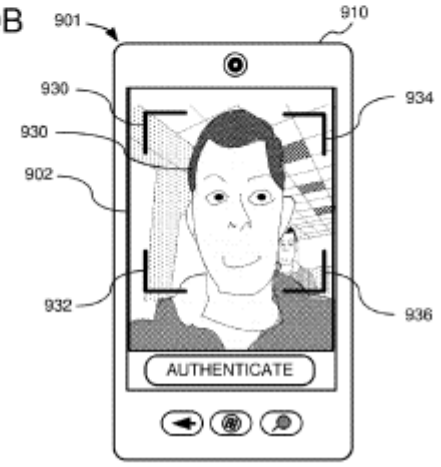


FIG. 9B



"In one exemplary embodiment disclosed herein, an indication of a request by a user to unlock a mobile device in a locked state is received. One or more images of the face of the user are captured. Facial components of the user are extracted from the one or more captured images. A determination is made as to whether the user is an authorized user based at least in part on a comparison of the facial components of the user extracted from the one or more captured images to facial components of the authorized user from one or more authentication images of the authorized user stored on the mobile device. The mobile device is unlocked if the user is determined to be the authorized user, but maintained in its locked state if the user is determined not to be the authorized user. In certain implementations, the one or more authentication images include a first authentication image of the authorized user in a first lighting condition and a second authentication image of the authorized user in a second lighting condition, the second lighting condition being different than the first light condition. In some implementations, the one or more authentication images include an authentication image of the authorized user where the face of the authorized user is illuminated primarily by a screen of the mobile device. In certain implementations, the act of capturing the one or more images includes prompting the user to make a facial expression or head motion, and the one or more authentication images include at least one authentication image of the user making the facial expression or head motion. In some implementations, the one or more

captured images are pre-processed to compensate for lighting conditions in which the one or more images are captured (e.g., by performing one or more of white balancing, global exposure compensation, local exposure compensation, or downsampling of the one or more captured images). In certain implementations, the comparison is performed by generating feature descriptors representative of the facial components of the user in the one or more captured images and determining a difference between the feature descriptors of the user in the one or more captured images and respective facial descriptors of the authorized user generated from the one or more authentication images. In other implementations, the comparison is performed by generating a graph-based representation of the facial components of the user in the one or more captured images and determining a difference between the graph-based representation of the facial components of the user and respective graph-based representations of the authorized user generated from the one or more authentication images. In such implementations, the graph-based representation of the facial components of the user is indicative of appearances and relative geometric relationships of the facial components of the user. In some implementations, the act of determining whether the user is an authorized user comprises, if the facial components of the user extracted from the one or more captured images match the facial components of the authorized user from the one or more authentication images, generating an indication that the user is authorized; and, if the facial components of the user extracted from the one or more captured images do not match the facial components of the authorized user from the one or more authentication images, causing a secondary authentication method to be performed on the mobile device. In certain implementations, the act of capturing the one or more images of the face of the user comprises capturing two or more images of the face of the user in succession, and the act of determining whether the user is an authorized user comprises is based at least in part on a comparison of the facial components of the user extracted from the two or more captured images to the facial components of the authorized user from the two or more authentication images stored on the mobile device." [1:64-2:65]

"FIG. 2 is a schematic block diagram depicting a detailed example of a mobile computing device 200 capable of implementing the techniques and solutions described herein. The mobile device 200 includes a variety of optional hardware and software components. In general, a component in the mobile device can communicate with any other component of the device, although not all connections are shown, for ease of illustration. The mobile device can be any of a variety of computing devices (e.g., cell phone, smartphone, handheld computer, laptop computer, notebook computer, tablet device, netbook, media player, Personal Digital Assistant ("PDA"), camera, video camera, or other such devices) and can allow wireless two-way communications with one or more mobile communications networks 204, such as a Wi-Fi, cellular, or satellite network." [8:25-39]

14. U.S. PATENT NO. 8,984,622 ("BALDWIN '622")

Baldwin ’622 discloses a method of authenticating a user of a computing device using facial recognition algorithms and detecting live users to avoid spoofing that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Baldwin ’622 include:

> “A user of a computing device can be authenticated using image information captured by at least one camera of the computing device. In addition to analyzing the image information using a facial recognition algorithm, for example, variations in color of a portion of the captured image information corresponding to a user's face can be monitored over a period of time. The variations can be analyzed to determine whether the captured image information likely corresponds to an actual human user instead of a representation (e.g., photo) of a human user, such as where the chroma variations in at least a red channel occur with an oscillation frequency and amplitude consistent with changes due to a pulse or heartbeat.” [Abstract]

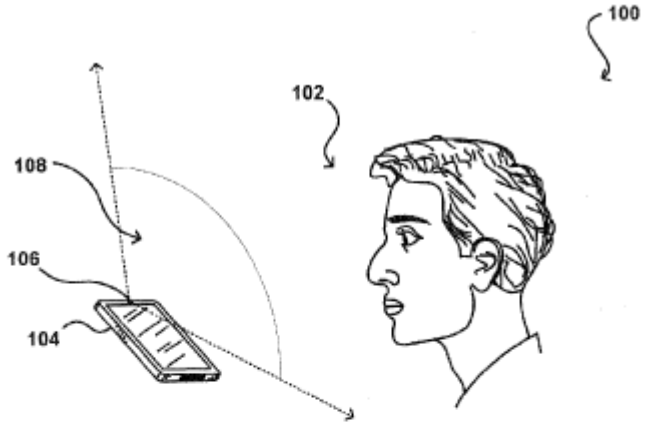


FIG. 1

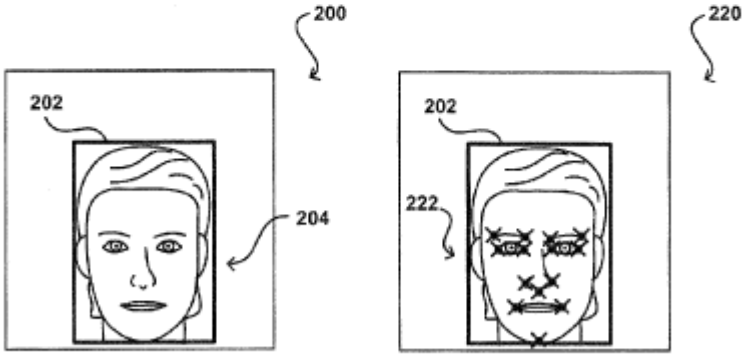


FIG. 2(a) FIG. 2(b)

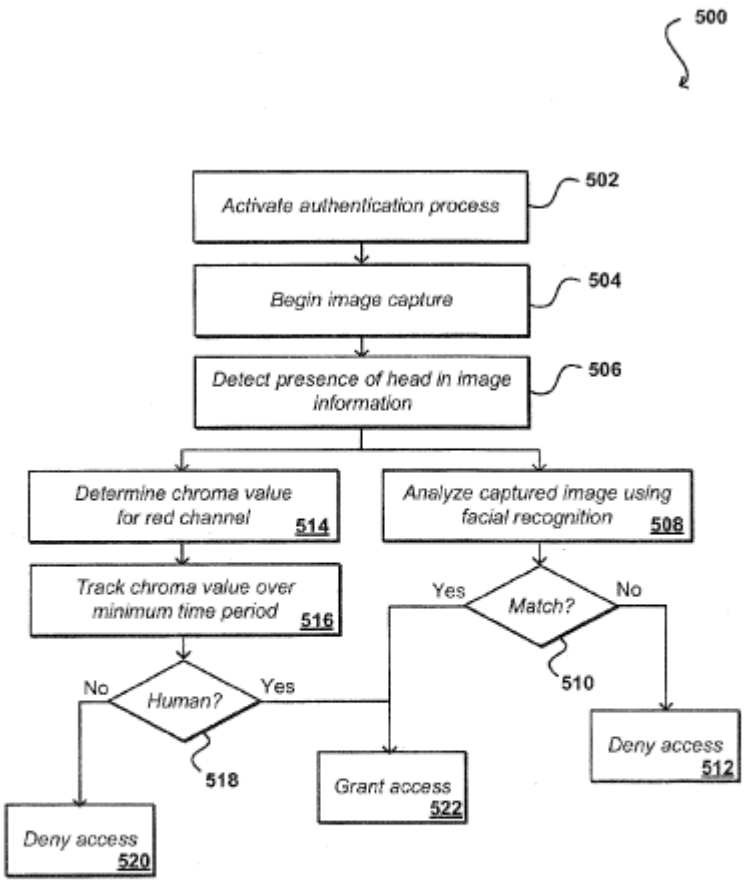

500
Activate authentication process
502
Begin image capture
504
Detect presence of head in image information
506
Determine chroma value for red channel
514
Analyze captured image using facial recognition
508
Track chroma value over minimum time period
516
Yes
Match?
No
510
No
Human?
Yes
518
Deny access
512
Grant access
522
Deny access
520

FIG. 5

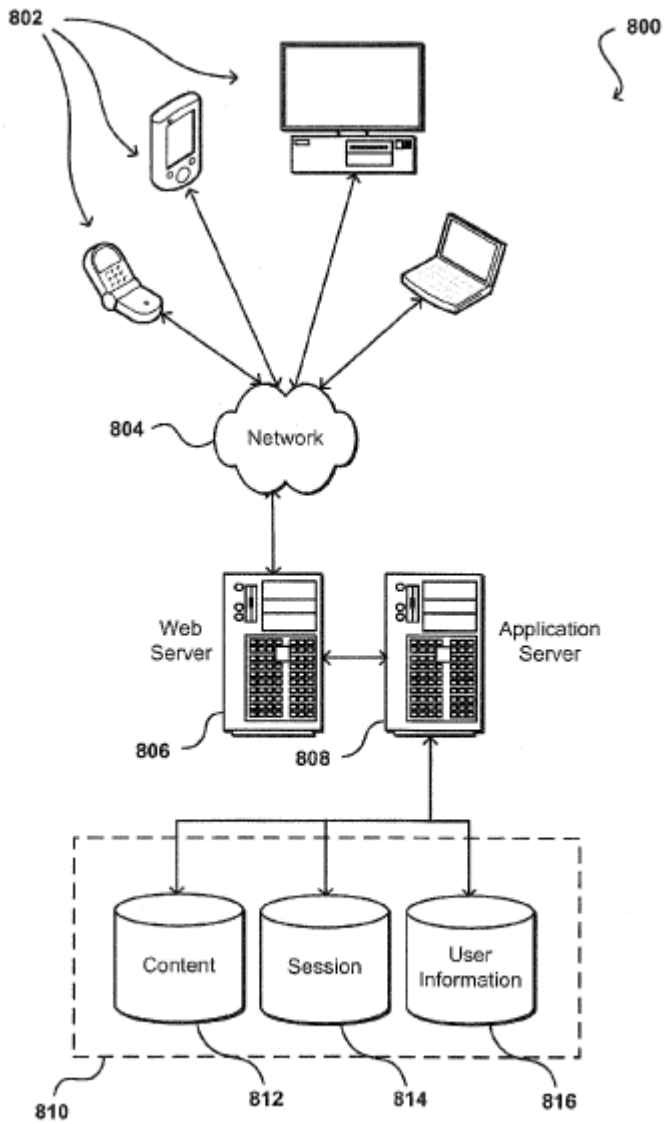


FIG. 8

"In particular, various embodiments utilize image information to not only identify a user, but also verify that the user is actually a physical person and not a false representation of that user. For example, a computing device can capture one or more frames of video information to use with a facial recognition process, in order to attempt to verify an identity of a current user of the device. The computing device also can capture and analyze video over a period of time sufficient to encompass one or more cycles of a human pulse or heartbeat. The location of the user's head in the captured video can be determined, and color values of a portion of the video corresponding to the head can be analyzed for variations corresponding to the fluctuations in a human face for a human pulse." [1:63-2:9]

"The camera 106 in this example is positioned on the device such that the person 102 likely will be at least partially included in the field of view 108 when the person

is interacting with the device, such as by looking and/or interacting with a display screen of the device. It should be understood, however, that there can be additional and/or alternative cameras placed in similar or alternative locations in accordance with various embodiments, and that information from any or all of these cameras can be analyzed as appropriate." [2:38-46]

"A head or face detection algorithm can be used in some embodiments to attempt to locate a portion 202 of the image 200 that corresponds to the approximate head location in the image. The head or face detection algorithm can include any appropriate algorithm known or used for such purposes, such as a template matching algorithm, a neural network algorithm, a Fisher linear discriminant algorithm, a maximal rejection classifier algorithm, a support vector machine algorithm, an edge filtering algorithm, an edge detection algorithm, and the like. The ability to locate the head position in an image can reduce the amount of resources otherwise needed to perform in facial recognition, as the analysis can be performed only on the portion of the image corresponding to the head position. Further, in some embodiments facial recognition might not be performed unless a head or face can first be detected in the captured image." [3:10-26]

"In this example, the detected head portion can be analyzed using one or more facial recognition algorithms to attempt to identify the person contained in the image. As illustrated in FIG. 2(b), this can include identifying unique or distinguishing points 222, landmarks, geometric shapes or distances, or other such features on the face, which can be compared or mapped against information stored for an authorized user of the device. Example facial recognition algorithms can include, for example, a linear discriminate analysis algorithm, a Fisherface algorithm, a Hidden Markov model-based algorithm, a principal component analysis algorithm, and a neuronal motivated dynamic link matching algorithm, among others. The image should be of sufficient resolution, clarity, and focus, for example, enabling the algorithms to adequately match the image to information stored for the user. As known, a facial recognition algorithm can take an amount of time to analyze an image, such that other processes can be executed during the analysis." [3:27-44]

"Once the facial region to be analyzed is determined, and tracked or updated over time in the video information, one or more color analysis algorithms can attempt to detect certain variations in that region over time. For example, the image portions 340, 360 of FIGS. 3(c) and 3(d), respectively, show (with an exaggerated difference) that there can be variations in the color of a person's face over time, due to changes in blood flow corresponding to the human pulse, which can be detected by a camera of the computing device. In this particular example, the changes will primarily be detected in a red channel, such as in the chroma (color purity), intensity, or saturation of red colors in the image portions. It should be understood, however, that variations can similarly be detected in other color channels or portion as well. For example, as blood is pushed through the human face as a result of a pulse or heartbeat, the face will appear slightly redder. During other periods, the face will appear somewhat less red. By monitoring for changes in color corresponding in time to a period of a human pulse, and in amount of variance to that of human skin, a

determination can be made as to whether the face in the image likely corresponds to an actual user and not a photograph or other such representation." [4:4-25]

15. U.S. PATENT NO. 9,607,138 ("BALDWIN '138")

Baldwin '138 discloses a method utilizing image information to identify a user and verify that the user is a live person that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Baldwin '138 include:

> "Approaches utilize image information to not only identify a user, but also verify that the user is actually a physical person and not a false representation of that user. For example, a computing device can utilize image information with a facial recognition process in order to verify an identity of a current user of the device. A fingerprint or other verification metric can be generated from the image information and can be used to verify that the user is actually a physical human user instead of a representation (e.g., photo) of a human user. The fingerprint can include a number of cues, such as a shape of the face, a stereo disparity signature of the face, facial feature movement, as well as a presence of a human pulse. The cues can be combined and utilized for authenticating a user into the device as well as for verifying that the user is actually a physical person and not a false representation of that user." [Abstract]

FIG. 1A

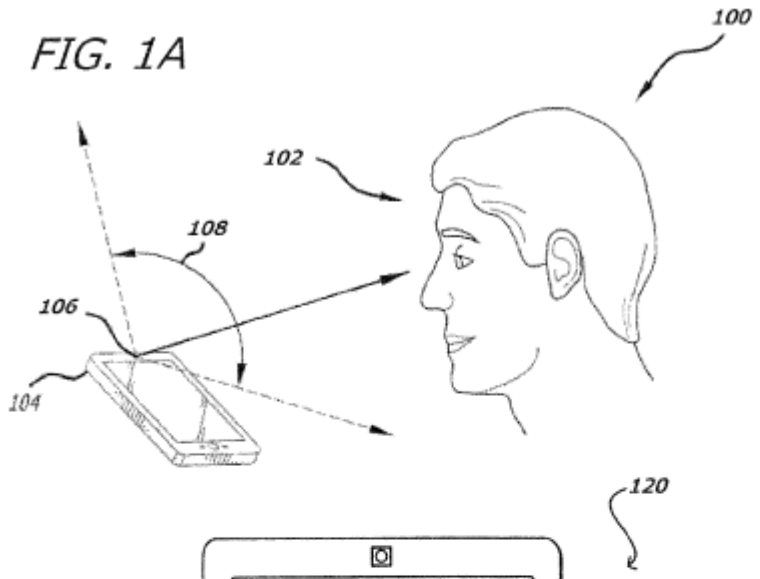


FIG. 1B

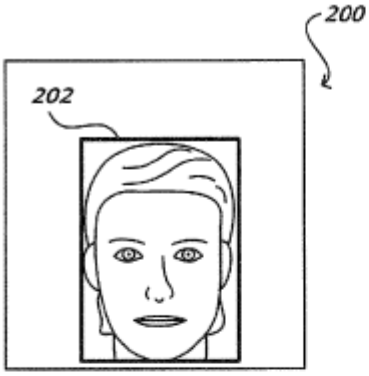


FIG. 2A

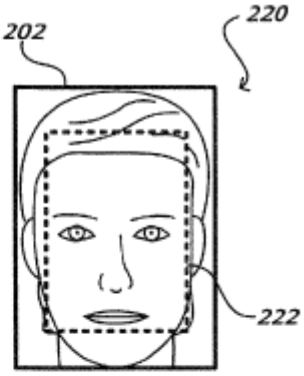


FIG. 2B

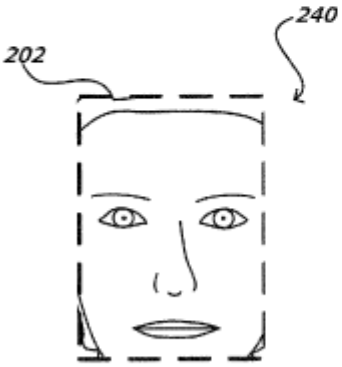


FIG. 2C

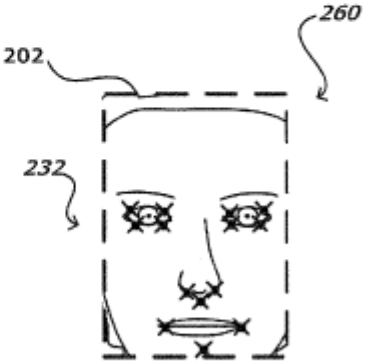


FIG. 2D

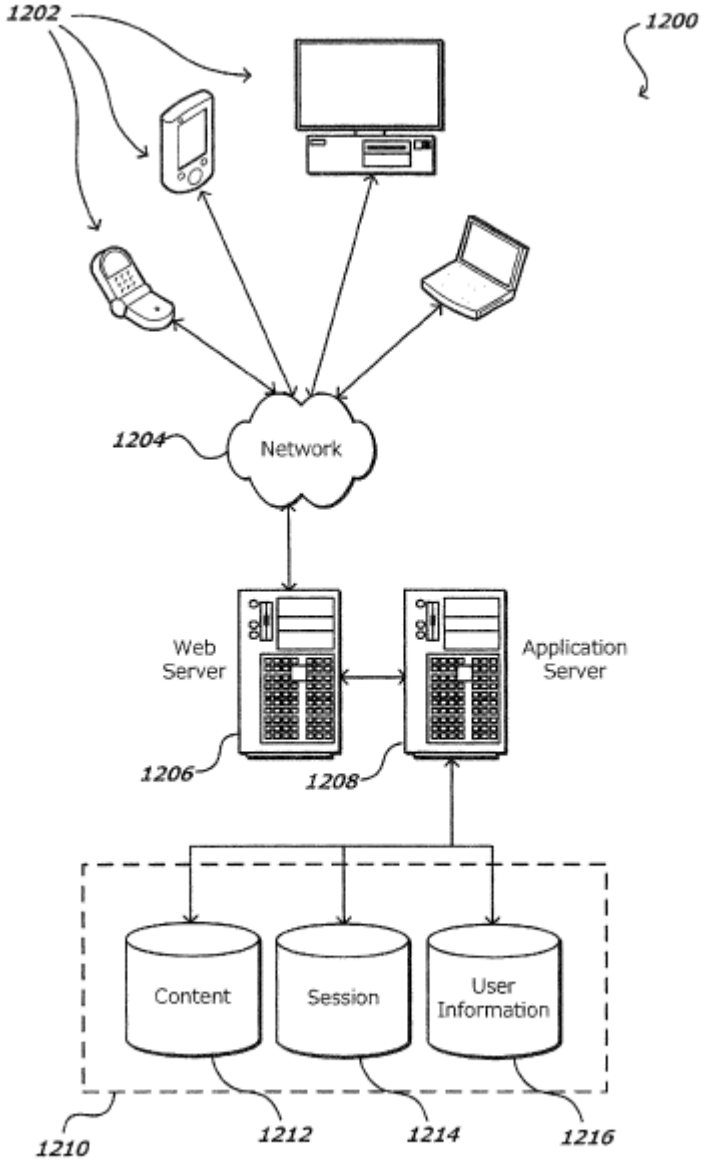


FIG. 12

"FIG. 1A illustrates an example situation 100 wherein a person 102 is attempting to gain access to a computing device 104. The computing device 104 in this example includes at least one image capture element 106 that is operable to capture image information over a range of angles 108, or field of view, with respect to the device. Although a portable computing device (e.g., a cell phone, an electronic book reader, or tablet computer) is shown, it should be understood that any electronic device capable of receiving and processing input, or at least capable of rendering and/or displaying visual content, can be used in accordance with various embodiments discussed herein. Example devices can also include, for example, desktop computers, notebook computers, personal data assistants, smart phones, video

gaming consoles, television set top boxes, wearable computers (e.g., smart glasses, smart watches, etc.), and portable media players.

The camera 106 in this example is positioned on the device such that the person 102 likely will be at least partially included in the field of view 108 when the person is interacting with the device, such as by looking and/or interacting with a display screen of the device. It should be understood, however, that there can be additional and/or alternative cameras placed in similar or alternative locations in accordance with various embodiments, and that information from any or all of these cameras can be analyzed as appropriate. For example, a computing device might have a high resolution still camera that is able to capture images useful for performing facial recognition, and might have a lower resolution video camera that can be useful for performing pulse detection. In other embodiments, a single camera might be used to capture image information for both types of analysis, while still other embodiments might utilize stereo cameras or other elements to determine distance information or perform three dimensional modeling, among other such aspects. As mentioned, some devices might have digital still cameras that are able to capture single images at specific points in time, or digital video cameras that are able to continuously capture image information, which can be referred to as a set of frames in at least some embodiments. In some embodiments, a series of still images can be captured over a period of time and analyzed for purposes of color variation and pulse detection instead of video information. Also, for a process such as image recognition to be relatively accurate, the mage being analyzed may have to meet some minimum criteria. This can include, for example, adequate lighting and contrast, but can also include factors such as quality of focus and spatial resolution. Accordingly, a device can include additional elements as well, such as illumination elements and focusing optics as discussed elsewhere herein." [3:40-4:23]

"FIG. 3A illustrates an example wherein the approximate position and orientation of the head of a user 302 has been determined and a virtual "box" 320 is placed around the user's head using one or more of the various user detection processes discussed herein. A similar or different approach can also be used to determine an approximate location and area 322 of each of the user's eyes (or in some cases the eyes in tandem) and mouth or other facial features. By determining the location of the user's eyes and mouth as part of facial detection, advantages may be obtained as it can be more likely that the image determined to be the user's face actually includes the user's face, and it can be determined that the user is in front of the device. Further, the relative movement of the user's eyes and mouth can be easier to detect than the overall movement of the user's face when the user is performing motions such as nodding or shaking the head back and forth. Further still, the relative movement of the user's eyes and mouth can be used to verify that the face represented in the image(s) undergoing the recognition process corresponds to an actual human face, and not a representation of a human face. As described, movement of the user's eyes and mouth can be determined by capturing video information and/or a series of images over a period of time sufficient to determine movement of such facial features of the user." [6:36-60]

> "Various other approaches can also be used to verify that the face represented in the image(s) undergoing the recognition process corresponds to an actual human face, and not a representation of a human face. For example, FIG. 3B illustrates an example wherein various features on a user's face are identified and assigned a point 324 in the image. The system thus can detect various aspects of user facial features and can determine changes such as movement or change in shape or expression. Such an approach can provide advantages over the general approach of FIG. 3A in certain situations, as various points along a facial feature can be determined, such as the end points and at least one center point of a user's mouth. Accordingly, expressions such as a smile or frown can be captured even though the overall position of the user's mouth or face did not move and the expressions can be used to verify that the face represented in the image(s) undergoing the recognition process corresponds to an actual human face, and not a representation of a human face. For example, once the facial features of a user are detected, relative motion or changes in facial expression can be tracked and utilized as input to verify that the face represented in the image(s) undergoing the recognition process corresponds to an actual human face, and not a representation of a human face." [6:61-7:17]

16. U.S. PATENT NO. 9,600,649 ("PARRY")

Parry discloses an authentication method that requires users to perform a certain gesture or act that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Parry include:

> "An authentication method requires receiving an order from a server to perform an act which is then verified by the server for liveness. The act may comprise shining a color on an object such as the face of the user, holding a flash at a particular location or a combination of these and other similar acts." [Abstract]

