

24. **A Framework for Vulnerability Detection in European Train Control Railway Communications.**

By: Arsuaga, Irene; Toledo, Nerea; Lopez, Igor; Aguado, Marina. *Security & Communication Networks* , 5/15/2018, p1-9, 9p Abstract: Railway systems have evolved considerably in the last years with the adoption of new communication technologies. Aiming to achieve a single European railway network, the European Rail Traffic Management System (ERTMS) emerged in Europe to substitute multiple and noninteroperable national railway communication systems. This system and its security strategies were designed in late 1990s. Recent works have identified vulnerabilities related to integrity, authenticity, availability, and confidentiality. In the context of defining effective countermeasures to mitigate potential vulnerabilities, these vulnerabilities have to be analysed. In this article we introduce a framework that attempts to challenge ERTMS security by evaluating the exploitability of these vulnerabilities. [ABSTRACT FROM AUTHOR]; DOI: 10.1155/2018/5634181; (AN 129613787), Database: Applied Science & Technology Source

Subjects: Railroad engineering; **Communication** of technical information; Support Activities for Rail Transportation; Joint use of railroad facilities; Integrity; Vulnerability (Psychology)

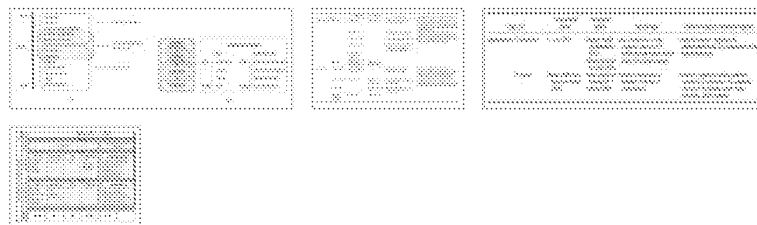
[HTML Full Text](#) [PDF Full Text \(1.9MB\)](#) [USPTO Full Text Options](#)

25. Multilevel complexity measurement in enterprise architecture models.

By: González-Rojas, Oscar; López, Alexandra; Correal, Dario. *International Journal of Computer Integrated Manufacturing*. Dec2017, Vol. 30 Issue 12, p1280-1300. 21p. 6 Diagrams, 4 Charts, 1 Graph. Abstract: The authors create a model to measure the complexity associated with enterprise architecture (EA) proposals at the design stage. At this stage, existing methods measure the complexity of business capabilities regardless of their leveraging business and technical architectures. Measuring their complexity at the implementation level restricts product changes and generates higher costs. Our proposed model analyses the detailed EA design, thereby improving enterprise modelling and integration. **First**, we define the EA functionalities and dependencies to measure the complexity of a project roadmap. Next, we extend an existing mathematical formula to measure complexity in terms of these functionalities and dependencies at three additional and increasingly granular levels of detail: gap analysis model, target architecture design and implementation architecture design. We apply our multilevel complexity measurement to EA case studies. The **results** show that our model provides a more accurate complexity measurement compared with existing methods; the complexity effort estimated at the implementation design level has an accuracy between 63% and 94% with respect to the actual roadmap's implementation effort. Our method provides an early predictor of EA reliability, which could enable organisations to better control project scope, time and budget, especially in reuse-based implementations such as service-oriented architectures. [ABSTRACT FROM AUTHOR] DOI: 10.1080/0951192X.2017.1307453. (AN: 125128085), Database: Computer Source

Subjects: INFORMATION & communication technologies; PROJECT management; RISK management in business; GAP analysis (Planning); SERVICE-oriented architecture (Computer science); COMPUTER network architectures

Show all 12 images



[HTML Full Text](#) [PDF Full Text \(1.4MB\)](#) [USPTO Full Text Options](#)

26. **Communication: Innovation & Quality**

By: Tufiez-López, Miguel. Series: Studies in Systems, Decision and Control, v. 154. Cham, Switzerland : Springer, 2019. eBook. Description: This book explores the disruptive changes in the media ecosystem caused by convergence and digitization, and analyses innovation processes in content production, distribution and commercialisation. It has been edited by Professors Miguel Tufiez-López (Universidade de Santiago de Compostela, Spain), Valentín-Alejandro Martínez-Fernández (Universidade da Coruña, Spain), Xosé López-García (Universidade de Santiago de Compostela, Spain), Xosé Rúas-Araújo (Universidade de Vigo, Spain) and Francisco Campos-Freire ... (AN 1847332), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; BUSINESS & ECONOMICS / Industries / Media & **Communications**; COMPUTERS / Interactive & Multimedia; LANGUAGE ARTS & DISCIPLINES / **Communication** Studies; LAW / General; SOCIAL SCIENCE / Media Studies; Information technology; **Communication**--Technological innovations; Telecommunication systems; Telecommunication--Quality control



Full Text Finder

USPTO Full Text Options

27. **Broadband Communications**

By: Kumar, Balaji. Series: McGraw-Hill Series on Computer **Communications**. Edition: Signature ed. New York : McGraw-Hill Professional, 1998. eBook. (AN 2069), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Networking / General; Broadband **communication** systems

PDF Full Text

USPTO Full Text Options

Full Download

Table of Contents

Most Relevant Pages From This eBook

28. Inner source software development: Current thinking and an agenda for future research

By Edison, Henry; Carroll, Noel; Morgan, Lorraine; Conboy, Kieran. In *The Journal of Systems & Software*. May 2020 163 Language: English. DOI: 10.1016/j.jss.2020.110520 Abstract: Highlights •An in-depth review of inner source research reported in the literature to date. •Framework analysis for the inner source software development approach. •Five key themes for further research in inner source. (AN: S0164121220300030), Database: ScienceDirect

Subjects: Inner source; Inner source software development; Research agenda; Systematic literature review



Full Text Finder

USPTO Full Text Options

29. Wireless Technologies : Concepts, Methodologies, Tools and Applications

By: Information Resources Management Association. Hershey, PA : IGI Global. 2012. eBook. (AN 396408), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Mobile & Wireless Communications; TECHNOLOGY & ENGINEERING / Radio; Wireless communication systems; Telecommunication

PDF Full Text

USPTO Full Text Options

Full Download

Table of Contents

Most Relevant Pages From This eBook

30. **Proceedings of the 2nd Workshop on
Communication Security : Cryptography and
Physical Layer Security**

By: Baldi, Marco; Quaglia, Elizabeth A.; Tomasin, Stefano. Series: Lecture Notes in Electrical Engineering, Vol. 447. Cham : Springer, 2018. eBook.

Description: This book focuses on techniques that can be applied at the physical and data-link layers of **communication** systems in order to secure transmissions against eavesdroppers. It discusses topics ranging from information theory-based security to coding for security and cryptography, and presents cutting-edge research and innovative findings from leading researchers. The characteristic feature of all the contributions in this book is their relevance for the practical application of security principles to ... (AN 1555253), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications;
COMPUTERS / Programming / Algorithms; COMPUTERS / Security /
General; Data encryption (Computer science)--Congresses;
Telecommunication systems--Security measures--Congresses; Computer
networks--Security measures--Congresses



Full Text Finder

USPTO Full Text Options

[EBSCO Connect](#) | [Privacy Policy](#) | [A/B Testing](#) | [Terms of Use](#) | [Copyright](#) | [Cookie Policy](#) | [Contact Us](#)

powered by *EBSCOhost*

© 2020 EBSCO Industries, Inc. All rights reserved.

User authentication for devices with touch sensitive elements, such as touch sensitive display screens

S Bayram, AE Dirik, N Memon, U Topkara - US Patent 8,941,466, 2015 - Google Patents

User authentication for devices with touch sensitive elements, such as touch sensitive **display screens**. Download PDF **Info** ... US 8941466 B2 US8941466 B2 US 8941466B2 Authority US United States Prior art keywords **user** signature finger touch **information** computer system ...

☆  Cited by 146 Related articles All 4 versions 

User profiling for selecting user specific voice input processing information

AP Haughay - US Patent 8,682,667, 2014 - Google Patents

This is directed to processing voice inputs received by an electronic device. In particular, this is directed to receiving a voice input and identifying the user providing the voice input. The voice input can be processed using a subset of words from a library used to identify the words ...

☆  Cited by 162 Related articles All 4 versions 

Personalized information retrieval using user-defined profile

VS Dasan - US Patent 5,761,662, 1998 - Google Patents

... **Info** ... More specifically, the present invention relates to a client/server model for **information** retrieval based upon a **user-defined** profile, for example, for ... these resources is filtering the vast amount of **information** which is available in order that a **user** obtain that **information** which is ...

☆  Cited by 889 Related articles All 2 versions 

Personal communication system to send and receive voice data positioning information

ML Obradovich, J Dinkel, M Kent - US Patent 6,148,261, 2000 - Google Patents

... **Info** ... US 6148261 A US6148261 A US 6148261A Authority US United States Prior art keywords map processor map **information information** communicator Prior ... a legal analysis and makes no representation or warranty as to the accuracy of the list.) Silver **State** Intellectual Tech ...

☆  Cited by 634 Related articles All 2 versions 

Dynamic integration of computer generated and real world images

K Abbott, D Newell, J Roberts - US Patent App. 09/879,827, 2002 - Google Patents

... 2002044152 A1 US2002044152 A1 US 2002044152A1 Authority US United States Prior art keywords **information user** recited method ... G02B2027/0112—Head-up **displays** characterised by optical features comprising device for generating colour **display**. G—PHYSICS; ...

☆  Cited by 640 Related articles All 2 versions 

Dynamic information management system and method for content delivery and sharing in content-, metadata- and viewer-based, live social networking among users ...

J Robinson, P Muller, T Noke, TL Lim, W Glausi... - US Patent ..., 2014 - Google Patents

Dynamic information management system and method for content delivery and sharing in content-, metadata- and viewer-based, live social networking among **users** concurrently engaged in the same and/or similar content. Download PDF **Info** ...

☆  Cited by 436 Related articles All 4 versions 

Interactive display device, such as in context-aware environments

I Sands, V Russ - US Patent App. 11/393,636, 2007 - Google Patents

... G09F27/00—Combined visual and audible advertising or **displaying**, eg for public address; G09F2027/001—Comprising a presence or proximity detector ... The technology includes a **display** component (eg, public **display screen**) that **displays** or otherwise presents content to ...

☆  Cited by 111 Related articles All 2 versions 

Detecting and transporting dynamic presence information over a wireless and wireline communications network

A Mukherjee, FF Ozog, CC Chen - US Patent 7,844,055, 2010 - Google Patents

Detecting and transporting **dynamic** presence **information** over a wireless and wireline communications network. Download PDF **Info** ... US 18063602 A US18063602 A US 18063602A US 7844055 B2 US7844055 B2 US 7844055B2 Authority US United States Prior art keywords ...

☆  Cited by 266 Related articles All 4 versions 

Method and apparatus for automatically **determining** and **dynamically** updating **user** preferences in an entertainment system

CD Williams, JMG Iki, AA Shah-Nazaroff... - US Patent ..., 1999 - Google Patents

... an apparatus comprises a storage medium to store **user** preference **information** corresponding to ... agent, communicatively coupled to the storage medium, is operative to **monitor user** interaction with ... 22, 1996, for a Television **Viewing Behavior Monitor by** Jean Goldschmidt, Tony ...

☆  Cited by 766 Related articles All 2 versions 

Automated selection of appropriate **information based** on a computer **user's** context

JO Roberts, D Newell, KH Abbott - US Patent 7,395,507, 2008 - Google Patents

Automated selection of appropriate **information based** on a computer **user's** context. Download

PDF **Info** ... A US43532606 A US 43532606A US 7395507 B2 US7395507 B2 US 7395507B2

Authority US United **States** Prior art keywords **user information** context computer ...

☆  Cited by 502 Related articles All 4 versions 

Combined **fingerprint acquisition** and control device

AW Senior - US Patent 6,400,836, 2002 - Google Patents

... The status flag, along with the finger coordinates extracted at steps 450 and 460, are **transmitted** to the relevant computer software at step 490 ... 22. The system of claim 1 further comprising a data **transmission** circuit for **transmitting** said at least one contact parameter to the ...

☆  Cited by 228 Related articles All 4 versions 

Method and system in a client-server for automatically converting messages **from a first** format to a **second** format compatible with a message retrieving device

ST Segur - US Patent 6,212,550, 2001 - Google Patents

... (d) receiving a **transmit** selected message command **from** one of the one or more subscriber units for selecting a message to be **transmitted** to the ... of claim 14, wherein step (a) further includes the steps of: (a1) receiving a message query; (a2) **transmitting** a greeting ...

☆  Cited by 549 Related articles All 2 versions 

System, method and apparatus for secure **transmission** of confidential information

P Björndahl - US Patent 6,901,241, 2005 - Google Patents

US6901241B2 - System, method and apparatus for secure **transmission** of confidential **information** - Google Patents. System, method and apparatus for secure **transmission** of confidential **information**. Download PDF Info ...

☆  Cited by 188 Related articles All 4 versions 

Using a **first device** to engage in a digital rights management transaction on behalf of a **second device**

A Narin, MA DeMello - US Patent 7,185,363, 2007 - Google Patents

... 6 is a block diagram of an exemplary system in which content may be **acquired**; ... **by** remote processing **devices** that are linked **through** a **communications** network or other data **transmission** medium ... use of the content in the presence of the **first** private key; and, **transmitting** the data ...

☆  Cited by 56 Related articles All 2 versions 

Communication device for **transmitting** or receiving location information and determining relative location information

M Bascobert - US Patent App. 10/364,757, 2004 - Google Patents

... and more particularly, the present invention relates to a **communication device** for **transmitting** or receiving ... as marine radios or CB radios, do not need to be receiving a **transmission** to obtain ... **By** this way, if **multiple** users are **broadcasting** on a broadcast frequency, the user of ...

☆  Cited by 75 Related articles All 2 versions 

Hand held physiological signal **acquisition device**

HL Platt - US Patent 6,730,025, 2004 - Google Patents

... blood glucose, pCO₂, pO₂ and pacemaker pulses, and condition the signals and **transmit** data representing ... the signals into data specific to the signal type prior to **transmitting** the data ... the data **transmitted through** the isolation barrier and prepares the data for **transmission** to an ...

☆  Cited by 96 Related articles All 2 versions 

System and method of secure **information** transfer

R Ziegler - US Patent 7,387,240, 2008 - Google Patents

... created (**Communications** and Data) to support and protect **information** during the **Transmission** process ... **second device** and a **second** encryption key for encrypting the data **transmitted** between the ... data; appending a CRC to the final cryptographic hash; and **transmitting** the final ...

☆  Cited by 65 Related articles All 4 versions 

Methods and systems for performing credit transactions with a wireless **device**

CA Pizarro - US Patent 7,865,448, 2011 - Google Patents

... The **biometric information** is **transmitted from** the wireless **device** to the point-of-sale **device** ... The location-positioning chip is adapted to **transmit** a location-positioning signal **from** the wireless **device** ... The antenna permits wirelessly **transmitting** and receiving electromagnetic signals ...

☆  Cited by 145 Related articles All 4 versions 

Data transmission system using electronic apparatus having a plurality of **transmission** protocols

Y Iijima - US Patent 5,581,708, 1996 - Google Patents

Data transmission system using electronic apparatus having a plurality of **transmission** protocols.Download PDF Info ... means together with a coded signal, eg in the form of personal identification **information**, like personal identification number [PIN] or **biometric** data; ...

☆ 59 Cited by 89 Related articles All 2 versions

Wireless inter-device data processing configured **through** inter-**device** **transmitted** data

R Dua - US Patent 8,244,179, 2012 - Google Patents

US8244179B2 - Wireless inter-device data processing configured **through** inter-**device** **transmitted** data - Google Patents. **Wireless inter-device** data processing configured **through** inter-**device** **transmitted** data. Download PDF Info ...

☆ 59 Cited by 606 Related articles All 4 versions



acquiring static biometric information by a static biometric information ac



Sign in

[All](#)
[News](#)
[Images](#)
[Shopping](#)
[More](#)
[Settings](#)
[Tools](#)

About 31,100 results (0.70 seconds)

www.google.com/patents/US7361919
Multi-biometric finger sensor having different selectivities ...

Grant - Filed Sep 3, 2004 - Issued Apr 22, 2008 - Dale R. Setlak - Authentec, Inc.
 The sensor may also include a second set of biometric sensing pixels on the integrated circuit. The characteristics of a sample fingerprint may be compared to information for reference fingerprints already stored in a memory of the electronic device. ... static ... of a first embodiment of an electronic device including an infrared finger sensor in accordance with the present invention. ... acquired ...

[Overview](#) · [Related](#) · [Discuss](#)
www.google.com/patents/US9552525
Noise reduction in biometric images

Grant - Filed Sep 8, 2013 - Issued Jan 24, 2017 - Michal Breznicky - Apple Inc.
 One calibration image characterizes noise of the biometric sensing device at a first signal level while another calibration image ... where each segment of the biometric image can be acquired by a single sensing element. ... Additionally, the I/O device(s) 406 can include a display that displays information relating to the ...

[Overview](#) · [Related](#) · [Discuss](#)
www.google.com/patents/US7358515
Multi-biometric finger sensor including electric field ...

Grant - Filed Sep 3, 2004 - Issued Apr 15, 2008 - Dale R. Setlak - Authentec, Inc.
 A multi-biometric finger sensor includes a plurality of electric field fingerprint sensing pixels on an integrated circuit. The characteristics of a sample fingerprint may be compared to information for reference fingerprints already stored in a memory of the electronic device. ... static ... is a schematic diagram of a second embodiment of an electronic device including an optical ... acquired ...

[Overview](#) · [Related](#) · [Discuss](#)
www.google.com/patents/US7915601
Electronic device including optical dispersion finger sensor ...

Grant - Filed Sep 3, 2004 - Issued Mar 29, 2011 - Dale R. Setlak - Authentec, Inc.
 The characteristics of a sample fingerprint may be compared to information for reference fingerprints already stored in a memory of the electronic device. ... false matches in one biometric characteristic are uncorrelated to false matches to a second biometric characteristic. ... The illustrated embodiment of the optical dispersion sensor 55 is a static placement sensor. ... acquired ...

[Overview](#) · [Related](#) · [Discuss](#)
www.google.com/patents/US9314193
Biometric apparatus and method for touch-sensitive devices

Grant - Filed Oct 13, 2012 - Issued Apr 19, 2016 - Waleed Sami Haddad - Biogy, Inc.
 The processor is further configured to generate biometric signature ... modern touch screen technology to acquire the patterns of one, two, ... information, a time-dependent pattern is used, not just a simple static finger geometry pattern. ... and a touch sensor of the electronic device is acquired, from which a ...

[Overview](#) · [Related](#) · [Discuss](#)
www.google.com/patents/US7214953
Multi-biometric finger sensor including optical dispersion ...

Grant - Filed Sep 3, 2004 - Issued May 8, 2007 - Dale R. Setlak - Authentec, Inc.
 A multi-biometric finger sensor may include at least one optical dispersion ... The characteristics of a sample fingerprint may be compared to information for ... other finger biometric sensor may operate based upon static placement of the ... 2 is a schematic diagram of a second embodiment of an electronic device ... acquired ...

[Overview](#) · [Related](#) · [Discuss](#)
www.google.com/patents/EP3035243A1?ci=en
Method of updating biometric feature pattern and electronic ...

App - Filed Dec 14, 2015 - Published Jun 22, 2016 - Young-Eun Han - Samsung Electronics Co., Ltd.
 The method includes acquiring a plurality of biometric images. ... Among the various pieces of biometric information, a security method using ... another aspect of the present disclosure, an electronic device for updating a ... includes a sensor device configured to receive an input of a biometric image. ... acquisition ... Static ...

[Overview](#) · [Related](#) · [Discuss](#)

www.google.com/patents/US20160162673

Technologies for learning body part geometry for use in ...

