



(51) International Patent Classification:
B65G 47/26 (2006.01)

(21) International Application Number:
PCT/US2010/037983

(22) International Filing Date:
9 June 2010 (09.06.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/187,520 16 June 2009 (16.06.2009) US

(71) Applicant (for all designated States except US): **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, MS: RNB-4-150, Santa Clara, California 95052 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **FERREN, Bran** [US/US]; 1236 Benedict Canyon Dr., Beverly Hills, California 90210 (US).

(74) Agents: **VINCENT, Lester J.** et al.; Blakely Sokoloff Taylor & Zafman, 1279 Oakmead Parkway, Sunnyvale, California 94085 (US).

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

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK,

[Continued on next page]

(54) Title: CONTROLLED ACCESS TO FUNCTIONALITY OF A WIRELESS DEVICE

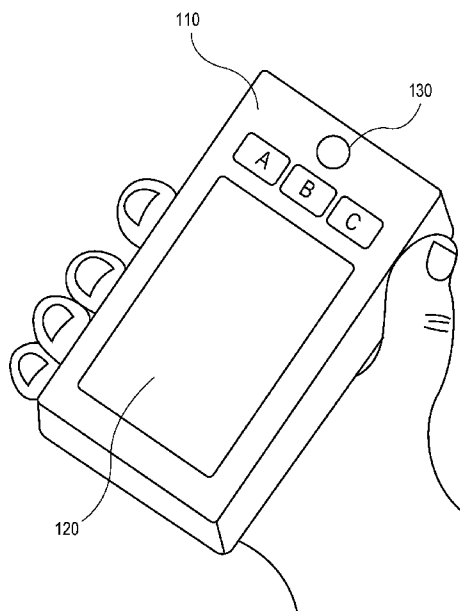


FIG. 1

(57) Abstract: Various embodiments of the invention may be used to verify that a person being authorized by biometric techniques to use a device is a living person and not some form of recording intended to spoof the system. Some embodiments may try to cause a change in a measured biometric feature, and compare images taken before and after the change to verify the change occurred. In some embodiments, multiple stages of verification may be used, either to increase the difficulty of spoofing the security system, or to provide different levels of security for different levels of access to the device's functionality.

WO 2010/147823 A1



SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, **Published:**
GW, ML, MR, NE, SN, TD, TG).

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