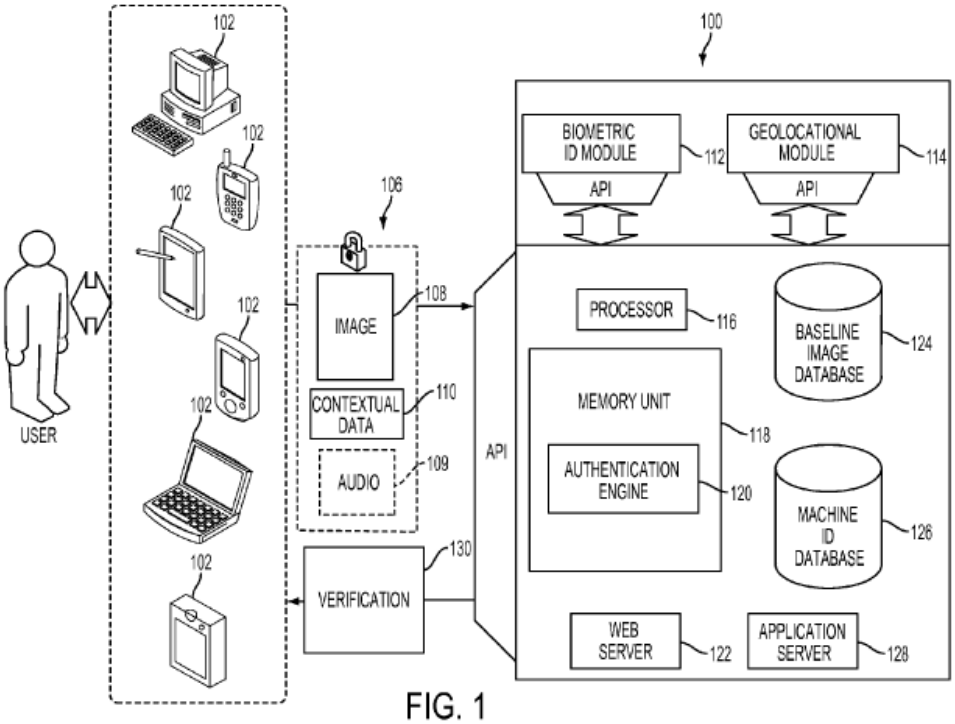


FIG. 1

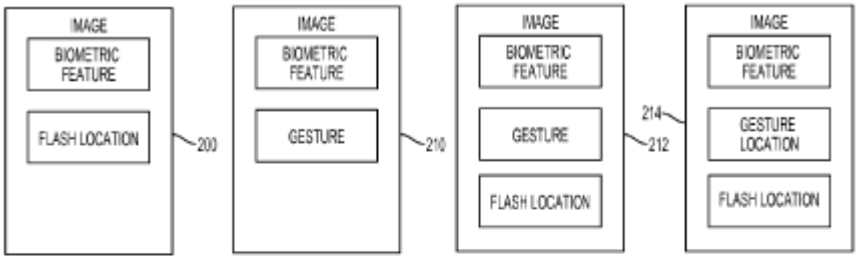


FIG. 2A FIG. 2B FIG. 2C FIG. 2D

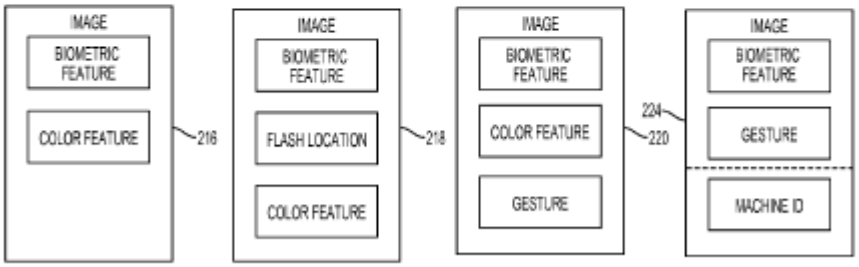


FIG. 2E FIG. 2F FIG. 2G FIG. 2H

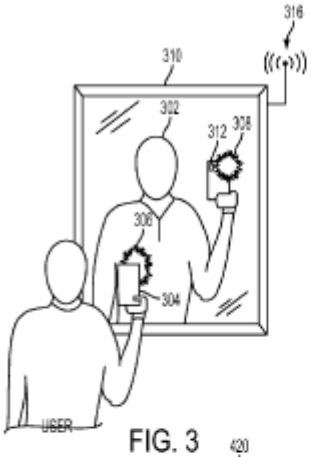


FIG. 3

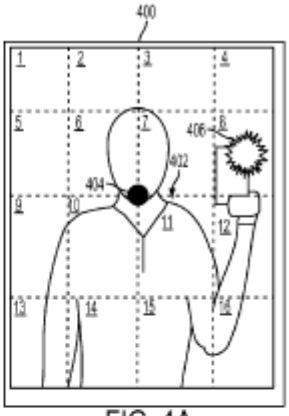


FIG. 4A

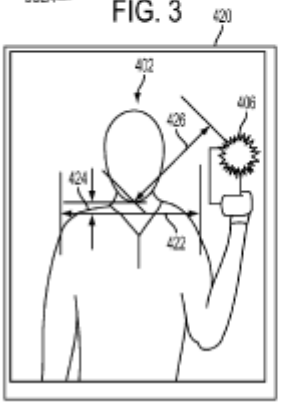


FIG. 4B

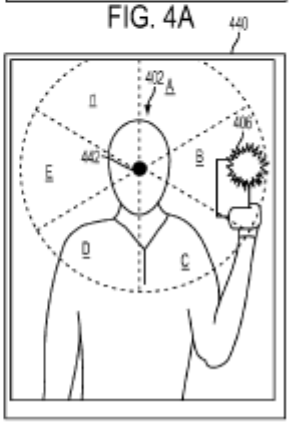


FIG. 4C

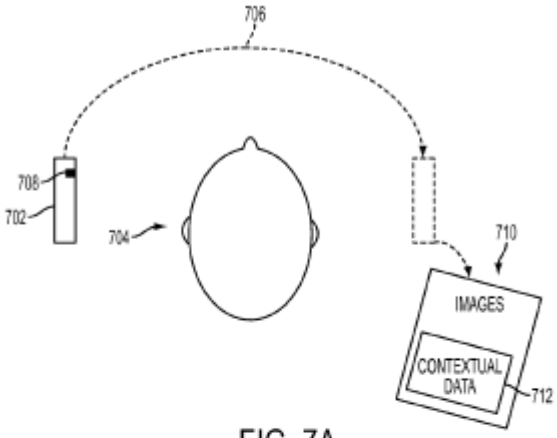

706
708
702
704
710
IMAGES
CONTEXTUAL DATA
712

FIG. 7A

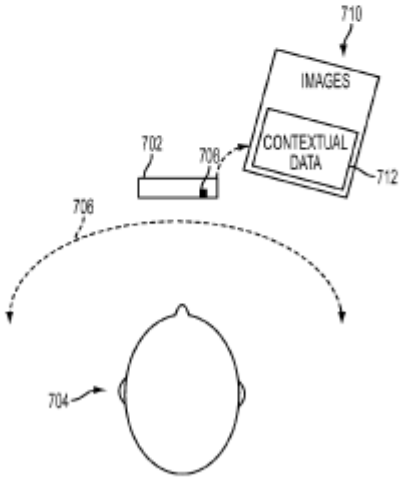

710
IMAGES
CONTEXTUAL DATA
712
702
708
706
704

FIG. 7B

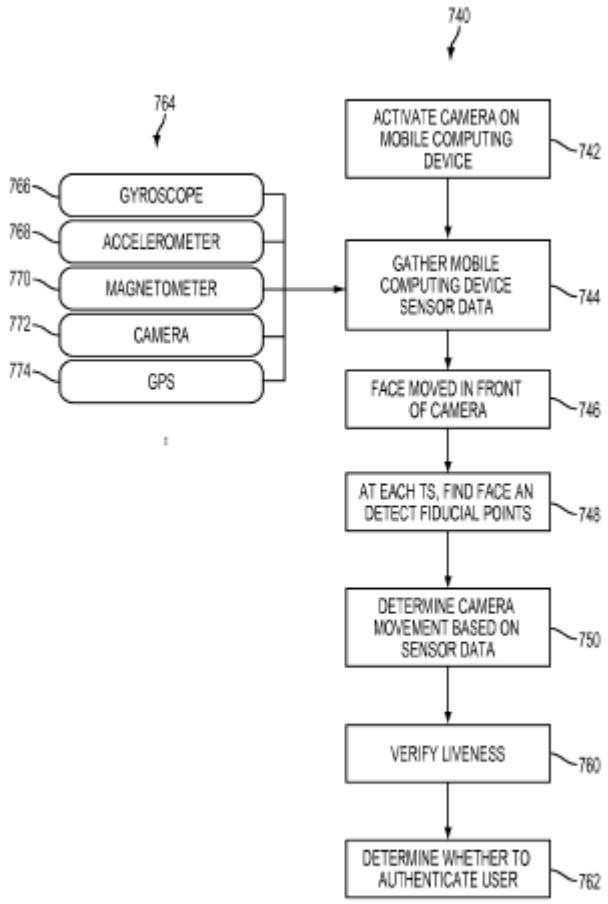


FIG. 7C

"Generally, the presently disclosed systems and methods may authenticate a user before giving the user access to a mobile computer device, access to an application on a computer device, access to a building or other structure, access to a web portal, access to any other type of computing device, access to data, or access to any other secured virtual or physical destination. The authentication can be based on a combination of biometric analysis and contextual data analysis, with the contextual data based on a user device of the user seeking authentication. Therefore, the presently disclosed systems and methods generally bind man and machine to effectuate the authentication paradigms described in more detail below." [4:31-43]

"Referring now to FIG. 1, one example embodiment of the present disclosure may comprise an authentication computing system 100 that receives and processes identity-based information to execute user authorization. The authentication computing system 100 may be provided using any suitable processor-based device or system, such as a personal computer, laptop, server, mainframe, or a collection (e.g., network) of multiple computers, for example. The authentication computing system 100 may include one or more processors 116 and one or more computer memory units 118." [4:58-5:1]

"As shown in FIG. 1, the authentication computing system 100 may include several computer servers and databases. For example, the authentication computing system 100 may include one or more web servers 122 and application servers 128. For convenience, only one web server 122 and one application server 128 are shown in FIG. 1, although it should be recognized that this disclosure is not so limited. The web server 122 may provide a graphical web user interface through which users of the system may interact with the authentication computing system 100. The web server 122 may accept requests, such as HTTP requests, from clients (such as web browsers on the device 102), and serve the clients responses, such as HTTP responses, along with optional data content, such as web pages (e.g., HTML documents) and linked objects (such as images, etc.)." [7:47-61]

"FIG. 7A depicts an example moving image scan in accordance with one non-limiting embodiment. A user device 702 includes an onboard camera 708 that may collect video and/or still images. As part of an authentication process the user 704 sweeps the user device 702 in a path 706 while the camera 708 collects image data. While the path 706 is shown as an arc, a variety of paths may be used, such as saw-tooth paths, v-shaped paths, linear paths, and so forth. FIG. 7B depicts an example moving image scan where the user 704 sweeps their head side to side in a path 706 while the camera 708 collects the image data. In other embodiments, the user may be required to nod their head up and down, move their head in a circular pattern, or otherwise execute a particular head and/or body movement. In any event, during or subsequent to the sweep, images 710 may be provided to an authentication computing system, such as the authentication computing system 100 shown in FIG. 1. The images 710 may include contextual data 712, which may include speed data, orientation data, machine ID, GPS data, and so forth. The images 710 and the contextual data 712 may be transmitted to the authentication computing system in an encrypted network packet, similar to the encrypted network packet 106 shown in FIG. 1. The authentication computing system can analyze the images 710 and the contextual data 712 to determine if the user 704 should be authenticated. For example, the images 710 may be compared to images in a baseline image database 124 (FIG. 1)." [18:17-44]

17. U.S. PATENT NO. 8,705,812 ("KARAKOTSIOS")

Karakotsios discloses systems and methods to enable a computing device to select one or more frames from captured video to be used for facial recognition that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Karakotsios include:

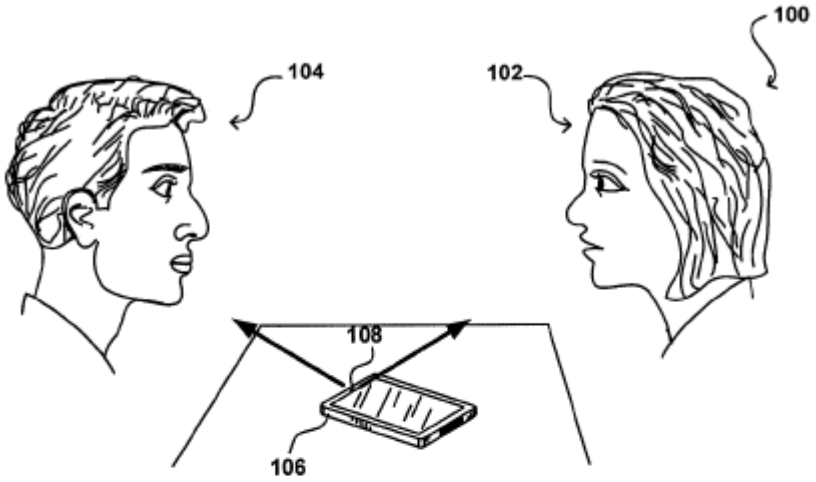


FIG. 1

FIG. 2(a)

FIG. 2(b)

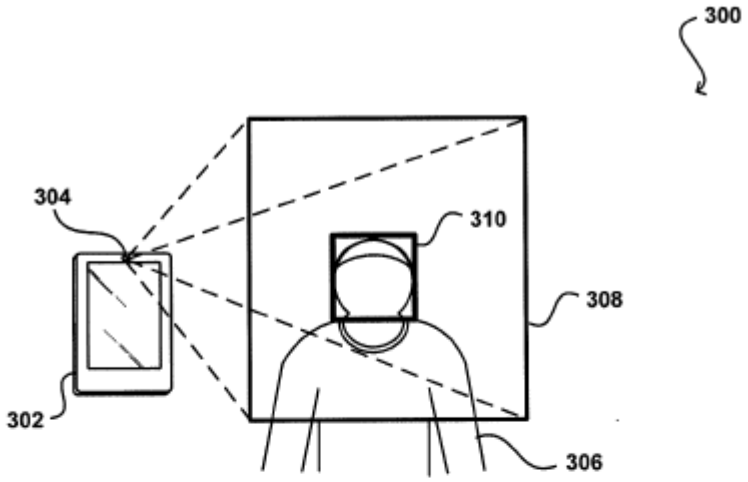


FIG. 3(a)

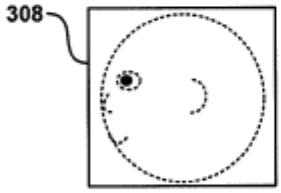


FIG. 3(b)

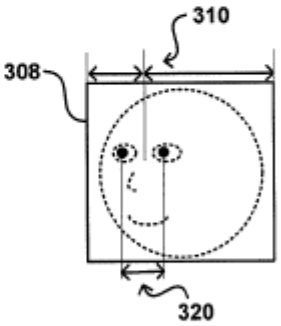


FIG. 3(c)

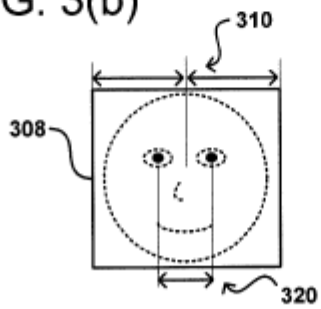


FIG. 3(d)

"In one embodiment, a video feed is continually analyzed using a head or face detection algorithm. In other embodiments, the video feed and/or analysis might be started in response to a specific action or event, such as a motion detector or light sensor detecting motion nearby or an accelerometer detecting motion of a computing device. Once a face or head is detected, the device can utilize a relative orientation-determining algorithm to attempt to determine whether the person corresponding to the detected face is facing substantially towards the camera. In response to a determination that the person is facing substantially towards the camera, a corresponding frame of the video can be selected for processing, such as to perform

facial recognition on the portion of the image frame corresponding to the user's head." [2:3-16]

"Different computing devices can have different types of image capture element. For example, some devices might have digital still cameras that are able to capture single images at specific points in time, or digital video cameras that are able to continuously capture image information, which can be referred to as a set of frames in at least some embodiments. For a process such as image recognition to be relatively accurate, the image being analyzed typically has to meet some minimum criteria. This can include, for example, adequate lighting and contrast, but can also include factors such as the direction the person is facing in the image and the quality of focus of the image. For example, FIG. 2(a) illustrates an example image 200 wherein the person in the image is facing at an angle with respect to the image, or is not at an orientation where the user is facing substantially towards the image capture element. Such orientation can occur when, for example, images are captured at random or otherwise without prior analysis of the orientation. Similar issues can arise when selecting a frame from a video stream unless there is some processing of the video stream. To analyze each frame of video, or capture a large number of still images, can require a significant amount of processing, which can be undesirable in particular for portable devices which typically have limited available resources and battery life. Capturing an image with the person at an angle as in FIG. 2(a), however, can result in an image that cannot accurately be analyzed using a conventional facial recognition algorithm, as such algorithms typically require the user to be facing substantially towards the image capture element when the image is captured, to within a limited range such as plus or minus twenty degrees from normal.

Similarly, the image in FIG. 2(b) might not produce accurate results for a facial recognition process due at least in part to an amount of motion blur in the image 202. Blur can result, for example, from motion of the user during the image capture, or motion of the device while capturing the image. Blur can also occur due to other factors, such as improper focusing of the imaging element, or lenses associated with the element. Any of a number of other issues can exist as well that can prevent randomly selected images from being able to be accurately processed by a facial recognition or other image processing algorithm." [3:22-63]

18. U.S. PATENT NO. 8,630,493 ("GOKTURK")

Gokturk discloses systems that facilitate and enhance image recognition processes that meet many of the limitations of the FaceTec Asserted Claims. The relevant portions of Gokturk include:

"Embodiments described herein facilitate or enhance the implementation of image recognition processes which can perform recognition on images to identify objects and/or faces by class or by people." [Abstract]

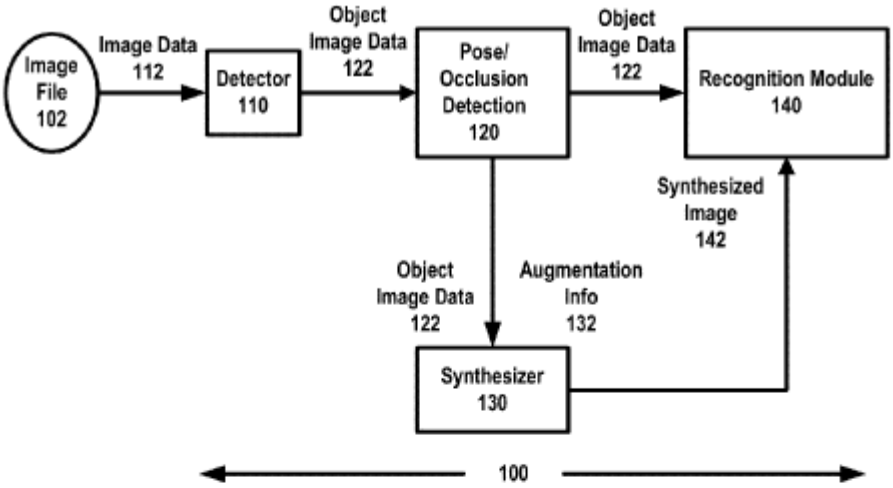


FIG. 1A

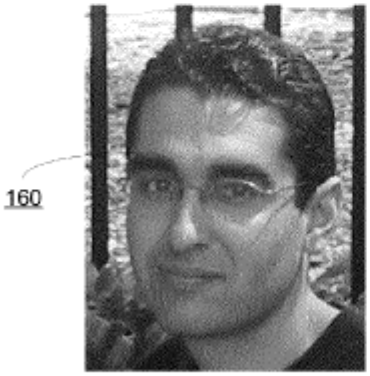


FIG. 1B

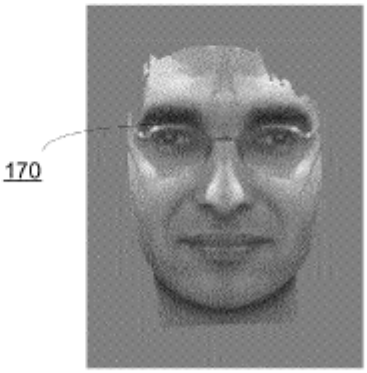


FIG. 1C

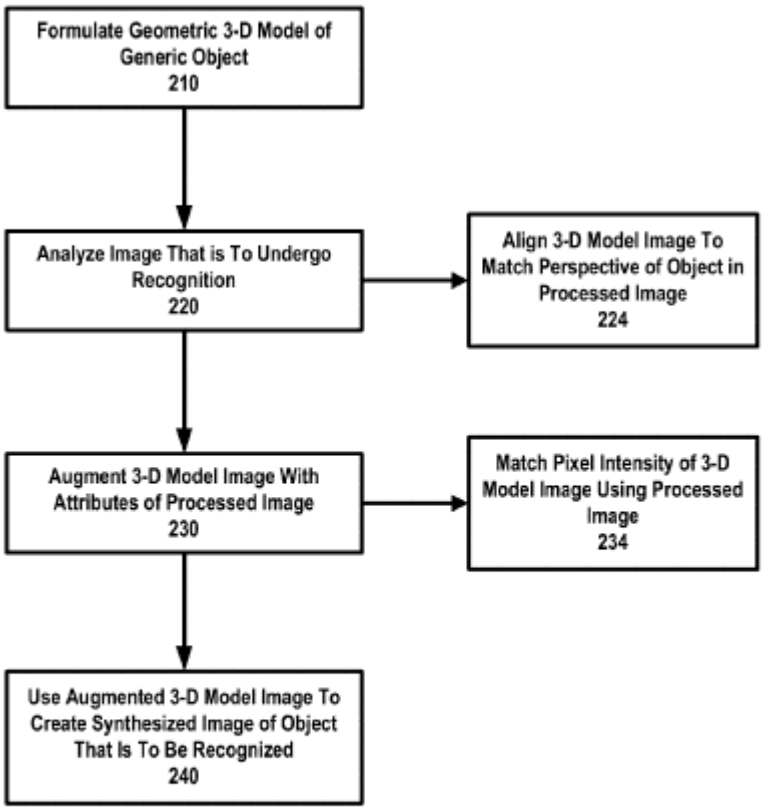

Formulate Geometric 3-D Model of Generic Object
210
Analyze Image That is To Undergo Recognition
220
Align 3-D Model Image To Match Perspective of Object in Processed Image
224
Augment 3-D Model Image With Attributes of Processed Image
230
Match Pixel Intensity of 3-D Model Image Using Processed Image
234
Use Augmented 3-D Model Image To Create Synthesized Image of Object That Is To Be Recognized
240

FIG. 2

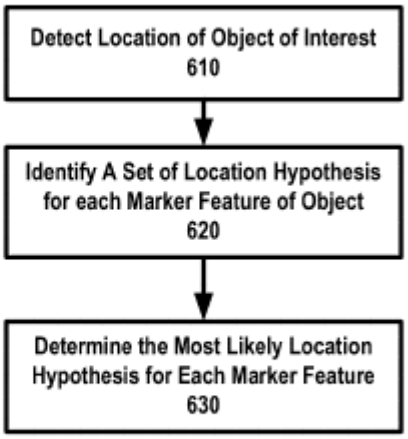

Detect Location of Object of Interest
610
Identify A Set of Location Hypothesis for each Marker Feature of Object
620
Determine the Most Likely Location Hypothesis for Each Marker Feature
630

FIG. 6

"According to another embodiment, image recognition includes determining a region of an image where an object that is to be recognized is likely located. The object of interest may be known to have specific set of features, which may be defined in variety of ways (e.g. geometric constraints) through two or three dimensional models. For each of a plurality of features of the object of interest, a set of hypotheses regions of the image may be determined. These hypotheses regions may correspond to likely locations of that feature in the object that is to be recognized. A most likely location of at least some of the plurality of features using may then be determined using the set of one or more hypothesis regions for all of the plurality of features." [2:47-59]

"In step 220, the image that is to undergo recognition is analyzed to determine pose and position of the object of interest. Given a non-frontal face photograph, one embodiment provides a computer-implemented algorithm that analyzes the image in order to recover information indicating a rotation or position of the object in the image relative to the camera. For example, with regard to facial recognition, such an algorithm may first seek to recover the rotation and position of the face three-dimensionally, from the perspective of the camera lens. This can be formulated as the task of "virtually" orienting and positioning the three-dimensional model in space in such a way that the simulated projection of rays from the model to the camera best match the face in the photograph. For example, the ray departing from the tip of the nose of the three-dimensional model may intersect the camera image plane at the tip of nose of the face in the photograph. The relationship between the points of the three-dimensional model in space and the image points of the face in the photograph can be described by a mathematical camera model, such as orthographic or full perspective projection." [6:58-7:10]

"According to one embodiment, sub-step 224 (of step 220) provides that attributes of position and orientation may be determined from use of projective three-dimensional models. In one embodiment, an unknown orientation and position of the object (such as a face) in three-dimensional space can be specified in terms of a rotation matrix, and a translation vector. These unknown parameters can be computed by establishing a set of correspondences between the three-dimensional model points and the image points. For example, an image registration algorithm (such as described with one or more embodiments of FIG. 6) can identify specific object or facial key-points in the image source 102. In the case where the object is a face, the points may correspond to the corners of the eyes and mouth, and the tip of the nose. Since the positions of these key-points on the three-dimensional model are established in advance, the unknown rotation matrix and translation vector can be computed by solving the system of equations resulting from the camera projection model. For example, closed-form, linear least-square minimization methods or iterative, gradient descent techniques can be applied for such task. In another embodiment, the pose estimation problem can be formulated as a classical vision tracking problem, where optical flow computation between the original image and the synthesized image is calculated in order to solve for pose and appearance at the same time." [7:11-35]

19. U.S. PATENT NO. 8,966,613 ("HORVITZ")

Horvitz discloses systems, methods, and computer storage media for identifying, authorizing, and/or authenticating a user to a device that meet many of the limitations of the FaceTec Asserted Claims. The relevant portions of Horvitz include:

> "Embodiments of the present invention relate to systems, methods, and computer storage media for identifying, authenticating, and authorizing a user to a device. A dynamic image, such as a video captured by a depth camera, is received. The dynamic image provides data from which geometric information of a portion of a user may be identified as well as motion information of a portion of the user may be identified. Consequently, a geometric attribute is identified from the geometric information. A motion attribute may also be identified from the motion information. The geometric attribute is compared to one or more geometric attributes associated with authorized users. Additionally, the motion attribute may be compared to one or more motion attributes associated with the authorized users. A determination may be made that the user is an authorized user. As such the user is authorized to utilize functions of the device." [Abstract]

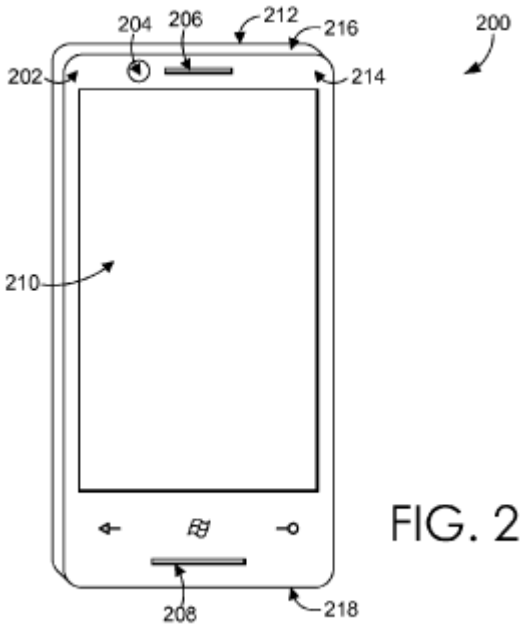


FIG. 2

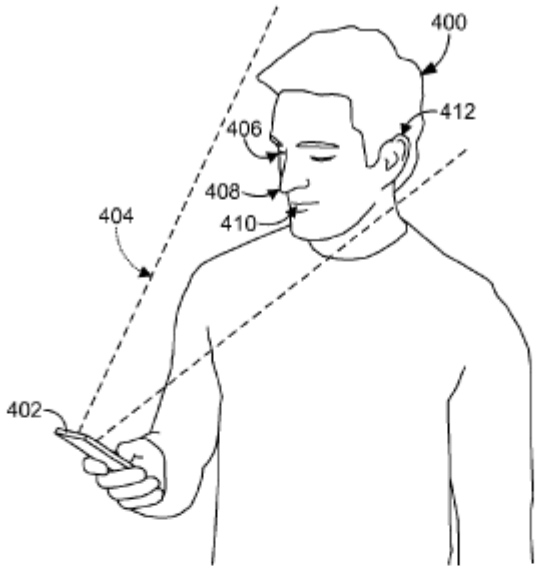

400
412
406
408
410
404
402

FIG. 4

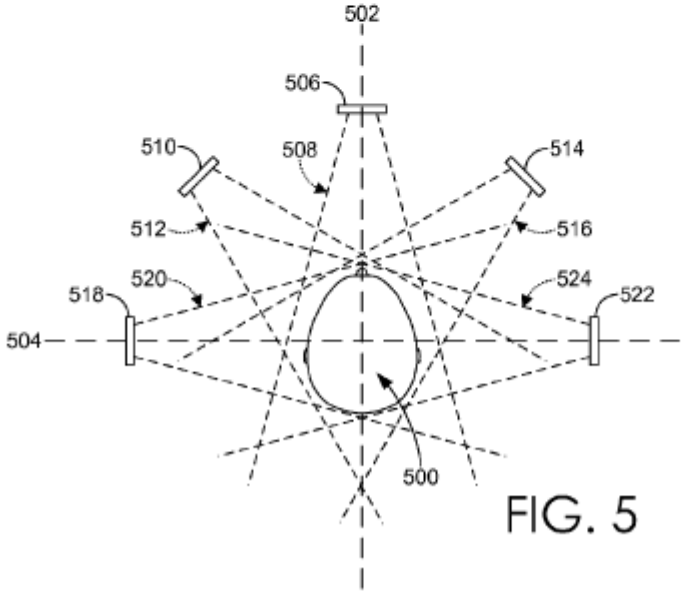

502
506
510
508
514
512
516
520
524
518
522
504
500

FIG. 5

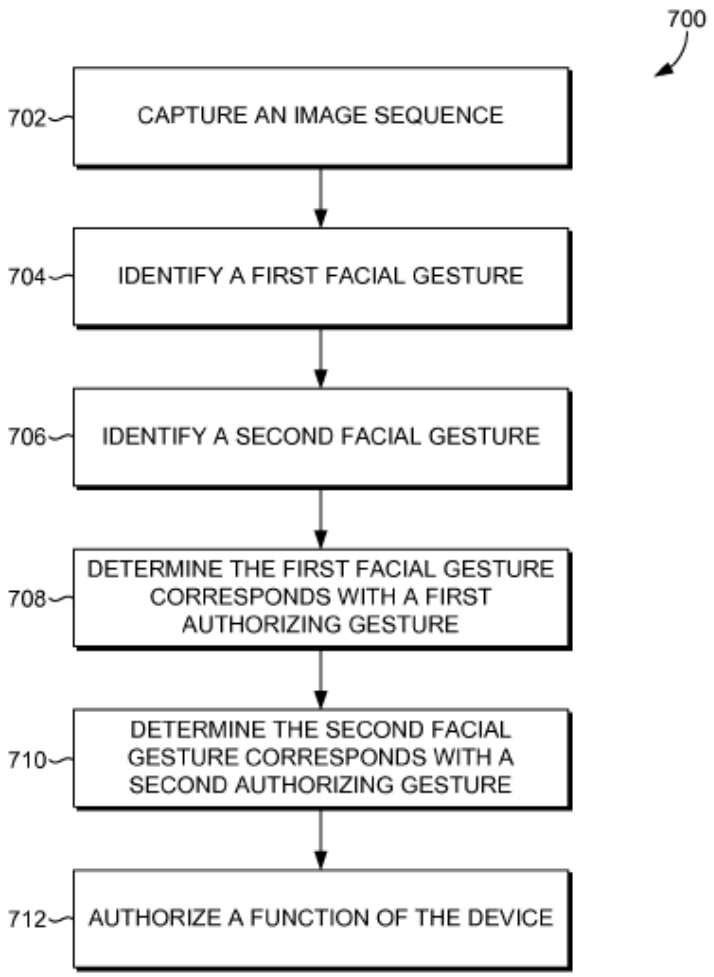


FIG. 7

"Accordingly, in one aspect, the present invention provides a method in a computing environment utilizing a processor and memory for authenticating a user to a device. The method is comprised of receiving a dynamic image. The dynamic image is comprised of geometric information of a portion of the user and motion information of a portion of the user. The method is further comprised of identifying, with the processor, a first attribute from the geometric information and a second attribute from the motion information. The method also is comprised of comparing, with the processor, the first attribute from the geometric information and the second attribute from the motion information to one or more attributes associated with an authorized entity. Additionally, the method is comprised of authorizing the user to utilize one or more functions of the device." [2:42-56]

"In another aspect, the present invention provides a handheld device for authenticating a user to the handheld device. The handheld device is comprised of a

processor, a depth camera, and computer storage media having computer-executable instructions embodied thereon, that when executed by the processor, cause the handheld device to perform a method. The method is comprised of capturing, with the depth camera, a series of images of at least a portion of a head of the user; identifying a first attribute within the series of images; determining the user is an authorized user of the device based, at least in part, on the first attribute; and providing a first functionality of the device to the user in response to determining the user is an authorized user." [2:57-3:2]

"Motion information that may be captured in a dynamic image may include, but is not limited to, one or more points on an observed object as it transitions from a first point at a first time to a second point at a second time. For example, a user's pupil may provide a point, that when tracked over time, provides an indication of movement of an eye. Motion may also be captured through a transition of a particular geometry from a first state to a second state. Together, geometric information and motion information may provide tools for identifying a particular gesture performed by a particular user. For example, geometric information may be utilized to identify a particular person through facial recognition techniques. The motion information (in possible conjunction of geometric information) allows for a predefined gesture, sequence of gestures, and/or various speeds of gesture(s) to occur in three-dimensional space. Therefore, it is contemplated that a device is able to reduce a number of false positive authorizations through a paired analysis of geometric information and motion information." [7:21-39]