 App - Filed Dec 5, 2014 - Published Jun 9, 2016 - Gershom Kutliroff - Gershom Kutliroff
The Biometric authentication processes utilizing the technologies are also described. ...
static ... a biometric reference template, whereas a second electronic device is ...
biometric information obtained from at least a second body part of a ... then be acquired,
e.g., with a depth sensor such as a depth camera.
[Overview](#) · [Related](#) · [Discuss](#)

www.google.com/patents/US6193153

Method and apparatus for non-intrusive biometric capture

 Grant - Filed Apr 13, 1998 - Issued Feb 27, 2001 - Francis Lambert - Francis Lambert
Another drawback to present biometric capture devices include that they are ... use of the
computer or restrict the access to information on a network, and the like. ... peripheral
device, and a biometric acquisition portion for acquiring biometric ... comprise semi-
reflective patterns, that reflect light between static light sources ...
[Overview](#) · [Related](#) · [Discuss](#)

www.google.com/patents/US7197168

Method and system for biometric image assembly from multiple ...

 Grant - Filed Jul 12, 2002 - Issued Mar 27, 2007 - Anthony P. Russo - Atrua Technologies,
Inc
Capability to adjust sensor settings during acquisition process to obtain ... that any
fingerprint processing system can use information if when called upon to do so.
[Overview](#) · [Related](#) · [Discuss](#)

1 2 3 4 5 6 7 8 9 10 Next

[Help](#) [Send feedback](#) [Privacy](#) [Terms](#)



performing communication with a second communication interface relati



Sign in

All
 News
 Images
 Videos
 More

[Settings](#)
[Tools](#)

About 960,000 results (0.51 seconds)

www.google.com/patents/CN103647577B?cl=en

通信系统、通信设备和通信设备的控制方法 Method of controlling a communication ...

Grant - Filed Jun 2, 2009 - Issued Jan 20, 2016 - 森友和夫 - 佳能株式会社
 The present invention includes the **communication** system with DSC and ... the connection status in the **first communication** layers, perform the authentication ... relates ... and **second communication** equipment via **communication interface**, wherein, ... **second communication** layer when the result of described authentication ...
[Overview](#) · [Related](#) · [Discuss](#)

www.google.com/patents/US20130124651

File-based application programming interface providing ...

App. - Filed Nov 11, 2011 - Published May 16, 2013 - Michael T. Kain - Michael T. Kain
 In particular, the present disclosure relates to a file-based API providing ... in a **second** aspect, a method of securing data at a **communication interface** of a ...
[Overview](#) · [Related](#) · [Discuss](#)

www.google.com/patents/US20130267205

Communication apparatus, communication system, notification ...

App. - Filed Jun 6, 2013 - Published Oct 10, 2013 - Kazuo Takada - Sony Corporation
 ... unit having a **second communication** range wider than the **first communication** range; ... CROSS REFERENCES TO RELATED APPLICATIONS ... Then, after the **second communication** unit receives a result of authentication ... a notification unit which carries out a notification for a user, to perform a function as a ... **interface** ...
[Overview](#) · [Related](#) · [Discuss](#)

www.google.com/patents/WO2010048350A1?cl=en

Card credential method and system

App. - Filed Oct 21, 2009 - Published Apr 29, 2010 - G. Wouter Habraken - Habraken G Wouter
 In one embodiment, a device includes a **first interface**, a **second interface**, a memory ... to perform a challenge-response authentication interaction via the **first interface**. ... Another result may be that security-relevant communications through the ...
[Overview](#) · [Related](#) · [Discuss](#)

www.google.com/patents/US20150350197

Signature verification system, communication device, ...

App. - Filed May 14, 2015 - Published Dec 3, 2015 - Kenjiro Ike - Panasonic Intellectual Property Management Co., Ltd.
 The communication device derives a first hash value from a first random number, ... using a secret key of the **communication device** with respect to the **second** hash value, ... unit 58 includes, for example, a serial I/F or a **communication interface**. ... before the device authentication sequence to be described later is performed.
[Overview](#) · [Related](#) · [Discuss](#)

www.google.com/patents/US8218459

Topology hiding of a network for an administrative interface ...

Grant - Filed Dec 20, 2007 - Issued Jul 10, 2012 - Brian Stucker - Genbrand US LLC
 A **communications session signaling interface** refers to a signaling ... between **first** and **second** networks through the **communications** ... The Diameter Protocol defines messages that are used for performing authentication, authorization, and ... While the invention has been disclosed with respect to a limited ...
[Overview](#) · [Related](#) · [Discuss](#)

www.google.com/patents/US9622088

Communication system, communication device, program and ...

Grant - Filed Dec 18, 2015 - Issued Apr 11, 2017 - Ryo Sawai - Sony Corporation
 There is provided a **communication system** comprising: a **first communication** ... on the sensed data transmitted from the **second communication** device, ... result ... node and the **secondary communication** authentication node is performed as a ... an output device 42, a storage device 44, a **communication interface** (I/F) 46 ...
[Overview](#) · [Related](#) · [Discuss](#)

www.google.com/patents/US20070191056

Controlling alternative communication pathway utilization in ...



App. - Filed May 24, 2006 - Published Aug 16, 2007 - Jeyhan Karaoguz - Jeyhan Karaoguz
CROSS-REFERENCE TO RELATED APPLICATIONS/INCORPORATION BY ... 2 is a block diagram illustrating a second exemplary mobile communication device ... in an exemplary configuration where the first communication interface module ... performing general communication tasks in a mobile communication device.

[Overview](#) - [Related](#) - [Discuss](#)

www.google.com/patents/WO2014122076A2?cl=en

Body coupled communication system



App. - Filed Jan 31, 2014 - Published Aug 14, 2014 - Sotir Filipov OUZOUNOV - Koninklijke Philips N.V.
The first and second body coupled communication interfaces (114, 134) ... the body of the user results, up to some degree, in a secure communication technology ... This basically means that the physical communication is performed via the ... it is only relevant that the authenticator at least needs the key to authenticate the ...

[Overview](#) - [Related](#) - [Discuss](#)

www.google.com/patents/US6836814

Mobile communication terminal device



Grant - Filed Mar 19, 2001 - Issued Dec 28, 2004 - Toshiaki Takaoka - Kabushiki Kaisha Toshiba
CROSS-REFERENCE TO RELATED APPLICATIONS ... a first external interface and a second external interface for sending and receiving a ... and the communication terminal device itself via the first external interface and the second ... performs ... device based on the authentication result by the authentication means; and.

[Overview](#) - [Related](#) - [Discuss](#)

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

[Help](#) [Send feedback](#) [Privacy](#) [Terms](#)



1. Patent Application Titled 'Information Processing Device, Application Software Start-Up System, And Application Software Start-Up Method' Published Online (USPTO 20190362061)

In: **Information Technology Newsweekly**. Dec 17, 2019, 2279; NewsRX LLC
Language: English. Abstract: 2019 DEC 17 (VerticalNews) -- By a News Reporter-Staff News Editor at **Information Technology Newsweekly** --
According to news reporting originating from Washington, D.C., by
VerticalNews journalists, a patent application [...] (AN: edsgcl.608720217).
Database: Gale General OneFile

Subjects: Japan; Software quality; Software -- Methods; Software --
Intellectual property; Control equipment -- Methods; Control equipment --
Intellectual property

 [Full Text Finder](#) [USPTO Full Text Options](#)

2. **Mind Your Mind: EEG-Based Brain-Computer Interfaces and Their Security in Cyber Space.**

By: LANDAU, OFIR; PUZIS, RAMI; NISSIM, NIR. *ACM Computing Surveys*, Feb2020, Vol. 53 Issue 1, p1-38, 38p Abstract: A brain-computer interface (BCI) system is a system that leverages brainwave information acquired by a designated brain monitoring device to interact with a computerized system. Over the past 40 years, many BCI applications have been developed in a variety of domains, from entertainment to medical field and even to computer security mechanisms. Until now, the development of BCI systems has focused on improving their accuracy, functionality, and ease of use, and not enough effort and attention has been invested in securing these systems and the sensitive data they acquire. In this article, we present the principles of brain activity data acquisition, with a special focus on EEG, and we present a taxonomy of BCI applications and domains. We also provide a comprehensive survey that covers eight possible attacks aimed at BCI systems. For each BCI application, we created an ecosystem and data and attack flow-diagram, which comprehensively describes the roles and interactions of the players associated with the BCI application and presents the most vulnerable vectors and components within its ecosystem; we identified gaps between existing security solutions and the presented attacks and vulnerabilities. Finally, we provide several concrete suggestions for improving the security of BCI systems in cyber-space. [ABSTRACT FROM AUTHOR]; DOI: 10.1145/3372043; (AN 141670891), Database: Applied Science & Technology Source

Subjects: Brain-computer interfaces; Internet security; Acquisition of data; Security systems; Systems development; Electroencephalography; Wired Telecommunications Carriers; Internet Publishing and Broadcasting and Web Search Portals; Security Systems Services (except Locksmiths); Brain

[PDF Full Text \(6.2MB\)](#) [USPTO Full Text Options](#)

3. ELAKA: Energy-Efficient and Lightweight Multi-Server Authentication and Key Agreement Protocol Based on **Dynamic Biometrics**.

By: Liu, Xiaoxue; Li, Yanping; Qu, Juan; Lu, Laifeng. *Wireless Personal Communications*, Jun2018, Vol. 100 Issue 3, p767-785, 19p Abstract: Authentication and key agreement (AKA) provides flexible and convenient services. Most traditional AKA protocols are designed to apply in single-server environment, where a user has to register at different servers to access different types of network services and the user have to remember or manage a large number of usernames and passwords. Later, multi-server AKA protocols resolve the repeated registration problem of single-server AKA protocols, where a user can access different servers to get different services using a single registration and the same username and password. Recently, in 2015, Lu et al proposed a light-weight ID based authentication and key agreement protocol for multi-server architecture, referred to as LAKA protocol. They claimed their protocol can overcome all shortcomings which existed in Xue et al's protocol. Unfortunately, our further research shows that LAKA protocol still suffers from server spoofing attack, stolen smart card attack etc. To overcome the weakness of LAKA protocol, an energy-efficient and lightweight authentication and key agreement protocol for multi-server architecture is proposed (abbreviated to ELAKA). The ELAKA protocol not only provides the security features declared by LAKA protocol, but also has some other advantages. First, the ELAKA protocol can realize authentication and key agreement just by three handshakes with extremely low **communication** cost and computation cost between users and servers, which can achieve a delicate balance of security and performance. Second, ELAKA protocol can enable the user enjoy the remote services with privacy protection. Finally the ELAKA protocol is proved secure against known possible attacks by using BAN logic. As a result, these features make ELAKA protocol is very suitable for computation-limited mobile devices (such as smartphone, PAD, tablets) in comparison to other related existing protocols. [ABSTRACT FROM AUTHOR]; DOI: 10.1007/s11277-018-5348-7; (AN 129610872), Database: Applied Science & Technology Source

Subjects: **Biometric** identification; Phishing; Computer security; Key agreement protocols (Computer network protocols); False personation

[HTML Full Text](#) [PDF Full Text](#) (1004KB)

[USPTO Full Text Options](#)

4. Efficient and Secure **Biometric**-Based User Authenticated Key Agreement Scheme with Anonymity.

By: Kang, Dongwoo; Jung, Jaewook; Kim, Hyoungshick; Lee, Youngsook; Won, Dongho. *Security & Communication Networks*, 6/20/2018, p1-14, 14p
Abstract: At present, a number of users employ an authentication protocol so as to enjoy protected electronic transactions in wireless networks. In order to establish an efficient and robust the transaction system, numerous researches have been conducted relating to authentication protocols. Recently, Kaul and Awasthi presented an user authentication and key agreement scheme, arguing that their scheme is able to resist various types of attacks and preserve diverse security properties. However, this scheme possesses critical vulnerabilities. First, the scheme cannot prevent two kinds of attacks, including off-line password guessing attacks and user impersonation attacks. Second, user anonymity rule cannot be upheld. Third, session key can be compromised by an attacker. Fourth, there is high possibility that the time synchronization trouble occurs. Therefore, we suggest an upgraded version of the user authenticated key agreement method that provides enhanced security. Our security and performance analysis shows that compared, to other associated protocols, our method not only improves the security level but also ensures efficiency. [ABSTRACT FROM AUTHOR]; DOI: 10.1155/2018/9046064; (AN 130253394), Database: Applied Science & Technology Source

Subjects: Biometric identification; Computer access control; **Information & communication** technologies; Cryptography; Passwords (Computers)

[HTML Full Text](#) [PDF Full Text](#) (2.9MB) [USPTO Full Text Options](#)

5. Context-aware access control and anonymous authentication in WBAN

By Arfaoui, Amel; Boudia, Omar Rafik Merad; Kribeche, Ali; Senouci, Sidi-Mohammed; Hamdi, Mohamed. In *Computers & Security*. January 2020 88 Language: English. DOI: 10.1016/j.cose.2019.03.017 Abstract: The emergence of the Internet of Things (IoT) as the next generation megatrend has paved the way for pervasive, ubiquitous and proficient healthcare monitoring systems. In the diverse kinds of networks, Wireless Body Area Network (WBAN) has been perceived as one of the most promising wireless sensor technologies for improving healthcare services thanks to its potential for continuous and real-time monitoring of health conditions. However, the open nature of wireless **communication** introduces wide security and privacy concerns as personal health **information** could be exposed to unauthorized parties or even malicious adversaries. Furthermore, in such a **dynamic** and heterogeneous environment where the context conditions continuously and frequently change, adaptive and context-aware solutions become mandatory to satisfy burgeoning security and privacy requirements. Therefore, it is indispensable to adaptively secure the extra-body **communication** between the smart portable device held by the WBAN client and the healthcare providers while considering the **dynamic** context changes. In this paper, we propose a context-aware access control and anonymous authentication approach based on a secure and efficient Hybrid Certificateless Signcryption (H-CLSC) scheme. Particularly, it incorporates the merits of Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) and Identity-Based Broadcast Signcryption (IBBSC) in order to meet the security requirements and provide adaptive contextual privacy. From a security perspective, the proposed mechanism achieves confidentiality, integrity, anonymity, context-aware privacy, key escrow resistance, public verifiability, and ciphertext authenticity. Performance analysis proves the efficiency and the effectiveness of the H-CLSC scheme compared to benchmark schemes in terms of functional security, storage, **communication**, and computational cost. (AN: S0167404818304802), Database: ScienceDirect

Subjects: IoT; WBAN; Certificateless signcryption; Anonymous authentication; Context-aware authorization



Full Text Finder

USPTO Full Text Options

6. LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment

By Wazid, Mohammad; Das, Ashok Kumar; Bhat K, Vivekananda; Vasilakos, Athanasios V.. In *Journal of Network and Computer Applications*. 15 January 2020 150 Language: English. DOI: 10.1016/j.jnca.2019.102496 Abstract: Internet of Things (IoT) becomes a new era of the Internet, which consists of several connected physical smart objects (i.e., sensing devices) through the Internet. IoT has different types of applications, such as smart home, wearable devices, smart connected vehicles, industries, and smart cities. Therefore, IoT based applications become the essential parts of our day-to-day life. In a cloud-based IoT environment, cloud platform is used to store the data accessed from the IoT sensors. Such an environment is greatly scalable and it supports real-time event processing which is very important in several scenarios (i.e., IoT sensors based surveillance and monitoring). Since some applications in cloud-based IoT are very critical, the information collected and sent by IoT sensors must not be leaked during the communication. To accord with this, we design a new lightweight authentication mechanism in cloud-based IoT environment, called LAM-CIoT. By using LAM-CIoT, an authenticated user can access the data of IoT sensors remotely. LAM-CIoT applies efficient "one-way cryptographic hash functions" along with "bitwise XOR operations". In addition, fuzzy extractor mechanism is also employed at the user's end for local biometric verification. LAM-CIoT is methodically analyzed for its security part through the formal security using the broadly-accepted "Real-Or-Random (ROR)" model, formal security verification using the widely-used "Automated Validation of Internet Security Protocols and Applications (AVISPA)" tool as well as the informal security analysis. The performance analysis shows that LAM-CIoT offers better security, and low communication and computation overheads as compared to the closely related authentication schemes. Finally, LAM-CIoT is evaluated using the NS2 network simulator for the measurement of network performance parameters that envisions the impact of LAM-CIoT on the network performance of LAM-CIoT and other schemes. (AN: S108480451930356X), Database: ScienceDirect

Subjects: Internet of Things (IoT); Cloud computing; Authentication; Key agreement; Security; AVISPA simulation



Full Text Finder

USPTO Full Text Options

7. An approach to develop the smart health using Internet of Things and authentication based on biometric technology

By Hamidi, Hodjat. In *Future Generation Computer Systems*. February 2019 91:434-449 Language: English. DOI: 10.1016/j.future.2018.09.024 Abstract: Internet of things is a new pattern in wireless communications of things. The basic theory of IoT is the comprehensive presence of different kinds of things in surrounding environment. The three main dimensions of data security in the Internet are integration, privacy and availability. One of the major tools for maintaining the security of Internet medical things is biometric technology. Biometric systems are used in different fields of the smart healthcare. In this regard, we also need a means for identifying people's identity based on their physical characteristics; the use of biometric data is absolutely critical for IoT functions. Considering this emerging pattern, everything integrated will connect to a virtual chain of connected things with address in the dynamic world of networks. Given the importance of secure connections of things to the Internet and access to them, biometric features are used as identifiers; because they cannot be borrowed, bought, forgotten and they are very difficult to forge or copy. The smart healthcare and IoT resulted in the emergence of a new standard in the applications of biometric data. In this paper, we present a new standard for applying biometric technology to develop smart healthcare using IoT which includes high capacity to access data in addition to being easy to use. In this paper, we reached a more secure way of accessing IoT based on biometrics and fast identity standard by which we can expect significant advances in smart healthcare systems. (AN: S0167739X18313517), Database: ScienceDirect

Subjects: Internet of Things (IoT); Biometric; Data protection standard; Identifiers; Smart healthcare



Full Text Finder

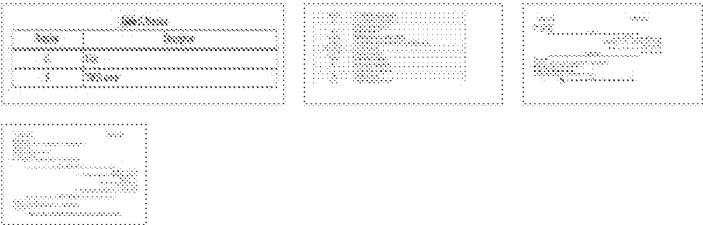
USPTO Full Text Options

8. Robust **Biometric**-based Anonymous User Authenticated Key Agreement Scheme for Telecare Medicine **Information Systems**.