"In use, it is contemplated that a dynamic image is captured of the user 400, which allows for a facial recognition utilizing three-dimensional input. In addition to capturing information useable for a facial recognition-type process, it is contemplated that the dynamic aspect of the dynamic image provides motion information that is useable for identifying unique muscular-skeletal interactions of the user. Further, the dynamic image provides motion information that is useable for identifying one or more gestures performed by the user. For example, it is contemplated that a user performs a series of gestures that are captured in three-dimensional space. The sequence of gestures may be a predefined sequence that is useable by the user to access one or more functions of a device. Further, because a three-dimensional image (including depth information) is utilized in this example, replicating the gesture by a different entity is substantially more difficult. Therefore, three-dimensional image information may be useable for authenticating a user based on both three-dimensional geometric characteristics of one or more features, but also by motion of one or more portions of the user." [9:12-31]

"FIG. 5 depicts a top-down perspective of a user 500 with a plurality of field of views from which a device may capture a dynamic image, in accordance with aspects of the present invention. Exemplary axes are depicted, such as a z-axis 502 and an x-axis 504. A y-axis, which is not depicted, may extend into the figure through an intersection of the z-axis 502 and the x-axis 504. While the plurality of devices are depicted at an approximate equidistance (e.g., depth) from the user 500, it is understood that a device may be moved in any direction at any orientation of

any axis in three-dimensional space. An advantage of utilizing a depth camera is the ability to capture a dynamic image from a variety of locations to evaluate a common feature. For example, a traditional two-dimensional image may not be effective for capturing a useable facial recognition image if the captured image is not oriented within a few degrees of a source image. However, inclusion of depth information allows geometric attributes to be identified from a variety of angles. Similarly, motion attributes may be identified from a variety of angles." [9:53-10:4]

20. U.S. PATENT NO. 10,049,287 ("HOLZ")

Holz discloses a computer authentication system that determines whether the captured image is an actual person that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Holz include:

FIG. 1

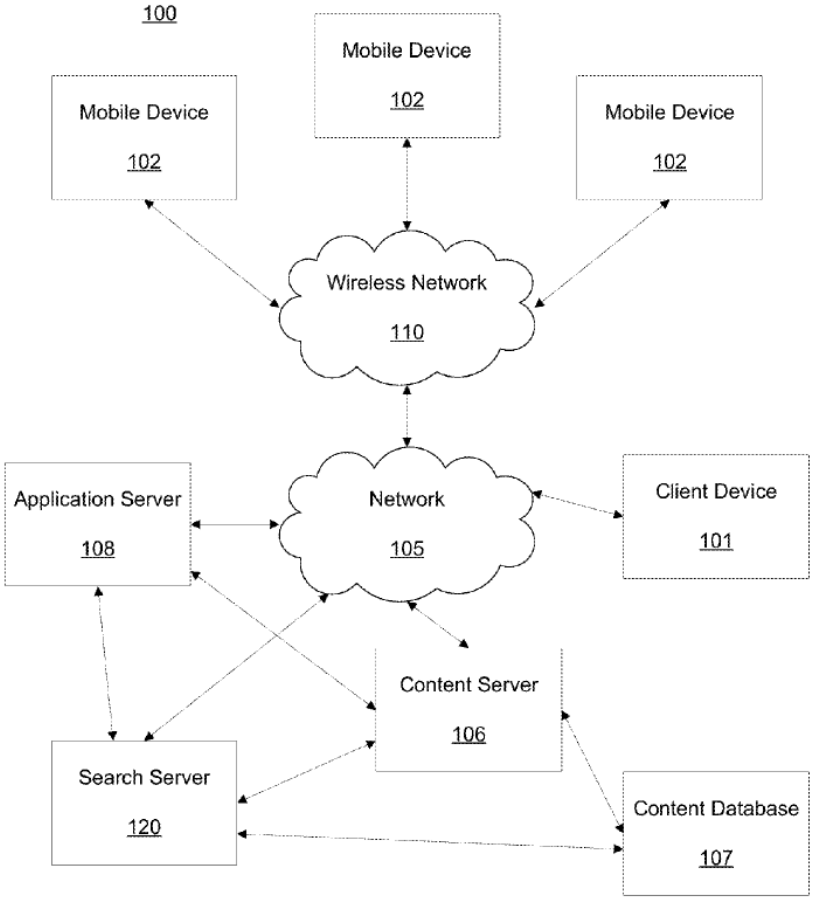


FIG. 4A 400

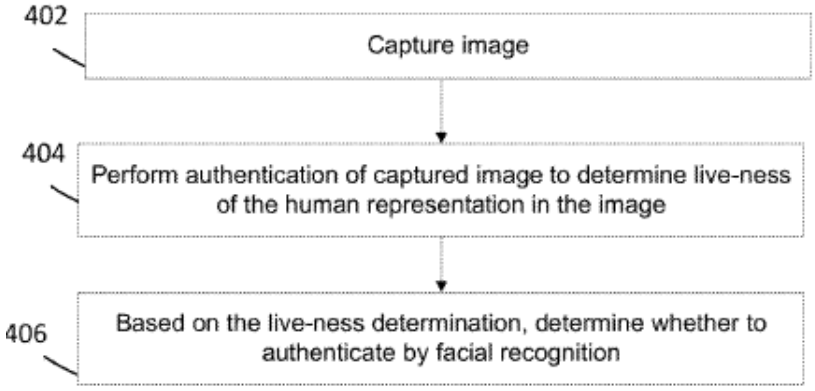
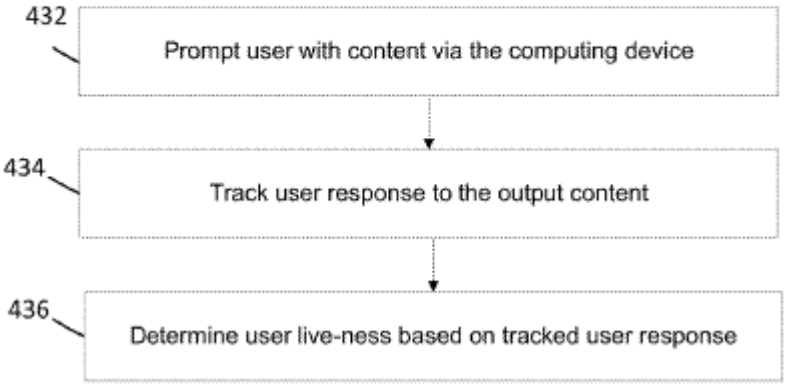


FIG. 4D 430



"For purposes of this disclosure, a client (or consumer or user) device may include a computing device capable of sending or receiving signals, such as via a wired or a wireless network. A client device may, for example, include a desktop computer or a portable device, such as a cellular telephone, a smart phone, a display pager, a radio frequency (RF) device, an infrared (IR) device an Near Field Communication (NFC) device, a Personal Digital Assistant (PDA), a handheld computer, a tablet computer, a phablet, a laptop computer, a set top box, a wearable computer, an integrated or distributed device combining various features, such as features of the forgoing devices, or the like." [7:31-42]

"For example, the disclosed systems and methods can, according to embodiments of the present disclosure, detect inadvertent actions and reactions of a user in order to establish live-ness and physical presence of a face captured by the camera. Thus, as discussed in more detail below, the disclosed systems and method provide additional functionality to existing facial recognition systems that enables such systems to actually determine whether the image being captured and/or recorded is that of an actual person (e.g., the user's face), as opposed to a non-human

representation. According to some embodiments, reference to capturing a user's face can include capturing of the face as a whole, including, but not limited to, all or a subset of the other features of the face, such as, for example, the outline of the face, user's eyes, irises, features of the iris, eyebrows, lips, nose, ears, hair, brow, and the like." [9:3-18]

"Certain embodiments will now be described in greater detail with reference to the figures. In general, with reference to FIG. 1, a system 100 in accordance with an embodiment of the present disclosure is shown. FIG. 1 shows components of a general environment in which the systems and methods discussed herein may be practiced. Not all the components may be required to practice the disclosure, and variations in the arrangement and type of the components may be made without departing from the spirit or scope of the disclosure. As shown, system 100 of FIG. 1 includes local area networks ("LANs")/wide area networks ("WANs")-network 105, wireless network 110, mobile devices (client devices) 102 and client device 101. FIG. 1 additionally includes a variety of servers, such as content server 106, application (or "App") server 108, and search server 120." [9:19-34]

"Generally, however, mobile devices 102 may include virtually any portable computing device capable of receiving and sending a message over a network, such as network 105, wireless network 110, or the like. Mobile devices 102 may also be described generally as client devices that are configured to be portable. Thus, mobile devices 102 may include virtually any portable computing device capable of connecting to another computing device and receiving information. Such devices include multi-touch and portable devices such as, cellular telephones, smart phones, display pagers, radio frequency (RF) devices, infrared (IR) devices, Personal Digital Assistants (PDAs), handheld computers, laptop computers, wearable computers, tablet computers, phablets, integrated devices combining one or more of the preceding devices, and the like." [9:36-51]

"Content server 106 can further provide a variety of services that include, but are not limited to, authentication services and/or identity verification services … ." [12:37-39]

"According to embodiments of the present disclosure, the anti-spoofing engine 302 is a special purpose machine or processor and could be hosted by a computing device, such as, but not limited to, a web server, application server, search server, content provider, email service provider, ad server, user's computing device, or any combination thereof. The database 318 can be any type of database or memory modified to perform as described herein, and can be associated with the anti-spoofing engine 302 and/or a hosting device, such as, for example, content server 106 or application server 108. The database 318 can store user information including, but not limited to, user identifying information, user demographic information, and user biometric information, and the like." [15:47-60]

"FIG. 4A is a Process 400 diagram illustrating steps performed in accordance with embodiments of the present disclosure for determining and verifying that the images recorded by a facial recognition system actually represent a human being. … FIG.

> 4A begins with Step 402 where a computing device, having at least one camera, captures an image. In some embodiments, Step 402 can involve capturing a recording of an image. Thus, the captured image can be a static image rendering or a video recording of sequential image frames (i.e., video frames). …
>
> Step 402 can include, as understood by those of skill in the art, identification of a face, facial features, and/or head of a user within the captured image, as discussed in more detail below. For example, Step 402 can involve identifying the location of at least one eye, a mouth, nose, hair, ears, eyebrows, outline of the head, and the like, from within the captured image. As discussed above, the captured image maybe an image, a series of images, or a video recording, and can additionally be used for authentication by a facial recognition system (by the facial recognition module 304).
>
> In Step 404, the anti-spoofing engine 302 then performs authentication of the captured image to determine the live-ness of the human representation in the captured image." [17:28-58]
>
> "FIG. 4D is a Process 430 diagram illustrating steps performed in accordance with embodiments of the present disclosure for explicitly (i.e., with a user's knowledge) triggering a user for a response that indicates that the image being captured/recorded of the user is an actual human being. … In another non-limiting example, the disclosed systems and methods can prompt a user to perform a series of randomized actions (e.g., turning the head), asking the user to follow, with their eyes, an object moving on the screen, and the like, whereby the detection of such movements is matched to the requested action to determine if the actions match the requested actions. Thus, Process 430 actively prompts the user for a reaction, which requires the user to explicitly act and verify his/her live-ness. …
>
> In response to the prompt, Step 434 involves tracking the user's response. That is, using the camera of the computing device, the user's response is tracked and analyzed. This enables the anti-spoofing engine 302 to compile the user's involuntary movements that occurred immediately in response to the generated output. Based on the tracked user response, a determination is then made as to whether the response can be attributed to that of a human user, as opposed to a digital representation of a user used in connection with a spoofing attempt. Step 436." [22:19-54]

21. U.S. PATENT NO. 8,856,541 ("CHAUDHURY")

Chaudhury discloses a method for liveness detection using facial movements that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Chaudhury include:

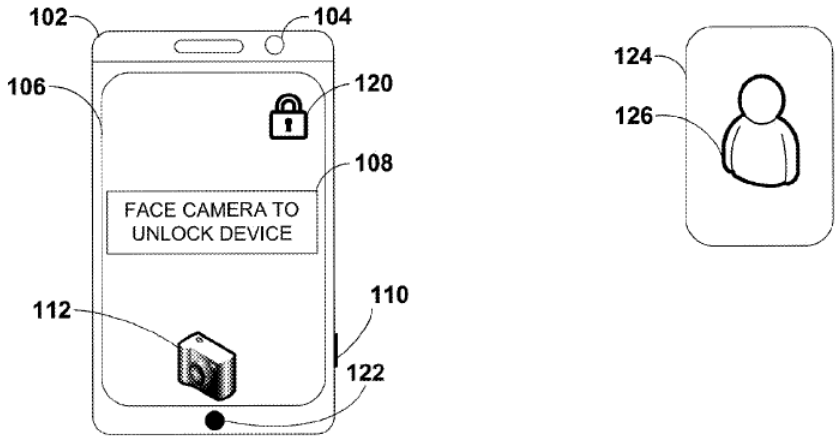


FIG. 1A

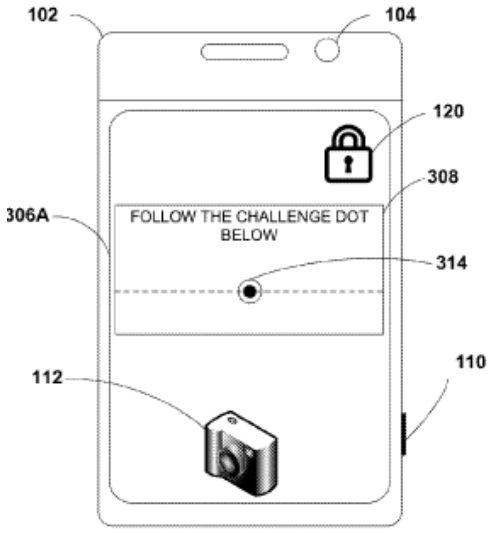


FIG. 3A

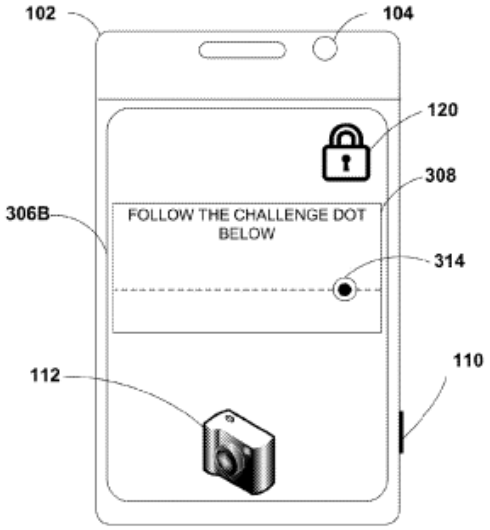


FIG. 3B

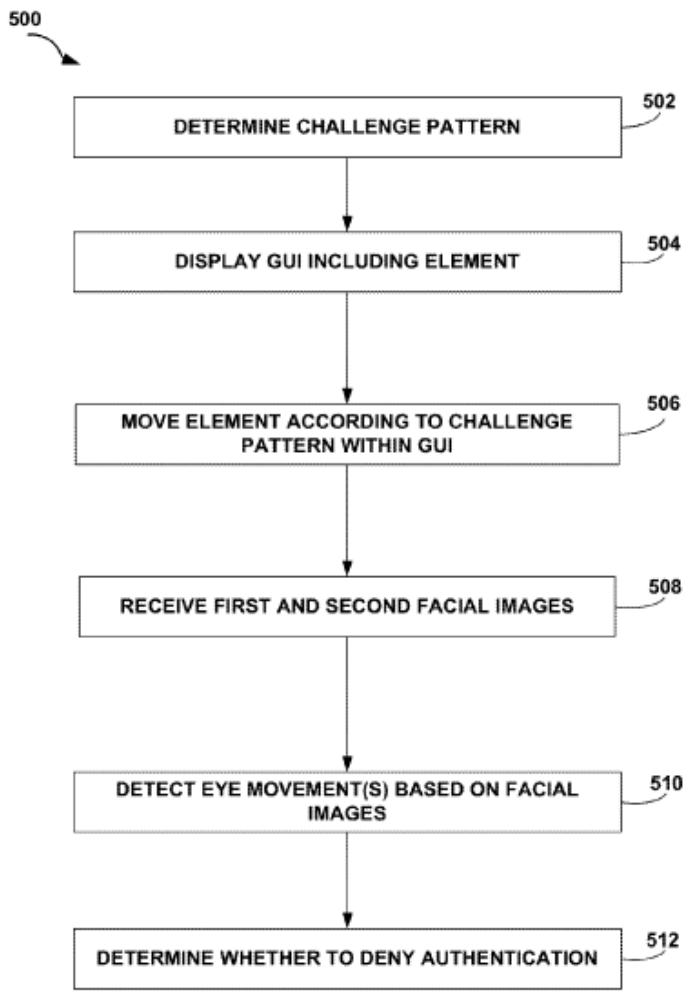


FIG. 5

"A user may activate or otherwise gain access to functionalities controlled by a computing device by "unlocking" the device. In some instances, a computing device may be configured to permit unlocking based on authentication information provided by the user. Authentication information may take various forms, including alphanumeric passcodes and biometric information. Examples of biometric information include fingerprints, retina scans, and facial images. A computing device may authenticate a facial image input using facial recognition technology." [1:5-15]

"In one example, a method includes determining, by a computing device, a challenge pattern against which to match an authentication input to detect liveness, displaying, using a display device coupled to the computing device, a graphical user interface including an element, and moving the element according to the challenge pattern within the graphical user interface. The method may further include receiving, from an image capture device coupled to the computing device, at least a first image of a face of a user and a second image of the face of the user, and detecting, by the computing device, one or more eye movements based at least in

part on the first image of the face of the user and the second image of the face of the user. The method may further include determining whether to deny authentication to the user with respect to accessing one or more functionalities controlled by the computing device." [1:19-34]

"In general, this disclosure is directed to techniques for preventing erroneous authentication caused by spoofing attempts. A computing device may implement one or more anti-spoofing (or anti-playback) programs that detect suspected spoofing attempts, and prevent erroneous authentication due to the spoofing attempts. In some examples, the anti-spoofing techniques may include capturing multiple facial images of a user, and analyzing the facial images for indications of liveness. Liveness may be indicated by various gestures, such as movement of the eyes. In accordance with the techniques of this disclosure, the anti-spoofing programs may, in various implementations, detect eye movements and compare the nature of the detected eye movements to a predetermined set of movements." [3:26-39]

"FIG. 1A illustrates computing device 102 that may capture facial images associated with a user (e.g., authorized user 126), analyze the captured facial image for possible spoofing, and determine whether to allow or deny authentication based on the analysis. Computing device 102 may include, be, or be part of one or more of a variety of types of devices, such as a mobile phone (including a smartphone), tablet computer, netbook, laptop, desktop, personal digital assistant ("PDA"), set-top box, television, biometric door lock, watch, vehicle ignition, and presence verification device, among others." [4:37-47]

"More specifically, authorized user 126 may set up a facial recognition application or embedded process of computing device 102 by storing an enrollment image that represents the face of authorized user 126. Authorized user 126 may cause a camera of computing device 102 to capture the authentication using camera lens 104. Computing device 102 may store the enrollment image to one or more storage devices of computing device 102, and/or to a remote location, commonly known as 'cloud storage.'" [5:24-33]

"Computing device 102 may then compare the captured authentication image with the enrollment image, and determine whether or not the images are sufficiently similar to each other for facial recognition purposes. For example, computing device 102 may utilize one or more facial recognition programs to compare metrics associated with the authentication image to metrics associated with the enrollment image. Some examples of metrics may include distances between facial elements (pupil-to-pupil, mouth width, etc.), contours of various facial features, pixilation corresponding to skin tone or texture, hair and/or eye color, and many others." [5:56-66]

"In some implementations, to determine whether or not an object of a facial image captured using a camera of computing device 102 is a live person, computing device 102 may detect whether a series of facial images display a movement of the eyes. For instance, computing device 102 may use the front-facing camera coupled to

camera lens 104 to capture video data corresponding to the object of the captured facial image. … For example, computing device 102 may extract distinct frames of the captured video data, and utilize the frames as a first image, second image, and so on of the face of the user." [6:42-55]

"In examples, computing device 102 may display, as part of GUI 106, one or more elements that instruct the user to perform the challenge pattern. In one implementation, computing device 102 may display, in conjunction with unlock prompt 108 or subsequent to removing unlock prompt 108, instructions for performing the challenge pattern." [7:53-58]

"Although described largely with respect to unlocking a device, the techniques of this disclosure may be implemented in several different use cases. As some examples, the facial recognition and liveness detection techniques may be implemented on a remote server, to provide access to a user attempting to log in to an email account or social network account." [9:43-49]

"FIGS. 3A-3B are conceptual diagrams illustrating example graphical user interfaces (GUIs) 306A-306B that a computing device may display to prompt a user to perform an eye movement pattern, in accordance with one or more aspects of this disclosure." [16:59-63]

"In turn, computing device 102 may capture multiple images (e.g., as frames of video) using a camera coupled to camera lens 104." [17:31-33]

22. NON-INTRUSIVE LIVENESS DETECTION BY FACE IMAGES ("KOLLREIDER")

Kollreider discloses a liveness detection method using optical flow and biometric information that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Kollreider include:

Fig. 1. Example face image sequence: differently moving center and side face parts suggest the "live" presence of a person.

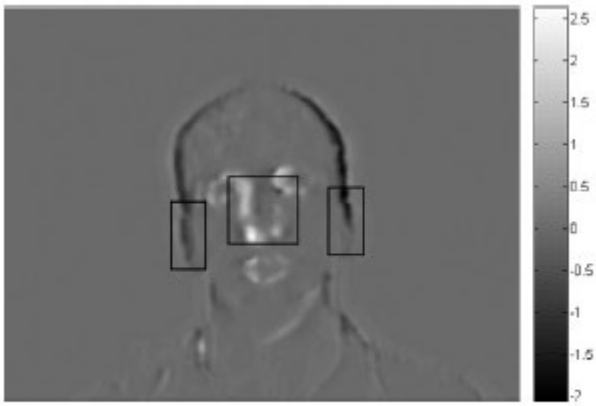


Fig. 2. Horizontal OFL (Gabor-based [5]) at the center frame of the image sequence in Fig. 1. Rectangles indicate the focused regions when comparing different face parts' motion.

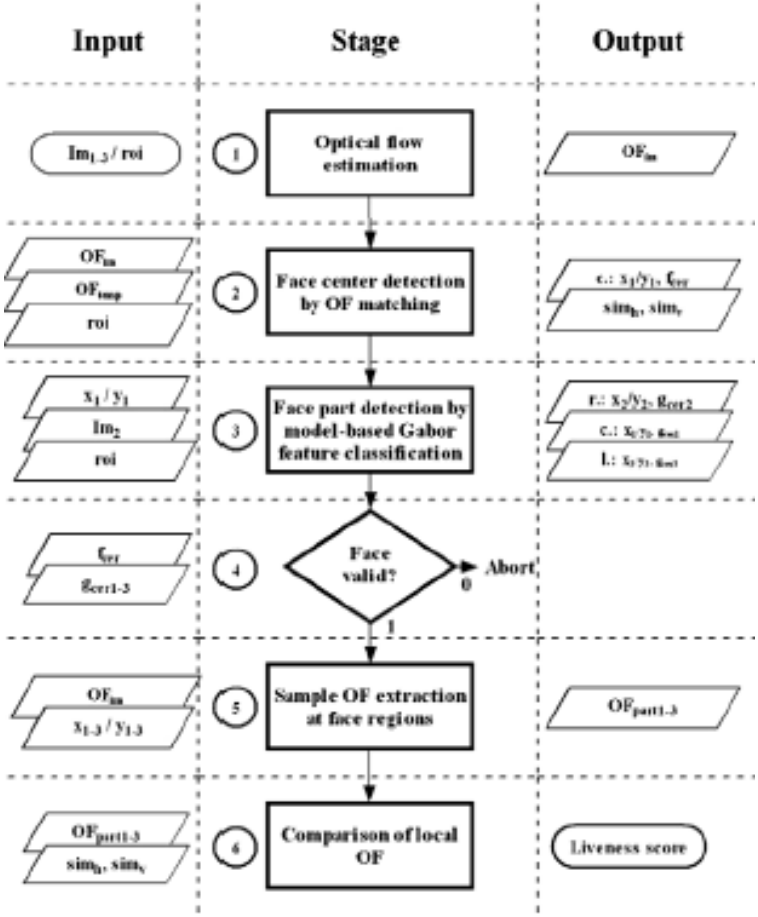


Fig. 8. Flow chart detailing the liveness detection.

"A technique evaluating liveness in face image sequences is presented. To ensure the actual presence of a live face in contrast to a photograph (playback attack), is a significant problem in face authentication to the extent that anti-spoofing measures are highly desirable. The purpose of the proposed system is to assist in a biometric authentication framework, by adding liveness awareness in a non-intrusive manner. Analyzing the trajectories of certain parts of a live face reveals valuable information

to discriminate it against a spoofed one. The proposed system uses a lightweight novel optical flow, which is especially applicable in face motion estimation based on the structure tensor and inputs of a few frames. For reliable face part detection, the system utilizes a model-based local Gabor decomposition and SVM experts, where selected points from a retinotopic grid are used to form regional face models. Also the estimated optical flow is exploited to detect a face part. The whole procedure, starting with three images as input and finishing in a liveness score, is executed in near real-time without special purpose hardware. Experimental results on the proposed system are presented on both a public database and spoofing attack simulations." [Abstract]

"In our approach, we combine face part detection and optical flow estimation to determine a liveness score. The typical trajectory of certain face parts in case of a live face sequence is exploited to discriminate it against a spoofed one. We use the optical flow of lines, [5], (OFL) which is inspired by optical flow approaches capable to differ between motion of points and motion of lines (e.g. Tensor approach [6]). As the name suggests, it is specialized on motion of lines only. Requiring only 2–3 images, the OFL approach is a lightweight energy based OF method, which can be realized by using 2D Gabor filters [5,7–9]. However, in this study we implement the OFL by employing 1D Gaussians and their derivatives. A review of optical flow techniques is given in [10]." [Pg. 1]

"Our method analyzes a face image sequence captured by one camera and delivers a probability, whether it detected a face and whether it is live. The basic idea relies on the assumption that a 3D face generates a special 2D motion which is higher at central face parts (e.g. nose) compared to the outer face regions (e.g. ears). Ideally, in terms of liveness detection, the outer and the inner parts move additionally in opposite directions." [Pg. 2]

"In other words, parts nearer to the camera move differently to parts which are further away in a live face. The experimental results, we report below, support that a small rotational movement of the head is natural and unintentional human behavior. On the contrary, a translated photograph generates constant motion at various face regions. In order to exploit these characteristics, we utilize optical flow estimation and face part detection. For the latter we employ a model-based Gabor decomposition [13], but we also present an intuitive approach by OF pattern matching. Knowing the face parts' position and comparing how fast they are moving relative to each other and into which directions, enables us to discriminate a live face against a photograph." [Pg. 2]

"In what follows are the input images referred to as Im_l,with l = 1, 2, 3. First, a region-of-interest image roi is derived by setting a threshold to the intensity differences between each of two subsequent images." [Pg. 4]

"4. Face part detection. We wish to track the three facial regions eyes/nose, left and right ear. To reliably detect these face parts we combine optical flow pattern matching and a model-based Gabor feature classification. The assumption of having

a moving face is exploited to speed up its parts' detection by taking the region-of-interest image roi into account." [Pg. 5]

"4.1. Optical flow pattern matching. The face center can be approximated by reusing information from the optical flow estimation, because the region around the eyes and the nose shows a characteristic flow pattern. A template containing the flow information of an average face center is created offline. The face center's position and the directions it moves into, are retrieved by matching this template in specific ways with the optical flow image OFim … of any sequence." [Pg. 5]

"Depending on the primary movement, the ratios cr and cl compare the real or the imaginary part of OFpart1 with OFpart2 and OFpart3, respectively. A ratio between the center and a side motion having an absolute value greater than 1, indicates liveness. In the ideal case, we expect the face center part moving in an opposite direction compared to the sides, which is indicated by negative ratios. By including this observation, the liveness score is divided into a velocity dependent and a direction dependent part. The final liveness score is then constructed … . … The score is a value in [0, 1], where 0 indicates no liveness and 1 represents the maximum liveness." [Pgs. 7-8]

23. U.S. PATENT NO. 2014/0366113 ("LECUN")

LeCun discloses a method of biometric authentication using an individual's palm that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of LeCun include:

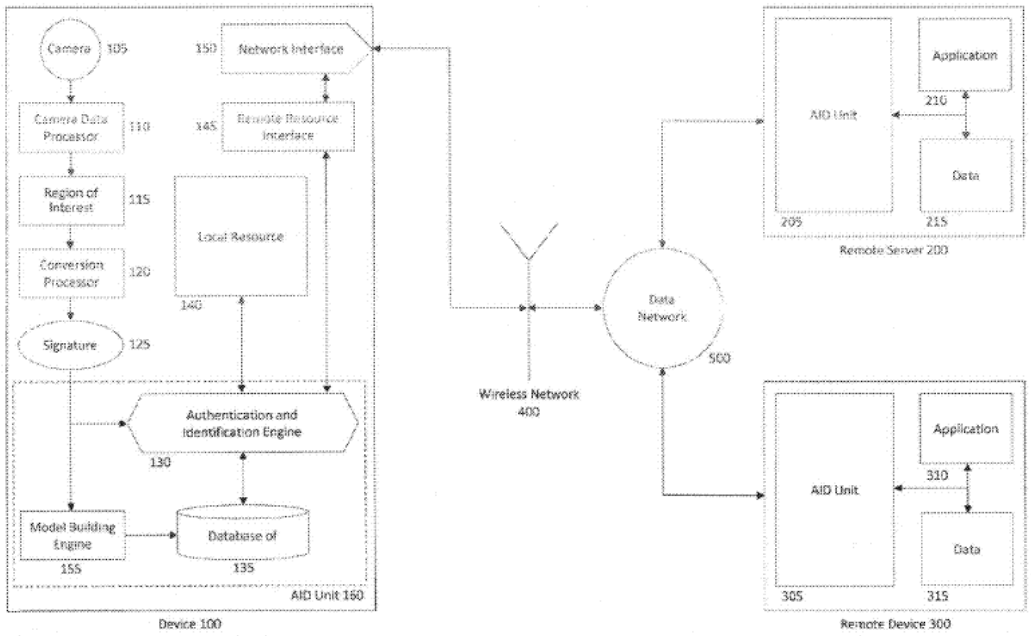


FIGURE 1

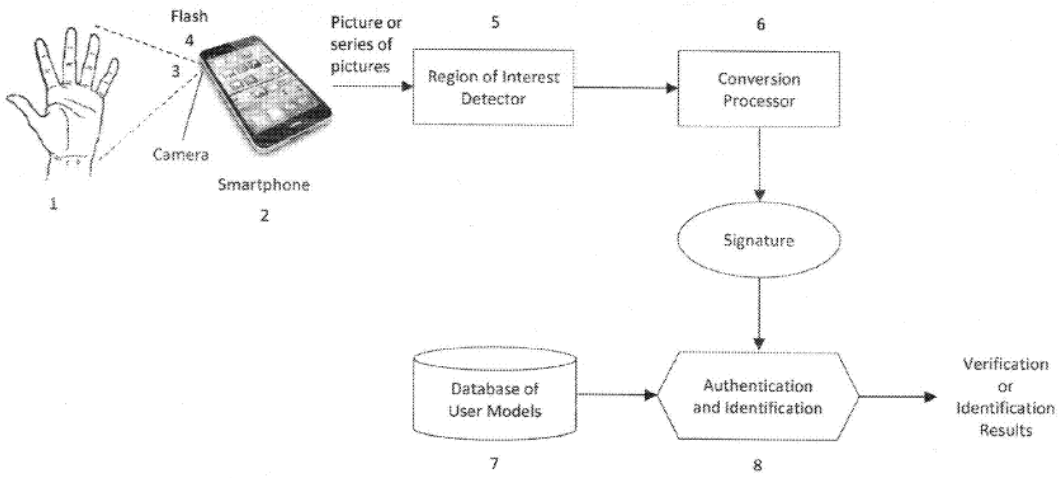


FIGURE 2

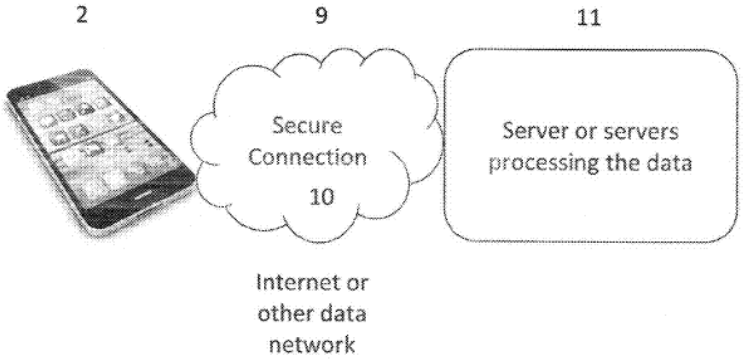


FIGURE 3

"One important issue that arises in the context of mobile devices and their widespread use in connection with so much functionality and their need to interact with so many different resources is the need to control access to each of these resources so that only those individuals or devices that should be authorized to access the applicable resources are actually able to do so." [0007]

"In one embodiment of the present invention, users of such camera-equipped devices (hereinafter referred to at times as "smartphones" for convenience, although the devices are to be understood as including all devices with a camera capability, including both mobile devices and stationary devices, such as desktop computers) who are required to identify or authenticate themselves as a condition of obtaining access to one or more resources take one or a series of photos of their palm or both palms using the smartphone camera. The system of the present invention then

employs computer vision technology to analyze the palm print image and either verify that the palm print signature matches the user's model in a database (user authentication) or find the matching user model among many models in a database (user identification)." [0013]

"Device 100 can be any device that contains a camera capable of taking high quality photographs. Preferably, the camera of Device 100 also contains a flash element capable of being selectively and rapidly activated and deactivated for illuminating the area to be photographed. Examples of such Devices 100 include smartphones, tablet computers, notebooks, and any other device that can be carried by a user and that provides a computing platform that allows for the functionality of the present invention to be operative, as well as desktop computers or a variety of stationary embedded devices." [0023]

"By way of example only, the present invention permits users of Device 100 or Device 100 itself to be authenticated or identified by remote servers and applications and other resources residing on remote servers. As illustrated in FIG. 1, Remote Server 200 can communicate with Device 100 via the communication path discussed above. In this manner and as controlled by Remote Resource Interface 145 residing on Device 100, AID Unit 205 residing on Remote Server 200 can request and receive authentication and identification data from Device 100 for comparison with known and validated user models residing on or accessible by Remote Server 200 … ." [0033]

"In the case of authentication, the user presents an identity in the form of a user ID or user name and the system of the present invention verifies that the user is indeed who he or she claims to be. The system then compares the signature derived from an image or images of the user's palm with the corresponding model in the database of user models. If they match, the user is authenticated. If they do not match, the user is rejected." [0036]

"Further methods for detecting a real hand include 3-D modeling of the hand. In this case, the system of the present invention may prompt the user to turn his or her hand while a series of multiple pictures are taken. A true 3-D object will reveal different parts of the hand with each successive image while a 2-D object will always show the exact same part of the hand, just with varying degrees of distortion. This lets the system of the present invention distinguish between a printed photograph and a real hand. Similarly, instead of rotating the hand, the user can be prompted to close the hand to a first or open it from a first while the series of pictures is taken. Other methods of distinguishing a real hand from the photograph of a hand are also possible." [0048]

24. U.S. PATENT NO. 7,840,034 ("TAKAHASHI")

Takahashi discloses a method and system of biometric authentication with a user's fingerprints that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Takahashi include:

FIG. 1

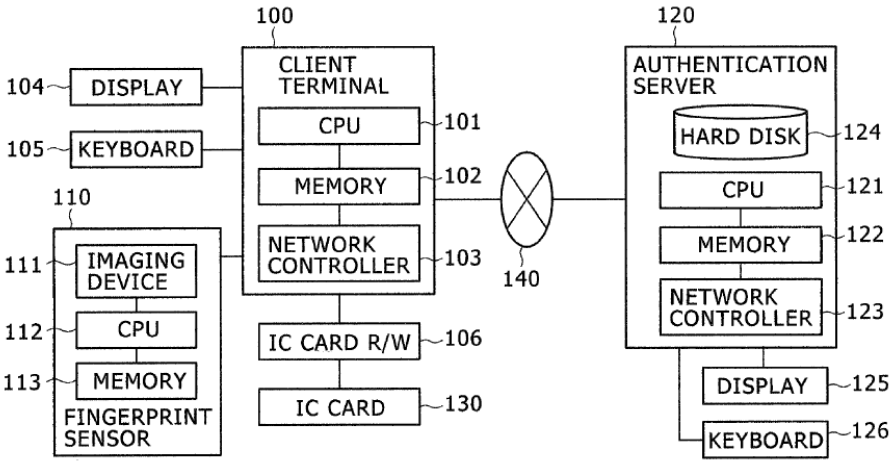
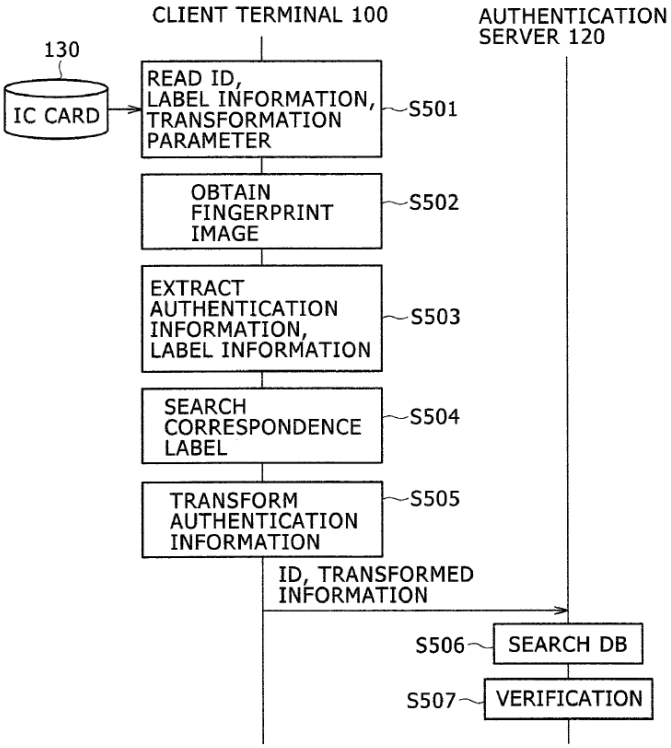


FIG. 5



"An authentication system using fingerprint information obtains a fingerprint image of a user to extract and register a feature quantity upon registration. This registration information is called a template. Upon authentication, the system newly obtains a fingerprint image from the user to extract a feature quantity, and verifies this against

the template to verify the identity of the user. In a system in which a client and a server are connected via a network, a typical example is that a template is maintained by the server in the case of authenticating a user on the client side. The client obtains the user's fingerprint upon authentication, extracts a feature quantity, and transmits the feature quantity to the server. The server verifies the feature quantity against the template to authenticate the user." [1:19-32]

"A biometric authentication method according to the present invention is a method for authenticating a user by obtaining and registering biometric information of the user into a memory of a verification unit in advance, and by verifying the registered biometric information against biometric information obtained by a feature-point transformation unit." [3:15-20]

"In the embodiment, a description will be given of an example of a cancelable fingerprint authentication system of a server-client type that performs authentication with the fingerprint feature quantity kept confidential to the server." [6:13-16]

"FIG. 1 shows a hardware configuration to which a fingerprint authentication system is applied according to an embodiment of the invention. The fingerprint authentication system includes a client terminal 100 used for providing a service to a user, and an authentication server 120 for confirming whether the user who receives the service is a normal person. The client terminal 100 and the authentication server 120 are connected via a network 140. In this system, an IC card 130 carried by the user is used. For example, when the authentication system is applied to an Internet banking service, there are connected a PC (personal computer) that the user has in home as the client terminal 100 and a server machine that the bank manages as the authentication server 120, via the network 140 such as the Internet." [6:17-30]

"The client terminal 100, for example a typical PC, includes a CPU 101, a memory 102, and a network controller 103 in a body thereof to which a display 104, a keyboard 105, an IC card R/W 106, a fingerprint sensor 110 and the like are connected." [6:31-35]

25. U.S. PATENT PUB. NO. US 2014/0309880 ("RICCI")

Ricci discloses a vehicle security system that includes facial recognition prompts in the vehicle console to unlock certain features and make personal profiles available that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Ricci include:

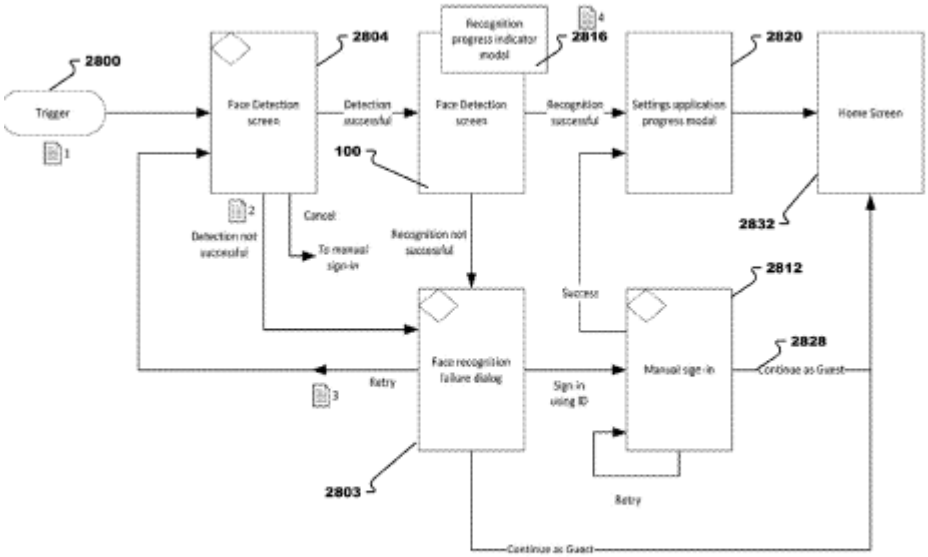


FIG. 28

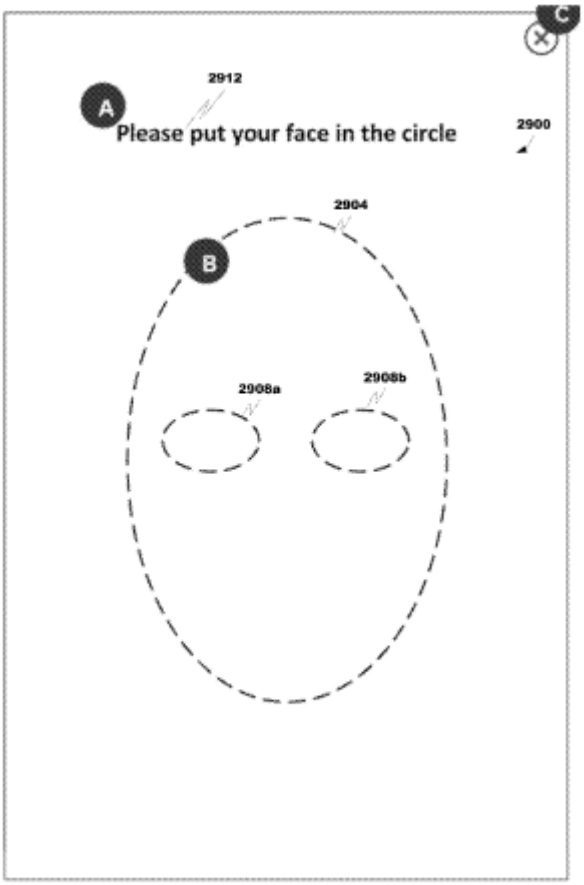


FIG. 29

"Another application of the vehicle control system 204 for authentication by facial recognition is shown in FIGS. 28-29." [0830]

"In step 2800, the vehicle control system 204 detects a stimulus or trigger event." [0831]

"In step 2804, the vehicle control system 204 provides, via the device or user interface 212, 248, user interface (s)/input interface(s) 324 and/or I/O module 312, the user with a face detection screen, such as that shown in FIG. 29. As shown in FIG. 29, the face detection screen 2900 is a dashed outline 2904 of a human face having eye holes 2908 a and b to enable the user to align his or her face with the screen for a higher quality video image of the user's face. This screen 2900 prompts the user to align his or her face such that the facial recognition camera can obtain a good image. The screen can show the video feed from the facial recognition camera with the dashed outline as an overlay. The dashed outline is intended to assist users situate his or her image properly in the camera's field of view. An instruction line 2912 can appear at the top of the screen 2900." [0832]

"When an acceptable facial image is not obtained so that facial recognition cannot be performed, the vehicle control system 204 proceeds 2803 to a manual sign-in step (discussed below) and provides the user with a face recognition failure notification dialog over the screen 2900 of the device or user interface 212, 248, user interface (s)/input interface(s) 324 and/or I/O module 312 in step 2812. If a proper facial image is obtained, the vehicle control system 204, in step 2816, searches through a repository of stored facial images to find a match and, during the mapping, provides the user with a recognition progress indicator modal on the screen 2900." [0833]

"When recognition is not successful or no match is found, the vehicle control system 204 proceeds to step 2812 and the manual sign-in step discussed below." [0834]

"When recognition is successful and a match is found, the vehicle control system 204 proceeds to step 2820 and applies the personal settings of the user, such as any or all of the settings referenced above." [0835]

"When the credentials are received and successfully authenticated, the vehicle control system 204 in step 2820 applies the personal settings of the user." [0838]

26. SECURING SENSITIVE DATA STORED ON SMARTPHONES ("WILSON")

Wilson discloses biometric security features used to lock smartphones, including face recognition, that meet many of the limitations of the FaceTec Asserted Claims. The relevant portions of Wilson include:

3.1 Face Alignment

Face alignment is an extremely important factor when employing any face recognition security measure because human faces have so many variations and viewing angles. This issue is most notable in unmonitored video surveillance in which face recognition software must analyze a dynamic image and match that image to a known face. Due to constant motion of a person's body, poor resolution, side-views and profiles, and changes in appearance such as facial hair, sunglasses, etc., the recognition device may provide false negatives or false positives when matching an identity with a face.

Face recognition is dramatically improved when faces are analyzed with known parameters, including: fixed distance, centered in front of the camera or scanner, known expression, eyes open, and non-moving [5][11]. Naturally, images such as mug shots or passport photos in which these parameters are strictly controlled offer the highest accuracy of face recognition with the actual identity of a particular person.

Facial alignment is an easily solved problem on the modern smartphone. When entering the pass code or security pattern, the user generally looks at the screen and touches the appropriate places to unlock the smartphone. Many of today's smartphones are installed with forward-facing cameras to allow for video conferencing; this same camera could be used to capture an image of the user's face for recognition purposes. By using the forward-facing camera, the user would be able to see himself on the screen and guarantee the image was centered for proper recognition. The image would also be taken from a fixed distance (arm's length, or shorter) that would be approximately the same each time the user unlocked his smartphone.

[pg. 3]

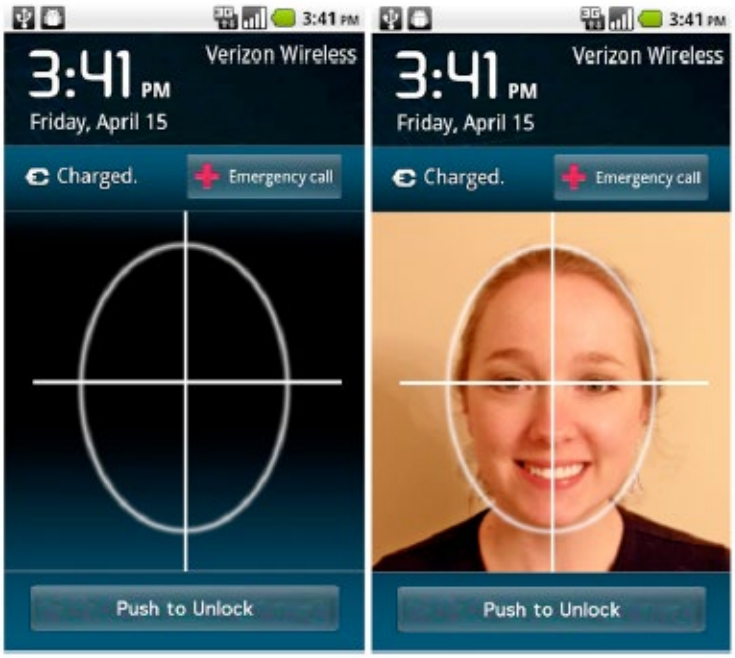


Figure 2. Example of the face capture crosshair (left) and proper face positioning in the crosshair (right)

"By properly positioning the user's face in the crosshair, the common problem of face alignment would be corrected because a consistent image of the face would be taken each time. In order to center the user's face within the oval and the eyes along the horizontal line, the smartphone would capture an image that had extremely similar proportions each time. This would solve the obvious problems of side-views and profiles, and the distance from where the image was taken in relation to the camera." [Pg. 4]

"After capturing the user's image, the smartphone would analyze it and compare it to a previous image taken to verify that it is the same authorized user. The comparison method could be performed using two different methods; the captured image could be compared to an image of the designated user upon initially setting up the security measure on his smartphone, or images of successful attempts to unlock his smartphone would be saved and used for comparison. The latter option would compare each subsequent captured image to a previously authorized image allowing the user's images to somewhat evolve and change slightly over time. This option would allow for minor facial changes, such as: five o'clock shadow, healing injuries, and possibly conservative haircuts. This would also allow for the smartphone to only save one captured image at a time, reducing the amount of hard drive space necessary to run the software." [Pg. 4]

27. U.S. PATENT NO. 10,042,993 ("BEIGI")

Beigi discloses a system in which a person uses a mobile phone or other handheld computer with multifactor authentication, including facial recognition, to make purchases that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Beigi include:

FIG. 1 Registration

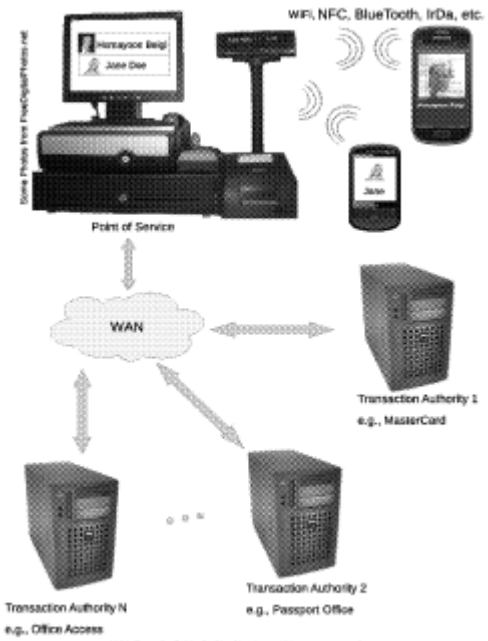


FIG. 16 POS Sales Transaction

FIG. **17** Electronic Commerce Transaction

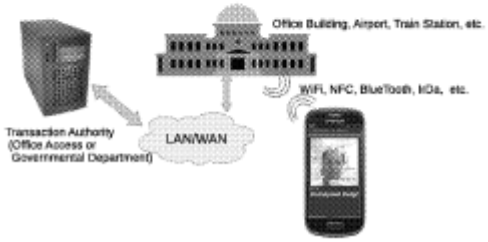


FIG. **18** Passport or Office Entry Transaction

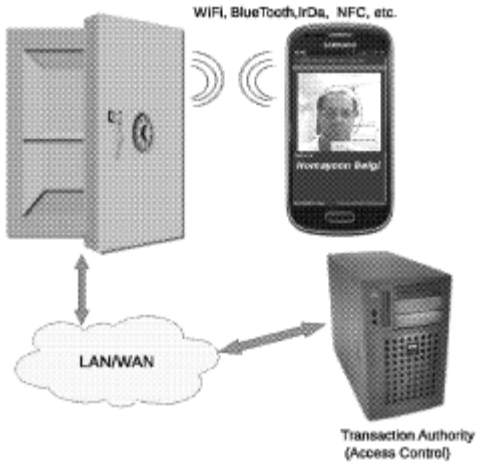


FIG. **19** Vault Access Transaction

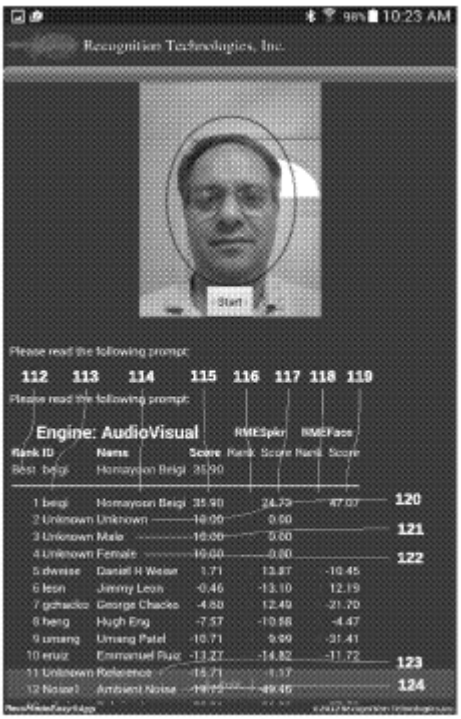


FIG. **22** Fusion Results for Speaker and Face Recognition

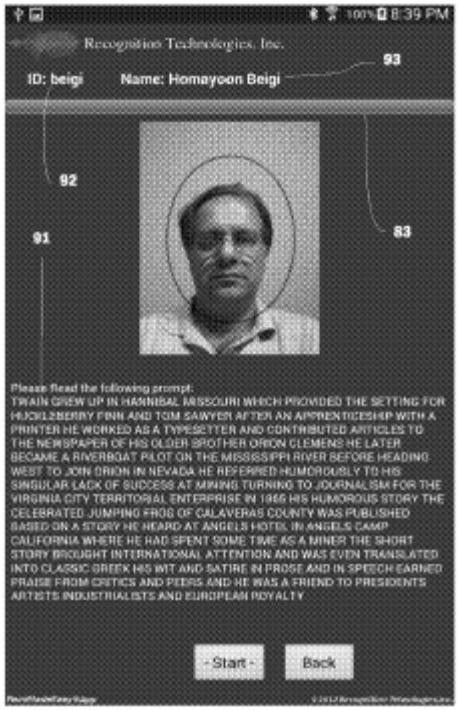


FIG. **25** Access Control – Enrollment Beginning

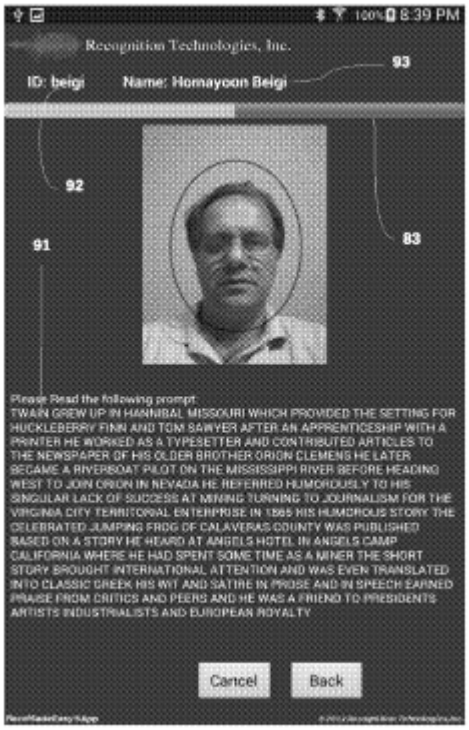


FIG. **26** Access Control – Enrollment Video Capture Progress

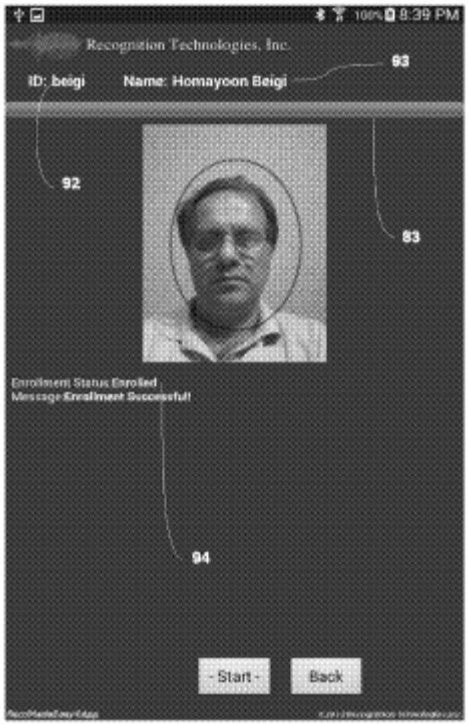


FIG. **27** Access Control – Enrollment Successful

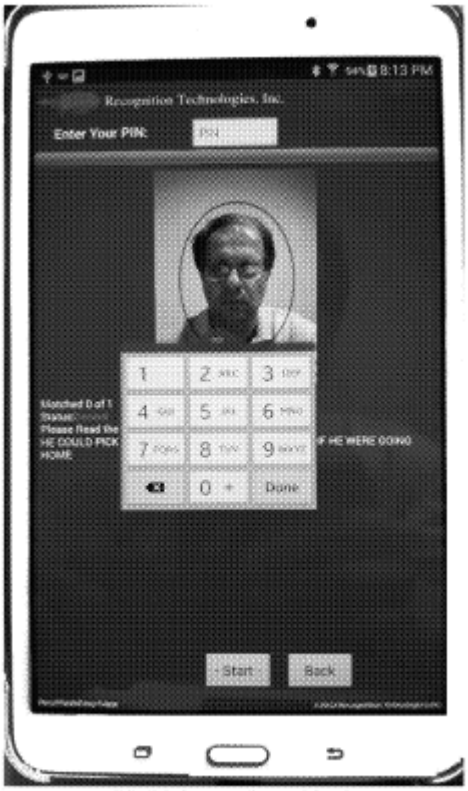


FIG. **29** Access Control Device

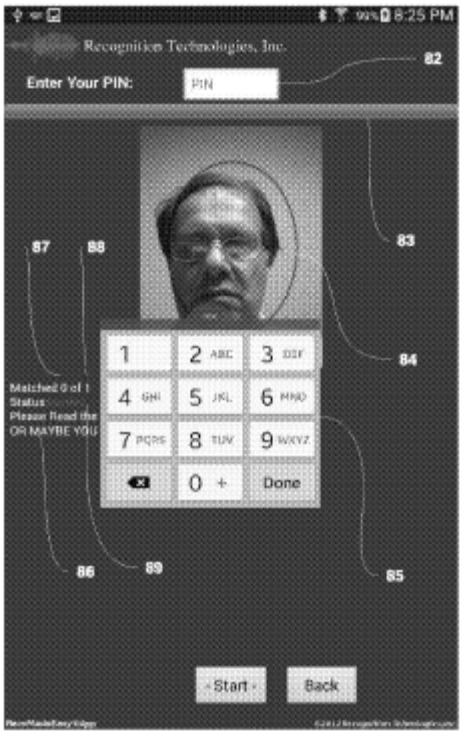


FIG. **30** Access Control PIN Entry

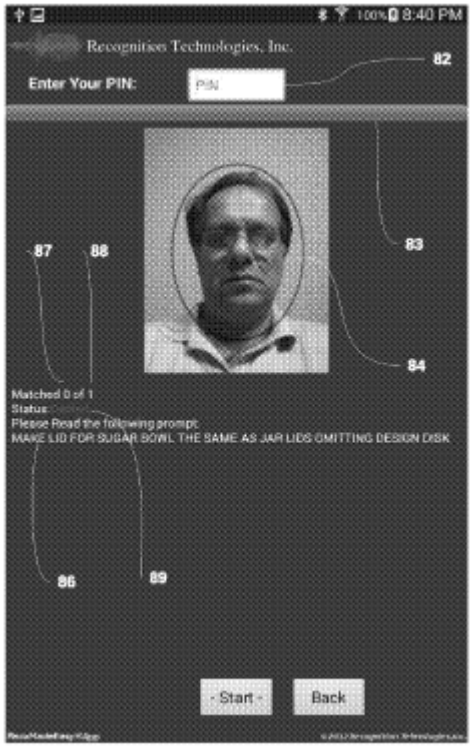


FIG. 32 Access Control Begin – Default Status: Denied

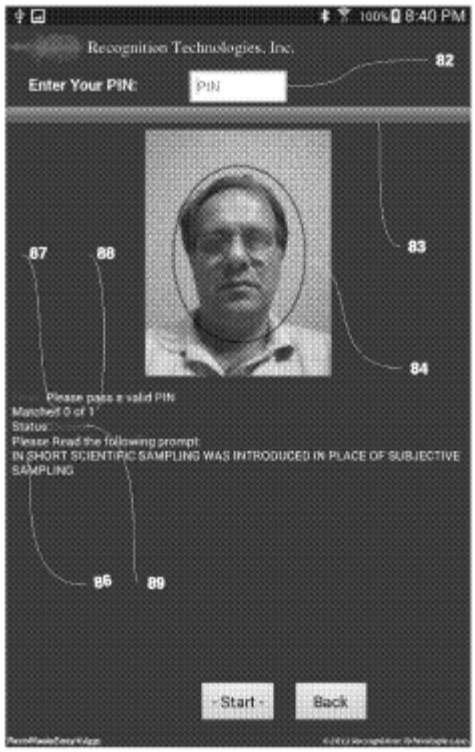


FIG. 33 Access Control – PIN Required

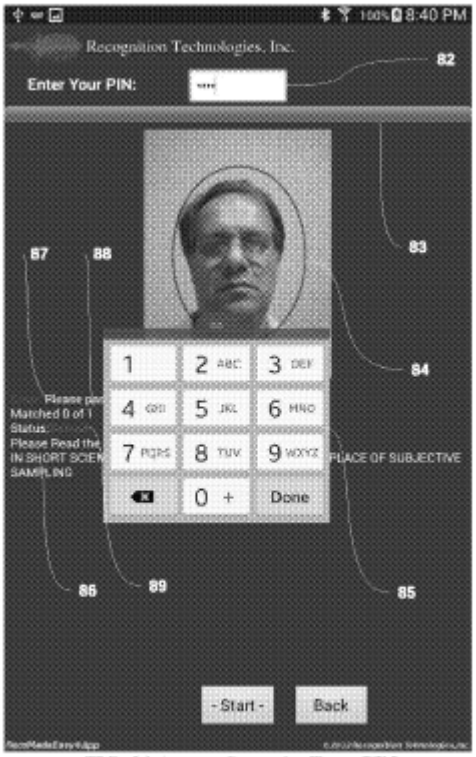


FIG. **34** Access Control – Enter PIN

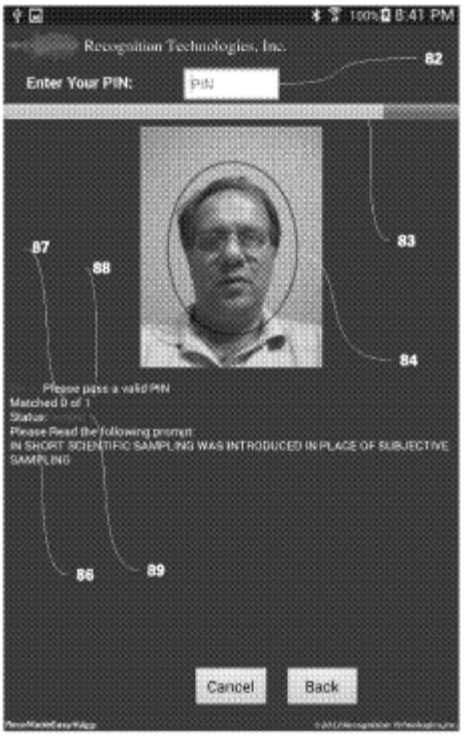


FIG. **35** Access Control – Video Capture Progress

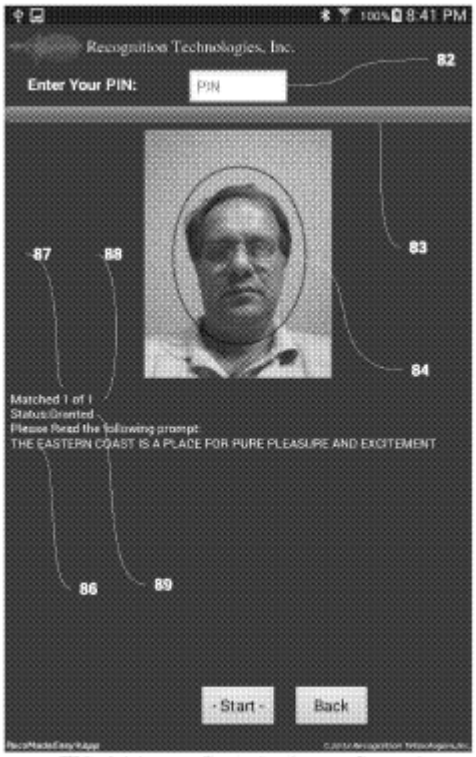


FIG. **36** Access Control – Access Granted

"FIG. 1 describes the process of registering the essential authentication data such as the digest (hash) of the subscriber ID, biometric models, and the binary code of the software being run with certificate authorities. This is the process that takes place once, either when the user has first activates the device or once for each new security level and access credential which is added." [4:25-31]

"Liveness Factor: As described in and Section, this may be a reaction to a random prompt. For example, this can be the reading of a displayed random prompt, a valid response to a displayed random question, a facial or hand gesture such as the blinking of a specific eye, a number of times, or the performance of a hand or body gesture such as the snapping of a finger, holding up a number of fingers with a requested orientation, the turning of the face in a special way instructed by the application, etc. Each liveness test is a mode of this factor type and one or more of them may be used." [16:61-67]

"1.2.1.1.3 Prompted Facial Gestures (Factors 3+4)

The face of the person is used as discussed above, in the form of a biometric (Section 1.3.4). However, the recognition system is capable of recognizing different facial gestures by using a standard description associated with each gesture. The system randomly prompts the user to perform different gestures. In this case, the point is to ensure liveness and that the system is not being supplied with a pre-recorded or artificially generated series of facial images." [18:16-24]

"1.3.1.2 Liveness Challenge

> It is important to make sure that the user of the device is not using a prerecorded message captured from the authorized user of the phone to spoof (see [6]) the speaker recognition engine. To do this, a challenge may be used that would test the liveness of the individual using the phone. Basically, these are some methods for doing such a liveness test.
>
> A phrase is prompted or a question is asked. The user responds to the question or repeats the phrase. The audio is used to do the verification.
>
> In this case, the response to the challenge may be combined with the phrase so that the content of the phrase being said may be decoded using a speech recognizer and the content may be matched against the expected the challenge response." [21:55-22:3]

28. A LIVENESS DETECTION METHOD FOR FACE RECOGNITION BASED ON OPTICAL FLOW FIELD ("BAO")

Bao (Wei Bao, Hong Li, Nan Li, and Wei Jiang, A liveness detection method for face recognition based on optical flow field, In Image Analysis and Signal Processing, 2009, IASP 2009, International Conference on, pages 233 –236, April 2009), discloses a liveness detection system that meets many of the limitations of the FaceTec Asserted Claims. Multiple images are taken ("sampling rate of 30 frames per second"), the images are analyzed ("[t]he system made a calculation every 10 frames and then produced a report"), and a calculation of the differences between two optical flow fields "D" is compared to a threshold "T" to determine liveness. One of the known "basic types" of motion represented by an optical flow field is "moving forward or backward". *See also Bao*, Fig. 1c.

29. FACE LIVENESS DETECTION USING VARIABLE FOCUSING ("KIM")

Kim (Sooyeon Kim, Sunjin Yu, Kwangtaek Kim, Yuseok Ban, Sangyoun Lee, Face liveness detection using variable focusing, Biometrics (ICB), 2013 International Conference on, On page(s): 1 – 6, 2013) discloses a face liveness detection system using variable focusing that meets many of the limitations of the FaceTec Asserted Claims. The system "utilizes the variation of pixel values by focusing between two images sequentially taken in different focuses." Kim notes the "obvious difference in focus values between real and fake faces when two sequential images (in/out-focus) are collected from each subject" and by focusing on facial components such as a nose and ears, "[i]n case of real faces, focused regions are clear and others are blurred due to depth

information." In addition, Kim notes that "in order to make high out-focusing effect, depth of field (DOF) should be narrow and one way to achieve that is "to decrease the distance between the camera and the subject."

30. Liveness Measurements Using Optical Flow for Biometric Person Authentication ("Smiatacz")

Smiatacz discloses a liveness detection method using optical flow and biometric information that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Smiatacz include:

> "Finally, the difference *D* between the linear model and the actual motion field is calculated with a simple formula. The higher the value of *D*, the larger the probability that the face is real, not fake."
> [Pg. 260]

> "We assumed that in order to verify the liveness, the user would have to rotate the head to the left, then to the right and once again to the left."
> [Pg. 261]

> "First, the video sequence is treated as a stack of consecutive frames. In a spatio-temporal image volume like this, the "vertical" axis corresponds to the moments of time. A moving point depicted in the image sequence will create a line inside this three-dimensional space. The orientation of the line can be expressed with the so-called orientation tensor **T.** …Finally a motion vector is determined for each small neighbourhood (Fig. 3)…. Each frame is converted to an 8-bit greyscale image in which the intensity of a pixel corresponds to the speed detected at the given point. These images are normalized in order to utilize the whole intensity range of 0..255. Finally a histogram equalization for each frame is performed and images are saved as regular bitmaps. Fig. 4 shows some examples."
> [Pg. 262]

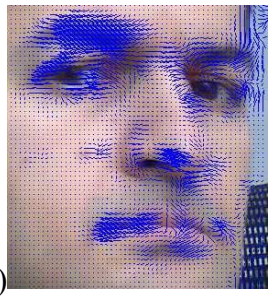
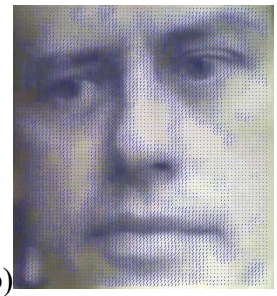
a)  b) 

Fig. 3. The examples of optical flow extracted by Farnebäck algorithm: a) live frame, b) fake frame.

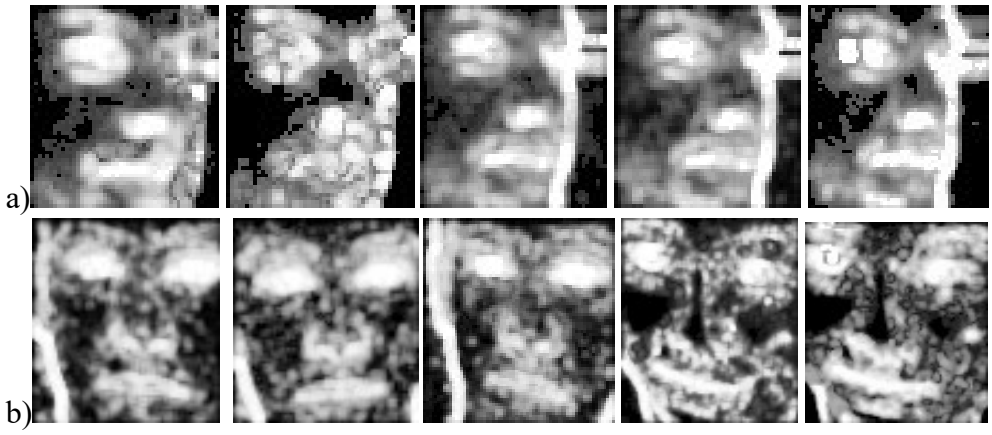


Fig. 4. The examples of "motion frames": a) live sequence, b) fake sequence.

"On the other hand, for each individual, one of the "live" sequences was used as a positive set during training. This setup simulated real-life conditions, in which the user would be requested to record only one live sequence during the registration."
[Pg. 266]

31. U.S. PATENT PUB. NO. US 2002/0113884 ("TANII")

Tanii discloses a digital photographing apparatus, image processing apparatus and recording medium Patent that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Tanii include:

"Where the main object 9 and the cellular phone 1 are located at a sufficient distance from each other when image capture is performed, as shown in FIG. 3A, a natural image can be obtained, as in the image shown in FIG. 3B. However, where the main object 9 and the cellular phone 1 are close together, as shown in FIG. 4A, an unnatural image results in which the perspective is exaggerated, as in the image shown in FIG. 4B."
[0047]

"It is believed that this unnatural image is caused because, where the center area of the main object protrudes toward the imaging portion 2 relative to the peripheral areas, i.e. where the main object has an essentially convex configuration that protrudes toward the imaging portion 2, when the main object and the imaging portion 2 come closer to each other, the peripheral surfaces of the main object become increasingly parallel to the line that connects the imaging portion 2 and the peripheral areas. More specifically, as shown in FIG. 5, the unnaturalness is believed to be caused in the image because the difference between the angle 01 formed between the light ray that strikes the lens unit 211 from a point 91 in a peripheral area of the main body 9 and the optical axis 211*a* of the lens unit 211, and the angle θ2 formed between the light ray that strikes the lens unit 211 from a point 92 located in front of the point 91 and the optical axis 211*a*, decreases as the lens unit 211 comes closer to the main object 9. In the following description, this unnaturalness of image will be referred as "warp' or "distortion'."
[0048]

Fig.3A

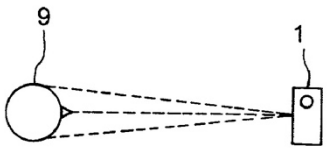
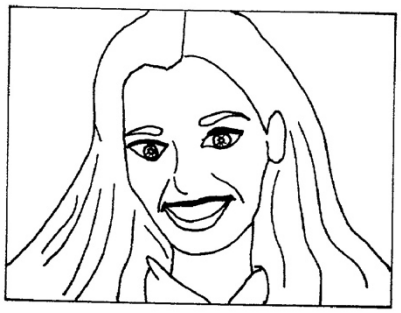


Fig.3B



[Figs. 3A–3B]

Fig.4A

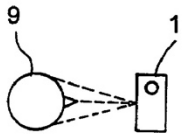
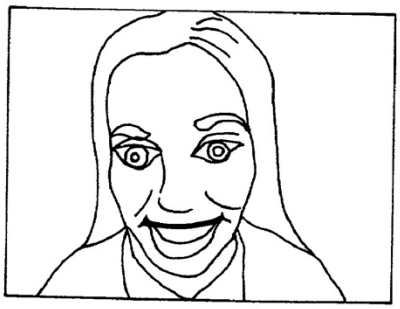


Fig.4B



[Figs. 4A–4B]

32. U.S. PATENT NO. US 8,437,513 ("DERAKHSHANI")

Derakhshani discloses a spoof detection technology for use in biometric authentication that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Derakhshani include:

> "This specification describes technologies relating to biometric authentication based on images of the eye. In general, one aspect of the subject matter described in this specification can be embodied in methods that include obtaining images of a subject including a view of an eye. The methods may further include determining a behavioral metric based on detected movement of the eye as the eye appears in a plurality of the images, determining a spatial metric based on a distance from a sensor to a landmark that appears in a plurality of the images each having a different respective focus distance, and determining a reflectance metric based on detected changes in surface glare or specular reflection patterns on a surface of the eye. The methods may further include determining a score based on the behavioral, spatial, and reflectance metrics and rejecting or accepting the one or more images based on the score."

[Abstract]

"This specification describes technologies relating to biometric authentication based on images of the eye. In general, one aspect of the subject matter described in this specification can be embodied in a method that includes obtaining two or more images of a subject including a view of an eye, wherein the images collectively include a plurality of focus distances."
[1:20-25]

"The method may further include rejecting or accepting the one or more images based on the score.

In general, one aspect of the subject matter described in this specification can be embodied in a system that includes a sensor configured to capture two or more images of a subject including a view of an eye, wherein the images collectively include a plurality of focus distances. The system may further include an illumination element provide photic stimuli in synchronization with the capture of one or more images by the sensor. The system may further include a means for determining a behavioral metric based on, at least, detected movement of the eye as the eye appears in a plurality of the images. The behavioral metric is a measure of deviation of detected movement and timing from expected movement of the eye. The system may further include a module configured to determine a spatial metric based on, at least, a distance from a sensor to a landmark that appears in a plurality of the images each having a different respective focus distance. The system may further include a module configured to determine a reflectance metric based on, at least, detected changes in surface glare or specular reflection patterns on a Surface of the eye as the eye appears in a plurality of the images, wherein the reflectance metric is a measure of changes in glare or specular reflection patches on the surface of the eye. The system may further include a module configured to determine a score based on, at least, the behavioral, spatial, and reflectance metrics. The system may further include an interface configured to reject or accept the one or more images based on the score.

In general, one aspect of the subject matter described in this specification can be embodied in a system that includes a data processing apparatus and a memory coupled to the data processing apparatus. The memory having instructions stored thereon which, when executed by the data processing apparatus cause the data processing apparatus to perform operations including obtaining two or more images of a subject including a view of an eye, wherein the images collectively include a plurality of focus distances. The operations may further include determining a behavioral metric based on, at least, detected movement of the eye as the eye appears in a plurality of the images. The behavioral metric may be a measure of deviation of detected movement and timing from expected movement of the eye. The operations may further include determining a spatial metric based on, at least, a distance from a sensor to a landmark that appears in a plurality of the images each having a different respective focus distance. The operations may further include determining a reflectance metric based on, at least, detected changes in surface glare or specular reflection patterns on a surface of the eye as the eye appears in a plurality of the images, wherein the reflectance metric is a measure of changes in glare or specular

reflection patches on the surface of the eye."
[1:42-2:25]

"In this example, a spatial metric is determined 714 based on a distance from a sensor to a landmark that appears in a plurality of the images each having a different respective focus distance. Focus distance is the distance from a sensor to a point in its field of view that is perfectly in focus. For some sensors, the focus distance may be adjusted for different images by adjusting a focus configuration setting for the sensor. For example, a landmark (e.g., an iris, an eye corner, a nose, an ear, or a background object) may be identified and located in the plurality of images with different focus distances. A landmark's representation in a particular image has a degree of focus that depends on how far the object corresponding to the landmark is from an in focus point in the field of view of the sensor. Degree of focus is a measure of the extent to the image of the landmark is blurred by optical effects in the light sensor (e.g., due to diffraction and convolution with the aperture shape). The degree of focus for a landmark in a particular image may be estimated by deter mining the high frequency components of the image signal in the vicinity of the landmark. When the landmark is in focus, more high frequency components in its vicinity are expected. When the degree of focus is low for a landmark, smaller high frequency components are expected. By comparing the degree of focus for a landmark in images with different focus distances, the distance from the sensor to the landmark may be estimated. In some implementations, distances from the sensor (e.g. a camera) for multiple landmarks are estimated to form a topological map (consisting of a set of three-dimensional landmark positions) of the subject in the view of the sensor. The positions of these landmarks in the space viewed by the camera may be compared to a model by determining a spatial metric (e.g., the mean square difference between the detected location of one or more landmarks and the corresponding modeled locations of the one or more landmarks) that reflects deviation from the model."
[16:44-17:11]

"In some implementations, the spatial metric is a measure of the deviation of the subject from a two-dimensional plane. One possible spoofing strategy is to present a two dimensional image (e.g., a photograph) of a registered user's eye to the sensor. However the locations of landmarks (e.g., an eye, nose, mouth, and ear) in the two dimensional image will occur in a two dimensional plane, unlike landmarks in and around a real live eye. For example, the locations of multiple landmarks may be fit to the closest two dimensional plane and the average distance of the landmarks from this fit plane can be determined as the spatial metric. A high value for this spatial metric may indicate a three-dimensional Subject and a higher likelihood that the subject is a live eye, while a low value may indicate a higher likelihood that the subject is a two-dimensional spoof attack."
[17:12-26]

"In some implementations, determining 714 the spatial metric comprises determining parallax of two or more landmarks that appear in a plurality of the images. Parallax is the apparent displacement of an observed object due to a change in the position of the observer. A plurality of images taken from different perspectives on the subject may result in landmarks within the images appearing to move by different amounts because of differences in their distance from the sensor. This parallax effect may be measured and used as a spatial metric that reflects the three-dimensional nature of a subject in the view of the sensor. If all the landmarks in the images undergo the same apparent displacement due to relative motion of the sensor, i.e., the difference in the parallax effect for the landmarks is small, then the subject viewed by the camera has higher likelihood of being a two-dimensional spoof attack. In some implementations, the sensor is moved about the subject during image capture to collect image data from different orientations relative to the subject. For example, a single camera may be rotated or slid slightly or multiple cameras at different positions may be used for image capture. In some implementations, a user is prompted to move in order to change the relative orientation of the subject and the sensor. In some implementations, it is

assumed that sensor will naturally move relative to the subject. For example, where the sensor is a camera in hand-held user device (e.g. a Smartphone or tablet) the sensor may naturally move relative to the users face due to involuntary haptic motion."
[17:45-18:4]

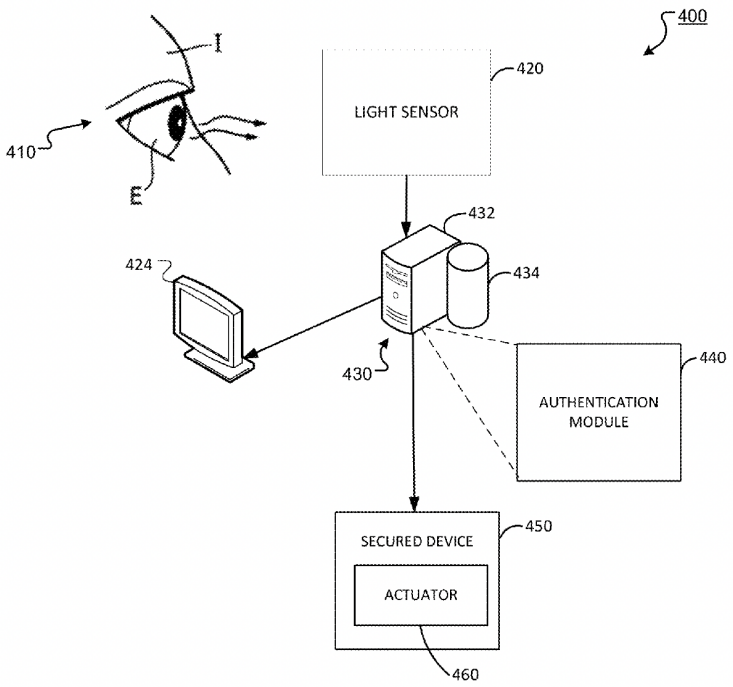


FIG. 4

[Fig. 4]

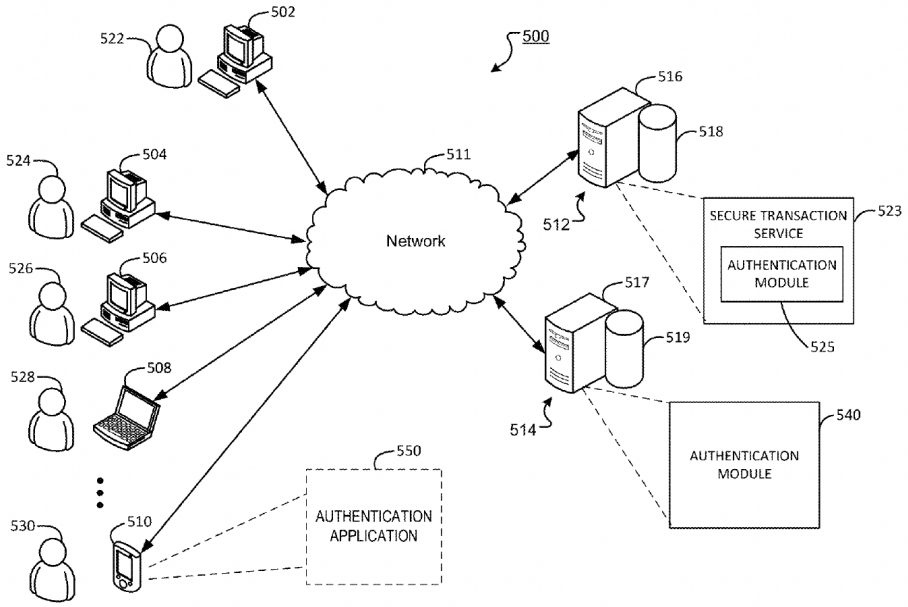


FIG. 5

[Fig. 5]

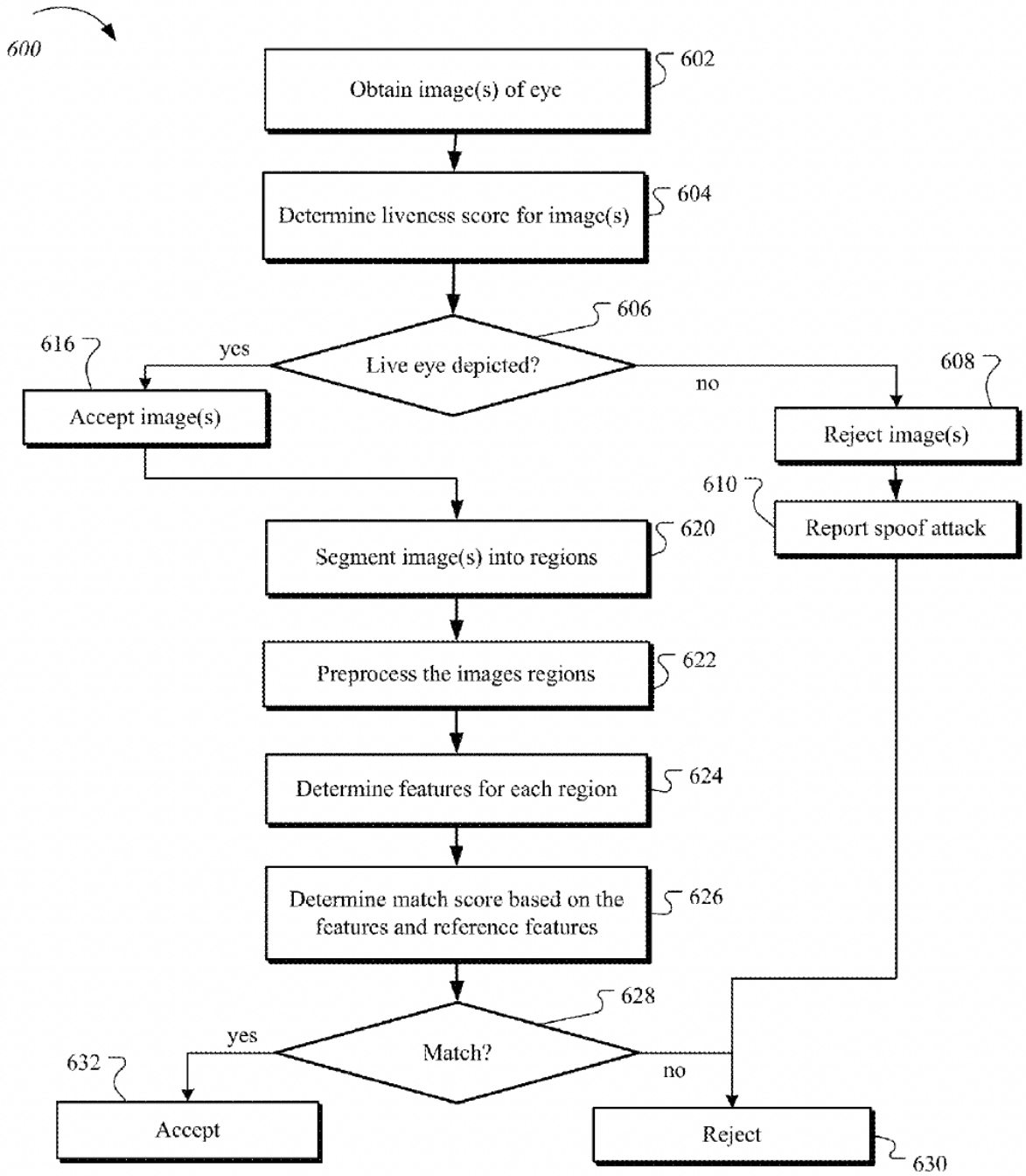

600
Obtain image(s) of eye
602
Determine liveness score for image(s)
604
Live eye depicted?
606
yes
no
616
Accept image(s)
608
Reject image(s)
610
Report spoof attack
Segment image(s) into regions
620
Preprocess the images regions
622
Determine features for each region
624
Determine match score based on the features and reference features
626
Match?
628
yes
no
632
Accept
Reject
630

Fig. 6

[Fig. 6]

33. U.S. PATENT PUB. NO. 2010/0014720 ("HOYOS")

Hoyos discloses a fraud resistant biometric financial transaction system and method that meets many of the limitations of the FaceTec Asserted Claims. The relevant portions of Hoyos include:

> "A preferred formula used in calculating a decision whether to authenticate a transaction is D=P(p)*(1+P(m)), where D is the decision probability, P(m) is the probability of a match with a range of 0 to 1, and P(p) is the probability the person is real and the biometric data is valid from 0 to 1. If the algorithm detects person is not live, and no match detected: D=0*(1+0)=0. If the algorithm detects strongly that the per son is live, and yet no match is detected: D=1*(1+0)=1. If the algorithm detects strongly that the person is live, and a very good match is detected: D=1*(1+1)-2. If the algorithm detects strongly that the person is live (or more specifically, that biometric data has been collected that can be used by a manual or automatic method after-the-fact to identify the person in prosecution for example), and a poor match is detected of 0.3: D=1*(1+0.3)=1.3 If the threshold is set at, for example, 1.2 for D, then essentially in the latter case, the transaction will be authorized even though the biometric match is not high. This is because the system determined that the biometric data collected can be used by a manual or automatic method after-the-fact to identify the person in prosecution for example. A higher transaction may be authorized if the value of D is higher. Many other functions of Pp and Pm can be used. We use the parallel result to authorize a transaction or access control or other permission, where rejection of a true customer has significant penalty Such as a loss of a customer. In the prior art, false rejects and true accepts are often addressed only in consideration of the biometric match performance, and the Substantial business consequences of a false reject is often not considered, and therefore few systems have been implemented practically."
> [0028]
>
> "In the prior art, only Pm has been involved in the decision metric. According to the present invention, Pp is combined so that for a given Pm, the decision criteria, D, is moved toward acceptance compared to when only Pm is involved if Pp is near 1, so that if the system has acquired good biometric data with sufficient quality for potential prosecution and manual or automatic biometric matching, then it is more likely to accept a match based on given biometric data used to calculate Pm, thereby moving the performance of a transaction system for authentic users from 98 percent to virtually 100 percent while still gathering data which can be used for prosecution or deterrent."
> [0031]
>
> "Referring first to FIG. 1, the overall process is to compute 11 the probability, Pp. of a live person being presented, compute 13 the probability of a biometric match, Pm, computing 14 D according to the aforementioned formula, wherein at decision block 15 if D exceeds a preset threshold, the transaction is authorized 17 or, if D does not exceed the preset threshold, the transaction is not authorized, 16.
>
> Referring now to FIG. 2, an example of a system and method of obtaining data used for calculating the probability of a live person 21 is shown. First, an image is displayed on a screen 23 with a black bar 24 on the right and a white area 25 on the left, and an image from a web-camera 26 that the person 21 looks at is recorded. A second image is displayed on

the screen (not shown), but this time the black bar is on the left and the white area is on the right and a second image from the web-camera 26 is recorded.