By: Jaewook Jung; Jongho Moon; Dongho Won. *KSII Transactions on Internet & Information Systems* , Jul2017, Vol. 11 Issue 7, p3720-3746, 27p, 4 Diagrams, 11 Charts Abstract: At present, numerous hospitals and medical institutes have implemented Telecare Medicine **Information Systems** (TMIS) with authentication protocols to enable secure, efficient electronic transactions for e-medicine. Numerous studies have investigated the use of authentication protocols to construct efficient, robust health care services, and recently, Liu et al. presented an authenticated key agreement mechanism for TMIS. They argued that their mechanism can prevent various types of attacks and preserve a secure environment. However, we discovered that Liu et al.'s mechanism presents some vulnerabilities. **First**, their mechanism uses an improper identification process for user **biometrics**; second, the mechanism is not guaranteed to protect against server spoofing attacks; third, there is no session key verification process in the authentication process. As such, we describe how the above-mentioned attacks operate and suggest an upgraded security mechanism for TMIS. We analyze the security and performance of our method to show that it improves security relative to comparable schemes and also operates in an efficient manner. [ABSTRACT FROM AUTHOR]; DOI: 10.3837/tiis.2017.07.023; (AN 125005081), Database: Applied Science & Technology Source

Subjects: Medicine **information** services; Medical **communication**; **Biometric** identification; Medical protocols; Medical care

Show all 15 images



PDF Full Text (9.2MB) USPTO Full Text Options

9. Optimized in-network authentication against pollution attacks in software-defined-networked data networking

By Boussaha, Ryma; Challal, Yacine; Bouabdallah, Abdelmadjid; Bessedik, Malika. In *Journal of Information Security and Applications*. February 2020 50 Language: English. DOI: 10.1016/j.jisa.2019.102409 Abstract: The exponential growth of multimedia content in today's Internet traffic and the increasing need of bandwidth-consuming or location-independent services motivated the research community to design a viable replacement for the current IP-based Internet architecture. Named Data Networking or NDN is a novel network architecture that uses universal in-network caching and routing by name functionalities to deliver content efficiently and to improve service quality. Network coding benefits named data networking with its inherent algebraic structure and the maximum flow rates performance it achieves in multicast. With network coding, the content can be requested via multiple interfaces thus improving significantly content delivery efficiency. However, it is vulnerable to pollution attacks, which can cause a crucial degradation of network bandwidth. In this paper, we propose an efficient and optimized authentication technique for a content distribution NDN architecture based on network coding. Our solution uses homomorphic signature mechanism, which allows intermediate nodes to verify the authenticity of flows to overcome the pollution problem without having access to content. We formulate NDNAuth, an optimal coding and homomorphic signature scheme as a MIP problem. Furthermore, we show how to leverage Software Defined Networking to provide seamless implementation of the proposed solution. We measure the processing overhead and the dynamic system security state based on three metrics: (1) defence power; (2) threat severity and (3) system vulnerability. Finally, we discuss how to minimize the computational cost of coding and signature scheme operations. Experimentation results prove the efficiency of the proposed coding scheme, which achieves better performance than conventional NDN with random coding especially in terms of transmission cost and security. (AN: S2214212619302790), Database: ScienceDirect

Subjects: Named data networking; Network coding; Software defined networking; Homomorphic signature



Full Text Finder

USPTO Full Text Options

10. **Handbook of Green Information and Communication Systems**

By: Woungang, Isaac; Anpalagan, Alagan; Obaidat, Mohammad S.
Amsterdam : Academic Press. 2013. eBook. Description: This book gives a comprehensive guide on the fundamental concepts, applications, algorithms, protocols, new trends and challenges, and research results in the area of **Green Information and Communications Systems**. It is an invaluable resource giving knowledge on the core and specialized issues in the field, making it highly suitable for both the new and experienced researcher in this area. Key Features: Core research topics of green **information and communication** systems are covered from a network ... (AN 485200), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Signals & Signal Processing; SCIENCE / Environmental Science; Sustainable engineering--Handbooks, manuals, etc; Telecommunication--Environmental aspects--Handbooks, manuals, etc; Telecommunication--Energy conservation--Handbooks, manuals, etc

[PDF Full Text](#) [USPTO Full Text Options](#) [Full Download](#)
[Table of Contents](#) [Most Relevant Pages From This eBook](#)

11. Grand challenges for ambient intelligence and implications for design contexts and smart societies.

By: Strelitz, Norbert; Charitos, Dimitris; Kaptein, Maurits; Böhlen, Marc.
Journal of Ambient Intelligence & Smart Environments, 2019, Vol. 11 Issue 1, p87-107, 21p Abstract: This paper highlights selected grand challenges that concern especially the social and the design dimensions of research and development in Ambient Intelligence (Aml) and Smart Environments (SmE). Due to the increasing deployment and usage of 'smart' technologies determining a wide range of everyday life activities, there is an urgent need to reconsider their societal implications and how to address these implications with appropriate design methods. The paper presents four perspectives on the subject grounded in different approaches. First, introducing and reflecting on the implications of the 'smart-everything' paradigm, the resulting design trade-offs and their application to smart cities. Second, discussing the potential of non-verbal communication for informing the design of spatial interfaces for Aml design practices. Third, reflecting on the role of new data categories such as 'future data' and the role of uncertainty and their implications for the next generation of Aml environments. Finally, debating the merits and shortfalls of the world's largest professional engineering community effort to craft a global standards body on ethically aligned design for autonomous and intelligent systems. The paper benefits from taking different perspectives on common issues, provides commonalities and relationships between them and provides anchor points for important challenges in the field of ambient intelligence. [ABSTRACT FROM AUTHOR]; DOI: 10.3233/AIS-180507; (AN 134294073), Database: Applied Science & Technology Source

Subjects: Artificial intelligence; Computer interfaces; Systems design; Data science; Nonverbal communication

[HTML Full Text](#) [PDF Full Text](#) (226KB)

[USPTO Full Text Options](#)

12. **Biometric-Based Attendance Tracking System for Education Sectors: A Literature Survey on Hardware Requirements.**

By: Hoo, Seng Chun; Ibrahim, Haidi. *Journal of Sensors*. 9/15/2019, p1-25. 25p. Abstract: The application of **biometric** recognition in personal authentication enables the growth of this technology to be employed in various domains. The implementation of **biometric** recognition systems can be based on physical or behavioral characteristics, such as the iris, voice, fingerprint, and face. Currently, the attendance tracking system based on **biometric** recognition for education sectors is still underutilized, thus providing a good opportunity to carry out interesting research in this area. As evidenced in a typical classroom, educators tend to take the attendance of their students by using conventional methods such as by calling out names or signing off an attendance sheet. Yet, these types of methods are proved to be time consuming and tedious, and sometimes, fraud occurs. As a result, significant progress had been made to mark attendance automatically by making use of **biometric** recognition. This progress enables a new and more advanced **biometric**-based attendance system being developed over the past ten years. The setting-up of **biometric**-based attendance systems requires both software and hardware components. Since the software and hardware sections are too broad to be discussed in one paper, this literature survey only provides an overview of the types of hardware used. Emphasis is then placed on the microcontroller platform, **biometric** sensor, **communication** channel, database storage, and other components in order to assist future researchers in designing the hardware part of **biometric**-based attendance systems. [ABSTRACT FROM AUTHOR] DOI: 10.1155/2019/7410478. (AN: 138630860), Database: Computers & Applied Sciences Complete

Subjects: Educational literature; Microcontrollers; Attendance; School attendance; Hardware

[HTML Full Text](#) [PDF Full Text \(1.9MB\)](#) [USPTO Full Text Options](#)

13. **Cybersecurity challenges in vehicular communications**

By El-Rewini, Zeinab; Sadatsharan, Karthikeyan; Selvaraj, Daisy Flora; Plathottam, Siby Jose; Ranganathan, Prakash. In *Vehicular Communications*. January 2019 Language: English. DOI: 10.1016/j.vehcom.2019.100214 Abstract: As modern vehicles are capable to connect to an external infrastructure and Vehicle-to-Everything (V2X) communication technologies mature, the necessity to secure communications becomes apparent. There is a very real risk that today's vehicles are subjected to cyber-attacks that target vehicular communications. This paper proposes a three-layer framework (sensing, communication and control) through which automotive security threats can be better understood. The sensing layer is made up of vehicle dynamics and environmental sensors, which are vulnerable to eavesdropping, jamming, and spoofing attacks. The communication layer is comprised of both in-vehicle and V2X communications and is susceptible to eavesdropping, spoofing, man-in-the-middle, and sybil attacks. At the top of the hierarchy is the control layer, which enables autonomous vehicular functionality, including the automation of a vehicle's speed, braking, and steering. Attacks targeting the sensing and communication layers can propagate upward and affect the functionality and can compromise the security of the control layer. This paper provides the state-of-the-art review on attacks and threats relevant to the communication layer and presents countermeasures. (AN: S221420961930261X), Database: ScienceDirect

Subjects: Cyber-physical systems; Security; Vehicle safety; Cyber-attacks; Vehicle-to-vehicle



Full Text Finder

USPTO Full Text Options

14. **SUBBASE: An Authentication Scheme for Wireless Sensor Networks Based on User Biometrics.**

By: Riaz, Rabia; Gillani, Noor-ul-Ain; Rizvi, SanamShahla; Shokat, Sana; Kwon, Se Jin. *Wireless Communications & Mobile Computing*, 4/4/2019, p1-11, 11p Abstract: To keep a network secure, a user authentication scheme that allows only authenticated users to access network services is required. However, the limited resources of sensor nodes make providing authentication a challenging task. We therefore propose a new method of security for a wireless sensor network (WSN). Our technique, Secure User Biometric Based Authentication Scheme (SUBBAsE), is based on the user biometrics for WSNs. It achieves a higher security level as well as improved network performance. This solution consists of easy operations and light computations. Herein, the proposed technique is evaluated and compared with previous existing techniques. This scheme increases the performance of the network by reducing network traffic, defending against DOS attacks, and increasing the battery life of a node. Consequently, the functionality and performance of the entire network is improved. [ABSTRACT FROM AUTHOR]; DOI: 10.1155/2019/6370742; (AN 135732106), Database: Applied Science & Technology Source

Subjects: Wireless sensor networks; Network performance; Denial of service attacks; **Biometric** identification; Telecommunication; All Other Telecommunications; Telecommunications Resellers; **Communication** Equipment Repair and Maintenance; Other telecommunications

[HTML Full Text](#) [PDF Full Text \(1.5MB\)](#) [USPTO Full Text Options](#)

15. Securing internet of medical things systems:
Limitations, issues and recommendations

By Yaacoub, Jean-Paul A.; Noura, Mohamad; Noura, Hassan N.; Salman, Ola; Yaacoub, Elias; Couturier, Raphaël; Chehab, Ali. In *Future Generation Computer Systems*. April 2020 105:581-606 Language: English. DOI: 10.1016/j.future.2019.12.028 Abstract: Traditional health-care systems suffer from new challenges associated with the constant increase in the number of patients. In order to address this issue, and to increase the accuracy, reliability, efficiency, and effectiveness of the health-care domain, the Internet of Medical Things (IoMT) was proposed. IoMT can be considered as an enhancement and investment to respond more effectively and efficiently to patients' needs. However, IoMT suffers from different issues and challenges such as the lack of security and privacy measures, in addition to the necessary training and awareness. In this paper, we highlight the importance of implementing the right security measures and the required training skills, in order to enhance the immunity of IoMT against cyber-attacks. Moreover, we review the main IoMT security and privacy issues, and the existing security solutions. These solutions are classified as cryptographic or non-cryptographic. Then, the different solutions are analyzed and compared in terms of computational complexity and required resources. It is important to note that the security measures for IoMT exhibit a trade-off between the security level and the system performance, especially in the rise of digital healthcare v4.0 era. Next, we discuss the appropriate security solutions such as lightweight cryptographic algorithms, and protocols that attempt to reduce the overhead in terms of computations and resources. This leads to the conclusion that there is a need to design an efficient intrusion detection/prevention system that cooperates with **dynamic** shadow honeypots. Finally, we propose a security solution, which is divided into five different layers to detect and prevent attacks, in addition to reducing/correcting the damage of these known attacks and preserving the patients' privacy. However, it should be noted that zero-day attacks and exploits are still the main challenging issue that surrounds IoMT. (AN: S0167739X19305680), Database: ScienceDirect

Subjects: Healthcare; IoMT; Medical cyber physical systems; Medical devices



Full Text Finder

USPTO Full Text Options

16. Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks

By Santos-González, Iván; Rivero-García, Alexandra; Burmester, Mike; Munilla, Jorge; Caballero-Gil, Pino. In *Information Systems*. February 2020 88 Language: English. DOI: 10.1016/j.is.2019.101423 Abstract: Several three-party password authenticated key exchange (3-PAKE) protocols have recently been proposed for heterogeneous wireless sensor networks (HWSN). These are efficient and designed to address security concerns in ad-hoc sensor network applications for a global Internet of Things framework, where a user may request access to sensitive information collected by resource-constrained sensors in clusters managed by gateway nodes. In this paper we first analyze three recently proposed 3-PAKE protocols and discuss their vulnerabilities. Then, based on Radio Frequency Identification technologies we propose a novel 3-PAKE protocol for HWSN applications, with two extensions for additional security features, that is provably secure, efficient and flexible. (AN: S0306437918305234), Database: ScienceDirect

Subjects: Password authenticated key exchange; Heterogeneous wireless sensor networks; Provable security



Full Text Finder

USPTO Full Text Options

17. A Lightweight Secure User Authentication and Key Agreement Protocol for Wireless Sensor Networks.

By: Mo, Jiaqing; Chen, Hang. *Security & Communication Networks*, 12/16/2019, p1-18, 18p Abstract: Wireless sensor networks (WSNs) have great potential for numerous domains of application because of their ability to sense and understand unattended environments. However, a WSN is subject to various attacks due to the openness of the public wireless channel. Therefore, a secure authentication mechanism is vital to enable secure communication within WSNs, and many studies on authentication techniques have been presented to build robust WSNs. Recently, Lu et al. analyzed the security defects of the previous ones and proposed an anonymous three-factor authenticated key agreement protocol for WSNs. However, we found that their protocol is vulnerable to some security weaknesses, such as the offline password guessing attack, known session-specific temporary information attack, and no session key backward secrecy. We propose a lightweight security-improved three-factor authentication scheme for WSNs to overcome the previously stated weaknesses. In addition, the improved scheme is proven to be secure under the random oracle model, and a formal verification is conducted by ProVerif to reveal that the proposal achieves the required security features. Moreover, the theoretical analysis indicates that the proposal can resist known attacks. A comparison with related works demonstrates that the proposed scheme is superior due to its reasonable performance and additional security features. [ABSTRACT FROM AUTHOR]; DOI: 10.1155/2019/2136506; (AN 140476816), Database: Applied Science & Technology Source

Subjects: Wireless sensor networks; Passwords (Computers); Wireless channels; Data integrity

[HTML Full Text](#) [PDF Full Text \(1.7MB\)](#) [USPTO Full Text Options](#)

18. Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment

By Bera, Basudeb; Chattaraj, Durbadal; Das, Ashok Kumar. In *Computer Communications*. 1 March 2020 153:229-249 Language: English. DOI: 10.1016/j.comcom.2020.02.011 Abstract: In recent years, the Internet of Drones (IoD) has emerged as an important research topic in the academy and industry because it has several potential applications ranging from the civilian to military. In IoD environment, several drones, called Unmanned Aerial Vehicles (UAVs), are deployed in different flying zones that communicate each other to exchange crucial information, and then the information are collected by the Ground Station Server (GSS). All the drones and the GSS are registered with a central trusted authority, Control Room (CR) prior to their deployment. Since the drones and the GSS communicate over open channel (e.g., wireless medium), there are security and privacy issues in the IoD environment. To handle such issues, in this paper we introduce a blockchain-based access control scheme in the IoD environment that allows secure communication among the drones, and also among the drones and the GSS. Secure data gathered by the GSS form transactions, and those transactions are made into the blocks. The blocks are finally added in the blockchain by the cloud servers connected with the GSS via the Ripple Protocol Consensus Algorithm (RPCA) in a peer-to-peer cloud server network. Once the blocks are added into the blockchain, the transactions containing in the blocks cannot be altered, modified or even removed. We provide all sorts of security analysis including formal security under the random oracle model, informal security and simulation-based formal security verification to assure that the proposed scheme can resist various potential attacks with high probability needed in an IoD environment. In addition, a meticulous comparative analysis among the proposed scheme and other closely related existing schemes shows that our scheme offers more functionality attributes and better security, and also low communication and computation costs as compared to other schemes. (AN: S0140366419318377), Database: ScienceDirect

Subjects: Internet of Drones (IoD); Access control; Blockchain; Consensus; Security; AVISPA

 Full Text Finder  USPTO Full Text Options

19. Location of three-dimensional movement for a human using a wearable multi-node instrument implemented by wireless body area networks

By Wang, Dong; Huang, Qingcheng; Chen, Xin; Ji, Lijuan. In *Computer Communications*. 1 March 2020 153:34-41 Language: English. DOI: 10.1016/j.comcom.2020.01.070 Abstract: A wireless human body local area network is a wireless network composed of lightweight, wearable or implantable sensor nodes that sense various physiological parameters of the human body. This paper introduces the key technologies and characteristics of wireless sensor networks and the research status of node localization, analyzes the wireless sensor network localization algorithms and their performance evaluation indicators, and conducts in-depth research on wearable 3D node localization algorithms. The 3D positioning algorithm uses static beacon nodes to achieve the 3D positioning of public nodes. The positioning accuracy and positioning rate depend on the number of beacon nodes, and the number of beacon nodes increases, which increases network costs and energy consumption. Aiming at the spatiotemporal correlation between motion data collected by multiple sensors in a wireless human local area network, an RSSI-based multi-node 3D motion monitoring auxiliary algorithm is used, including the planning of wearable device motion trajectories. Throughout the positioning process, the workflow belongs to the public node and involves the format of the relevant information packet. The 3D wearable multi-node positioning algorithm based on RSSI is a distance-dependent distributed positioning algorithm. The public node uses the RSSI ranging method to obtain the distance during the two-stage positioning process, and then uses the three-dimensional multilateral positioning method to perform its own calculation. (AN: S014036641931477X), Database: ScienceDirect

Subjects: Wireless body area network; Motion recognition; Wearable device; Three-dimensional motion monitoring; Multi-node



Full Text Finder

USPTO Full Text Options

20. A General Architecture for Multiserver Authentication Key Agreement with Provable Security.

By: Zhang, Yunru; Luo, Min; Choo, Kim-Kwang Raymond; He, Debiao.
Security & Communication Networks, 11/6/2018, p1-9, 9p Abstract: In a typical single-server architecture, when a user wishes to access multiple servers to obtain different services, the user needs to register with every single server. This results in multiple identities and password pairs. To eliminate the limitation of the user having to possess and remember multiple identities and password pairs, a number of multiserver authentication protocols have been proposed where a user only needs to register once. However, most existing protocols are subsequently found to be insecure and this topic remains one of the ongoing research interests. Thus, in this paper, we present a multiserver authentication key agreement protocol. We then demonstrate the security of the protocol under the random oracle model, as well as the practicality of the protocol in terms of low computation and communication costs, minimal storage requirements, and operation costs. [ABSTRACT FROM AUTHOR]; DOI: 10.1155/2018/2462901; (AN 132881603), Database: Applied Science & Technology Source

Subjects: Information & communication technologies; Computer architecture; Computer access control; Elliptic curve cryptography; Key agreement protocols (Computer network protocols)

[HTML Full Text](#) [PDF Full Text \(1.7MB\)](#) [USPTO Full Text Options](#)

21. RAMHU: A New Robust Lightweight Scheme for Mutual Users Authentication in Healthcare Applications.

By: Al-Zubaidie, Mishail; Zhang, Zhongwei; Zhang, Ji. *Security & Communication Networks*, 3/17/2019, p1-26, 26p Abstract: Providing a mechanism to authenticate users in healthcare applications is an essential security requirement to prevent both external and internal attackers from penetrating patients' identities and revealing their health data. Many schemes have been developed to provide authentication mechanisms to ensure that only legitimate users are authorised to connect, but these schemes still suffer from vulnerable security. Various attacks expose patients' data for malicious tampering or destruction. Transferring health-related data and information between users and the health centre makes them exposed to penetration by adversaries as they may move through an insecure channel. In addition, previous mechanisms have suffered from the poor protection of users' authentication information. To ensure the protection of patients' information and data, we propose a scheme that authenticates users based on the information of both the device and the legitimate user. In this paper, we propose a Robust Authentication Model for Healthcare Users (RAMHU) that provides mutual authentication between the server and clients. This model utilizes an Elliptic Curve Integrated Encryption Scheme (ECIES) and PHOTON to achieve strong security and good overall performance. RAMHU relies on multiple-pseudonym, physical address, and one-time password mechanisms to authenticate legitimate users. Moreover, extensive informal and formal security analysis with the automated validation of Internet security protocols and applications (AVISPA) tool demonstrate that our model offers a high level of security in repelling a wide variety of possible attacks. [ABSTRACT FROM AUTHOR]; DOI: 10.1155/2019/3263902; (AN 135370515), Database: Applied Science & Technology Source