The difference between the two images is recorded and the difference at each pixel is squared. The images are then blurred by convolving with a low-pass filter and then threshold the image. Areas above threshold are areas of change between the two images. The system expects to see a change primarily on the cornea, where a sharp image of the screen is reflected.

Referring to FIGS.3 and 4 which represent cornea C with pupil P and section S1 at time T1 and S2 at timeT2, with I representing an iris, given the curved geometry of the cornea, for a live curved and reflective cornea, the black and white area should have a particular curved shape—specifically a curved black bar and a curved white area (much like a fish-eye lens view). A template of the expected view is correlated with the first image obtained on the web-camera only in the region of the eye as detected by the prior step), and the peak value of the correlation is detected. The process is then repeated with the template expected from the second image.

The minimum of the two correlation scores (which will lie between -1 to 1) is correlated and normalized it to be between 0 and 1 by adding 1 and dividing by 2. This is the probability of measure of liveness=P(p).

Using the method described in Turk, et al., U.S. Pat. No. 5,164,992, a face recognition match score, Pm, is calculated and then normalized to be between 0 and 1.

The system then computes D=(P(L)*(1+P(M))/2. If P(L) ranges from 0 to 1, and P(M) ranges from 0 to 1, then D ranges from 0 to 1. A threshold of 0.55 is set. If the value of D for a particular transaction/customer is above 0.55, then the transaction authenticated and allowed to proceed. If the value of D is less than or equal to 0.55, then authentication fails and the transaction is not allowed to proceed. If P(L)=0.95 (high) and P(M)=0.95 ((high), then D=0.95, which is well above the threshold—the transaction goes through as expected. If P(L) =0.95 (high), but P(M)=0.25 (poor), then D=0.6, and the transaction still goes through.

The present invention, therefore, is well adapted to carry out the objects and attain the ends and advantages mentioned, as well as others inherent therein. While the invention has been depicted and described and is defined by reference to particular preferred embodiments of the inven tion, such references do not imply a limitation on the invention, and no such limitation is to be inferred. The invention is capable of considerable modification, alteration and equivalents in form and function, as will occur to those ordinarily skilled in the pertinent arts. The depicted and described preferred embodiments of the invention are exemplary only and are not exhaustive of the scope of the invention. Consequently, the invention is intended to be limited only by the spirit and scope of the appended claims, giving full cognizance to equivalents in all respects."
[0033]-[0040]

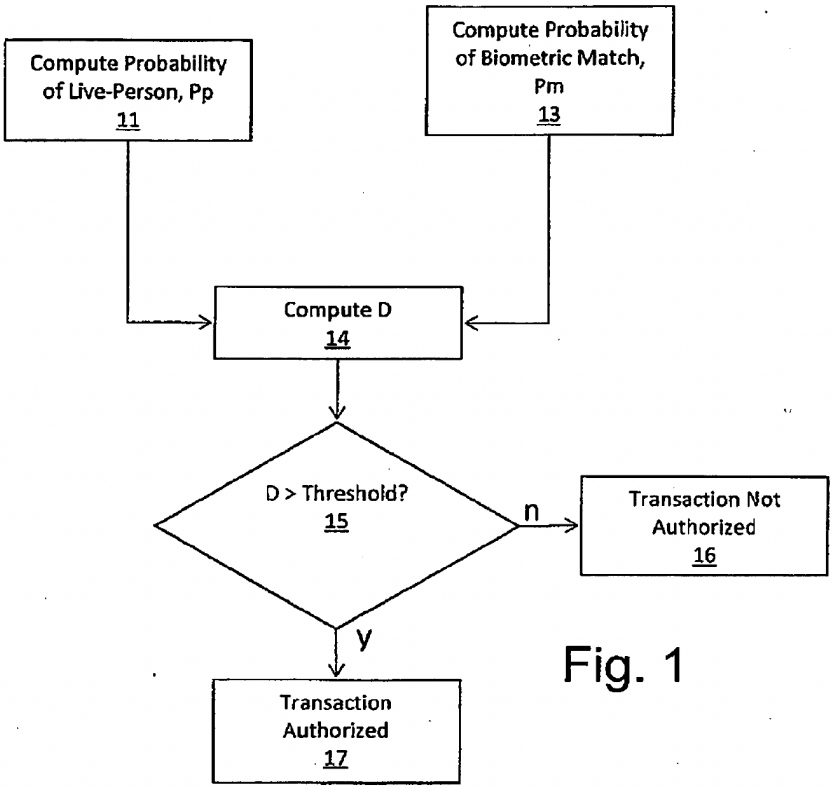
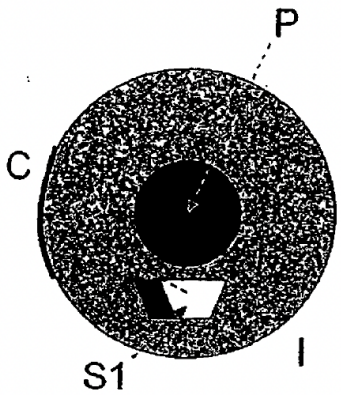


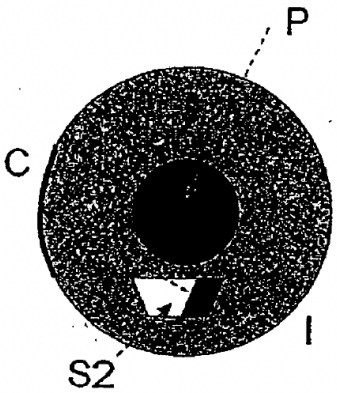
Fig. 1

[Fig. 1]



Time = T1

Fig. 3



Time = T2

Fig. 4

[Figs. 3–4]

Additionally, U.S. Patent No. 8,280,120 ("Hoyos '120"), e.g. at 7:22-32, further discloses aspects of the FaceTec Asserted Claims as described herein.

iii. STATE OF THE ART AND OBVIOUSNESS

The primary references identified above, as further described in the Exhibits, each discloses, either expressly or inherently, every element of the FaceTec Asserted Claims, thereby anticipating those claims. Additionally, each of the primary references alone (including in combination with the knowledge of a person of ordinary skill in the art) renders obvious the FaceTec Asserted Claims. To the extent Plaintiff contends that any primary reference does not anticipate or render obvious the FaceTec Asserted Claims as set forth above, it would have been obvious to combine or modify the primary references with concepts from other prior art, as explained throughout these Preliminary Invalidity Contentions. In particular, for each limitation of the FaceTec Asserted Claims that Plaintiff contends is not met by a particular primary reference, iProov contends that the limitation (and claim as a whole) would have been obvious based on a combination of that particular reference with one or more of (1) any other primary or secondary reference disclosing that limitation, (2) any reference identified in these Preliminary Invalidity Contentions as disclosing that limitation, (3) any statements made in the intrinsic record of the FaceTec Asserted Patents, and/or (4) the knowledge of one of ordinary skill in the art (as explained in additional detail below).

iProov does not yet have the benefit of Plaintiff's positions regarding the prior art, including what element(s), if any, Plaintiff contends are not disclosed by each prior art reference, whether Plaintiff contends that a reference is not in fact prior art, and whether Plaintiff contends that a person of ordinary skill in the art would not be motivated to combine specific references. iProov reserves the right to supplement these obviousness positions (including identifying additional prior art combinations and the associated reasons to combine) in view of such positions and/or as discovery in the case, including expert discovery, progresses.

The information discussed in the prior art raised in these Preliminary Invalidity Contentions forms the background knowledge of a person of ordinary skill in the art at the time the FaceTec Asserted Patents was filed and would have been used in determining whether and how to combine references to achieve the claimed invention(s), as discussed herein.[6] Indeed, the existence, nature,

[6] *See Randall Mfg. v. Rea*, 733 F.3d 1355, 1362 (Fed. Cir. 2013) (stating that "the knowledge [of a person of ordinary skill in the art] is part of the store of public knowledge that must be consulted when considering whether a claimed invention would have been obvious").

and content of each prior art reference, including the prior art references cited herein, provide further evidence regarding the knowledge of a person of ordinary skill in the art at the relevant time. iProov expressly reserves the right to rely on each of the prior art references, systems, concepts, and technologies discussed in these Preliminary Invalidity Contentions, including to demonstrate that a particular claim element was known at the time of the FaceTec Asserted Patents to a person of ordinary skill in the art, to show that the differences between a claimed invention and a prior art reference would have been obvious to a person of ordinary skill in the art, and to establish that a person of ordinary skill in the art would have been motivated to combine teachings of one or more references to achieve a claimed invention.

iv. MOTIVATIONS FOR MAKING COMBINATIONS OF PRIOR ART

iProov believes that no showing of a specific motivation to combine prior art is required to combine the references disclosed in the attached charts; there was a reason to make each combination, each combination of art would have produced no unexpected results, and each combination at most would simply represent a known alternative to one of ordinary skill in the art. *See KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 414–18 (2007) (rejecting the Federal Circuit's "rigid" application of the teaching, suggestion, or motivation to combine test instead espousing an "expansive and flexible" approach). Indeed, the Supreme Court held that a person of ordinary skill in the art is "a person of ordinary creativity, not an automaton" and "in many cases a person of ordinary skill in the art will be able to fit the teachings of multiple patents together like a pieces of a puzzle." *Id*. at 420–21.

Nevertheless, in addition to the information contained elsewhere in these contentions, iProov identifies additional motivations and reasons to combine the cited art. A person of ordinary skill in the art would have been motivated to combine the primary and additional prior art references as set forth above. Multiple teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references come from many sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, obvious to

try, the nature of the problem faced, and/or knowledge possessed by one of ordinary skill in the art.[7] In addition, the patentee admits in the intrinsic record, including the specification and prosecution history of the FaceTec Asserted Patents, that many of the claimed features were conventional and known in the art (as described in further detail below).

In general, a claimed invention is unpatentable if the differences between it and the prior art "are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art." 35 U.S.C. § 103(a); *Graham v. John Deere Co.*, 383 U.S. 1, 13–14 (1966). The ultimate determination of whether an invention is or is not obvious is a legal conclusion based on underlying factual inquiries including: "(1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences between the claimed invention and the prior art; and (4) objective evidence of nonobviousness." *Miles Labs., Inc. v. Shandon, Inc.*, 997 F.2d 870, 877 (Fed. Cir. 1993).

KSR International Co. v. Teleflex Inc., et al., 550 U.S. 398 (2007) ("*KSR*"), reaffirmed *Graham*, holding that a claimed invention can be obvious even if there is no teaching, suggestion, or motivation for combining the prior art to produce that invention. In determining whether a claim is obvious, "[o]ften, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *Id.* at 418. In determining whether a claim is obvious, "a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ." *Id.* When prior art elements are combined according to known methods to yield

[7] iProov reserves the right to present qualified expert testimony on any or all of these items as well as testimony of fact witnesses familiar with a prior art reference or the state of the art.

predictable results, the claimed invention is obvious. *Id.* at 417. In addition, "[o]ne of the ways in which a patent's subject matter can be proved obvious is by noting that there existed at the time of the invention a known problem for which there was an obvious solution encompassed by the patent's claims." *Id.* at 419–20. "Under the correct analysis, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id.* at 420.

Any suggested obviousness combinations set forth herein are in the alternative to iProov's anticipation contentions and are not to be construed to suggest that any reference included in any combination is not anticipatory in its own right or is not the basis for a single-reference obviousness defense. In particular, iProov is currently unaware of the extent, if any, to which Plaintiff will contend that certain limitations of the FaceTec Asserted Claims are not disclosed in the art identified by iProov as anticipatory. To the extent that an issue arises with respect to any such claim limitation, Defendant reserves the right to identify other references and combinations, which may make obvious the allegedly missing limitation in the disclosed system or method.

The rationale to combine or modify prior art references is significantly stronger when the references seek to solve the same problem, come from the same field, and correspond well. *In re Inland Steel Co.*, 265 F.3d 1354, 1362–64 (Fed. Cir. 2001).

In view of the Supreme Court's *KSR* decision, the PTO issued, and updated, a set of Examination Guidelines. *See* Examination Guidelines for Determining Obviousness Under 35 U.S.C. § 103 in view of the Supreme Court Decision in *KSR International Co. v. Teleflex, Inc.*, 72 Fed. Reg. 57,526 (October 10, 2007); Examination Guidelines Update: Development in the Obviousness Inquiry After *KSR v. Teleflex*, 75 Fed. Reg. 53643-60 (September 2010); *see also* MPEP § 2141 (https://www.uspto.gov/web/offices/pac/mpep/s2141.html) (accessed February 22, 2022). These Guidelines summarized the *KSR* decision and subsequent case law, as well as identified various rationales for finding a claim obvious, including those based on other precedents. Those rationales include:

(1) Combining prior art elements according to known methods to yield predictable results;

(2) Simple substitution of one known element for another to obtain predictable results;

(3) Use of known technique to improve similar devices (methods, or products) in the same way;

(4) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;

(5) "Obvious to try" – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;

(6) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; and

(7) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

iProov contends that one or more of these rationales apply in considering the obviousness of the FaceTec Asserted Claims.

To the extent that prior art identified by iProov as anticipatory are found not to anticipate the FaceTec Asserted Claims: (1) the prior art establishes that the claimed subject matter was obvious to a person of ordinary skill in the art at the time of the alleged invention; (2) the claims are nevertheless unpatentable because the FaceTec Asserted Claims contain nothing that goes beyond "ordinary innovation"; (3) no FaceTec Asserted Claim goes beyond combining known elements to achieve predictable results (particularly in the predictable art(s) of the FaceTec Asserted Patents) or does more than choose between clear alternatives known to those of skill in the art; and/or (4) the prior art renders the FaceTec Asserted Claims obvious either alone or in combination with each other or one or more of the other references identified in these Preliminary Invalidity Contentions.

v. STATE OF THE ART AND MOTIVATIONS TO COMBINE

The Exhibits to these Preliminary Invalidity Contentions illustrate the state of the art and the knowledge of a person of ordinary skill in the art at the relevant times with respect to specific

limitations, elements, or concepts either claimed in the FaceTec Asserted Patents or alleged to be claimed in the FaceTec Asserted Patents under Plaintiff's apparent view of the scope of the claims of the FaceTec Asserted Patents. To the extent it is asserted that a specific limitation or element discussed below is not found in a primary reference charted in one of the attached Exhibits, that missing limitation or element would have been well known to one of ordinary skill in the art, and a person of ordinary skill in the art would have been motivated to provide that missing limitation or element, based on his or her knowledge of the state of the art, as explained below and as shown in the other Exhibits. Specifically, a person of ordinary skill in the art would have been motivated to combine any of the primary references with any other primary reference(s) or any of the references discussed herein. The FaceTec Asserted Patents is nothing more than the combination of known prior art elements according to known methods to yield predictable results.

vi. SPECIFIC MOTIVATIONS

Motivation to make the proposed combinations of prior art references and knowledge of one skilled in the art generally exists within the references themselves as well as within the knowledge of one skilled in the art in the relevant time frame. Below are exemplary specific motivations to combine references.

As discussed in more detail below, it would have been obvious to combine known elements from the prior art references identified above, or use known techniques from the prior art references with other prior art references. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. Many of these prior art references cite to, rely upon, incorporate, or are described as part of other prior are references, and a person of ordinary skill in the art would have been motivated to look to these various references in solving known problems in the art. To the extent the aforementioned prior art references have the same prior art author(s) and/or assignees, a person of ordinary skill in the art would have been motivated to look at other publications or contributions from the same author(s) and/or assignees.

As shown in the attached Exhibits, and as discussed below, each of the references identified comes from the same field—*i.e.*, user enrollment/authentication/verification based on the analysis of images. The problems sought to be solved by the identified references and systems (e.g. liveness detection) were the same ones that had already been solved in the prior art. Indeed, the FaceTec Asserted Claims recite one of a finite number of known, available alternatives to solve these known problems. The FaceTec Asserted Claims simply combine previously known methods in a way that was explicitly and implicitly taught and suggested in the prior art. Implementing the teachings of the references identified herein would achieve the same desired result of the FaceTec patents, namely the goal of authenticating the liveness and authenticity of the user to reduce spoofing. A person of ordinary skill in the art would be motivated to use the known techniques in the prior art references discussed herein to achieve this known goal, including the known techniques of taking images, prompting users to take different images, collecting information from those images, analyzing that information from both a basic photography and human feature perspective, and then applying the results to make a determination about the user. One of ordinary skill in the art would be motivated to combine references that both minimized the burden on the user as well as increase the degree of success in identifying spoofs.

vii. GROUPS OF REFERENCES

In addition to combinations of references and motivations to combine identified elsewhere herein, including within claim charts, Defendant identifies combinations and motivations to combine based on references grouped by subject matter.

Furthermore, the particular cited disclosures for each prior art reference addressed in the numbered subsections within this section constitute additional charts identifying where specifically in each item of prior art each applicable element of each FaceTec Asserted Claim is found. The cited disclosures identified in this section are provided in addition to the citations set forth in the claim charts submitted separately herewith.

1. CAMERA-BASED 3D AUTHENTICATION

For example, one or more Asserted Independent Claims recite capturing images to authenticate the three-dimensionality of the user's face. Nothing about these claim limitations add

anything novel or non-obvious over the prior art. References and products with these features were well-known, routine, conventional, and widely available before the alleged invention.

Authenticating the three-dimensionality of users as recited in the claims would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use of authentication and security systems that take measures to prevent spoofing.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Ramaswamy, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(p), 606.1(p), 606.19(p), 938.1(p), and 910.10(p)
- Nechyba, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(p), 606.1(p), 606.19(p), 938.1(p), and 910.10(p)

- Ganong, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(p), 606.1(p), 606.19(p), 938.1(p), and 910.10(p)
- Zhang, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(p), 606.1(p), 606.19(p), 938.1(p), and 910.10(p)
- Park, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(p), 606.1(p), 606.19(p), 938.1(p), and 910.10(p)
- Frischholz, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(p), 606.1(p), 606.19(p), 938.1(p), and 910.10(p)
- Marsico, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(p), 606.1(p), 606.19(p), 938.1(p), and 910.10(p)
- Bud, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(p), 606.1(p), 606.19(p), 938.1(p), and 910.10(p)
- Ferren, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(p), 606.1(p), 606.19(p), 938.1(p), and 910.10(p)
- Hirose, *e.g.*, Abstract, Fig. 2A, Fig. 2B, [0015], [0018], [0033], [0060], [0077-0078], (describing capturing multiple images and providing them to the face recognition device for authentication)
- Derakhshani, *e.g.*, Abstract, Fig. 4, Fig. 5, Fig. 6, 1:42-48, 2:3-25, (describing using biometric data to authenticate a user and detect liveness)
- Ross, *e.g.*, Abstract, Fig. 3, 2:52-67, 4:40-45, 7:49-8:14 (disclosing authentication measures to prevent spoofing of an authenticated user's image)
- Negi, *e.g.*, Abstract, Fig. 1, Fig. 2, Fig. 5, Fig. 6, 2:9-23, (describing techniques for detecting spoofing detection in image based biometric authentication)
- Uchida, *e.g.*, Abstract, Fig. 1, Fig. 2, 1:32-40, 3:25-34, 6:7-15, (describing capturing images of user and using biometric data to detect liveness for authentication)
- Wang, *e.g.*, Abstract, Fig. 1, Fig. 2, Pg. 1, Pg. 2 (describing method of determining liveness based on 3D face structure across a sequence of images of a user)

- Chen, *e.g.*, Abstract, Fig. 2, Fig. 5, 2:8-44, 2:45-56, 3:64-4:12 (describing capturing a series of images to authenticate a user)
- Turgeman, *e.g.*, Abstract, Fig. 5, [0034], [0151-0152] (authenticating and verifying liveness of users)
- Langley, *e.g.*, Abstract, Fig. 1, Fig. 5, 3:45-56, 4:20-27. 7:3-16 (describing using biometric data for authentication and liveness detection)
- Evans, *e.g.*, Fig. 1, Fig. 3, Fig. 4, 2:19-25, (describing authenticating user using images and facial gestures)
- Sensharma, *e.g.*, Fig. 1, Fig. 3, Fig. 4, (using captured images from mobile device camera to authenticate users)
- Lau, *e.g.*, Fig. 6, Figs. 7-10, Abstract, 1:64-2:65 (comparing images taken by camera to authenticate users)
- Baldwin '622, *e.g.*, Fig. 1, Fig. 5, 1:62-2:9, 3:10-26 (describing process to verify live users and authenticate based on captured images and video)
- Horvitz, *e.g.*, Fig. 7, Abstract, 2:42-56, (describing a system to authenticate a user using captured images from a device's camera)
- Chaudhury, *e.g.*, Fig. 1A, Fig. 5, 1:5-15, 1:19-34, 4:37-47, 5:24-33, 17:31-33 (describing authentication and liveness detection based on facial movements)
- LeCun, *e.g.*, Fig. 2, [0013], [0023], [0036], [0048] (describing a method of biometric authentication with a device with a camera)

2. MULTIPLE IMAGES

For example, the Asserted Independent Claims each recite capturing at least two images to authenticate the three-dimensionality of the user's face. Nothing about these claim limitations add anything novel or non-obvious over the prior art. References and products with these features were well-known, routine, conventional, and widely available before the alleged invention.

The capturing and use of two images as recited in the claims would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple

substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use of authentication and security systems that take or capture multiple images.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Ramaswamy, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(a), 471.10(d) 606.1(a), and 606.1(c)
- Nechyba, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(a), 471.10(d) 606.1(a), and 606.1(c)
- Ganong, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(a), 471.10(d) 606.1(a), and 606.1(c)
- Zhang, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(a), 471.10(d) 606.1(a), and 606.1(c)

- Park, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(a), 471.10(d) 606.1(a), and 606.1(c)
- Frischholz, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(a), 471.10(d) 606.1(a), and 606.1(c)
- Marsico, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(a), 471.10(d) 606.1(a), and 606.1(c)
- Bud, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(a), 471.10(d) 606.1(a), and 606.1(c)
- Ferren, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(a), 471.10(d) 606.1(a), and 606.1(c)
- Hirose, *e.g.*, Abstract, Fig. 2A, Fig. 2B, [0015], [0018], [0033], [0060], [0077-0078], (describing capturing multiple images and providing them to the face recognition device for authentication)
- Derakhshani, *e.g.*, Fig. 4, Fig. 5, Fig. 6, 1:42-48, 2:3-25, (describing using biometric data to authenticate a user and detect liveness)
- Negi, *e.g.*, Fig. 5, 3:23-26, 3:57-63, 6:55-67 (describing capturing a sequence of images or multiple sequences of images for authentication)
- Uchida, *e.g.*, Fig. 2, 2:26-26, 3:25-34, 3:41-50 (describing capturing images of a user as they move their face to detect liveness)
- Wang, *e.g.*, Abstract, Fig. 1, Fig. 2, Pg. 1, Pg. 2 (describing method of determining liveness based on 3D face structure across a sequence of images of a user)
- Chen, *e.g.*, Abstract, Fig. 2, Fig. 3, Fig. 5, 2:8-44, 2:45-56, 3:64-4:12, 5:31-39, 5:49-56, 8:5-16 (describing capturing a series of images of a user's face from different positions to authenticate a user)
- Turgeman, *e.g.*, [0151-0152], [0156], [0164], [0202], [0205] (describing taking multiple images or a stream of images)
- Langley, *e.g.*, Fig. 4, 3:8-20, 11:1-20 (describing capturing a series of images for authentication)

- Evans, *e.g.*, 2:4-9 (using multiple images or multiple series of images to authenticate facial gestures)
- Sensharma, *e.g.*, 2:65-3:10 (capturing images from the front and rear-facing cameras)
- Lau, *e.g.*, Figs. 7-10, 1:64-67, (capturing multiple images of user when necessary for authentication)
- Baldwin '622, *e.g.*, Fig. 1, Fig. 5, 1:62-2:9 (describing process to verify live users and authenticate based on captured images and video)
- Horvitz, *e.g.*, Fig. 4, 2:42-56, 7:21-39, (describing a step of a method where dynamic images such as video are captured for authentication)
- Chaudhury, *e.g.*, Fig. 3A, Fig. 3B, Fig. 5, 1:19-34, 3:26-39, 6:42:55, 17:31-33 (describing capturing at least 2 images for authentication and liveness detection)
- LeCun, *e.g.*, Fig. 2, [0013], [0023], [0036], [0048] (describing capturing a series of pictures)
- Smiatacz, *e.g.,* Pg. 262 (Describing how the video is treated as multiple images for analysis)

3. BIOMETRIC DATA

For example, the Asserted Independent Claims each recite obtaining and using data and/or biometric data from images for security purposes. Nothing about these claim limitations add anything novel or non-obvious over the prior art. References and products with these features were well-known, routine, conventional, and widely available before the alleged invention.

Obtaining and using data (and specifically biometric data; and more specifically, biometric data including facial feature data[8]) from images for security purposes would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily

[8] *See e.g.,* '471 Patent claim 17.

appreciated the well-known and widespread use of authentication and security systems that use biometric data.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Ramaswamy, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(b), 471.10(e), 471.16, 606.1(b), 606.1(d), 606.19(a), and 606.19(b)
- Nechyba, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(b), 471.10(e), 471.16, 606.1(b), 606.1(d), 606.19(a), and 606.19(b)
- Ganong, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(b), 471.10(e), 471.16, 606.1(b), 606.1(d), 606.19(a), and 606.19(b)
- Zhang, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(b), 471.10(e), 471.16, 606.1(b), 606.1(d), 606.19(a), and 606.19(b)
- Park, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(b), 471.10(e), 471.16, 606.1(b), 606.1(d), 606.19(a), and 606.19(b)
- Frischholz, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(b), 471.10(e), 471.16, 606.1(b), 606.1(d), 606.19(a), and 606.19(b)

- Marsico, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(b), 471.10(e), 471.16, 606.1(b), 606.1(d), 606.19(a), and 606.19(b)
- Bud, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(b), 471.10(e), 471.16, 606.1(b), 606.1(d), 606.19(a), and 606.19(b)
- Ferren, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(b), 471.10(e), 471.16, 606.1(b), 606.1(d), 606.19(a), and 606.19(b)
- Hirose, *e.g.*, Abstract, Fig. 2A, Fig. 2B, [0016-0019], [0037-0039], [0041], and [0124-0130] (describing obtaining information about facial features to use in a comparison with a pre-registered identity profile)
- Derakhshani, *e.g.*, Abstract, Fig. 4, Fig. 5, Fig. 6
- Ross, *e.g.*, 4:14-39, 6:12-34, 7:49-8:14 (obtaining facial features for comparison and authentication purposes)
- Negi, 2:37-39, 4:41-49 (describing obtaining facial information to identify user)
- Uchida, *e.g.* Fig. 2, 3:41-50, 4:66-5:29 (describing obtaining facial information for authentication and liveness detection)
- Wang, *e.g.*, Abstract, Fig. 1, Fig. 2, Pg. 1, Pg. 2, Pg. 4, Pg. 6 (describing obtaining 3D face structure information for liveness determination)
- Chen, *e.g.*, Abstract, Fig. 2, Fig. 3, Fig. 5, 2:8-44, 2:62-65, 3:4-9, 3:64-4:12, 5:49-56 (describing measuring facial angles to authenticate a user)
- Landschaft, *e.g.*, Fig. 4, Fig. 5, [0010], [0026], [0030], [0040] (describing obtaining biometric information to authenticate a user)
- Turgeman, *e.g.*, [0045], [0151], (storing biometric data to identify users)
- Evans, *e.g.*, 2:19-25 (obtaining biometric data from sequences of capture images)
- Sensharma, *e.g.*, 2:65-3:10, 7:15-47 (gathering biometric data to identify a user, including pulse rate and facial recognition data)
- Langley, *e.g.*, Fig. 4, 2:18-30, 3:8-20, 6:30-50 (comparing biometric data against expected biometric data differences that are expected to result from the directed operation)

- Lau, *e.g.*, Fig. 6, 1:64-2:1 (extracting facial components from captured images for authentication)
- Baldwin '622, *e.g.*, Fig. 2(a), Fig. 2(b), 3:27-44 (describing extracting distinguishing features or facial features to compare to stored biometric data)
- Parry, *e.g.*, Figs. 2A-2H, 4:31-43 (describing uses of biometric data)
- Holz, *e.g.*, Fig. 1, Fig. 4A, Fig. 4D, 9:3-18, 17:28-58, 22:19-54 (disclosing an authentication method using biometric information of a user)

4. CHANGING CAMERA LOCATION

For example, claim 10 of the '471 Patent recites changing the position or distance of a camera device to authenticate the three-dimensionality of the user's face. Nothing about these claim limitations add anything novel or non-obvious over the prior art. References and products with these features were well-known, routine, conventional, and widely available before the alleged invention.

Changing the position or distance of a camera device as recited in the claims would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the application of a known technique to a known device ready for improvement to yield predictable results, and would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use of different camera positions, distances, and angles for taking the ideal photograph.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference

disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Ramaswamy, disclosed in the accompanying claim chart, for example, as set forth in element 471.10(c)
- Nechyba, disclosed in the accompanying claim chart, for example, as set forth in element 471.10(c)
- Ganong, disclosed in the accompanying claim chart, for example, as set forth in element 471.10(c)
- Zhang, disclosed in the accompanying claim chart, for example, as set forth in element 471.10(c)
- Park, disclosed in the accompanying claim chart, for example, as set forth in element 471.10(c)
- Frischholz, disclosed in the accompanying claim chart, for example, as set forth in element 471.10(c)
- Marsico, disclosed in the accompanying claim chart, for example, as set forth in element 471.10(c)
- Bud, disclosed in the accompanying claim chart, for example, as set forth in element 471.10(c)
- Ferren, disclosed in the accompanying claim chart, for example, as set forth in element 471.10(c)
- Hirose, *e.g.*, Abstract, Fig. 2A, Fig. 2B, Fig. 3, [0015], [0018], [0033], [0060], [0074], (describing using multiple camera positions and angles to capture a user's face)
- Negi, *e.g.,* 2:24-36, 7:1-8 (determining different distances between user and background objects as part of the authentication method)

- Wang, *e.g.*, Fig. 1, Fig. 2, Pg. 2, Pg. 6 (describing capturing a sequence of images of a user's face from different viewpoints either through a fixed camera/moving face or moving camera/fixed face)
- Chen, *e.g.*, Abstract, Fig. 2, Fig. 3, Fig. 5, 2:8-44, 2:45-56, 4:33-43, 5:23-30, 5:31-39 (describing capturing a user's face from different positions to authenticate a user)
- Turgeman, *e.g.*, [0157], [0163], [0173], [0205] (describing moving the mobile device and taking pictures from different angles)
- Tippett, *e.g.*, [0018], [0034], [0035] (movement of user's face and/or camera to capture gestures for authentication)
- Langley, *e.g.*, 9:55-10:8 (changing orientation of user's head and changing angle of camera when authenticating)
- Baldwin '622, *e.g.*, 2:38-46 (describing use of multiple cameras at different locations and angles for capturing images)
- Parry, *e.g.*, Figs. 7A-7C, 18:7-44 (describing moving camera/device and comparing images)
- Karakotsios, *e.g.*, Figs. 3-4(b), 2:3-16 (describing functionality to determine whether a user is facing a camera)
- Gokturk, *e.g.*, Fig. 1, 6:58-7:10, 7:11-35 (describing calculating position, orientation, and pose of face using optical flow computation between original image and a synthesized image)
- Horvitz, *e.g.*, Fig. 4, Fig. 5, 7:21-39, 9:12-31, 9:53-10:4 (describing capturing motion of user's head and different angles from which the image may be captured)
- Smiatacz, *e.g.,* Pg. 261 (Describing user/camera movement, such as head rotation, is required for liveness detection)

5. COMPARING IMAGES

For example, the Asserted Independent Claims each recite comparing multiple captured images to authenticate a user. Nothing about these claim limitations add anything novel or non-obvious over the prior art. References and products with these features were well-known, routine,

conventional, and widely available before the alleged invention. The concept that different distances between a person and a camera cause distortion, or perspective distortion, was also well known in the art.[9]

The comparison of two images as recited in the claims would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use of authentication and security systems that use image comparison based facial recognition.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

---

[9] *See, e.g.,* A Matter of Perspective, Cornicello Photography (May 8, 2007), https://cornicello.com/itfigures/focal-length-and-perspective; Nathan Yan, Assignment, Week 11: Perspective in Portraits, EECS 98/198 (2007), https://inst.eecs.berkeley.edu/~ee198-4/fa07/week11_assignment.shtml; Bill Wadman, Impact of Focal Length on Portraits, On Taking Pictures (Aug. 9, 2010), www.ontakingpictures.com/2010/08/impact_of_focal_length_on_port; Daniel Baker, Face Distortion Is Not Due To Lens Distortion, Daniel's Visionarium (May 5, 2012), https://bakerdh.wordpress.com/2012/05/05/face-distortion-is-not-due-to-lens-distortion; What Is Lens Distortion And How To Correct It, Discover Digital Photography (Mar. 6, 2013), https://www.discoverdigitalphotography.com/2013/what-is-lens-distortion-and-how-to-correct-it.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Ramaswamy, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(f), 606.1(e), 606.1(f), 609.19(c), and 606.19(d)
- Nechyba, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(f), 606.1(e), 606.1(f), 606.19(c), and 606.19(d)
- Ganong, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(f), 606.1(e), 606.1(f), 606.19(c), and 606.19(d)
- Zhang, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(f), 606.1(e), 606.1(f), 606.19(c), and 606.19(d)
- Park, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(f), 606.1(e), 606.1(f), 606.19(c), and 606.19(d)
- Frischholz, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(f), 606.1(e), 606.1(f), 606.19(c), and 606.19(d)
- Marsico, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(f), 606.1(e), 606.1(f), 606.19(c), and 606.19(d)
- Bud, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(f), 606.1(e), 606.1(f), 606.19(c), and 606.19(d)
- Ferren, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(f), 606.1(e), 606.1(f), 606.19(c), and 606.19(d)
- Hirose, *e.g.*, Abstract, Fig. 2A, Fig. 2B, Fig. 4, [0016-0019], [0037-0039], [0041], and [0124-0130] (describing obtaining information about facial features to use in a comparison with a pre-registered identity profile)
- Ross, *e.g.*, Fig. 3, 4:14-39, 6:34-58, 8:23-38 (describing comparing a captured image with an enrollment image)
- Uchida, *e.g.*, Fig. 2, 1:32-40, 4:66-5:29 (describing comparing biometric features between captured image and a registered face image)

- Wang, *e.g.*, Abstract, Fig. 1, Fig. 2, Pg. 1, Pg. 2, Pg. 4, Pg. 6 (describing comparing face structure across images for liveness determination)
- Chen, *e.g.*, Abstract, Fig. 2, Fig. 3, Fig. 5, 2:8-44, 2:45-56, 3:64-4:12, 5:23-30, 5:31-39, 5:57-59, 12:9-16 (describing comparing a user's face from different positions to authenticate a user)
- Turgeman, *e.g.*, [0151-0152], [0156], [0205] (describing comparing sequences of images to determine liveness)
- Evans, *e.g.*, 5:33-38 (comparing each facial gesture from the sequence of facial gestures to a corresponding baseline representation of the facial gesture)
- Sensharma, *e.g.*, 7:15-47 (capturing biometric information and facial features to compare to an authenticated user profile)
- Langley, *e.g.,* Fig. 5, 7:3-16, 11:1-20 (comparing expected differences in images)
- Lau, *e.g.*, Fig. 6, Figs. 7-10, Abstract, 1:64-2:65 (comparing images taken by camera to authenticate users)
- Baldwin '622, *e.g.*, 3:27-44 (describing comparison of facial features or distinguishing points to stored information or images for facial recognition)
- Parry, *e.g.*, Figs. 7A-7C, 18:7-44 (describing moving camera/device and comparing images)
- Gokturk, *e.g.*, Fig. 1, 6:58-7:10, 7:11-35 (describing calculating position, orientation, and pose of face using optical flow computation between original image and a synthesized image)
- Chaudhury, *e.g.*, Fig. 5, 1:19-34, 5:24-33, 5:56-66 (describing comparing captured images with enrollment images)
- Kollreider, *e.g.*, Fig. 1, Fig. 2, Fig. 8, Abstract, Pg. 1, Pg. 2, Pg. 4, Pg. 5, Pg. 7-8 (describing the use of optical flow to compare image measurements with expected differences)
- LeCun, *e.g.*, Fig. 2, [0033], [0036], [0048] (describing comparing pictures taken with previously validated user models for authentication and for 3-D detection)

- Takahashi, *e.g.*, Fig. 5, 1:19-32, 3:15-20 (describing an authentication method that compares biometric information with registered information)
- Bao (disclosing that multiple images are taken ("sampling rate of 30 frames per second"), the images are analyzed ("[t]he system made a calculation every 10 frames and then produced a report"), and a calculation of the differences between two optical flow fields "D" is compared to a threshold "T" to determine liveness. One of the known "basic types" of motion represented by an optical flow field is "moving forward or backward". *See* Fig. 1c.)
- Kim (disclosing a system that "utilizes the variation of pixel values by focusing between two images sequentially taken in different focuses." Kim notes the "obvious difference in focus values between real and fake faces when two sequential images (in/out-focus) are collected from each subject" and by focusing on facial components such as a nose and ears, "[i]n case of real faces, focused regions are clear and others are blurred due to depth information." In addition, Kim notes that "in order to make high out-focusing effect, depth of field (DOF) should be narrow and one way to achieve that is "to decrease the distance between the camera and the subject.")
- Smiatacz, *e.g.,* Pg. 260 (Describing how a numerical calculation outputs a difference variable between the linear model and the actual motion field generated of the user)

6. AUTHENTICATION BASED ON IMAGE DIFFERENCES

For example, the Asserted Independent Claims each recite authenticating or verifying a user based on expected differences between multiple captured images. Nothing about these claim limitations add anything novel or non-obvious over the prior art. The comparison of expected distortion or expected differences to help authenticate a user was well-known, routine, conventional, and widely available before the alleged invention, often by over a decade. The concept that different distances between a person and a camera cause distortion, or perspective

distortion, was also well known in the art.[10] References and products with these features were well-known, routine, conventional, and widely available before the alleged invention.

The capturing of two images and authenticating based on expected differences as recited in the claims would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use of authentication and security systems that use expected or predicted differences in images.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

---

[10] *See, e.g.,* A Matter of Perspective, Cornicello Photography (May 8, 2007), https://cornicello.com/itfigures/focal-length-and-perspective; Nathan Yan, Assignment, Week 11: Perspective in Portraits, EECS 98/198 (2007), https://inst.eecs.berkeley.edu/~ee198-4/fa07/week11_assignment.shtml; Bill Wadman, Impact of Focal Length on Portraits, On Taking Pictures (Aug. 9, 2010), www.ontakingpictures.com/2010/08/impact_of_focal_length_on_port; Daniel Baker, Face Distortion Is Not Due To Lens Distortion, Daniel's Visionarium (May 5, 2012), https://bakerdh.wordpress.com/2012/05/05/face-distortion-is-not-due-to-lens-distortion; What Is Lens Distortion And How To Correct It, Discover Digital Photography (Mar. 6, 2013), https://www.discoverdigitalphotography.com/2013/what-is-lens-distortion-and-how-to-correct-it.

Furthermore, certain claims also recite determining that the user does not exhibit three-dimensional shape, *see e.g.,* '938 Patent claim 1(d). The step of determining whether a user exhibits three-dimensional features as recited by the claims is a binary operation; thus, any reference that determines whether a user exhibits three-dimensional features for authentication (from the processing of the two images) inherently also determines when the user does not exhibit three-dimensional features.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Ramaswamy, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(g), 606.1(g), 606.1(g)(i), 606.1(g)(ii), 606.19(e), 606.19(e)(i), and 606.19(e)(ii)
- Nechyba, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(g), 606.1(g), 606.1(g)(i), 606.1(g)(ii), 606.19(e), 606.19(e)(i), and 606.19(e)(ii)
- Ganong, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(g), 606.1(g), 606.1(g)(i), 606.1(g)(ii), 606.19(e), 606.19(e)(i), and 606.19(e)(ii)
- Zhang, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(g), 606.1(g), 606.1(g)(i), 606.1(g)(ii), 606.19(e), 606.19(e)(i), and 606.19(e)(ii)
- Park, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(g), 606.1(g), 606.1(g)(i), 606.1(g)(ii), 606.19(e), 606.19(e)(i), and 606.19(e)(ii)
- Frischholz, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(g), 606.1(g), 606.1(g)(i), 606.1(g)(ii), 606.19(e), 606.19(e)(i), and 606.19(e)(ii)
- Marsico, disclosed in the accompanying claim charts, for example, set forth in elements 471.10(g), 606.1(g), 606.1(g)(i), 606.1(g)(ii), 606.19(e), 606.19(e)(i), and 606.19(e)(ii)
- Bud, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(g), 606.1(g), 606.1(g)(i), 606.1(g)(ii), 606.19(e), 606.19(e)(i), and 606.19(e)(ii)

- Ferren, as disclosed in the accompanying claim charts, for example, set forth in elements 471.10(g), 606.1(g), 606.1(g)(i), 606.1(g)(ii), 606.19(e), 606.19(e)(i), and 606.19(e)(ii)
- Hirose, *e.g.*, Abstract, Fig. 2A, Fig. 2B, Fig. 4, [0016-0019], [0037-0039], [0041], and [0124-0130] (describing obtaining information about facial features to use in a comparison with a pre-registered identity profile)
- Ross, *e.g.*, 6:34-58, 8:23-38 (describing method of comparing different distances between facial features to verify authentication)
- Negi, 2:60-3:22, 3:30-43, 7:31-54 (determines whether there is a potential spoofing attack based on comparison of distances and position of features)
- Uchida, *e.g.*, Fig. 1, Fig. 2, 1:32-40, 3:41-50, 3:56-60 (describing authenticating a user based on liveness determination and a comparison with pre-registered image)
- Chen, *e.g.*, Abstract, Fig. 2, Fig. 3, Fig. 5, 2:28-44, 3:64-4:12, 4:33-43, 5:57-59 (describing method of authenticating a user based on facial angles across a sequence of images)
- Turgeman, *e.g.*, [0157], [0163], [0205] (describing authenticating users if there is differences between frames)
- Evans, *e.g.*, 5:33-58 (comparing similarity of facial gestures to stored baseline gestures and expected difference of head position)
- Langley, *e.g.*, Fig. 4, Fig. 5, 2:18-30, 3:8-20, 6:51-63, 7:3-16, 11:1-20 (comparing illumination characteristics of biometric data against illumination characteristics that are expected to result from the directed operation)
- Baldwin '622, *e.g.*, 4:4-25 (verifying that a live user is attempting to access device by comparing and tracking expected changes in color and pulse over a short period of time)
- Gokturk, *e.g.*, Fig. 2, Fig. 6, 2:47-59 (performs facial recognition by calculating expected location of features and comparing to the actual image)
- Gokturk, *e.g.*, Fig. 1, 6:58-7:10, 7:11-35 (describing calculating position, orientation, and pose of face using optical flow computation between original image and a synthesized image)

- Chaudhury, *e.g.*, Fig. 1A, Fig. 3A, Fig. 3B, Fig. 5, 1:19-34, 3:26-39, 5:56-66, 6:42-55, 16:59-63 (describing authentication and liveness detection based on eye movements across images)
- LeCun, *e.g.*, Fig. 2, [0033], [0036] (describing comparing pictures taken with previously validated user models)
- Kollreider, *e.g.*, Fig. 1, Fig. 2, Fig. 8, Abstract, Pg. 1, Pg. 2, Pg. 4, Pg. 5, Pg. 7-8 (describing the use of optical flow to compare image measurements with expected differences)
- Bao (disclosing that multiple images are taken ("sampling rate of 30 frames per second"), the images are analyzed ("[t]he system made a calculation every 10 frames and then produced a report"), and a calculation of the differences between two optical flow fields "D" is compared to a threshold "T" to determine liveness. One of the known "basic types" of motion represented by an optical flow field is "moving forward or backward". *See* Fig. 1c.)
- Kim (disclosing a system that "utilizes the variation of pixel values by focusing between two images sequentially taken in different focuses." Kim notes the "obvious difference in focus values between real and fake faces when two sequential images (in/out-focus) are collected from each subject" and by focusing on facial components such as a nose and ears, "[i]n case of real faces, focused regions are clear and others are blurred due to depth information." In addition, Kim notes that "in order to make high out-focusing effect, depth of field (DOF) should be narrow and one way to achieve that is "to decrease the distance between the camera and the subject.")

7. USER PROMPTS

For example, the Asserted Independent Claims each recite displaying user prompts directing a user. Nothing about these claim limitations add anything novel or non-obvious over the prior art. References and products with these features were well-known, routine, conventional, and widely available before the alleged invention.

The use of prompts to direct a user would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use of authentication and security systems that take or capture multiple images.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Ramaswamy, as disclosed in the accompanying claim charts, for example, set forth in elements 471.13 and 606.4
- Nechyba, as disclosed in the accompanying claim charts, for example, set forth in elements 471.13 and 606.4
- Ganong, as disclosed in the accompanying claim charts, for example, set forth in elements 471.13 and 606.4

- Zhang, as disclosed in the accompanying claim charts, for example, set forth in elements 471.13 and 606.4
- Park, as disclosed in the accompanying claim charts, for example, set forth in elements 471.13 and 606.4
- Frischholz, as disclosed in the accompanying claim charts, for example, set forth in elements 471.13 and 606.4
- Marsico, disclosed in the accompanying claim charts, for example, set forth in elements 471.13 and 606.4
- Bud, as disclosed in the accompanying claim charts, for example, set forth in elements 471.13 and 606.4
- Ferren, as disclosed in the accompanying claim charts, for example, set forth in elements 471.13 and 606.4
- Uchida, *e.g.*, Fig. 2, 6:7-15 (describing the display of instructions to make the user move their face in front of the camera)
- Chen, *e.g.*, Abstract, Fig. 2, Fig. 3, 2:28-44, 2:62-65, 3:64-4:12, 5:23-30 (describing instructions displayed on a smartphone requiring users to move the device)
- Turgeman, *e.g.*, [0157], [0164] (prompting user to take a self image)
- Evans, *e.g.*, 2:4-9, 3:23-32, 4:4-18, 7:60-8:3 (use of user prompts to capture images)
- Tippett, *e.g.*, Fig. 5A, Fig. 5B, Fig. 5C, [0042] (providing user with a prompt to input a facial gesture)
- Langley, *e.g.*, 6:51-63 (prompting user to perform illumination function and/or other instructions)
- Holz, *e.g.*, Fig. 4A, Fig. 4D, 22:19-54 (disclosing an authentication method involving prompting a user to perform certain actions such as turning head)
- Chaudhury, *e.g.*, Fig. 1A, Fig. 3A, Fig. 3B, Fig. 5, 1:19-34, 7:53-58, 16:59-63 (describing user prompts as images are captured)
- LeCun, *e.g.*, Fig. 2, [0048] (describing prompts to user to capture images)

- Ricci, *e.g.*, Fig. 28, Fig. 29, [0830-0835], [0838] (vehicle provides users with a facial recognition prompt that requires users to align head with the oval on the screen)
- Wilson, *e.g.*, Figure 2, pg. 3, pg. 4 (discussing proper facial alignment and smartphone prompts to unlock smartphones)
- Beigi, *e.g.*, Fig. 1, Figs. 16-19, Fig. 22, Figs. 25-27, Fig. 29, Fig. 30, Figs. 32-36, 4:25-31, 16:61-67, 18:16-24, 21:55-22:3 (providing prompts for user to perform an action or speak a phrase that includes an oval shaped authentication prompt on the device's screen)
- Smiatacz, *e.g.,* Pg. 266 (Experiments of the system resembled real-life conditions where the user would be requested to record a live sequence)

8. OVAL PROMPTS

For example, claim 5 of the '606 Patent, claim 14 of the '471 Patent, and claim 14 of the '910 Patent each recite using prompts that contain an oval shape with which the user aligns his/her face. Nothing about these claim limitations add anything novel or non-obvious over the prior art. References and products with oval shaped prompts were well-known, routine, conventional, and widely available before the alleged invention.

The use of oval prompts recited in the claims would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use of authentication and security systems that take or prompt users for multiple images.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to

combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Ganong, as disclosed in the accompanying claim charts, for example, set forth in elements 938.11, and 910.14.
- Bud, as disclosed in the accompanying claim charts, for example, set forth in elements 938.11, and 910.14.
- Ricci, *e.g.*, Fig. 28, Fig. 29, [0830-0835], [0838] (vehicle provides users with a facial recognition prompt that requires users to align head with the oval on the screen)
- Wilson, *e.g.*, Figure 2, pg. 3, pg. 4 (discussing proper facial alignment and smartphone prompts to unlock smartphones)
- Beigi, *e.g.*, Fig. 1, Figs. 16-19, Fig. 22, Figs. 25-27, Fig. 29, Fig. 30, Figs. 32-36, 4:25-31, 16:61-67, 18:16-24, 21:55-22:3 (providing prompts for user to perform an action or speak a phrase that includes an oval shaped authentication prompt on the device's screen)

9. HAND-HELD DEVICES

For example, claim 6 of the '606 Patent and Claim 15 of the '471 Patent each recite the use of a hand-held device. Nothing about these claim limitations add anything novel or non-obvious over the prior art. To the contrary, using authentication and security methods that work on hand-held devices was routine, conventional, and widely available before the alleged invention.

The use of a hand-held device as recited in the claims would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use and disclosure of hand-held systems and devices that practice and/or embody the described features and/or functionality of a biometric authentication, and the associated benefits and advantages of its use.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Ramaswamy, as disclosed in the accompanying claim charts, for example, set forth in elements 471.15 and 606.6
- Nechyba, as disclosed in the accompanying claim charts, for example, set forth in elements 471.15 and 606.6

- Ganong, as disclosed in the accompanying claim charts, for example, set forth in elements 471.15 and 606.6
- Zhang, as disclosed in the accompanying claim charts, for example, set forth in elements 471.15 and 606.6
- Park, as disclosed in the accompanying claim charts, for example, set forth in elements 471.15 and 606.6
- Frischholz, as disclosed in the accompanying claim charts, for example, set forth in elements 471.15 and 606.6
- Marsico, disclosed in the accompanying claim charts, for example, set forth in elements 471.15 and 606.6
- Bud, as disclosed in the accompanying claim charts, for example, set forth in elements 471.15 and 606.6
- Ferren, disclosed in the accompanying claim charts, for example, set forth in elements 471.15 and 606.6
- Ross, *e.g.*, 4:53-56 (discloses an embodiment of the invention being used on a smartphone)
- Uchida, *e.g.*, 1:7-9, 7:6-13 (disclosing that the invention may be used on a mobile phone)
- Chen, *e.g.*, Abstract, Fig. 2, Fig. 3, Fig. 5, 1:24-31, 2:28-44, 3:64-4:12, 4:33-43, 14:10-16 (disclosing an authentication method that may be implemented on a smartphone)
- Landschaft, *e.g.*, Fig. 2, Fig. 3, Fig. 4, Fig. 5, [0001], [0010], [0026], [0030], [0039], [0040] (disclosing an authentication method on a handheld electronic device such as mobile phone)
- Turgeman, *e.g.*, [0047], [0070], [0160] (describing use of mobile devices)
- Evans, *e.g.*, 3:33-49 (describing use of mobile devices)
- Sensharma, *e.g.*, 8:40-51 (using mobile devices including cell phones, PDAs, and tablets)

- Langley, *e.g.*, Fig. 1, 3:45-56, 4:20-27 (the remote authentication device is a smartphone)
- Lau, *e.g.*, 8:25-39 (use of a mobile device to implement the disclosed method)
- Parry, *e.g.*, 4:58-5:1 (describing use of computer, laptop, or server to perform authentication)
- Horvitz, *e.g.*, Fig. 2, 2:57-3:2 (portraying an exemplary hand held device)
- Holz, *e.g.*, Fig. 1, Fig. 4A, Fig. 4D, 7:31-42, 9:36-51 (disclosing an authentication method that may be implemented on mobile devices)
- Chaudhury, *e.g.*, Fig. 1A, Fig. 3A, Fig. 3B, Fig. 5, 4:37-47 (describing authentication and liveness detection method that may be implemented on a handheld device)
- LeCun, *e.g.*, Fig. 2, Fig. 3, [0007], [0013], [0023] (describing authentication method that can be implemented on mobile devices and smartphones)

10. MOVEMENT OF DEVICES

For example, claim 19 of the '471 Patent recites moving the device before capturing subsequent images. Nothing about these claim limitations add anything novel or non-obvious over the prior art. Further, moving a camera or adjusting the location of a camera is inherently obvious.

The movement of devices as recited in the claims would have been obvious to a person of ordinary skill in the art at least because doing so would have involved a routine and conventional action. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use and results of moving a device between taking pictures.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have

considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Ramaswamy, as disclosed in the accompanying claim charts, for example, set forth in elements 471.19
- Nechyba, as disclosed in the accompanying claim charts, for example, set forth in elements 471.19
- Ganong, as disclosed in the accompanying claim charts, for example, set forth in elements 471.19
- Zhang, as disclosed in the accompanying claim charts, for example, set forth in elements 471.19
- Park, as disclosed in the accompanying claim charts, for example, set forth in elements 471.19
- Frischholz, as disclosed in the accompanying claim charts, for example, set forth in elements 471.19
- Marsico, disclosed in the accompanying claim charts, for example, set forth in elements 471.19
- Bud, as disclosed in the accompanying claim charts, for example, set forth in elements 471.19
- Ferren, as disclosed in the accompanying claim charts, for example, set forth in elements 471.19

- Ross, *e.g.*, 3:5-32, 3:59-4:13, 8:39-62 (describing calculating distances between device and objects, including distances from the user's face)
- Negi, *e.g.*, Fig. 3, 5:55-64,
- Wang, *e.g.*, Fig. 1, Fig. 2, Pg. 2, Pg. 6 (describing capturing a sequence of images of a user's face from different viewpoints either through a fixed camera/moving face or moving camera/fixed face)
- Chen, *e.g.*, Abstract, Fig. 2, Fig. 3, Fig. 5, 2:28-44, 2:45-56, 2:62-65, 3:64-4:12, 4:33-43, 5:31-39 (disclosing an authentication method requiring user to move a smartphone to different positions)
- Turgeman, *e.g.*, [0058], [0160], [0163], [0173], [0205] (describing user moving and rotating mobile device)
- Tippett, *e.g.*, [0018], [0034], [0035] (movement of user's face and/or mobile device to capture gestures for authentication)
- Karakotsios, *e.g.*, Fig. 2(a), Fig. 2(b), Figs. 3-4(b), 2:3-16, 3:22-63 (describing functionality to determine whether a user is facing a camera)
- Horvitz, *e.g.*, Fig. 4, Fig. 5, 7:21-39, 9:12-31, 9:53-10:4 (describing capturing motion of user's head and different angles from which the image may be captured)
- Smiatacz, *e.g.,* Pg. 261 (Describing user/camera movement, such as head rotation, is required for liveness detection)

11. LAPTOP OR DESKTOP COMPUTER DEVICES

For example, claim 7 of the '606 Patent recites using a laptop or desktop computer as the computing device that practices the invention. Nothing about these claim limitations add anything novel or non-obvious over the prior art. References and products using laptop or desktop computers were well-known, routine, conventional, and widely available before the alleged invention.

The use of a laptop or desktop computer as recited in the claims would have been obvious to a person of ordinary skill in the art because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution

of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use of laptop and desktop computer devices.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Nechyba, as disclosed in the accompanying claim chart, for example, set forth in element 606.7
- Ramaswamy, as disclosed in the accompanying claim chart, for example, set forth in element 606.7
- Ganong, as disclosed in the accompanying claim chart, for example, set forth in element 606.7
- Zhang, as disclosed in the accompanying claim chart, for example, set forth in element 606.7
- Park, as disclosed in the accompanying claim chart, for example, set forth in element 606.7

- Frischholz, as disclosed in the accompanying claim chart, for example, set forth in element 606.7
- Marsico, as disclosed in the accompanying claim chart, for example, set forth in element 606.7
- Bud, as disclosed in the accompanying claim chart, for example, set forth in element 606.7
- Ferren, as disclosed in the accompanying claim chart, for example, set forth in element 606.7
- Uchida, *e.g.*, 7:6-13 (disclosing that the invention may be used on a computer system)
- Chen, *e.g.*, Abstract, Fig. 2, 12:52-62, 14:10-16 (disclosing an authentication method that may be implemented on computers)
- Landschaft, *e.g.*, Fig. 5, [0001], [0010], [0026] (disclosing an authentication method that may be implemented on a laptop computer or other devices)
- Turgeman, *e.g.*, [0172] (this invention can be used on a variety of devices)
- Evans, *e.g.*, 3:33-49 (describing that this invention may be used in a personal computer or laptop computer)
- Sensharma, *e.g.*, 8:40-51 (using laptop computers to implement the invention)
- Langley, *e.g.*, Fig. 1, 4:20-27 (remote authentication device can be a laptop computer)
- Holz, *e.g.*, Fig. 1, Fig. 4A, Fig. 4D, 7:31-42, 9:36-51 (disclosing an authentication method that may be implemented on laptop computers or other devices)
- Chaudhury, *e.g.*, Fig. 1A, Fig. 3A, Fig. 3B, Fig. 5, 4:37-47 (describing authentication and liveness detection method that may be implemented on laptop or other devices)
- LeCun, *e.g.*, Fig. 2, Fig. 3, [0007], [0013], [0023] (describing authentication method that can be implemented on computers and other devices)
- Takahashi, *e.g.*, Fig. 1, 6:17-30, 6:31-35 (describing an authentication system implemented on a computer)

12. USER IMAGE

For example, claim 8 of the ’606 Patent recites displaying an image on the screen of the computing device while capturing the images used. Nothing about these claim limitations add anything novel or non-obvious over the prior art.

The use of user images as recited in the claims would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use and disclosure of systems and devices that practice and/or embody the described features and/or functionality of the claimed use of expected distortion, and the associated benefits and advantages of its use.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these

teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Nechyba, as disclosed in the accompanying claim chart set forth in element 606.8
- Ramaswamy, as disclosed in the accompanying claim chart, for example, set forth in element 606.8
- Ganong, as disclosed in the accompanying claim chart, for example, set forth in element 606.8
- Frischholz, as disclosed in the accompanying claim chart, for example, set forth in element 606.8
- Marsico, as disclosed in the accompanying claim chart, for example, set forth in element 606.8
- Bud, as disclosed in the accompanying claim chart, for example, set forth in element 606.8
- Negi, *e.g.*, Fig. 2, 5:47-54
- Tippett, *e.g.*, Fig. 5A, Fig. 5D, Fig. 5E, (showing image of users' gestures on screen)
- Lau, *e.g.*, Figs. 7-10 (embodiments showing user's image on screen while capturing and authenticating)
- Baldwin '138, Fig. 1A, Fig. 1B, Fig. 2A, 3:40-4:23 (describing the user being in the field of view of the device when the user's image shows on the screen)
- Landschaft, *e.g.*, Fig. 3, [0039] (describing displaying a preview of the user's image on the device)

13. SERVER-BASED SOLUTIONS

For example, claims 9 and 20 of the '606 Patent, claim 10 of the '471 Patent, and claim 18 of the '938 Patent each recite transmitting biometric data over a network to a server. Nothing about these claim limitations add anything novel or non-obvious over the prior art. References and

products with these features were well-known, routine, conventional, and widely available before the alleged invention.