Subjects: Biometric identification; Passwords (Computers); Computer security; Data security; Internet security; Internet Publishing and Broadcasting and Web Search Portals; Wired Telecommunications Carriers; Computer systems design and related services (except video game design and development); Other Computer Related Services

[HTML Full Text](#) [PDF Full Text \(5MB\)](#) [USPTO Full Text Options](#)

22. Secure IoT **communications** for smart healthcare monitoring system

By El Zouka, Hesham A.; Hosni, Mustafa M.. In *Internet of Things*. January 2018 Language: English. DOI: 10.1016/j.iot.2019.01.003 Abstract: Healthcare monitoring systems in hospitals and other health centers have witnessed throughout the last decade a tremendous growth and wireless healthcare monitoring devices with various technologies have become of great interest in many nations around the world. The proposed paper aims at integrating artificial intelligence technology, such as the neural networks and fuzzy system in a secure healthcare monitoring system in order to enable the system to work as a smart healthcare model that decides the priority by itself depending on the collected health parameters from the sensor nodes. The proposed model consists of a trust environment that is responsible for collecting authenticated physiological data from patient's body which is then sent through GSM module to Azure IoT Hub where raw data is converted into linguistic representation, with the help of logic-based algorithm, which is trained in fuzzy-based inference system (FBIS) to get the status of the patient. The proposed system, then, provides reliable, accurate, secure and real-time patient monitoring. The following sections describe how the FBIS can be integrated with a secure healthcare monitoring system to get the states of the patient and send it to the medical advisory for the preliminary precautions. (AN: S254266051830088X), Database: ScienceDirect

Subjects: Internet of Things (IoT); health monitoring; sensors; security; trust; fuzzy



Full Text Finder

USPTO Full Text Options

23. Mapping the rise of digital mental health technologies: Emerging issues for law and society

By Gooding, Piers. In *International Journal of Law and Psychiatry*. November-December 2019 67 Language: English. DOI: 10.1016/j.ijlp.2019.101498 Abstract: The use of digital technologies in mental health initiatives is expanding, leading to calls for clearer legal and regulatory frameworks. However, gaps in knowledge about the scale and nature of change impede efforts to develop responsible public governance in the early stages of what may be the mass uptake of 'digital mental health technologies'. This article maps established and emerging technologies in the mental health context with an eye to locating major socio-legal issues. The paper discusses various types of technology, including those designed for information sharing, communication, clinical decision support, 'digital therapies', patient and/or population monitoring and control, bio-informatics and personalised medicine, and service user health informatics. The discussion is organised around domains of use based on the actors who use the technologies, and those on whom they are used. These actors go beyond mental health service users and practitioners/service providers, and include health and social system or resource managers, data management services, private companies that collect personal data (such as major technology corporations and data brokers), and multiple government agencies and private sector actors across diverse fields of criminal justice, education, and so on. The mapping exercise offers a starting point to better identify cross-cutting legal, ethical and social issues at the convergence of digital technology and contemporary mental health practice. (AN: 50160252719300950), Database: ScienceDirect



Full Text Finder

USPTO Full Text Options

24. Taxonomy and analysis of security protocols for Internet of Things

By Das, Ashok Kumar; Zeadally, Sherali; He, Debiao. In *Future Generation Computer Systems*. December 2018 89:110-125 Language: English. DOI: 10.1016/j.future.2018.06.027 Abstract: The Internet of Things (IoT) is a system of physical as well as virtual objects (each with networking capabilities incorporated) that are interconnected to exchange and collect information locally or remotely over the Internet. Since the communication often takes place over the Internet, it is vulnerable to various security threats in an IoT environment. We first discuss essential security requirements that are needed to secure IoT environment. We also discuss the threat model and various attacks related to the IoT environment. We then present a taxonomy of security protocols for the IoT environment which includes important security services such as key management, user and device authentication, access control, privacy preservation, and identity management. We also present a comparative study of recently proposed IoT-related state-of-art security protocols in terms of various security and functionality features they support. Finally, we discuss some future challenges for IoT security protocols that need to be addressed in the future. (AN: S0167739X18308112), Database: ScienceDirect

Subjects: Access control; Authentication; Identity management; IoT; Key management; Security; Privacy; Sensing devices

 Full Text Finder USPTO Full Text Options

25. Hunting the Pertinency of Bloom Filter in
Computer Networking and Beyond: A Survey.

By: Patgiri, Ripon; Nayak, Sabuzima; Borgohain, Samir Kumar. *Journal of Computer Networks & Communications* , 2/5/2019, p1-10, 10p Abstract: Bloom filter is a probabilistic data structure to filter a membership of a set. Bloom filter returns "true" or "false" with an error tolerance depending on the presence of the element in the set. Bloom filter is used to boost up the performance of a system using small space overhead. It is extensively used since its inception. The Bloom filter has met wide area of applications. Bloom filter is used in entire computing field irrespective of application and research domain. Bloom filter poses (i) high adaptability, (ii) low memory space overhead as compared to hashing algorithms, (iii) high scalability, and (iv) high performance. In this article, we uncover the application area of Bloom filter in computer networking and its related domain. [ABSTRACT FROM AUTHOR]; DOI: 10.1155/2019/2712417; (AN 134478807), Database: Applied Science & Technology Source

Subjects: Computer networks; Probabilistic databases; Computer storage devices; Computer systems; **Information** networks; Computer Systems Design Services; Computer and peripheral equipment manufacturing; Computer Storage Device Manufacturing; Computer systems design and related services (except video game design and development)

[HTML Full Text](#) [PDF Full Text](#) (1.6MB) [USPTO Full Text Options](#)

26. CLOUD-BASED TRANSACTIONS METHODS
AND SYSTEMS

Patent Application: 16/438178. Filed: June 11, 2019. Published: September 26, 2019. , Database: USPTO Patent Applications

Abstract: Systems and methods provide for **communication** of transaction data that is formatted according to a transaction type that is support by an access device. **First** transaction data may be formatted according to a **first** type of transaction supported by a **first** access device and second transaction data may be formatted according to a second type of transaction supported by a second access device. The **first** transaction data may be **transmitted** over a **first communication** link to the **first** access device and the second transaction data may be **transmitted** to the second access over a second **communication** link.

AN: edspap.20190295063

USPTO Full Text Options

27. A novel motion detecting strategy for rehabilitation
in smart home

By Peng, Tongqian. In *Computer Communications*. 15 January 2020
150:687-695 Language: English. DOI: 10.1016/j.comcom.2019.11.043

Abstract: Recent years have witnessed the flourish in research and development efforts towards clinical rehabilitation systems in smart home applications. One of the most prior is that such systems are needed to provide real-time motion **information** about patients. In this paper, a motion detecting approach is proposed for efficiently understanding the human movement on the foundation of the Internet of Things (IoT) based architecture. Specifically, the detection algorithm is based on the fuzzy neural network (FNN), which learns to detect the variation among different gait phases. The moving phases as well as the instability of the tester are identified for recognition. On the tasks of identifying the subject motion using wearable sensing devices, this model achieves a significant high accuracy. Experimental results prove that the system is feasible for application designs and could be implemented on technological platforms. (AN:

S0140366419312885), Database: ScienceDirect

Subjects: Clinical rehabilitation; IoT based network; Fuzzy neural network; Wearable sensors; Motion detection



Full Text Finder

USPTO Full Text Options

28. Recent progress in tactile sensors and their applications in intelligent systems

By Liu, Yue; Bao, Rongrong; Tao, Juan; Li, Jing; Dong, Ming; Pan, Caofeng.
In *Science Bulletin*. 15 January 2020 65(1):70-88 Language: English. DOI:
10.1016/j.scib.2019.10.021 Abstract: With the rapid development of
intelligent technology, tactile sensors as sensing devices constitute the core
foundation of intelligent systems. Biological organs that can sense various
stimuli play vital roles in the interaction between human beings and the
external environment. Inspired by this fact, research on skin-like tactile
sensors with multifunctionality and high performance has attracted extensive
attention. An overview of the development of high-performance tactile
sensors applied in intelligent systems is systematically presented. First, the
development of tactile sensors endowed with stretchability, self-healing,
biodegradability, high resolution and self-powered capability is discussed.
Then, for intelligent systems, tactile sensors with excellent application
prospects in many fields, such as wearable devices, medical treatment,
artificial limbs and robotics, are presented. Finally, the future prospects of
tactile sensors for intelligent systems are discussed. (AN:
S2095927319306164), Database: ScienceDirect

Subjects: Tactile sensor; Intelligent system; Self-powered capability;
Biodegradability; Self-healing



Full Text Finder

USPTO Full Text Options

29. Blockchain leveraged decentralized IoT eHealth framework

By Uddin, Md. Ashraf; Stranieri, Andrew; Gondal, Iqbal; Balasubramanian, Venki. In *Internet of Things*. March 2020 9 Language: English. DOI: 10.1016/j.iot.2020.100159 Abstract: Blockchain technologies recently emerging for eHealth, can facilitate a secure, decentralized and patient-driven, record management system. However, Blockchain technologies cannot accommodate the storage of data generated from IoT devices in remote patient management (RPM) settings as this application requires a fast consensus mechanism, careful management of keys and enhanced protocols for privacy. In this paper, we propose a Blockchain leveraged decentralized eHealth architecture which comprises three layers: (1) The Sensing layer – Body Area Sensor Networks include medical sensors typically on or in a patient body transmitting data to a smartphone. (2) The NEAR processing layer – Edge Networks consist of devices at one hop from data sensing IoT devices. (3) The FAR processing layer – Core Networks comprise Cloud or other high computing servers). A Patient Agent (PA) software replicated on the three layers processes medical data to ensure reliable, secure and private communication. The PA executes a lightweight Blockchain consensus mechanism and utilizes a Blockchain leveraged task-offloading algorithm to ensure patient's privacy while outsourcing tasks. Performance analysis of the decentralized eHealth architecture has been conducted to demonstrate the feasibility of the system in the processing and storage of RPM data. (AN: S2542660520300020), Database: ScienceDirect

Subjects: Internet of Things; Blockchain; Consensus mechanism; Proof of stake; Patient agent; Fog computing; Edge computing; Cloud; Patient monitoring; eHealth; Fuzzy inference process; Task offloading



Full Text Finder

USPTO Full Text Options

30. Bibliographical review on cyber attacks from a control oriented perspective

By Sánchez, Helem S.; Rotondo, Damiano; Escobet, Teresa; Puig, Vicenç; Quevedo, Joseba. In *Annual Reviews in Control*. 2019 48:103-128
Language: English. DOI: 10.1016/j.arcontrol.2019.08.002 Abstract: This paper presents a bibliographical review of definitions, classifications and applications concerning cyber attacks in networked control systems (NCSs) and cyber-physical systems (CPSs). This review tackles the topic from a control-oriented perspective, which is complementary to **information** or **communication** ones. After motivating the importance of developing new methods for attack detection and secure control, this review presents security objectives, attack modeling, and a characterization of considered attacks and threats presenting the detection mechanisms and remedial actions. In order to show the properties of each attack, as well as to provide some deeper insight into possible defense mechanisms, examples available in the literature are discussed. Finally, open research issues and paths are presented. (AN: S1367578819300288), Database: ScienceDirect

Subjects: Cyber-physical systems; Networked control systems; Cyber attacks; Attack detection; Secure control



Full Text Finder

USPTO Full Text Options

[EBSCO Connect](#) | [Privacy Policy](#) | [A/B Testing](#) | [Terms of Use](#) | [Copyright](#) | [Cookie Policy](#) | [Contact Us](#)

powered by EBSCOhost

© 2020 EBSCO Industries, Inc. All rights reserved.

Biometrics identification module and personal wearable electronics network based authentication and transaction processing

E Kursun, G Fernandez, A Berson... - US Patent ..., 2018 - Google Patents

... identification module may comprise a Personal ID module, a Static and **Dynamic Biometric ID** module ... Electrical signals (such as brain waves, EKG signals, etc.) may be **acquired** through a ... **device(s)**. In one embodiment, **biometrics ID module/device** may also **acquire** data from ...

☆ 99 Cited by 81 Related articles All 4 versions

A survey on touch **dynamics** authentication in mobile **devices**

PS Teh, N Zhang, ABJ Teoh, K Chen - Computers & Security, 2016 - Elsevier

... with other **biometrics** features, such as face and voice **biometrics**, the feature **acquisition** of touch **dynamics** ... This is because the **acquiring** and processing of touch **dynamics** patterns can be carried ... suited to this mode, as touch **dynamics** data can be **acquired** transparently over a ...

☆ 99 Cited by 83 Related articles All 6 versions

Information processing **device**, application software start-up system, and application software start-up method

M Hirabayashi, Y Hashimoto... - US Patent App. 16 ..., 2019 - Google Patents

... **Info** ... US 201916535574 A US201916535574 A US 201916535574A US 2019362061 A1 US2019362061 A1 US 2019362061A1 Authority US United States Prior art keywords **biometric information information** user processing **device dynamic biometric** Prior art date 2019 ...

☆ 99 All 2 versions

Automatic gain amplifier for **biometric sensor device**

HLJ Yeh, EW Cheng, AP Russo - US Patent 6,518,560, 2003 - Google Patents

... printed or written characters or for recognising patterns, eg fingerprints; G06K9/00006—**Acquiring** or recognising ... **Dynamic** finger detection mechanism for a **fingerprint sensor** ... 1999-11-16, Lucent Technologies, Apparatus for correcting fixed column noise in images **acquired** by a ...

☆ 99 Cited by 42 Related articles All 2 versions

Secure network and networked **devices** using **biometrics**

A Russo, P McCoy, T Roske - US Patent App. 10/194,949, 2003 - Google Patents

Secure network and networked **devices** using **biometrics**. Download PDF **Info** ... US 19494902 A US19494902 A US 19494902A US 2003115490 A1 US2003115490 A1 US 2003115490A1 Authority US United States Prior art keywords **biometric biometric data device data** secure ...

☆ 99 Cited by 151 Related articles All 2 versions

Personal authentication system

K Kitagawa, M Satoyama - US Patent 7,375,615, 2006 - Google Patents

... unit 505 for receiving **information** from a location **information** sending office 520 and **acquiring** the location of ... (2) The location/connection **information** thus **acquired** is checked ... a time-axis evaluation and a frequency-axis evaluation by using the **dynamic** weighted coefficient with ...

☆ 99 Cited by 35 Related articles All 4 versions

Combined **fingerprint acquisition** and control **device**

AW Senior - US Patent 6,400,836, 2002 - Google Patents

... would be scanned at 410 and then immediately stored in a **dynamically** accessible memory ... in computer 100, could enable or disable transmission of **acquired fingerprint** image data ... for combined **fingerprint acquisition** for user authentication and for **acquiring** control parameters ...

☆ 99 Cited by 228 Related articles All 4 versions

Authentication gets personal with **biometrics**

J Ortega-Garcia, J Bigun, D Reynolds... - IEEE signal ..., 2004 - IEEE Xplore

... in which signal processing methodology is applied to the **dynamically acquired** time sequences ... ii) feature-based approaches, in which statistical parameters are derived from the **acquired information** ... aspect ratio, center of mass, or horizontal span ratio), global **dynamic** (ie, total ...

☆ 99 Cited by 211 Related articles All 15 versions

Information processing device, application software start-up system, and application software start-up method

M Hirabayashi, Y Hashimoto, K Yoshizawa - US Patent 10,423,769, 2019 - Google Patents
... **Info** ... B2 US10423769 B2 US 10423769B2 US 201415315735 A US201415315735 A US
201415315735A US 10423769 B2 US10423769 B2 US 10423769B2 Authority US United States
Prior art keywords **biometric information device** user state **dynamic biometric** Prior art ...

☆ ⓘ Related articles All 4 versions ⓘ

Method and fingerprint sensing system for acquiring a fingerprint image

E Setterberg, MR Hansen, B Hu, MS Hansen - US Patent 9,971,925, 2018 - Google Patents
... 3a to 3d , it may be of interest to **acquire** a second **fingerprint** image using the ... based on a quality
metric, and. code for selecting at least one of the **acquired fingerprint** images satisfying ... en),
2015-12-14, 2016-12-01, Method and **fingerprint sensing** system for **acquiring a fingerprint** ...

☆ ⓘ Cited by 2 Related articles All 4 versions ⓘ

Biological information acquisition device, method for acquiring biological information, and biometrics device

K Amano, K Shimizu - US Patent 8,144,938, 2012 - Google Patents

... be achieved as well as biological information to be highly accurately and reliably **acquired** ... 7.
A method for **acquiring information** of a biological **body** by irradiating the biological ... A **biometrics device**, comprising: a biological **information acquisition** part to **acquire information** of a ...

☆ 77 Cited by 8 Related articles All 4 versions 🔗

Information fusion in biometrics

AA Ross, AK Jain, K Nandakumar - Handbook of Multibiometrics, 2006 - Springer

... the cost of adding new **sensors** and the additional time required for **acquiring** and processing ... the average processing time since a decision can be made without having to **acquire** all the ... Note that the evidence pertaining to the multiple sources may be **acquired** in a sequential ...

☆ 77 Cited by 261 Related articles All 20 versions 🔗

Biological information acquiring apparatus, biological information acquiring method and biometric authentication apparatus

K Amano, K Shimizu - US Patent 8,570,148, 2013 - Google Patents

... may include a biological **information acquiring** apparatus configured to **acquire** biological **information** ... received light become small, and the quality of the **acquired** biological **information** ... The biological **information acquiring** apparatus 1 receives the reflected light that is reflected ...

☆ 77 Cited by 15 Related articles All 4 versions 🔗

Multivariate Dynamic Biometrics System

D Palti-Wasserman, Y Wasserman - US Patent App. 11/792,318, 2008 - Google Patents

... Eye Tracking **Sensors**; Several technologies may be used for measuring and **acquiring** different types ... The **acquired** data is amplified and digitized (110), and then processed and analyzed (111 ... The track ball can include additional **sensors**, which may **acquire** parameters such as ...

☆ 77 Cited by 70 Related articles All 2 versions 🔗

To a combined fingerprint acquisition and control device

RM Boile, NK Ratha, A Senior - US Patent 6,941,001, 2005 - Google Patents

... G06F21/31—User authentication; G06F21/32—User authentication using **biometric** data, eg ... control **information** for an electronic **device**, said method comprising: **acquiring** through a ... correlations between a multiplicity of small regions of the **acquired fingerprint** images; extracting ...

☆ 77 Cited by 143 Related articles All 2 versions 🔗

Scalable searching of biometric databases using dynamic selection of data subsets

KJ Hanna, HT Hoyos - US Patent 8,364,646, 2013 - Google Patents

... is compared, and (ii) recognition, wherein a separate token is not used, and **user** data is **acquired** on site ... US9489416B2 (en), 2006-03-03, 2012-12-19, Scalable searching of **biometric** databases using **dynamic** selection of ... Mirror system and method for **acquiring biometric** data ...

☆ 77 Cited by 46 Related articles All 4 versions 🔗

Biometrics identification module and personal wearable electronics network based authentication and transaction processing

E Kursun, G Fernandez, A Berson... - US Patent ..., 2018 - Google Patents

... **biometric** identification module may comprise a Personal ID module, a Static and **Dynamic Biometric** ID module ... Electrical signals (such as brain waves, EKG signals, etc.) may be **acquired** through a ... ID module/**device** 180 may be a standalone **device**, and may **acquire** data itself ...

☆ 77 Cited by 81 Related articles All 4 versions 🔗

Garment for measuring physiological signal and system for processing physiological signal

YH Jeong, YJ Jeon, S Shin, YW Jang... - US Patent App. 12 ..., 2010 - Google Patents

... of limiting factors in terms of stably and accurately **acquiring** physiological **information** ... The **first** transmission unit 720 transmits the physiological **information acquired** by the ... 760 is a physiological **information** measurement/analysis module and **acquires** physiological **information** ...

☆ 77 Cited by 75 Related articles All 2 versions 🔗

Personal choice biometric signature

JY Wong - US Patent 7,035,443, 2006 - Google Patents

... or for recognising patterns, eg fingerprints; G06K9/00006—**Acquiring** or recognising ... partial **fingerprint** sequence techniques augments sentinel systems for **gaining** access to ... pairs of proximity **sensors** and accompanying novel software algorithm for **first obtaining** and processing ...

☆  Cited by 284 Related articles All 4 versions **Biometric information acquisition apparatus and biometric authentication apparatus**

H Otsubo, A Sakemoto - US Patent App. 12/402,292, 2009 - Google Patents

... Further, the components necessary for **acquiring biometric information** (the light source 21, the light guide 22, the ... between optical channels, thereby enabling the image pickup **device** 31 to **acquire** clearer vein ... the **fingerprint** image of the finger 96 can be thereby **acquired** by the ...

☆  Cited by 13 Related articles All 2 versions 

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : MAXELL, LTD. Confirmation No.5886
Serial No. : 16/535,574
Filed : August 8, 2019
For : INFORMATION PROCESSING DEVICE, APPLICATION
SOFTWARE START-UP SYSTEM, AND APPLICATION
SOFTWARE START-UP METHOD
Group : 2498
Examiner : Thanhnga B. TRUONG

RESPONSE TO RESTRICTION REQUIREMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

December 16, 2019

Sir:

In response to the Restriction Requirement mailed October 15, 2019, Applicant elects to prosecute Invention I represented by claims 1-11 and claims 19-29. This election is made with traverse.

The Commissioner is hereby authorized to charge any additional payment due to Deposit Account No. 50-1417.

Respectfully submitted,

MATTINGLY & MALUR, PC

/John R. Mattingly/
John R. Mattingly
Reg. No. 30,293
(703) 684-1120

Electronic Acknowledgement Receipt	
EFS ID:	38037719
Application Number:	16535574
International Application Number:	
Confirmation Number:	5886
Title of Invention:	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD
First Named Inventor/Applicant Name:	Masayuki HIRABAYASHI
Customer Number:	24956
Filer:	John Roberts Mattingly
Filer Authorized By:	
Attorney Docket Number:	SEI-10740-02
Receipt Date:	16-DEC-2019
Filing Date:	08-AUG-2019
Time Stamp:	14:26:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response to Election / Restriction Filed	10740-02-RestrictionRequirement.pdf	12516	no	1
			ad706fe2c48254a87f472b0d16cb4692682d15c7		

Warnings:

Information:	
Total Files Size (in bytes):	12516
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.	



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/535,574	08/08/2019	Masayuki HIRABAYASHI	SEI-10740-02

CONFIRMATION NO. 5886

24956
MATTINGLY & MALUR, PC
1800 DIAGONAL ROAD
SUITE 210
ALEXANDRIA, VA 22314

PUBLICATION NOTICE



OC000000112994272

Title: INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD

Publication No. US-2019-0362061-A1

Publication Date: 11/28/2019

NOTICE OF PUBLICATION OF APPLICATION

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

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

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

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

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

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,574	08/08/2019	Masayuki HIRABAYASHI	SEI-10740-02	5886
24956	7590	10/15/2019	EXAMINER	
MATTINGLY & MALUR, PC 1800 DIAGONAL ROAD SUITE 210 ALEXANDRIA, VA 22314			TRUONG, THANHNGA B	
			ART UNIT	PAPER NUMBER
			2498	
			NOTIFICATION DATE	DELIVERY MODE
			10/15/2019	ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail@mmpiaw.com

DETAILED ACTION

1. This action is responsive to the communication filed on August 8, 2019. Claims 1-29 are pending. At this time, claims 1-29 are being restricted.

Notice of Pre-AIA or AIA Status

2. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Election/Restrictions

3. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. **Claims 1-11** are drawn to a system, comprising: a first information processing device including: a dynamic biometric information acquisition sensor that acquires dynamic biometric information from a body of a user; and a first communication interface that transmits the acquired dynamic biometric information; and a second information processing device including: a static biometric information acquisition sensor that acquires static biometric information; a processor that performs user authentication based on the acquired static biometric information and obtains an authentication result; a second communication interface that performs communication relating to the authentication result with the first communication interface and receives the dynamic biometric information transmitted from the first communication interface; and a display screen, wherein the first information processing device: performs communication relating to the authentication result between the first communication interface and the second communication interface and executes an unlock operation to unlock itself in response to the communication relating to the authentication result, acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking, and maintains the unlocked state during a condition that the dynamic biometric information can be acquired, wherein the second information processing device receives the dynamic biometric information via communication between the first communication interface and the second communication interface and the display screen displays information based on a state of the user that is determined using the received dynamic biometric information; **claims 19-29** are drawn to a method, comprising: acquiring dynamic biometric information from a body of a user by a dynamic biometric information

acquisition sensor of a first device; transmitting the acquired dynamic biometric information through a first communication interface of the first device to a second device; acquiring static biometric information by a static biometric information acquisition sensor of the second device; performing user authentication to obtain an authentication result based on the acquired static biometric information; performing communication with a second communication interface relating to the authentication result with the first communication interface and receiving the dynamic biometric information transmitted from the first communication interface; performing communication relating to the authentication result between the first communication interface and the second communication interface and executing an unlock operation to unlock the first device in response to the communication relating to the authentication result, acquiring the dynamic biometric information from the dynamic biometric information acquisition sensor of the first device after unlocking, and maintaining the unlocked state during a condition that the dynamic biometric information can be acquired; receiving the dynamic biometric information by the second device via communication between the first communication interface and the second communication interface; and displaying on a display screen information based on a state of the user that is determined using the received dynamic biometric information, classified in class 726, subclass 5.

II. **Claims 12-18** is drawn to a information processing device, comprising: a dynamic biometric information acquisition sensor that acquires dynamic biometric information from a body of a user; a wireless communication interface is configured to: transmits the acquired dynamic biometric information to another information processing device; and perform communication relating to an authentication result based on static biometric information with the other information processing device; a processor that: executes an unlock operation to unlock the information processing device in response to the communication relating the authentication result; acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking; and maintains the unlocked state during a condition that the dynamic biometric information can be acquired, wherein the wireless communication interface is configured to transmit the dynamic biometric information to the other information processing device via wireless communications such that the dynamic biometric

information is used to determine a state of the user and generate information for display on the other information processing device, and wherein the dynamic biometric information is continuously acquired after the information processing device is unlocked and the wireless communication interface is configured to transmit the dynamic biometric information to the other information processing device continuously or based on starting of an application on the other information processing device; **claims 16-18** are drawn to a method being executed by a first information processing device, comprising: acquiring, by a dynamic biometric information acquisition sensor, dynamic biometric information from a body of a user; wirelessly transmitting the acquired dynamic biometric information to a second information processing device; performing communication relating to an authentication result based on static biometric information with the second information processing device; executing an unlock operation to unlock the first information processing device in response to the communication relating to the authentication result; acquiring the dynamic biometric information from the dynamic biometric information acquisition sensor after the unlocking; and maintaining the unlocked state during a condition that the dynamic biometric information can be acquired, wherein the dynamic biometric information is transmitted to the second information processing device via wireless communications such that the dynamic biometric information is used to determine a state of the user and generate information for display on the second information processing device, and wherein the dynamic biometric information is continuously acquired after the first information processing device is unlocked and the dynamic biometric information is transmitted to the second information processing device continuously or based on starting of an application on the second information processing device, classified in class 713, subclass 186.

4. The inventions are distinct, each from the other because of the following reasons:

Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct if they do not overlap in scope and are not obvious variants, and if it is shown that at least one subcombination is separately usable. In the instant case, **subcombination I** has separate utility such as **a system, comprising**: a first information processing device including: a dynamic

biometric information acquisition sensor that acquires dynamic biometric information from a body of a user; and a first communication interface that transmits the acquired dynamic biometric information; and a second information processing device including: a static biometric information acquisition sensor that acquires static biometric information; a processor that performs user authentication based on the acquired static biometric information and obtains an authentication result; a second communication interface that performs communication relating to the authentication result with the first communication interface and receives the dynamic biometric information transmitted from the first communication interface; and a display screen, wherein the first information processing device: performs communication relating to the authentication result between the first communication interface and the second communication interface and executes an unlock operation to unlock itself in response to the communication relating to the authentication result, acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking, and maintains the unlocked state during a condition that the dynamic biometric information can be acquired, wherein the second information processing device receives the dynamic biometric information via communication between the first communication interface and the second communication interface and the display screen displays information based on a state of the user that is determined using the received dynamic biometric information; **and a method, comprising:** acquiring dynamic biometric information from a body of a user by a dynamic biometric information acquisition sensor of a first device; transmitting the acquired dynamic biometric information through a first communication interface of the first device to a second device; acquiring static biometric information by a static biometric information acquisition sensor of the second device; performing user authentication to obtain an authentication result based on the acquired static biometric information; performing communication with a second communication interface relating to the authentication result with the first communication interface and receiving the dynamic biometric information transmitted from the first communication interface; performing communication relating to the authentication result between the first communication interface and the second communication interface and executing an unlock operation to unlock the first device in response to the communication relating to the authentication result, acquiring

the dynamic biometric information from the dynamic biometric information acquisition sensor of the first device after unlocking, and maintaining the unlocked state during a condition that the dynamic biometric information can be acquired; receiving the dynamic biometric information by the second device via communication between the first communication interface and the second communication interface; and displaying on a display screen information based on a state of the user that is determined using the received dynamic biometric information; **subcombination II** has separate utility such as **an information processing device, comprising**: a dynamic biometric information acquisition sensor that acquires dynamic biometric information from a body of a user; a wireless communication interface is configured to: transmits the acquired dynamic biometric information to another information processing device; and perform communication relating to an authentication result based on static biometric information with the other information processing device; a processor that: executes an unlock operation to unlock the information processing device in response to the communication relating the authentication result; acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking; and maintains the unlocked state during a condition that the dynamic biometric information can be acquired, wherein the wireless communication interface is configured to transmit the dynamic biometric information to the other information processing device via wireless communications such that the dynamic biometric information is used to determine a state of the user and generate information for display on the other information processing device, and wherein the dynamic biometric information is continuously acquired after the information processing device is unlocked and the wireless communication interface is configured to transmit the dynamic biometric information to the other information processing device continuously or based on starting of an application on the other information processing device; **and a method being executed by a first information processing device, comprising**: acquiring, by a dynamic biometric information acquisition sensor, dynamic biometric information from a body of a user; wirelessly transmitting the acquired dynamic biometric information to a second information processing device; performing communication relating to an authentication result based on static biometric information with the second information processing device; executing

an unlock operation to unlock the first information processing device in response to the communication relating to the authentication result; acquiring the dynamic biometric information from the dynamic biometric information acquisition sensor after the unlocking; and maintaining the unlocked state during a condition that the dynamic biometric information can be acquired, wherein the dynamic biometric information is transmitted to the second information processing device via wireless communications such that the dynamic biometric information is used to determine a state of the user and generate information for display on the second information processing device, and wherein the dynamic biometric information is continuously acquired after the first information processing device is unlocked and the dynamic biometric information is transmitted to the second information processing device continuously or based on starting of an application on the second information processing device.

The examiner has required restriction between subcombinations usable together. Where applicant elects a subcombination and claims thereto are subsequently found allowable, any claim(s) depending from or otherwise requiring all the limitations of the allowable subcombination will be examined for patentability in accordance with 37 CFR 1.104. See MPEP § 821.04(a). Applicant is advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application.

5. Restriction for examination purposes as indicated is proper because all these inventions listed in this action are independent or distinct for the reasons given above and there would be a serious search and examination burden if restriction were not required because one or more of the following reasons apply:

(a) the inventions have acquired a separate status in the art in view of their different classification;

(b) the inventions have acquired a separate status in the art due to their recognized divergent subject matter;

(c) the inventions require a different field of search (for example, searching different classes/subclasses or electronic resources, or employing different search queries);

(d) the prior art applicable to one invention would not likely be applicable to another invention;

(e) the inventions are likely to raise different non-prior art issues under 35 U.S.C. 101 and/or 35 U.S.C. 112, first paragraph.

6. Applicant is advised that the reply to this requirement to be complete **MUST** include (i) an election of a invention to be examined even though the requirement may be traversed (37 CFR 1.143) and (ii) identification of the claims encompassing the elected invention.

7. The election of the species may be made with or without traverse. To preserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the election of species requirement, the election shall be treated as an election without traverse. Traversal must be presented at the time of election in order to be considered timely. Failure to timely traverse the requirement will result in the loss of right to petition under 37 CFR 1.144. If claims are added after the election, applicant must indicate which of these claims are readable on the elected invention.

8. Should applicant traverse on the ground that the species are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the species to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the species unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103(a) of the other invention.

9. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Information Disclosure Statement

10. The information disclosure statement (IDS) filed on August 8, 2019 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) B. Truong whose telephone number is 571-272-3858. The examiner can normally be reached on First Shift.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Yin-Chen Shaw can be reached on 571-272-8593. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/THANHNGA B TRUONG/
Primary Examiner, Art Unit 2438

October 9, 2019

<i>Index of Claims</i> 	Application/Control No. 16/535,574	Applicant(s)/Patent Under Reexamination HIRABAYASHI et al.
	Examiner THANHNGA B TRUONG	Art Unit 2498

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

CLAIMS										
☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47										
CLAIM		DATE								
Final	Original	10/09/2019								
	1	÷								
	2	÷								
	3	÷								
	4	÷								
	5	÷								
	6	÷								
	7	÷								
	8	÷								
	9	÷								
	10	÷								
	11	÷								
	12	÷								
	13	÷								
	14	÷								
	15	÷								
	16	÷								
	17	÷								
	18	÷								
	19	÷								
	20	÷								
	21	÷								
	22	÷								
	23	÷								
	24	÷								
	25	÷								
	26	÷								
	27	÷								
	28	÷								
	29	÷								

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	2019-08-08
	First Named Inventor	Masayuki HIRABAYASHI
	Art Unit	
	Examiner Name	
	Attorney Docket Number	SEI-10740-02

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	9111085	B1	2015-08-18	Darmour; Jennifer Amy	
	2	8646060	B1	2014-02-04	Ben Ayed; Mourad	
	3	8543834	B1	2013-09-24	Barra; Hugo B.	
	4	8042061	B1	2011-10-18	Stotts; Benjamin Hunter	
	5	9112709	B1	2015-08-18	Tofigh; Mostafa	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20090083847	A1	2009-03-26	Fadell et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		2019-08-08
	First Named Inventor	Masayuki HIRABAYASHI	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		SEI-10740-02

	2	20100318636	A1	2010-12-16	Matsumura et al.	
	3	20050223234	A1	2005-10-06	McOwan, Peter William	
	4	20140347479	A1	2014-11-27	Givon; Dor	
	5	20110072502	A1	2011-03-24	Song; Zhexuan	
	6	20150035643	A1	2015-02-05	Kursun; Eren	
	7	20080045806	A1	2008-02-21	Keppler; Bernhard	
	8	20080229408	A1	2008-09-18	Dinges; Clemens	
	9	20080288291	A1	2008-11-20	Bartelt; Robert	
	10	20090039241	A1	2009-02-12	Ueki; Hironori	
	11	20150208244	A1	2015-07-23	NAKAO	Corresponds to Foreign Patent Document 13
	12	20130322705	A1	2013-12-05	WONG	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		
Filing Date		2019-08-08
First Named Inventor	Masayuki HIRABAYASHI	
Art Unit		
Examiner Name		
Attorney Docket Number		SEI-10740-02

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2005-293209	JP	A	2005-10-20	NTT Data Corp	English Abstract	
	2	2013-140440	JP	A	2013-07-18	Sharp Corp	English Abstract	
	3	2007-257666	JP	A	2007-10-04	Quality KK	English Abstract	
	4	2010-541046	JP	A	2010-12-24	Apple Inc.	Corresponds to US 20090083847 A1	
	5	2010-170314	JP	A	2010-08-05	Nec Corp	English Abstract	
	6	2009/096561	WO	A1	2009-08-06	Movida Solutions Inc.	Corresponds to US 20100318636 A1	
	7	103605459 w/abs	CN	A	2014-02-26	FUZHOU ROCKSHIP SEMICONDUCTOR CO., LTD.		
	8	1613425 w/abs	CN	A	2005-05-11	NANJING UNIV.		
	9	103744506 w/abs	CN	A	2014-04-23	LESHE ZHIXIN ELECTRONIC SCIENCE & TECH CO., LTD.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number			
	Filing Date		2019-08-08	
	First Named Inventor	Masayuki HIRABAYASHI		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		SEI-10740-02	

10	103716456 w/abs	CN	A	2014-04-09	LIUZHOU IMEHI NETWORK TECHNOLOGY CO., LTD.	
11	103634453 w/abs	CN	A	2014-03-12	SHANGHAI JINGYAN ELECTRONIC TECHNOLOGY CO., LTD.	
12	102655555 w/abs	CN	A	2012-09-05	NEIJING BENY WAVE SCIENCE AND TECHNOLOGY CO., LTD.	
13	2014-71476	JP	A	2014-04-21	KYOCERA CORP	Corresponds to U.S. Publication Document 11
14	2003-58269 w/abs	JP	A	2003-02-28	MITSUBISHI HEAVY IND LTD	

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	International Search Report of PCT/JP2014/065644 dated January 13, 2015	×
	2	Chinese Office Action received in corresponding Chinese Application No. 201480079782.0 dated September 11, 2018	☒
	3	Clarke, N.L., and S.M. Furnell. "A Composite User Authentication Architecture for Mobile Devices." Journal of Information Warfare, vol. 5, no. 2, 2006, pp. 11-29. JSTOR, www.jstor.org/stable/26504070. (Year: 2006)	☐
	4	Japanese Office Action received in corresponding Japanese Application No. 2017-103459 dated February 27, 2018	☒

If you wish to add additional non-patent literature document citation information please click the Add button

Add

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		2019-08-08
	First Named Inventor	Masayuki HIRABAYASHI	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		SEI-10740-02

EXAMINER SIGNATURE			
Examiner Signature	/THANHNGA B TRUONG/	Date Considered	10/09/2019
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.			
¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.			