The use of a server or network to perform the authentication recited in the claims would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use of authentication and security systems that utilize network resources or servers to perform their functionality.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Nechyba, as disclosed in the accompanying claim chart set forth in elements 606.9, 606.20, and 938.18
- Ramaswamy, as disclosed in the accompanying claim chart set forth in elements 606.9, 606.20, and 938.18

- Ganong, as disclosed in the accompanying claim chart set forth in elements 606.9, 606.20, and 938.18
- Zhang, as disclosed in the accompanying claim chart set forth in elements 606.9, 606.20, and 938.18
- Park, as disclosed in the accompanying claim chart set forth in elements 606.9, 606.20, and 938.18
- Frischholz, as disclosed in the accompanying claim chart set forth in elements 606.9, 606.20, and 938.18
- Bud, as disclosed in the accompanying claim chart set forth in elements 606.9, 606.20, and 938.18
- Ferren, as disclosed in the accompanying claim chart set forth in elements 606.9, 606.20, and 938.18
- Ross, *e.g.*, Fig. 2, 10:33-46, 10:59-11:9 (showing a network and server implementation of the authentication method described in this invention)
- Uchida, *e.g.*, 6:61-7:5, 7:6-13 (disclosing that the invention may be used on a network of computer systems)
- Chen, *e.g.*, 12:52-62, 14:10-16 (disclosing an authentication method that may be implemented on networked devices)
- Turgeman, *e.g.*, [0204] (suggested embodiment can have the authentication unit on a remote server)
- Sensharma, *e.g.*, 4:47-60 (describing some functions that are performed by another system, including remote servers)
- Langley, *e.g.*, Fig. 1, 3:45-56, 4:28-54, 4:51-60, 6:15-32 (using a remote server to control access to resources and provide data for authentication)
- Baldwin ’622, *e.g.*, Fig. 8 (authenticating device connected to a web and application server to run its authentication method)
- Parry, *e.g.*, 4:58-5:1, 7:47-61 (describing use of computer, laptop, or server to perform authentication)

- Holz, *e.g.*, Fig. 1, 9:19-34, 12:37-39, 15:47-60 (disclosing an authentication method that may be implemented on a computer system including a content server)
- Chaudhury, *e.g.*, Fig. 1A, Fig. 5, 4:37-47, 5:24-33, 9:43-49 (describing authentication and liveness detection method that may be implemented with a server)
- LeCun, *e.g.*, Fig. 1, Fig. 2, Fig. 3, [0033] (describing authentication method that may be implemented with a device connected to a server)
- Takahashi, *e.g.*, Fig. 1, Fig. 5, 1:19-32, 6:13-16, 6:17-30, 6:31-35 (describing a server-client authentication system with an authentication server)

14. FISH-EYE DISTORTION/EAR TRACKING

For example, claim 1 of the '938 Patent recites comparing the data for expected differences resulting from fish-eye type distortion. Similarly, and as another example, claim 12 of the '910 Patent recites verifying between the first and second images a reduction in visibility of the user's ears (a specific example of fish-eye type distortion). Nothing about this claim limitation adds anything novel or non-obvious over the prior art. References and products with these features were well-known, routine, conventional, and widely available before the alleged invention.

Comparison methods using fish-eye distortion to determine whether a user exhibits a three-dimensional shape as recited in the claim would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use of authentication and security systems that utilize network resources or servers to perform their functionality.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to

combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Nechyba, *see e.g.,* 28:6-27, 35:58-36:3.
- Marsico, *see e.g.,* Pg.5 (bending)
- Tanii, *see e.g.,* [0047], [0048], Figs. 3A and 3B, Figs. 4A and 4B.
- Derakhshani, *see e.g.,* Abstract, 1:20-25, 1:44-2:3, 16:44-17:11, 17:11-26, 17:45-18:4.
- Hoyos '120, *see e.g.,* Figs. 1, 3 and 4; 7:22-32.

15. Compare With Enrollment Image

For example, claim 5 of the '938 Patent recites comparing the data with enrollment data derived from an enrollment image. Nothing about this claim limitation adds anything novel or non-obvious over the prior art. References and products with these features were well-known, routine, conventional, and widely available before the alleged invention.

Using facial recognition methods to compare a recently taken photo of the user with enrollment photo data of the user (enrollment photo taken prior to the authentication session) as recited in the claim would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary

skill in the art would have readily appreciated the well-known and widespread use of authentication and security systems that utilize network resources or servers to perform their functionality.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Nechyba, *see e.g.,* Abstract, 1:25-41, 1:47-61, 1:62-2:17, 4:9-26, 5:27-54, 8:12-40.
- Ganong, *see e.g.,* 1:25-27, 1:46-63, 39:50-58, Fig. 3, 10:2-8, 10:18-29.
- Ferren, *see e.g.,* Fig. 2, Abstract, 2:51-3:2, 7:41-52.
- Hoyos, *see e.g.,* Fig. 1, [0028], [0031], [0033]-[0040].
- Smiatacz, *e.g.,* Pg. 266 (Experiments of the system resembled real-life conditions where the user would record a live sequence for processing during registration, which would then train the model to classify real and fake images of the user).

16. EXAMINING THIRD IMAGE (INTERPOLATING DATA)

For example, claims 11 of the ’471 and claim 2 of the ‘606 Patent recite taking a third picture between the first and second and performing the same comparison operation on it with interpolated data; the claims recite “interpolating” the first data and second data. In essence, the claims recite performing another comparison step with a third picture that is located in between the

first and second. Nothing about this claim limitation adds anything novel or non-obvious over the prior art. References and products with these features were well-known, routine, conventional, and widely available before the alleged invention.

Performing a comparison of a third picture located between the first two as recited in the claim would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use of authentication and security systems that utilize network resources or servers to perform their functionality.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Nechyba, *see e.g.*, 18:34-58, 20:9-27.
- Zhang, *see e.g.,* [0035], [0048].
- Frischholz, *see e.g.,* 13:50-59, 3:49-52.

- Park, *see e.g.,* [0052]-[0057], Fig. 3.
- Marsico, *see e.g.,* Fig. 4, Pg. 5.

17. REFLECTION DETECTION

For example, claim 18 of the ’471, claim 18 of the ’910 Patents, and claim 15 of the ‘938 Patent recite displaying an image on the screen or provide illumination, respectively, and detecting reflection in the image data. Nothing about this claim limitation adds anything novel or non-obvious over the prior art. References and products with these features were well-known, routine, conventional, and widely available before the alleged invention.

Performing a comparison of a third picture located between the first two as recited in the claim would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use of authentication and security systems that utilize network resources or servers to perform their functionality.

Persons of ordinary skill in the art would have been motivated to combine the teachings of these references with the other references cited herein, in view of the foregoing considerations and those further reflected in the references. iProov further hereby specifically incorporates by reference, and may rely upon for purposes of showing obviousness including motivations to combine, the disclosures cited for each reference with respect to the relevant limitations as cited in the prior art claim charts submitted herewith and the disclosures and teachings further cited below. Each cited disclosure evidences a teaching that a person of ordinary skill in the art would have considered relevant, and each cited disclosure may be relied upon as evidence of a teaching, suggestion, or motivation to combine the subject matter of the disclosure with other reference disclosures. Persons of ordinary skill in the art would have been motivated to combine these teachings of these references accordingly with the other references addressed herein to the extent they are not found to disclose this feature.

The following references are identified within this grouping for purposes of disclosing obviousness combinations.

- Nechyba, *see e.g.,* 4:53-5:54.
- Ramaswamy, *see e.g.,* 3:2-21, 6:65-7:50.
- Zhang, *see e.g.* 0031, 0033, and 0034
- Ganong, *see e.g.,* 42:53-60.
- Bud '169, *see e.g.,* 2:50-67, 9:63-10:10, 10:11-26, 10:27-37.
- Bud '975, *see e.g.,* 2:61-3:11.
- Ferren, *see e.g.,* 5:36-6:55.

viii. MOTIVATIONS BASED ON ADMITTED PRIOR ART

iProov reserves the right to rely on any admissions in the FaceTec Asserted Patents, the prosecution history, and on any admissions by the patentee and/or the named inventors of the FaceTec Asserted Patents, including in publications published contemporaneously to the FaceTec Asserted Patents. For example, Defendant hereby expressly incorporates by reference any statements and reasons set forth in the FaceTec Asserted Patents themselves or by the Examiner during prosecution of the FaceTec Asserted Patents and/or related patent applications or by the Board in any past, pending, or future post-grant proceeding related to the FaceTec Asserted Patents and/or related patents as to why it would have been obvious to modify or combine prior art references to achieve the limitations of the FaceTec Asserted Claims.

ix. SECONDARY CONSIDERATIONS

A patentee bears the burden of production with respect to evidence of secondary considerations of non-obviousness. *ZUP, LLC v. Nash Mfg., Inc.*, 896 F.3d 1365, 1373 (Fed. Cir. 2018). As of the date of these Preliminary Invalidity Contentions, Plaintiff has not identified any secondary considerations. iProov reserves all rights to respond to any secondary considerations of non-obviousness raised by Plaintiff, including by updating and/or modifying these Preliminary Invalidity Contentions. iProov is not aware of any unexpected results (none is mentioned in the FaceTec Asserted Patents or its file history), long felt need, commercial success (or any nexus to any allegedly successful commercial embodiment), or awards for the FaceTec Asserted Patents.

Indeed, as shown in these Preliminary Invalidity Contentions, dozens of other companies and individuals described, built, and/or patented the exact same concepts in the FaceTec Asserted Patents before Plaintiff ever did—often many years before. Even where others' inventions occurred at approximately the same time as the alleged invention in the FaceTec Asserted Patents, such simultaneous invention further demonstrates the obviousness of the FaceTec Asserted Patents. Thus, to the extent it is determined that one or more of the references discussed in these Preliminary Invalidity Contentions is not prior art under 35 U.S.C. §§ 102(a)(1), 102(a)(2), or otherwise, iProov may still rely on such reference(s) as demonstrating the state of the art and/or simultaneous invention.

e. INVALIDITY CHARTS [PATENT L.R. 3-3(C)]

The attached claim charts (Exhibits 471-A through 471-I, 606-A through 606-I, 938-A through 938-I, and 910-A through 910-I) are based, in whole or in part, on Plaintiff's asserted theories of infringement in this case, to the extent discernible from Plaintiff's Infringement Contentions. As an initial matter, all portions of each prior art reference cited in each of the attached claim charts are relied upon to support the disclosure of each patent claim limitation, as all portions provide general support. Representative descriptions and supporting citations are nevertheless provided, but are merely exemplary; they do not necessarily reflect every instance where a particular claim term or claim limitation may be disclosed in or taught by the prior art reference. References to figures or drawings refer to the figures/drawings themselves, as well as to any accompanying text or text necessary to understand the figures or drawings. References to text refers to the text itself, as well as the accompanying figures or drawings that accompany the text. iProov reserves the right to rely on additional, or different, portions of the prior art references, other publications and expert testimony to establish what these references would have taught one of ordinary skill in the art, or in what manner they would have motivated a particular combination of references. Moreover, in certain instances, representative documents for certain prior art systems are cited, but, again, are merely exemplary; they do not necessarily reflect or include every document relating to the prior art system that exists and that discloses or teaches a particular claim term or claim limitation. iProov reserves the right to rely on any and all documents that describe

or relate to prior art systems, including relying on the system itself. iProov also reserves the right to rely on the testimony of the authors, named inventors, or anyone else with knowledge of the prior art references and systems identified herein, as well as expert testimony regarding any such references or systems.

f. SECTION 101 AND 112 DEFENSES [PATENT L.R. 3-3(D)]

iProov provides the following grounds for invalidity under 35 U.S.C. §§ 101 and 112. iProov's investigation of the FaceTec Asserted Patents is ongoing, and iProov reserves the right to amend or supplement these disclosures based on further investigation and in a manner consistent with the Federal Rules of Civil Procedure, or otherwise in accordance with any order or direction of this Court or agreement of the parties. Further, Plaintiff's Infringement Contentions fail to provide sufficient detail to fully understand its proposed application of the FaceTec Asserted Claims, and iProov reserves the right to assert additional grounds for invalidity under 35 U.S.C. §§ 101 and 112 in response to Plaintiff's claim interpretations. iProov also reserves the right to supplement, modify, or otherwise amend these grounds for invalidity under 35 U.S.C. §§ 101 and 112 based on the Court's claim construction rulings or opinions or the parties' positions or arguments taken in connection with the claim construction process.

Plaintiff has not yet provided a claim construction for many of the terms and phrases that iProov anticipates will be in dispute. iProov, therefore, cannot provide a complete list of its § 112 defenses because iProov does not know whether Plaintiff will proffer a construction for certain terms and phrases that is broader than, or inconsistent with, the construction that would be supportable by the disclosure set forth in the specification.

To the extent the following contentions reflect constructions of claim limitations consistent with or implicit in Plaintiff's Infringement Contentions, no inference is intended nor should any be drawn that iProov agrees with Plaintiff's claim constructions, and iProov expressly reserves the right to contest such claim constructions. iProov offers these contentions in response to Plaintiff's Infringement Contentions and without prejudice to any position it may ultimately take as to any claim construction issues.

iProov reserves the right to provide additional explanation and/or argument for their Preliminary Invalidity Contentions under Section 101 and 112, including, for example, based on expert testimony.

i. INDEFINITENESS

Subsection (b) of § 112 of the Patent Act requires that a patent claim "particularly point[] out and distinctly claim[] the subject matter which the inventor or a joint inventor regards as the invention." 35 U.S.C. § 112(b). Claim terms that fail to inform those skilled in the art "with reasonable certainty . . . about the scope of the invention" fail the definiteness requirement. *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014).

To the extent FaceTec proposes or discloses explicit or implicit claim construction positions or supporting arguments that reveal claim language that, in view of the intrinsic evidence, fails to provide reasonable certainty about the scope of the claimed invention, iProov reserves the right to raise the issue of indefiniteness with respect to such claim language. Furthermore, FaceTec's infringement contentions are both deficient and based only on publicly available information. To the extent FaceTec is later permitted to raise infringement contentions that reveal a claim interpretation supporting a holding of indefiniteness, iProov reserves the right to raise the issue of indefiniteness at such time.

For example, the following claim terms may be indefinite:

Claim Term	FaceTec Asserted Claims
"A method for ***authenticating*** three-dimensionality of a user via a user's camera equipped computing device, the method, during an authentication session comprising"	'471 Claim 10
"processing the at least one first image or a portion to create first ***data***"	'471 Claim 10
"distance from the user" / "change the distance" / "second distance being different than the first distance"	'471 Claim 10; '606 Claims 1, 19
"comparing the first data to the second data to determine whether ***expected distortion*** exist between the first data and the second data which indicated three-dimensionality of the user"	'471 Claim 10
"wherein the first data and the second data comprise ***biometric data***"	'471 Claim 16

"A method for ***verifying*** three-dimensionality of a user's face using images of the user's face captured using a camera equipped computing device, the method comprising"	'606 Claims 1, 19
"processing the at least one first image to obtain first ***biometric data*** from the at least one first image"	'606 Claims 1, 19
"comparing the first *biometric data* to second biometric data to determine whether differences between the at least one first image and the at least one second image ***match expected differences*** resulting from movement of the camera or the user which changed the distance between the user and camera from the first distance to the second distance"	'606 Claims 1, 19
"the first biometric data does ***not match*** the second biometric data	'606 Claim 1
the first biometric data is ***not identical*** to the second biometric data; and"	'606 Claim 19
"compare the first biometric data with second biometric data for ***expected differences*** that result from characteristics of a human face and the at least one first image and the at least one second image being captured at different distances from the user;"	'938 Claim 1
"determine that the three-dimensional shape is not exhibited when the second biometric data does not have ***expected differences*** compared to the first biometric data, the expected differences comprising at least differences due to the change in the relative distance between the user's facial features and the camera when the at least one first image was captured at the first distance and the at least one second image was captured at the second distance, wherein the expected differences result from fish-eye type distortion in at least one of the at least one first image and the at least one second image and due to the three-dimensional nature of the human face and the change in distance between the camera and the user."	'938 Claim 1
"the ***expected differences appear as changes in the relative size and shape of facial features of the user***."	'938 Claim 2
"examining the first data and the second data to determine whether differences between the first data and the second data indicate an ***expected type of distorting change*** in at least one image that is ***consistent with a real person being imaged and which is indicative of three-dimensionality***;"	'938 Claim 8
"determining the user's face is not three-dimensional when the first data and the second data do not have ***expected differences indicating the user exhibits three-dimensionality***."	'938 Claim 8
"examining the additional data, the first data, and the second data, or portions thereof, to determine whether ***expected differences therebetween indicate the user's face exhibits three-dimensionality***."	'938 Claim 9
"comparing one or more aspects of the head from the first image or first biometric data derived from the first image to one or more aspects of the head from the second image or second biometric data derived from the second image to determine whether ***expected***	'938 Claim 17

differences are not present, wherein the expected differences: would be present when the first image and second images of the head of the person being captured at different distances ***has three-dimensional characteristics but not if the head did not have three-dimensional characteristics;"***	
"***the expected differences result from differences in relative dimensions of a person's face appearing different*** when capturing images is done close to the person's face and far from the persons face"	'938 Claim 17
"***if the expected differences are not present***, denying authentication of the person and providing notice thereof to one or more of the person, a third party, or a software application, wherein the authentication is authentication of liveness, three-dimensionality, or both."	'938 Claim 17
"analyzing the first data to determine at least if the first data exhibits ***first characteristics that indicate the first data was derived from an image of the user captured at the first distance***"	'938 Claim 20
"analyzing the second data to determine at least if the second data exhibits ***second characteristics that indicate the second data was derived from an image the user captured at the second distance***, wherein the first characteristics or the second characteristics include at least ***distortion within the at least one first image or the at least one second image***;"	'938 Claim 20
"determining the user does not exhibit the ***expected degree of three-dimensionality*** when either or both of the following occur: the step of analyzing the first data determines the first data does not exhibit ***first characteristics that indicate the first data was derived from an image of the user captured at the first distance***; or the step of analyzing the second data determines the second data does not exhibit ***second characteristics that indicate the second data was derived from an image of the user captured at the second distance***."	'938 Claim 20
"comparing the first data to the second data to determine whether ***expected differences exist between the first data and the second data which indicate three-dimensionality of the user***;"	'910 Claim 10
"verifying the images of the user exhibit three-dimensional traits when the first data and the second data have ***expected differences resulting from the at least one first image being captured with the camera at a different distance from the user than when the at least one second image is captured***."	'910 Claim 10

ii. Lack of Written Description and/or Enablement

The patent statute requires a patentee to describe and enable the purported invention. *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1343 (Fed. Cir. 2010) (en banc). Written

description and enablement impose distinct but related requirements. *LizardTech, Inc. v. Earth Resource Mapping, Inc.*, 424 F.3d 1336, 1344-45 (Fed. Cir. 2005). For written description, "the test ... is whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date." *Ariad*, 598 F.3d at 1351. The "enablement requirement is satisfied when one skilled in the art, after reading the specification, could practice the claimed invention without undue experimentation." *Automotive Techs. Int'l, Inc. v. BMW of N. Am., Inc.*, 501 F.3d 1274, 1282 (Fed. Cir. 2007) (internal quotation omitted).

The description and enablement requirements are fundamental to the *quid pro quo* of the patent system, ensuring that the scope of the claims does not "overreach() the scope of the inventor's contribution." *Ariad*, 598 F.3d at 1353-54. Although the specification is evaluated from the perspective of a person of ordinary skill, the *specification itself* must satisfy the description and enablement requirements. Thus, regardless of the prior art's disclosures, a specification does not satisfy the written description requirement if it "merely renders the invention obvious" to a person of ordinary skill, "amount(s) to no more than a 'wish' or 'plan,'" or "simply claim(s) a desired result" without demonstrating that the patentee actually invented the full claim scope. *Id.* at 1349-52 (internal quotations omitted). Likewise, for enablement, "[i]t is the specification, not the knowledge of one skilled in the art, that must supply the novel aspects of an invention in order to constitute adequate enablement." *Genentech, Inc. v. Novo Nordisk A/S*, 108 F.3d 1361, 1366 (Fed. Cir. 1997).

To prevent overreaching claims, the law requires the patentee to describe and enable the "full scope" of the claims. *LizardTech*, 424 F.3d at 1344-45. For example, a patentee may not describe and enable one embodiment and then capture other, "distinctly different" embodiments within the claim scope. *Automotive Techs.*, 501 F.3d at 1285 (affirming summary judgment of non-enablement because the patentee described and enabled only mechanical sensors but the generic "sensor" claims also covered electronic sensors); *Ariad*, 598 F.3d at 1358 (overturning jury verdict of no invalidity on written description grounds).

The FaceTec Asserted Claims fail both the written description and enablement requirements. For example, the ’471 Patent does not sufficiently describe or enable “comparing the first data to the second data to determine whether ***expected distortion*** exist between the first data and the second data which indicated three-dimensionality of the user,” as recited in claim 1. A person of ordinary skill would not have understood reading the specification how to implement a method of authentication involving “expected distortion” as the specification fails to describe what is meant by expected distortion, how data information relates to this distortion, or how determinations could be made based on this data. The term “expected distortion” is only mentioned in the specification twice in that it may be based on a mobile device and that it may be used in validating images. (*See* ’471 Patent, 29:65–30:5 (“[T]he system may predict the expected fish-eye distortion of the images based on the mobile device used for enrollment and authentication, and based on known and trusted enrollment data. In addition or as an alternative, the known specifications of a mobile phone camera for a given model may be utilized to predict the **expected distortion** of the person's facial features at different distances from the lens.”), 30:11–18 (“During authentication, multiple images are captured in addition to images corresponding the close and far distances of the enrollment images and biometrics. Based on the **expected distortion** of these intermediary images according to the distanced traveled by the device, the system may validate that the change in distortion of the images is happening at the correct rate, even though only two enrollment profiles are obtained.”).)

Similarly, the ’606 Patent does not sufficiently describe or enable “comparing the first biometric data to second biometric data to determine whether differences between the at least one first image and the at least one second image ***match expected differences*** resulting from movement of the camera or the user which changed the distance between the user and camera from the first distance to the second distance,” as recited in claims 1 and 19. The specification does not state how to determine expected differences for an user, how biometric data relates to these expected differences, or what is considered a match between the biometric data and expected differences. The specification merely states that expected differences may be based on testing. (*See* ’606 Patent, 36:15–22 (“The expected values or expected rate of change of an item in an image, defined by pixel

location or values, may be based on testing over time such as expected location, expected displacement, expected rate of change of the item, or even **expected differences** in the rate to change which would indicate three-dimensionality (as opposed to a 2D photograph or video screen of a person)." A person of ordinary skill would not have understood reading the specification how to implement a method comparing biometric data to expected differences for a match.

Likewise, the '938 Patent does not does not sufficiently describe or enable "determine that the three-dimensional shape is not exhibited when the second biometric data ***does not have expected differences*** compared to the first biometric data" as recited in claim 1, or "examining the first data and the second data to determine whether differences between the first data and the second data indicate an ***expected type of distorting change*** in at least one image that is consistent with a real person being imaged and which is indicative of three-dimensionality" and "determining the user's face is not three-dimensional when the first data and the second data do not have ***expected differences indicating the user exhibits three-dimensionality***" as recited in claim 8, or "comparing one or more aspects of the head from the first image or first biometric data derived from the first image to one or more aspects of the head from the second image or second biometric data derived from the second image to determine whether ***expected differences are not present***" as recited in claim 17, or "determining the user does not exhibit the ***expected degree of three-dimensionality*** when either or both of the following occur: the step of analyzing the first data determines the first data does not exhibit first characteristics that indicate the first data was derived from an image of the user captured at the first distance; or the step of analyzing the second data determines the second data does not exhibit second characteristics that indicate the second data was derived from an image of the user captured at the second distance" as recited in claim 20.

A person of ordinary skill would not have understood reading the specification how to implement a method of authentication involving "expected" claim elements, as the specification fails to describe what is meant by "expected" distortion, how data information relates to this distortion, or how determinations could be made based on this data. The term "expected distortion" is only mentioned in the specification twice in that it may be based on a mobile device and that it may be used in validating images. (*See* '938 patent, 30:1-8 ("[T]he system may predict the expected

fish-eye distortion of the images based on the mobile device used for enrollment and authentication, and based on known and trusted enrollment data. In addition or as an alternative, the known specifications of a mobile phone camera for a given model may be utilized to predict the **expected distortion** of the person's facial features at different distances from the lens."), 30:14-21 ("During authentication, multiple images are captured in addition to images corresponding the close and far distances of the enrollment images and biometrics. Based on the **expected distortion** of these intermediary images according to the distanced traveled by the device, the system may validate that the change in distortion of the images is happening at the correct rate, even though only two enrollment profiles are obtained.").) A person of ordinary skill would not have understood reading the specification how to implement a method comparing biometric data to "expected results" for a match.

Lastly, the '910 Patent does not does not sufficiently describe or enable "comparing the first data to the second data to determine whether ***expected differences*** exist between the first data and the second data which indicate three-dimensionality of the user" or "verifying the images of the user exhibit three-dimensional traits when the first data and the second data have ***expected differences*** resulting from the at least one first image being captured with the camera at a different distance from the user than when the at least one second image is captured," as recited in claim 10. The specification does not state how to determine expected differences for a user, how biometric data relates to these expected differences, or what is considered a match between the biometric data and expected differences. The specification merely states that expected differences may be based on testing. (*See* '910 Patent, 35:59-66 ("The expected values or expected rate of change of an item in an image, defined by pixel location or values, may be based on testing over time such as expected location, expected displacement, expected rate of change of the item, or even **expected differences** in the rate to change which would indicate three-dimensionality (as opposed to a 2D photograph or video screen of a person).")). A person of ordinary skill would not have understood reading the specification how to implement a method comparing biometric data to expected differences for a match.

iii. MEANS PLUS FUNCTION CLAIMS

At his time, Defendant does not identify any terms that invoke 35 U.S.C. § 112(f) in the FaceTec Asserted Claims. FaceTec's infringement contentions are incomplete and do not provide iProov with sufficient information to fully understand the basis for FaceTec's infringement allegations or understand FaceTec's construction of the limitations in the FaceTec Asserted Claims. Moreover, the parties' understanding of the terms of the FaceTec Asserted Claims may change during claim construction and other proceedings in the case. iProov reserves its right to amend or supplement its identification of terms that invoke paragraph f of 35 U.S.C. § 112 (if any) in view of these future proceedings.

iv. INELIGIBILITY UNDER 35 U.S.C. § 101

The FaceTec Asserted Claims are further invalid for failure to meet the eligibility requirements of 35 U.S.C. § 101. iProov has filed a Motion for Judgment on the Pleadings for lack of patentable subject matter, the contents of which are incorporated herein by reference, Dkt. 57, in addition to iProov's reply brief and any oral argument on the motion.

II. DOCUMENT PRODUCTION [PATENT L.R. 3-4]

To the extent not already in FaceTec's possession from iProov's discovery produced in the action *FaceTec v. iProov*, Case No. 2:21-cv-02252-ART-BNW (D. Nev.) (the "Nevada Action"), iProov produces herewith copies of prior art and documents describing prior art systems, under Patent L.R. 3-4(b). iProov has already produced to Plaintiffs documents required under Patent L.R. 3-4(a) (source code and related documents), 3-4(c) (agreements), 3-4(d) (sales revenues and related information), and 3-4(e) (agreements) in connection with the Nevada Action, and incorporates those productions herein by reference.

As explained in iProov's pending Motion to Strike Plaintiff's Infringement Contentions (Dkt. 76), Plaintiff has not properly accused any single product or technology of infringement and, therefore, iProov does not possess any documents responsive to the other categories identified in PLR 3-4. iProov will not produce any documents regarding its technology but will revisit this issue if the pending motion to strike is denied or if iProov is ordered by the Court to produce.

III. ADDITIONAL CONTENTIONS AND DISCLOSURES INCORPORATED BY REFERENCE

iProov asserts additional grounds of invalidity, in addition to those described above. These

include, without limitation: (1) the Patent L.R. 3-3 and Patent L.R. 3-4 disclosures and document productions of defendant Jumio; (2) all prior art and documents submitted to or considered by the Patent Trial and Appeal Board ("PTAB") in IPR2025-00106, IPR2025-00107, IPR2025-00108, and IPR2025-00109; and (3) iProov Ltd's Non-Infringement, Invalidity, and Unenforceability Contentions Pursuant to Local Patent Rule 1-8, dated September 22, 2024, and any amendments thereto, provided in the Nevada Action. These materials are properly incorporated herein by reference in their entirety. *See, e.g., Rsa Protective Techs. v. Delta Sci. Corp.*, No. LA CV19-6024 JAK (PLAx), 2020 U.S. Dist. LEXIS 250247, at *11 (C.D. Cal. Dec. 14, 2020) (permitting incorporation by reference of additional grounds for invalidity into invalidity contentions).

Dated: January 17, 2025

/s/ Ryan E. Hatch

ALAN SEGE (CA BAR NO. 177350)
ALAN SEGE ESQ., PC
13323 Washington Blvd, Suite 302
Los Angeles, CA 90066
Telephone: (310) 957-3301
alan@alansege.com

RYAN E. HATCH (CA Bar No. 235577)
ADAM J. REIS (CA Bar No. 354712)
HATCH LAW PC
13323 Washington Blvd, Suite 302
Los Angeles, CA 90066
(310) 279-5076 Telephone
(310) 693-5328 Facsimile
ryan@hatchlaw.com

Attorneys for Intervenor iProov Ltd.