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		2019-08-08
	First Named Inventor	Masayuki HIRABAYASHI	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		SEI-10740-02

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/John R. Mattingly/	Date (YYYY-MM-DD)	2019-08-08
Name/Print	John R. Mattingly	Registration Number	30,293

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

~~ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.B.T/~~



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,574	08/08/2019	Masayuki HIRABAYASHI	SEI-10740-02	5886
24956	7590	09/10/2019	EXAMINER	
MATTINGLY & MALUR, PC 1800 DIAGONAL ROAD SUITE 210 ALEXANDRIA, VA 22314			PATEL, ASHOKKUMAR B	
			ART UNIT	PAPER NUMBER
			2491	
			NOTIFICATION DATE	DELIVERY MODE
			09/10/2019	ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail@mmpiaw.com

<i>Decision Granting Request for Prioritized Examination (Track I)</i>	Application No. 16/535,574	Applicant(s) HIRABAYASHI et al.	
	Examiner BRIAN W BROWN	Art Unit OPET	AIA (FITF) Status Yes
1. THE REQUEST FILED <u>08 August 2019</u> IS GRANTED . The above-identified application has met the requirements for prioritized examination A. ☒ for an original nonprovisional application (Track I). B. ☐ for an application undergoing continued examination (RCE). 2. The above-identified application will undergo prioritized examination. The application will be accorded special status throughout its entire course of prosecution until one of the following occurs: A. filing a <u>petition for extension of time</u> to extend the time period for filing a reply; B. filing an <u>amendment to amend the application to contain more than four independent claims, more than thirty total claims</u>, or a multiple dependent claim; C. filing a <u>request for continued examination</u> ; D. filing a notice of appeal; E. filing a request for suspension of action; F. mailing of a notice of allowance; G. mailing of a final Office action; H. completion of examination as defined in 37 CFR 41.102; or I. abandonment of the application. Telephone inquiries with regard to this decision should be directed to BRIAN BROWN at (571)272-5338. In his/her absence, calls may be directed to Petition Help Desk at (571) 272-3282.			
/BRIAN W BROWN/ Petitions Examiner, OPET			



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
16/535,574	08/08/2019		3080	SEI-10740-02	29	4

CONFIRMATION NO. 5886

FILING RECEIPT



0000000110553858

24956
MATTINGLY & MALUR, PC
1800 DIAGONAL ROAD
SUITE 210
ALEXANDRIA, VA 22314
UNITED STATES OF AMERICA

Date Mailed: 08/22/2019

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Masayuki HIRABAYASHI, Osaka, JAPAN;
Yasunobu HASHIMOTO, Osaka, JAPAN;
Kazuhiko YOSHIZAWA, Osaka, JAPAN;

Applicant(s)

Maxell, Ltd., Kyoto, JAPAN;

Power of Attorney: The patent practitioners associated with Customer Number 24956

Domestic Priority data as claimed by applicant

This application is a CON of 15/315,735 12/02/2016
which is a 371 of PCT/JP2014/065644 06/12/2014

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 08/20/2019

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/535,574**

Projected Publication Date: 11/28/2019

Non-Publication Request: No

Early Publication Request: No

Title

INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND
APPLICATION SOFTWARE START-UP METHOD

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

page 2 of 4

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

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

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 16/535,574				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	300			
SEARCH FEE (37 CFR 1.16(k), (j), or (m))	N/A	N/A	N/A			N/A	660			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	760			
TOTAL CLAIMS (37 CFR 1.16(i))	29	minus 20 = *	9			x 100 =	900			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4	minus 3 = *	1			x 460 =	460			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL		TOTAL	3080			
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=		x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=		x	=
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=		x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=		x	=
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.										

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	
	Filing Date	2019-08-08
	First Named Inventor	Masayuki HIRABAYASHI
	Art Unit	
	Examiner Name	
	Attorney Docket Number	SEI-10740-02

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	9111085	B1	2015-08-18	Darmour; Jennifer Amy	
	2	8646060	B1	2014-02-04	Ben Ayed; Mourad	
	3	8543834	B1	2013-09-24	Barra; Hugo B.	
	4	8042061	B1	2011-10-18	Stotts; Benjamin Hunter	
	5	9112709	B1	2015-08-18	Tofigh; Mostafa	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20090083847	A1	2009-03-26	Fadell et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		2019-08-08
	First Named Inventor	Masayuki HIRABAYASHI	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		SEI-10740-02

	2	20100318636	A1	2010-12-16	Matsumura et al.	
	3	20050223234	A1	2005-10-06	McOwan, Peter William	
	4	20140347479	A1	2014-11-27	Givon; Dor	
	5	20110072502	A1	2011-03-24	Song; Zhexuan	
	6	20150035643	A1	2015-02-05	Kursun; Eren	
	7	20080045806	A1	2008-02-21	Keppler; Bernhard	
	8	20080229408	A1	2008-09-18	Dinges; Clemens	
	9	20080288291	A1	2008-11-20	Bartelt; Robert	
	10	20090039241	A1	2009-02-12	Ueki; Hironori	
	11	20150208244	A1	2015-07-23	NAKAO	Corresponds to Foreign Patent Document 13
	12	20130322705	A1	2013-12-05	WONG	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		2019-08-08
	First Named Inventor	Masayuki HIRABAYASHI	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		SEI-10740-02

If you wish to add additional U.S. Published Application citation information please click the Add button.								Add
FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2005-293209	JP	A	2005-10-20	NTT Data Corp	English Abstract	
	2	2013-140440	JP	A	2013-07-18	Sharp Corp	English Abstract	
	3	2007-257666	JP	A	2007-10-04	Quality KK	English Abstract	
	4	2010-541046	JP	A	2010-12-24	Apple Inc.	Corresponds to US 20090083847 A1	
	5	2010-170314	JP	A	2010-08-05	Nec Corp	English Abstract	
	6	2009/096561	WO	A1	2009-08-06	Movida Solutions Inc.	Corresponds to US 20100318636 A1	
	7	103605459 w/abs	CN	A	2014-02-26	FUZHOU ROCKSHIP SEMICONDUCTOR CO., LTD.		
	8	1613425 w/abs	CN	A	2005-05-11	NANJING UNIV.		
	9	103744506 w/abs	CN	A	2014-04-23	LESHE ZHIXIN ELECTRONIC SCIENCE & TECH CO., LTD.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number			
	Filing Date		2019-08-08	
	First Named Inventor	Masayuki HIRABAYASHI		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		SEI-10740-02	

10	103716456 w/abs	CN	A	2014-04-09	LIUZHOU IMEHI NETWORK TECHNOLOGY CO., LTD.	
11	103634453 w/abs	CN	A	2014-03-12	SHANGHAI JINGYAN ELECTRONIC TECHNOLOGY CO., LTD.	
12	102655555 w/abs	CN	A	2012-09-05	NEIJING BENY WAVE SCIENCE AND TECHNOLOGY CO., LTD.	
13	2014-71476	JP	A	2014-04-21	KYOCERA CORP	Corresponds to U.S. Publication Document 11
14	2003-58269 w/abs	JP	A	2003-02-28	MITSUBISHI HEAVY IND LTD	

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	International Search Report of PCT/JP2014/065644 dated January 13, 2015	×
	2	Chinese Office Action received in corresponding Chinese Application No. 201480079782.0 dated September 11, 2018	☒
	3	Clarke, N.L., and S.M. Furnell. "A Composite User Authentication Architecture for Mobile Devices." Journal of Information Warfare, vol. 5, no. 2, 2006, pp. 11-29. JSTOR, www.jstor.org/stable/26504070. (Year: 2006)	☐
	4	Japanese Office Action received in corresponding Japanese Application No. 2017-103459 dated February 27, 2018	☒

If you wish to add additional non-patent literature document citation information please click the Add button

Add

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		2019-08-08
	First Named Inventor	Masayuki HIRABAYASHI	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		SEI-10740-02

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.			
¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.			

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		2019-08-08
	First Named Inventor	Masayuki HIRABAYASHI	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		SEI-10740-02

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/John R. Mattingly/	Date (YYYY-MM-DD)	2019-08-08
Name/Print	John R. Mattingly	Registration Number	30,293

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

SPECIFICATION

INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP
SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD

TECHNICAL FIELD

[0001]

The present invention relates to a start-up method of application software used in an information processing device.

BACKGROUND ART

[0002]

A background art of the present technical field, there is JP 2005-293209 A (Patent Document 1). A problem is described in Patent Document 1 as follows. "In an existing biometrics authentication, static biometric information is simply used, and it is possible to verify an authorized user, but reading the user's intension is not performed. For this reason, when the user is involved in a certain crime and threatened and forced to perform an illegal operation by a criminal, although a system is equipped with a biometrics authentication, it is likely that the system is illegally operated, leading to heavy damage."

A solution to this problem is described as follows. "A physical feature information measuring unit that measures

biometric information indicating a physical feature, a biometrics authentication unit that performs user identification based on information of the physical feature measured by the physical feature information measuring unit, an emotional feature information measuring unit that measures biometric information indicating an emotional feature, an emotional biometrics determination unit that determines a user mental state based on information of the emotional feature measured by the emotional feature information measuring unit, and an integrated authentication unit that determines that it is an authorized user and it is an authentication operation according to the user's intension based on information of a user identification result by the biometrics authentication unit and a mental state determination result by the emotional biometrics determination unit are provided."

CITATION LIST

PATENT DOCUMENT

[0003]

Patent Document 1: JP 2005-293209 A

SUMMARY OF THE INVENTION

PROBLEMS TO BE SOLVED BY THE INVENTION

[0004]

In the technique disclosed in Patent Document 1, by using

the emotional biometrics, it is possible to detect a situation in which the user is threatened and forced to perform an illegal operation by a criminal, in addition to an examination of the user authentication performed by the existing biometrics authentication. Further, it is possible to check the "user's will" and the "user's intension" for the operation of the user. However, in an information processing device using a plurality of pieces of application software, checking of the "user's will" and the "user's intension" is not necessarily necessary for all pieces of application software, and there are application software in which no checking is necessary and application software in which additional checking of the "state of the user" is desirable.

[0005]

In this regard, it is an object of the present invention to provide an information processing device and an application software start-up system which are convenient and capable of limiting application software according to the state of the user.

SOLUTIONS TO PROBLEMS

[0006]

In order to solve the above problem, for example, a configuration set forth in a claim is employed. The present invention includes a plurality of mechanisms capable of

solving the above problem, and as an example, provided is an application software start-up method of an information processing device which includes performing user authentication based on static biometric information, determining a state of a user by comparing dynamic biometric information acquired from a body of the user with dynamic biometric information which is measured in advance, and limiting application software to be started according to the determined state of the user based on a permission level which is set to each application software in advance.

EFFECTS OF THE INVENTION

[0007]

According to the present invention, it is possible to provide an information processing device, an application software start-up system, and an application software start-up method which are convenient.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008]

FIG. 1 is a configuration diagram illustrating a communication system including a handheld device according to a first embodiment.

FIG. 2 is a hardware configuration diagram illustrating the handheld device according to the first embodiment.

FIG. 3 is a functional block diagram illustrating the handheld device according to the first embodiment.

FIG. 4 is a flowchart illustrating an application permission operation of the handheld device according to the first embodiment.

FIG. 5A, 5B, 5C illustrate a display screen of the handheld device according to the first embodiment.

FIG. 6 is a configuration diagram illustrating a communication system including a handheld device according to a second embodiment.

FIG. 7 is a hardware configuration diagram illustrating the handheld device according to the second embodiment.

FIG. 8 is a functional block diagram illustrating the handheld device according to the second embodiment.

FIG. 9 is a functional block diagram illustrating the handheld device according to the second embodiment.

FIG. 10 is a flowchart illustrating an application permission operation of the handheld device according to the second embodiment.

FIG. 11A, 11B, 11C illustrate a display screen of the handheld device according to the second embodiment.

FIG. 12 is a flowchart illustrating an application permission operation of a handheld device according to a third embodiment.

FIG. 13 illustrates a display screen of the handheld

device according to the third embodiment.

FIG. 14 is a flowchart illustrating an application permission operation of a handheld device according to a fourth embodiment.

FIG. 15 illustrates a display screen of the handheld device according to the fourth embodiment.

FIG. 16 is a flowchart illustrating an application permission operation of a handheld device according to a fifth embodiment.

FIG. 17 is a flowchart illustrating an application permission operation of a handheld device according to a sixth embodiment.

MODE FOR CARRYING OUT THE INVENTION

[0009]

Hereinafter, exemplary embodiments of the present invention will be described with reference to the appended drawings.

First embodiment

[0010]

FIG. 1 is a configuration diagram illustrating a communication system including a handheld device 1 which is an example of an information processing device used in the present embodiment. The communication system according to the present embodiment is configured with the handheld device 1

worn on the body of the user, a base station 5 of a mobile telephone communication network, a wide area public network 6 such as the Internet, a router 7, and the like.

[0011]

The handheld device 1 is a wristwatch-type handheld device having a communication function and can establish a connection with the base station 5 or the router 7 and acquire various kinds of information from the network 6. The handheld device 1 includes a fingerprint sensor 11 and a touch panel 12 installed on the surface thereof. Although not illustrated, the handheld device 1 includes a heart rate sensor, a blood pressure sensor, a temperature sensor, and the like which are installed on the back surface to come into contact with the wrist when the user wears it. In the present embodiment, the wristwatch-type handheld device is described as the handheld device 1, but the handheld device 1 may be a glasses-type handheld device or a ring-type handheld device. Further, the handheld device 1 may be any other portable digital device. Furthermore, an information processing device which is equipped with a sensor that detects dynamic biometric information may be used, and for example, a personal computer (PC) which is equipped with a temperature detection sensor using infrared rays and capable of detecting a body temperature of the user may be used instead of the handheld device.

[0012]

The base station 5 is a device that performs a relay between the handheld device 1 and the network 6 and can perform transmission and reception of various kinds of information with the handheld device 1. The router 7 has a function of a wireless local area network (LAN) such as wireless fidelity (Wi-Fi) and can be connected to the network 6 via a communication line.

[0013]

FIG. 2 is a hardware configuration diagram illustrating the handheld device 1 of the present embodiment. A central processing unit (CPU) 101 controls the handheld device 1 in general according to a predetermined program. The CPU 101 may be an arbitrary control circuit or a dedicated circuit such as an application specific IC (ASIC).

[0014]

The system bus 102 is a data communication path in which transmission and reception of data are performed between the CPU 101 and the respective units of the handheld device 1.

[0015]

The memory 103 is configured with a read only memory (ROM), a random access memory (RAM), a flash ROM, or the like, and stores a program and various kinds of setting information for controlling the handheld device 1, an application program (hereinafter, referred to as an "application"), biometric

information of the user, and the like.

[0016]

The operation device 104 is an input device used to input an operation instruction to the handheld device 1, and in the present embodiment, the operation device 104 is configured with a touch panel and a button switch which is arranged to be superimposed on a display device 152 (which will be described later). Further, one of the touch panel and the button switch may be arranged. Furthermore, the handheld device 1 may be operated using a keyboard or the like which is connected to an expansion interface (I/F) 105 (which will be described later). Moreover, the handheld device 1 may be operated using a separate information terminal device connected via wired communication or wireless communication. The display device 152 may have the touch panel function.

[0017]

The expansion interface 105 is a group of interfaces for expanding the function of the handheld device 1, and in the present embodiment, the expansion interface 105 is configured with a video/audio interface, a universal serial bus (USB) interface, a memory interface, or the like. The video/audio interface receives a video signal or an audio signal from an external video/audio output device and outputs a video signal or an audio signal to the external video/audio output device. The USB interface establishes a connection with a keyboard or

any other USB device. The memory interface is connected to a memory card or any other memory medium and performs transmission reception of data.

[0018]

The fingerprint sensor 111 is a sensor that detects static biometric information of the user who uses the handheld device 1, and detects a fingerprint pattern when the user touches with a finger, compares the detected fingerprint pattern with a fingerprint pattern of the authorized user registered in the memory 103, and performs user authentication according to whether or not the fingerprint patterns are identical to each other.

[0019]

A heart rate sensor 112, a blood pressure sensor 113, and a temperature sensor 114 are a group of sensors for detecting the dynamic biometric information of the user who wears the handheld device 1, and detects the current state of the user by measuring the heart rate, the blood pressure, the body temperature, and the like through the group of sensors and comparing the heart rate, the blood pressure, the body temperature, and the like which are measured with measured values of the authorized user in the normal state which are registered in the memory 103 in advance. Further, any other sensor may be installed.

[0020]

A global positioning system (GPS) receiver 121, an acceleration sensor 122, a gyro sensor 123, a geomagnetism sensor 124, and a proximity sensor 125 are a group of sensors for detecting the state of the handheld device 1, and it is possible to detect a position, a motion, an inclination, a direction, an approach state of an object therearound, and the like through the group of sensors. Further, any other sensor may be installed.

[0021]

A mobile communication device 131 is configured with an antenna and communication circuits including as an encoding circuit and a decoding circuit, and performs telephone communication (call) and transmission reception of data through wireless communication with the base station 5 of the mobile telephone communication network. The LAN communication device 132 is connected to a wireless communication access point through wireless communication and performs transmission reception of data. A short-range wireless communication device 133 performs wireless communication with a peripheral device in a short range. For example, Bluetooth (registered trademark), infrared rays, Wi-Fi direct, or the like is used as the short-range wireless communication. Each of the LAN communication device 132 and the short-range wireless communication device 133 includes an encoding circuit, a decoding circuit, an antenna, and the like.

[0022]

An audio input device 141 and an audio output device 142 are audio processing devices of the handheld device 1. The audio input device 141 is a microphone and converts a voice of the user or the like into audio data and receives it. The audio output device 142 is a speaker and provides an audio signal to the user of the handheld device 1.

[0023]

A video input device 151 and the display device 152 are video processing devices of the handheld device 1. The video input device 151 is a camera unit that receives video data of a surrounding area or an object by converting light input from a lens into an electrical signal using an electronic device such as a charge coupled device (CCD) sensor or a complementary metal oxide semiconductor (CMOS) sensor. The display device 152 is a display such as a liquid crystal (LC) panel and provides a video signal to the user of the handheld device 1. The display device 152 includes a video RAM (not illustrated) and has a function of display a video based on video data input to the video RAM and performs format conversion, a process of superimposing a menu or other on screen display (OSD) signals, and the like as necessary.

[0024]

The exemplary configuration of the handheld device 1 includes components which are not essential in the present

embodiment, but effects of the present embodiment are obtained even through a configuration having no non-essential components. A component which is not illustrated such as a digital television broadcasting receiving function, an e-money payment function, or the like may be further added.

[0025]

FIG. 3 is a functional block diagram illustrating the handheld device 1 of the present embodiment. Functional blocks of the handheld device 1 are controlled by the control unit 1010.

[0026]

The control unit 1010 operates on the CPU 101 with which the handheld device 1 illustrated in FIG. 2 is equipped, includes a user authentication unit 1011, a state determination unit 1012, a lock control unit 1013, an application start unit 1014, and the like, and controls a memory 1030, a static biometric information acquisition unit 1110, a dynamic biometric information acquisition unit 1120, a communication unit 1310, or the like based on an instruction given from a user interface 1040 such that the static biometric information and the dynamic biometric information are acquired, stored, and compared, the handheld device 1 is locked or unlocked, or an application starts.

[0027]

The user interface 1040 is configured with the operation

device 104, the audio input device 141, the audio output device 142, the video input device 151, the display device 152, and the like which are illustrated in FIG. 2, and presents the user with various kinds of information and transfers the instruction of the user to the control unit 1010.

[0028]

The static biometric information acquisition unit 1110 is configured with the fingerprint sensor 111 and the like which are illustrated in FIG. 2 and detects a fingerprint and the like which are the static biometric information of the user who uses the handheld device 1.

[0029]

The dynamic biometric information acquisition unit 1120 is configured with the heart rate sensor 112, the blood pressure sensor 113, the temperature sensor 114, and the like which are illustrated in FIG. 2, and measures the heart rate, the blood pressure, the body temperature, and the like which are the dynamic biometric information of the user who wears the handheld device 1.

[0030]

The communication unit 1310 is configured with the mobile communication device 131, the LAN communication device 132, the short-range wireless communication device 133, and the like which are illustrated in FIG. 2 and performs acquisition of an application and transmission reception of various kinds

of data.

[0031]

The memory 1030 is configured with the memory 103 and the like which are illustrated in FIG. 2, and stores static biometric information 1031, dynamic biometric information 1032, an application 1033, a permission level table 1034 which is a table of levels at which applications are permitted to start, and the like, in addition to the program and various kinds of setting information for controlling the handheld device 1.

[0032]

The static biometric information 1031 is, for example, a fingerprint of the authorized user acquired through the static biometric information acquisition unit 1110. Before the handheld device 1 is used, the static biometric information of the authorized user is registered in advance.

[0033]

The dynamic biometric information 1032 is, for example, the heart rate, the blood pressure, and the body temperature of the user acquired through the dynamic biometric information acquisition unit 1120. When the handheld device 1 is used, for example, the dynamic biometric information of the user in the normal state is measured and registered.

[0034]

The application 1033 is an application program acquired through the communication unit 1310 or an application program

which is pre-installed. A plurality of application programs can be registered, and an application permission level can be registered in the permission level table 1034 in association with each application program.

[0035]

The user authentication unit 1011 determines whether or not the user is an authorized user by comparing the static biometric information acquired through the static biometric information acquisition unit 1110 when the handheld device 1 is used with the static biometric information 1031. When the user is authenticated to be the authorized user, the lock control unit 1013 is controlled such that the handheld device 1 is unlocked.

[0036]

The lock control unit 1013 is controlled by the user authentication unit 1011 such that the lock control unit 1013 unlocks the handheld device 1, and, for example, when the user interface 1040 is not operated for a certain period of time, the lock control unit 1013 locks the handheld device 1. Further, even when the state determination unit 1012 is determined to be in a sleep state, the lock control unit 1013 locks the handheld device 1.

[0037]

The state determination unit 1012 determines the state of the user by comparing the dynamic biometric information

acquired through the dynamic biometric information acquisition unit 1120 when the handheld device 1 is used with the dynamic biometric information 1032, and controls the lock control unit 1013 and the application start unit 1014. For example, when the user is determined to be in the sleep state, the lock control unit 1013 is controlled such that the lock control unit 1013 locks the handheld device 1. Further, when the user is determined to be in the normal state, all applications are set to enter a startable state, and when the user is determined to be in a stress state, applications that can be started are limited. Applications to be limited are registered in the permission level table 1034. A start permission level of each application may be decided in advance and may be registered by the user through the user interface 1040.

[0038]

An application to be started is not limited to the application 1033 stored in the memory 1030, and an application on the network 6 may be started through the communication unit 1310.

[0039]

FIG. 4 is a flowchart illustrating an application permission operation of the handheld device 1 of the present embodiment. This flowchart illustrates a process of performing the user authentication through the handheld device 1, checking the state of the user, and limiting an application to

be started according to the state of the user. First, the static biometric information is detected, and the user authentication is performed. The static biometric information acquisition unit 1110 acquires the static biometric information, and the user authentication unit 1011 performs the user authentication as to whether or not the acquired static biometric information is identical to the static biometric information 1031 which is registered in advance by comparing the acquired static biometric information with the static biometric information 1031 (S401). For example, the fingerprint serving as the static biometric information is detected, the user authentication is performed, and when the detected fingerprint is determined to be identical to the registered fingerprint, the lock control unit 1013 unlocks the handheld device 1 (S402), and the application start unit 1014 permits a start of an application of the permission level 1 (S403).

[0040]

For example, the application of the permission level 1 is an application that does not relate to information of the user him/herself and has no particular problem even when it is used by anyone else such as a clock application, a web browser, a map application, a camera application, a weather forecast application, a music application, a calculator application, a dictionary application, a game application, and a navigation

application. The permission level of each application is registered in the permission level table 1034.

[0041]

A display example of a screen of the handheld device 1 at this time is illustrated in FIG. 5A. The clock application, the web browser, the map application, the calculator application, and the dictionary application are the applications of the permission level 1 and thus are in the startable state, and the other applications have a different icon color which indicates that they are in the non-startable state.

[0042]

The user authentication may be performed through any other biometric authentication such as a vein authentication, a face authentication, an iris authentication, or a retina authentication, in addition to the fingerprint authentication, and for example, when the handheld device 1 is worn on the wrist, the user authentication may be performed through the vein authentication for the part on which the handled device 1 is worn, so that a situation in which anyone else wears the handheld device 1 and pretends to be the authorized user can be prevented. Alternatively, the unlocking operation may be performed by inputting a passcode, and a pattern lock may be released by the trajectory of the finger.

[0043]

Generally, there is no difference between a period of time in which the static biometric information for the fingerprint authentication, the vein authentication, the face authentication, the iris authentication, the retina authentication, or the like is acquired and a period of time in which the passcode is input, and a period of time taken until the application of the permission level 1 enters the startable state is about several seconds.

[0044]

Then, the dynamic biometric information is detected, and the state of the user is determined. The state of the user is determined such that the dynamic biometric information acquisition unit 1120 acquires the dynamic biometric information, and the state determination unit 1012 compares the acquired dynamic biometric information with the dynamic biometric information 1032 that is registered in advance (S404).

[0045]

For example, the heart rate, the blood pressure, and the body temperature which are the dynamic biometric information are measured in the normal state and registered in the dynamic biometric information 1032, the dynamic biometric information acquisition unit 1120 measures the heart rate, the blood pressure, and the body temperature, and when the heart rate, the blood pressure, and the body temperature are equal to or

less than lower limit values in the normal state, the sleep state is determined. Further, for example, when the heart rate and the blood pressure are equal to or larger than upper limit values in the normal state, the stress state is determined, and a state which corresponds to neither the sleep state nor the stress state is determined to be the normal state.

[0046]

Generally, a period of time in which the dynamic biometric information such as the heart rate, the blood pressure, the body temperature, the brain wave, or the amount of sweating is acquired is longer than a period of time in which the static biometric information is acquired, and a period of time taken until applications of permission levels 2 and 3 (which will be described later) enter the startable state is about several tens of seconds. For this reason, acquisition of the dynamic biometric information may start at the same time as when acquisition of the static biometric information starts, or the dynamic biometric information may be constantly acquired, and the state determination may be performed based on the biometric information obtained for previous 30 seconds.

[0047]

First, the process is switched according to whether or not the state of the user is the sleep state (S405). When the state of the user is determined to be the sleep state, the

handheld device 1 is locked (S410), and the process ends (the permission level 0). For example, when the user is asleep in a station, a park, or the like, although another person causes the handheld device 1 to touch the finger of the user and perform the fingerprint authentication, if the heart rate, the blood pressure, and the body temperature are equal to or less than the lower limit values in the normal state, the state of the user is determined to be the sleep state, and thus the handheld device 1 can be locked.

[0048]

When the state of the user is determined not to be the sleep state, the process is switched according to whether or not the state of the user is the stress state (S406). When the state of the user is determined to be the stress state, the applications of the permission levels 1 and 2 are permitted to be started (S407).

[0049]

For example, the application of the permission level 2 is an application that relates to the user him/herself and is considered to have a problem when it is used by anyone else such as a schedule application, a mail application, a photo application, a telephone application, or an address book application. The application of the permission level 2 is an application which is considered to have no particular problem regardless of the state of the user when the user is the

authorized user. A display example of a screen of the handheld device 1 at this time is illustrated in FIG. 5B. In addition to the fact that the applications of the permission level 1 are in the startable state, the schedule application and the mail application are the applications of the permission level 2 and thus are in the startable state, and the other applications have a different icon color which indicates that they are in the non-startable state.

[0050]

When the state of the user is determined not to be the stress state (determined to be the normal state), all applications of the permission levels 1 to 3 are permitted to be started (S408).

[0051]

For example, the application of the permission level 3 is an application that relates to information of the user him/herself and is considered to have a big problem when it is used by anyone else such as an e-money application or an online banking application. The application of the permission level 3 is an application which is considered to have a problem depending on the state of the user even when the user is the authorized user.

[0052]

For example, when the user is panicked and unable to make conscious determination due to a bank transfer fraud or the

like or when the user is coercive to perform an operation by another person, if the heart rate and the blood pressure are equal to or larger than the upper limit values in the normal state, the state of the user is determined to be the stress state, and the e-money application, the online banking application, and the like can be set not to be started.

[0053]

FIG. 5C illustrates a display example of the screen of the handheld device 1 when all applications are permitted to be started. In addition to the fact that the application of the permission level 1 and the application of the permission level 2 are in the startable state, the e-money application and the online banking application are the applications of the permission level 3 and thus are in the startable state, and it is indicated that all applications are in the startable state.

[0054]

Then, the process is switched according to whether or not a predetermined period of time has elapsed while the user does not perform an operation (S409). When a predetermined period of time (for example, 10 seconds) has elapsed, the handheld device 1 is locked (S410), and the process ends.

[0055]

When a predetermined period of time has not elapsed, the process returns to step S404, and the process is continued. For example, when the state of the user is determined to be

the stress state, and the application of the permission level 3 enters the non-startable state, if the state of the user returns to the normal state later, all applications enter the startable state. Thereafter, when the state of the user is determined to be the stress state again, the application of the permission level 3 enters the non-startable state, and when the state of the user is determined to be the sleep state, the handheld device 1 is locked.

[0056]

The permission level of each application may be decided in advance by the handheld device 1 or may be set to be changed by the user.

[0057]

The upper limit values and the lower limit values of the heart rate, the body temperature, and the blood pressure in the normal state may be decided in advance by the handheld device 1, but when the heart rate, the body temperature, and the blood pressure of the user are measured and learned, and the upper limit values and the lower limit values are obtained based on them, more accurate determination can be performed.

[0058]

Commonly, in the sleep state, the heart rate, the blood pressure, and the body temperature decrease, and in the stress state, the heart rate and the blood pressure increase, but when the user measures and registers the heart rate, the body

temperature, and the blood pressure in the sleep state and the stress state in advance, more accurate determination can be performed. Further, even when anyone else wears the handheld device 1 and causes the handheld device 1 to touch the finger of the authorized user and perform the fingerprint authentication, the heart rate, the body temperature, and the blood pressure are detected to be different from a tendency toward previous measured values of the authorized user, and in this case, the handheld device 1 may be locked.

[0059]

The determination of the state of the user may be performed based on other dynamic biometric information such as the brain wave or the amount of sweating in addition to the heart rate, the blood pressure, and the body temperature.

[0060]

Further, the terminal device 1 may perform the user authentication based on the dynamic biometric information obtained from a heart rate waveform, a brain wave, or the like instead of the static biometric information obtained from the fingerprint or the like.

[0061]

As described above, according to the present embodiment, an application software start-up method of an information processing device includes performing user authentication based on static biometric information, determining a state of

a user by comparing dynamic biometric information acquired from a body of the user with dynamic biometric information which is measured in advance, and limiting application software to be started according to the determined state of the user based on a permission level which is set to each application software in advance. Further, the information processing device is forcibly locked according to the determined state of the user.

[0062]

Further, an information processing device includes a static biometric information acquisition unit that acquires static biometric information, a user authentication unit that performs user authentication by comparing the acquired static biometric information with static biometric information which is registered in advance, a dynamic biometric information acquisition unit that acquires dynamic biometric information from a body of the user, a state determination unit that determines a state of the user by comparing the acquired dynamic biometric information which is measured in advance, a lock control unit that unlocks the information processing device through the authentication of the user authentication unit, and an application start unit that starts application software which is selected by the user among a plurality of pieces of application software, wherein the application start unit limits application software to be started according to

the state of the user determined by the state determination unit based on a permission level which is set to each application software in advance. Further, the lock control unit forcibly locks the information processing device according to the state of the user determined by the state determination unit.

[0063]

Accordingly, in the present embodiment, it is determined whether or not the user is the authorized user based on the static biometric information, the state of the user is determined based on the dynamic biometric authentication, and the start of an application is limited stepwise according to the state of the user. Thus, when determination of the user is suspected, it is possible to limit the start of the specific application, for example, when it is against the user's will.

Second embodiment

[0064]

FIG. 6 is a configuration diagram illustrating a communication system including a handheld device 2 and a handheld device 3 according to the present embodiment. The present communication system is configured with the handheld device 2, the handheld device 3 worn on the body of the user, a base station 5 such as a mobile telephone communication network, a wide area public network 6 such as the Internet, a router 7, and the like. The present embodiment is an example

in which functions are divided such that the sensors for detecting the dynamic biometric information in the handheld device 1 according to the first embodiment, for example, a heart rate sensor 312, a blood pressure sensor 313, a temperature sensor 314, and the like are installed in the handheld device 3, and the other functions of the handheld device 1 are implemented in the handheld device 2.

[0065]

In FIG. 6, the handheld device 2 is a smart phone. The handheld device 2 includes a fingerprint sensor 21 and a touch panel 22 installed on the surface thereof. The handheld device 2 can establish a connection with the base station 5 or the router 7 and acquire various kinds of information from the network 6. In the present embodiment, the smart phone is described as the handheld device 2, but the handheld device 2 may be a mobile phone, a tablet terminal, or the like or may be a personal digital assistants (PDA) or a laptop personal computer (PC). Further, the handheld device 2 may be a music player, a digital camera, a portable game machine, or the like having a communication function or an information processing device including any other digital device.

[0066]

The handheld device 3 is a wristwatch-type handheld device having a communication function and has a function of performing transmission reception of various kinds of

information with the handheld device 2. The handheld device 3 includes a touch panel 32 installed on the surface thereof. Although not illustrated, the handheld device 1 includes a heart rate sensor, a blood pressure sensor, a temperature sensor, and the like which are installed on the back surface to come into contact with the wrist when the user wears it. In the present embodiment, the wristwatch-type handheld device is described as the handheld device 3, but the handheld device 1 may be a glasses-type handheld device or a ring-type handheld device. Further, the handheld device 1 may be any other portable digital device.

[0067]

FIG. 7 is a hardware configuration diagram illustrating the handheld device 2 and the handheld device 3 according to the present embodiment. In FIG. 7, the same components as those in FIG. 2 which is a hardware configuration diagram illustrating the handheld device 1 according to the first embodiment are denoted by the same reference numerals. In FIG. 7, components of the handheld device 2 is similar to the components obtained by excluding the heart rate sensor 112, the blood pressure sensor 113, and the temperature sensor 114 from the components of FIG. 2, and a description of the components is omitted. Further, components of the handheld device 3 are similar to the components described above with reference to FIG. 2, and thus a description of the components

is omitted.

[0068]

The heart rate sensor 312, the blood pressure sensor 313, and the temperature sensor 314 of the handheld device 3 are a group of sensors for detecting the state of the user who wears the handheld device 3 and can detect, for example, the heart rate, the blood pressure, and the body temperature of the user through the group of sensors. Further, any other sensor may be installed. The handheld device 3 transmits the detected data to the handheld device 2 through the short-range wireless communication device 133. The handheld device 2 can receive the detected data through the short-range wireless communication device 133 and detect the state of the user who wears the handheld device 3. The handheld device 2 and the handheld device 3 are assumed to be in an authenticated state.

[0069]

The exemplary configurations of the handheld devices 2 and 3 illustrated in FIG. 7 includes components which are not essential in the present embodiment, but effects of the present embodiment are obtained even through a configuration having no non-essential components. A component which is not illustrated such as a digital television broadcasting receiving function, an e-money payment function, or the like may be further added.

[0070]

FIG. 8 is a functional block diagram illustrating the handheld device 2 according to the present embodiment. In FIG. 8, the same components as those in FIG. 3 which is a functional block diagram illustrating the handheld device 1 according to the first embodiment are denoted by the same reference numerals.

[0071]

In FIG. 8, the components of the handheld device 2 are similar to the components obtained by excluding the dynamic biometric information acquisition unit 1120, the dynamic biometric information memory 1032, and the state determination unit 1012 from the components of FIG. 3, and thus a description of the same components as in FIG. 3 is omitted.

[0072]

The functional blocks of the handheld device 2 are controlled by the control unit 2010. The control unit 2010 operates on the CPU 101 with which the handheld device 2 illustrated in FIG. 8 is equipped, includes the user authentication unit 1011, the lock control unit 1013, the application start unit 1014, and the like, and controls a memory 2030, the static biometric information acquisition unit 1110, the communication unit 1310, and the like based on an instruction given from the user interface 1040 such that the static biometric information is acquired, stored, and compared, the handheld device 2 is locked or unlocked, or an application

starts.

[0073]

The memory 2030 is configured with the memory 103 and the like which are illustrated in FIG. 7, and stores static biometric information 1031, an application 1033, a permission level table 1034 which is a table of levels at which applications are permitted to start, and the like, in addition to the program and various kinds of setting information for controlling the handheld device 2.

[0074]

The communication with the handheld device 3 is performed through the short-range wireless communication device 133.

[0075]

FIG. 9 is a functional block diagram illustrating the handheld device 3 according to the present embodiment. In FIG. 9, the same components as those in FIG. 3 which is a functional block diagram illustrating the handheld device 1 according to the first embodiment are denoted by the same reference numerals. In FIG. 9, the components of the handheld device 3 include the dynamic biometric information acquisition unit 1120, the dynamic biometric information memory 1032, and the state determination unit 1012 among the components of FIG. 3, and thus a detailed description thereof is omitted.

[0076]

The functional blocks of the handheld device 3 are

controlled by the control unit 3010. The control unit 3010 operates on the CPU 101 with which the handheld device 3 illustrated in FIG. 7 is equipped, includes the state determination unit 1012 and the like, and controls the dynamic biometric information acquisition unit 1120, a memory 3030, a communication unit 3310, and the like based on an instruction given from a user interface 3040 such that the dynamic biometric information is acquired, stored, transmitted, and displayed.

[0077]

The user interface 3040 is configured with the operation device 104, the audio output device 142, the display device 152, and the like which are illustrated in FIG. 7, and presents the user with various kinds of information and transfers the instruction of the user to the control unit 3010.

[0078]

The communication unit 3310 is configured with a short-range wireless communication device 333 and the like which are illustrated in FIG. 7 and performs communication with the handheld device 2.

[0079]

The memory 3030 is configured with the memory 103 and the like which are illustrated in FIG. 7, and stores a program and various kinds of setting information for controlling the handheld device 3.

[0080]

The state determination unit 1012 determines the state of the user by comparing the dynamic biometric information acquired through the dynamic biometric information acquisition unit 1120 when the handheld device 3 is used with the dynamic biometric information 1032, and transmits the state of the user to the handheld device 2 through the communication unit 3310.

[0081]

For example, when the user is determined to be in the sleep state, the sleep state is transmitted to the handheld device 2 through the communication unit 3310, so that the handheld device 2 is locked. Further, an application to be started in the handheld device 2 is limited according to the state of the user. Further, when the user is determined to be in the normal state, all applications are set to enter the startable state, and when the user is determined to be in the stress state, applications that can be started are limited.

[0082]

FIG. 10 is a flowchart illustrating an application permission operation of the handheld devices 2 and 3 of the present embodiment. This flowchart illustrates a process of performing the user authentication through the handheld device 2, checking the state of the user through the handheld device 3, and limiting an application to be started according to the

state of the user.

[0083]

First, the handheld device 2 detects the static biometric information, and performs the user authentication (S1001). For example, it is determined whether or not the user is the authorized user through the fingerprint authentication. In other words, a fingerprint pattern detected when the user touches the fingerprint sensor 211 with the finger is compared with the fingerprint pattern of the user registered in the memory 203, and it is determined whether or not the two fingerprints are identical to each other. When the two fingerprints are determined to be identical to each other, the handheld device 2 is unlocked (S1002), and the application of the permission level 1 is permitted to be started (S1003).

[0084]

A display example of a screen of the handheld device 2 at this time is illustrated in FIG. 11A. The clock application, the web browser, the map application, the camera application, the weather forecast application, the music application, the calculator application, and the dictionary application are the applications of the permission level 1 and thus are in the startable state, and the other applications have a different icon color which indicates that they are in the non-startable state.

[0085]

The user authentication may be performed through any other biometric authentication such as the vein authentication, the face authentication, the iris authentication, or the retina authentication, the unlocking operation may be performed by inputting a passcode, and a pattern lock may be released by the trajectory of the finger.

[0086]

The handheld device 3 measures the heart rate through the heart rate sensor 312, measures the blood pressure through the blood pressure sensor 313, and measures the body temperature through the temperature sensor 314 (S1011).

[0087]

The handheld device 2 requests the handheld device 3 to confirm the state of the user through a short-range wireless communication device 233 (S1012).

[0088]

The handheld device 3 detects the dynamic biometric information, and determines the state of the user (S1013). For example, the state of the user is determined based on a result of measuring the heart rate, the blood pressure, and the body temperature. In other words, for example, when the heart rate, the blood pressure, and the body temperature measured through the heart rate sensor 312, the blood pressure sensor 313, the temperature sensor 114 of the handheld device 3 are equal to or less than the lower limit values in the normal state, the

state of the user is determined to be the sleep state. Further, for example, when the heart rate and the blood pressure are equal to or larger than the upper limit values in the normal state, the state of the user is determined to be the stress state, and the state which corresponds to neither the sleep state nor the stress state is determined to be the normal state.

[0089]

The handheld device 3 constantly acquires the dynamic biometric information, and performs, for example, the state determination based on the biometric information obtained for previous 30 seconds.

[0090]

Then, the handheld device 3 transmits the state of the user to the handheld device 2 through the short-range wireless communication device 333 as a response (S1014).

[0091]

The handheld device 2 switches the process according to whether or not the state of the user received through the short-range wireless communication device 233 is the sleep state (S1005). When the state of the user is determined to be the sleep state, the handheld device 2 is locked (S1010), and the process ends.

[0092]

Further, even when the user does not wear the handheld

device 3 or even when the terminal device 3 does not transmit the state of the user to the handheld device 2 as a response, the handheld device 2 is locked, and the process ends.

[0093]

Steps S1006 to 1009 which are processes performed when the state of the user is determined not to be the sleep state are similar to steps S406 to 409 of FIG. 4 in the first embodiment, and thus a detailed description thereof is omitted.

[0094]

A display example of the screen of the handheld device 2 when the applications of the permission levels 1 and 2 are permitted to be started in S1007 is illustrated in FIG. 11B. In addition to the fact that the applications of the permission level 1 are in the startable state, the schedule application, the mail application, the photo application, the telephone application, and the address book application are the applications of the permission level 2 and thus are in the startable state, and the other applications have a different icon color which indicates that they are in the non-startable state.

[0095]

A display example of the screen of the handheld device 2 when all the applications of the permission levels 1 to 3 are permitted to be started in S1008 is illustrated in FIG. 11C. In addition to the fact that the applications of the

permission levels 1 and 2 are in the startable state, the e-money application and the online banking application are the applications of the permission level 3 and thus are in the startable state, and it is indicated that all applications are in the startable state.

[0096]

In the present embodiment, the handheld device 3 determines the state of the user, but the handheld device 3 may not determine the state of the user but transmit the measured values of the heart rate, the blood pressure, and the body temperature to the handheld device 2, and the handheld device 2 may determine the state of the user.

[0097]

Further, the terminal device 2 may not perform the user authentication for the user, and the terminal device 3 may control whether or not the terminal device 2 is locked by performing the user authentication through the fingerprint authentication or the like and transmitting an authentication result to the terminal device 2. At this time, the terminal device 3 may perform the user authentication based on the dynamic biometric information obtained from the heart rate waveform, the brain wave, or the like rather than the static biometric information obtained from the fingerprint or the like.

[0098]

In the present embodiment, the example in which the number of handheld devices is 2 has been described, but the number of handheld devices may be three or more, and the authentication function and the state determination function may be separated. In other words, the system including a plurality of handheld devices according to the present embodiment can be understood to be an application software start-up system including a plurality of information processing devices.

[0099]

As described above, according to the present embodiment, an application software start-up method of an information processing device including a plurality of information processing devices includes performing, by at least one of the information processing devices, user authentication based on static biometric information of a body of a user, determining, by another information processing device, a state of a user by comparing dynamic biometric information acquired from the body of the user with dynamic biometric information which is measured in advance, and limiting application software to be started according to the determined state of the user based on a permission level which is set to each application software in advance.

[0100]

Further, An application software start-up system includes

first and second first information processing devices, the first information processing device includes a static biometric information acquisition unit that acquires static biometric information of a body, a user authentication unit that performs user authentication by comparing the acquired static biometric information with static biometric information which is registered in advance, a lock control unit that unlocks a handheld device through the authentication of the user authentication unit, an application start unit that starts application software which is selected by a user among a plurality of pieces of application software, and a first communication unit that receives a state of the user from the second information processing device, and the second information processing device includes a dynamic biometric information acquisition unit that acquires dynamic biometric information from the body of the user, a state determination unit that determines a state of the user by comparing the acquired dynamic biometric information which is measured in advance, and a second communication unit that transmits the determined state of the user to the first information processing device, wherein the application start unit limits application software to be started according to the state of the user received from the first communication unit based on a permission level which is set to each application software in advance.

[0101]

Accordingly, in the present embodiment, the same effects as in the first embodiment are obtained, and when a plurality of handheld devices are registered in advance, and the user authentication function and the state determination function are distributed, each handheld device can be worn on a part of the body suitable for acquisition of each biometric information, and thus the handheld devices can be implemented in a form optimal for the respective functions.

Third embodiment

[0102]

FIG. 12 is a flowchart illustrating an application permission operation of the handheld device 1 of the present embodiment. In FIG. 12, steps S1201 to S1204 are similar to steps S401 to S404 of FIG. 4 in the first embodiment, and thus a description thereof is omitted.

[0103]

In step S1205, the process is switched according to whether or not the state of the user is the sleep state. When the state of the user is determined to be the sleep state, the handheld device 1 is locked (S1210), and the process ends. When the state of the user is determined not to be the sleep state in step S1205, all the applications of the permission levels 1 to 3 are permitted to be started (S1208).

[0104]

Here, the process is switched according to whether or not the state of the user is the stress state (S1206). When the state of the user is determined to be the stress state, if the user selects the application of the permission level 3, a caution screen is displayed (S1221), and it is started only when the user confirms it. When the state of the user is determined not to be the stress state (determined to be the normal state), the caution screen is not displayed.

[0105]

For example, when the application of the permission level 3 such as the e-money application or the online banking application is requested to be started, an application software start confirmation screen illustrated in FIG. 13 is displayed on the display device 152.

[0106]

Steps S1209 to S1210 are similar to steps S409 to S410 of FIG. 4, and thus a description thereof is omitted.

[0107]

The determination of the state of the user may be performed based on other dynamic biometric information such as the brain wave or the amount of sweating in addition to the heart rate, the blood pressure, and the body temperature.

[0108]

In the present embodiment, the example in which the number of handheld devices is 1 has been described, but the

number of handheld devices may be two or more, and the authentication function and the state determination function may be separated.

[0109]

Through the above configuration, in the present embodiment, the same effects as in the first embodiment can be obtained, and since it is checked when a specific application is started according to the state of the user, for example, when determination of the user is suspected, it is possible to encourage reconsideration of the start of the specific application.

Fourth embodiment

[0110]

FIG. 14 is a flowchart illustrating an application permission operation of the handheld device 1 of the present embodiment. In FIG. 14, steps S1401 to S1403 are similar to steps S401 to S403 of FIG. 4, and thus a process of inputting a passcode (S1431 to S1433) is added.

[0111]

First, the static biometric information is detected, and the user authentication is performed. The static biometric information acquisition unit 1110 acquires the static biometric information, and the user authentication unit 1011 performs the user authentication as to whether or not the acquired static biometric information is identical to the

static biometric information 1031 which is registered in advance by comparing the acquired static biometric information with the static biometric information 1031 (S1401). For example, the fingerprint serving as the static biometric information is detected, the user authentication is performed, and when the detected fingerprint is determined to be identical to the registered fingerprint, the process proceeds to step S1431. The user authentication may be performed through any other biometric authentication such as the vein authentication, the face authentication, the iris authentication, or the retina authentication, in addition to the fingerprint authentication.

[0112]

Then, the process is switched according to whether or not a sleep state detection log (which will be described later) in the memory 103 (S1431). When there is no sleep state detection log, the process proceeds to step S1402, and the lock control unit 1013 unlocks the handheld device 1, and the application start unit 1014 permits the start of the application of the permission level 1 (S1403).

[0113]

When there is a sleep state detection log, the process proceeds to step S1432, a passcode input request screen illustrated in FIG. 15 is displayed, and the process proceeds to step S1402 when a passcode which is information other than

the biometric information input from the user interface 1040 such as the operation device 104 or the audio input device 141 is identical to a passcode which is set in advance in step S1433. A pattern lock may be released by the trajectory of the finger instead of the passcode.

[0114]

Steps S1404 to S1410 are similar to step S404 to S410 of FIG. 4, but a process of recording the sleep state detection log (S1434) is added.

[0115]

When the state of the user is determined to be in the sleep state in step S1405, since it is suspected that anyone else causes the handheld device 1 to touch the finger of the user and perform the user authentication, in step S1434, position information which is a place in which the user authentication is performed is specified through the GPS receiver 121 and recorded as a log together with time information, the handheld device 1 is locked (S1410), and the process ends. The log is recorded in the memory 103.

[0116]

Further, in step S1434, a warning may be displayed on the display device 152, a vibrator for an incoming call may be operated, a photograph or a video may be captured through the video input device 151, attached to an e-mail together with the log, and transmitted to an address which is designated in

advance.

[0117]

In the present embodiment, the example in which the number of handheld devices is 1 has been described, but the number of handheld devices may be two or more, and the authentication function and the state determination function may be separated.

[0118]

Through the above configuration, in the present embodiment, the same effects as in the first embodiment can be obtained, and when the handheld device is likely to be operated by anyone else, a warning is displayed, a photograph is captured, and a log is recorded, and thus it can be expected that a family member or anyone else is prevented from furtively looking at an e-mail. Further, when the log is recorded, it is necessary to input the passcode in order to lock the handheld device, and thus it is possible to prevent anyone else from performing the unlocking operation.

Fifth embodiment

[0119]

FIG. 16 is a flowchart illustrating an application permission operation of the handheld device 1 of the present embodiment. In FIG. 16, steps S1601 to S1603 are similar to steps S401 to S403 of FIG. 4 in the first embodiment, and thus a process of inputting a passcode (S1631 to S1633) is added.

[0120]

First, the static biometric information is detected, and the user authentication is performed. The static biometric information acquisition unit 1110 acquires the static biometric information, and the user authentication unit 1011 performs the user authentication as to whether or not the acquired static biometric information is identical to the static biometric information 1031 which is registered in advance by comparing the acquired static biometric information with the static biometric information 1031 (S1601). For example, the fingerprint serving as the static biometric information is detected, the user authentication is performed, and when the detected fingerprint is determined to be identical to the registered fingerprint, the process proceeds to step S1631. The user authentication may be performed through any other biometric authentication such as the vein authentication, the face authentication, the iris authentication, or the retina authentication, in addition to the fingerprint authentication.

[0121]

Then, the process is switched according to whether or not there is a period of time in which it is unable to measure the dynamic biometric information after the handheld device 1 is previously unlocked (S1631). When there is not period of time in which it is unable to measure the dynamic biometric

information, the process proceeds to step S1602, the lock control unit 1013 unlocks the handheld device 1, and the application start unit 1014 permits the start of the application of the permission level 1 (S1603).

[0122]

When there is a period of time in which it is unable to measure the dynamic biometric information, since anyone else is likely to wear the handheld device 1, cause the handheld device 1 to touch the finger of the user, and perform the user authentication, the passcode input request screen illustrated in FIG. 15 is displayed on the handheld device 1, and when the input passcode is identical to the passcode which is set in advance in step S1633, the process proceeds to step S1602. A pattern lock may be released by the trajectory of the finger instead of the passcode.

[0123]

Steps S1604 to S1610 are similar to step S404 to S410 of FIG. 4, and thus a description thereof is omitted.

[0124]

In the present embodiment, the example in which the number of handheld devices is 1 has been described, but the number of handheld devices may be two or more, and the authentication function and the state determination function may be separated.

[0125]

Through the above configuration, in the present embodiment, the same effects as in the first embodiment can be obtained, and when the handheld device is removed, it is necessary to input the passcode in order to unlock the handheld device next time, and thus it is possible to prevent anyone else from performing the unlocking operation.

Sixth embodiment

[0126]

FIG. 17 is a flowchart illustrating an application permission operation of the handheld device 1 of the present embodiment. In FIG. 17, steps S1701 to S1710 are similar to steps S401 to S410 of FIG. 4 in the first embodiment, and thus a process of switching an application according to a current position (S1741) is added.

[0127]

In step S1706, the process is switched according to whether or not the state of the user is the stress state. When the state of the user is determined to be the stress state, the applications of the permission levels 1 and 2 are permitted to be started (S1707). When the state of the user is determined not to be the stress state (determined to be the normal state), the process is switched according to the current position of the handheld device 1 (S1741). The current position is specified through the GPS receiver 121, and when the current position is a predetermined position which is set

in advance, all the applications of the permission levels 1 to 3 are permitted to be started (S1708). The predetermined position is, for example, the user's home or company or the like. When the current position is not a predetermined position which is set in advance, the applications of the permission levels 1 and 2 are permitted to be started (S1707).

[0128]

Alternatively, all the applications of the permission levels 1 to 3 may be permitted to be started at a predetermined timing which is set in advance.

[0129]

Alternatively, a face photograph of the user may be registered, and all the applications of the permission levels 1 to 3 may be permitted to be started when a face is captured through the video input device 151, and the user is recognized. Alternatively, all the applications of the permission levels 1 to 3 may be permitted to be started when the user is recognized, but anyone else around the user except the user is not recognized.

[0130]

The determination of the state of the user may be performed based on other dynamic biometric information such as the brain wave or the amount of sweating in addition to the heart rate, the blood pressure, and the body temperature.

[0131]

In the present embodiment, the example in which the number of handheld devices is 1 has been described, but the number of handheld devices may be two or more, and the authentication function and the state determination function may be separated.

[0132]

Through the above configuration, in the present embodiment, the same effects as in the first embodiment can be obtained, and a specific application is permitted to be started when the user is at a safe position which is set in advance, and thus it is possible to limit the start of the application at a place which is not assumed by the user.

[0133]

The above embodiments have been described in detail in order to facilitate understanding of the present invention, and the present invention is not limited to one necessarily having all components described above. Further, a component of a certain embodiment may be replaced with a component of another embodiment, and a component of a certain embodiment may be added to a component of another embodiment. Furthermore, addition, deletion, or replacement of another component may be performed on a component of each embodiment.

[0134]

Further, all or some of the components, the functions, processing units, the processing devices, and the like

described above may be implemented by hardware, for example, may be designed by, for example, an integrated circuit (IC). Furthermore, each component, each function, or the like may be implemented by software by interpreting and executing a program that implements each function through a processor. Information such as a program that implements each function, a table, or a file may be stored in a memory, a recording device such as a hard disk or a solid state drive (SSD), or a recording medium such as an IC card or an SD card.

[0135]

Further, control lines or information lines considered to be necessary for the sake of description are illustrated, and all control lines or information lines necessary in a product are not necessarily illustrated. Practically, most of components may be considered to be connected with one another.

REFERENCE SIGNS LIST

[0136]

- 1, 2, 3 handheld device
- 5 base station
- 6 network
- 7 router
- 101 CPU
- 102 system bus
- 103 memory

104 operation device
105 expansion interface
111 fingerprint sensor
112 heart rate sensor
113 blood pressure sensor
114 temperature sensor
121 GPS receiver
122 acceleration sensor
123 gyro sensor
124 geomagnetism sensor
125 proximity sensor
131 mobile communication device
132 LAN communication device
133 short-range wireless communication device
141 audio input device
142 audio output device
151 video input device
152 display device
1010 control unit
1011 user authentication unit
1012 state determination unit
1013 lock control unit
1014 application start unit
1030 memory
1031 static biometric information

1032 dynamic biometric information
1033 application
1034 the permission level table
1040 user interface
1110 static biometric information acquisition unit
1120 dynamic biometric information acquisition unit
1310 communication unit

CLAIMS

1. A system, comprising:

- a first information processing device including:

- a dynamic biometric information acquisition sensor that acquires dynamic biometric information from a body of a user; and

- a first communication interface that transmits the acquired dynamic biometric information; and

- a second information processing device including:

- a static biometric information acquisition sensor that acquires static biometric information;

- a processor that performs user authentication based on the acquired static biometric information and obtains an authentication result;

- a second communication interface that performs communication relating to the authentication result with the first communication interface and receives the dynamic biometric information transmitted from the first communication interface; and

- a display screen,

- wherein the first information processing device:

- performs communication relating to the authentication result between the first communication interface and the second communication interface and executes an unlock operation to unlock itself in response to the communication

relating to the authentication result,

acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking, and

maintains the unlocked state during a condition that the dynamic biometric information can be acquired,

wherein the second information processing device receives the dynamic biometric information via communication between the first communication interface and the second communication interface and the display screen displays information based on a state of the user that is determined using the received dynamic biometric information.

2. The system according to claim 1,

wherein the first communication interface and the second communication interface are Bluetooth interfaces and communication between the first communication interface and the second communication interface is Bluetooth wireless communication.

3. The system according to claim 1,

wherein the first communication interface and the second communication interface are Wi-Fi interfaces and communication between the first communication interface and the second communication interface includes establishing a Wi-Fi Direct

connection.

4. The system according to claim 1,

wherein the dynamic biometric information is one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.

5. The system according to claim 1,

wherein the first information processing device is a wearable device that acquires the dynamic biometric information at least by being physically in contact with the body.

6. The system according to claim 1,

wherein the first information processing device is a smartwatch and the second information processing device is a smartphone or tablet.

7. The system according to claim 1,

wherein the first information processing device continuously acquires the dynamic biometric information after being unlocked and the second information processing device receives

the dynamic biometric information transmitted from the first communication device continuously or based on starting of an application on the second information processing device.

8. The system according to claim 1,

wherein the second information processing device gets position information denoting a position of the second information processing device and automatically transmits the position information to a predetermined address based on reception of a user input that is determined to be a predetermined type of user input during a time period, wherein the predetermined address is not inputted by the user during the time period.

9. The system according to claim 8,

wherein the position information is automatically transmitted in response to the user input and without requiring additional user input that explicitly requires approval of the automatic transmission of the position information during the time period.

10. The system according to claim 1,

wherein upon determining that the user is in a state matching predetermined criteria, the second information processing device limits an operation of the second

information processing device by displaying a screen seeking confirmation from the user that the user intended to execute the operation.

11. The system according to claim 10,

wherein the operation is executed on the second information processing device after the user provides confirmation in response to displaying of the screen.

12. An information processing device, comprising:

a dynamic biometric information acquisition sensor that acquires dynamic biometric information from a body of a user;

a wireless communication interface is configured to:

transmits the acquired dynamic biometric information to another information processing device; and

perform communication relating to an authentication result based on static biometric information with the other information processing device;

a processor that:

executes an unlock operation to unlock the information processing device in response to the communication relating the authentication result;

acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking; and

maintains the unlocked state during a condition that the dynamic biometric information can be acquired,

wherein the wireless communication interface is configured to transmit the dynamic biometric information to the other information processing device via wireless communications such that the dynamic biometric information is used to determine a state of the user and generate information for display on the other information processing device, and

wherein the dynamic biometric information is continuously acquired after the information processing device is unlocked and the wireless communication interface is configured to transmit the dynamic biometric information to the other information processing device continuously or based on starting of an application on the other information processing device.

13. The information processing device according to claim 12,

wherein the wireless communication interface is one of a Bluetooth interface for executing Bluetooth wireless communication or a Wi-Fi interface for executing Wi-Fi wireless communication.

14. The information processing device according to claim 12,

wherein the dynamic biometric information is one of heart rate, pulse, blood pressure, body temperature, amount of

sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.

15. The information processing device according to claim 12, wherein the processor is programmed to switch from the unlocked state to locked state when in a condition that the dynamic biometric information cannot be acquired.

16 . A method being executed by a first information processing device, comprising:

acquiring, by a dynamic biometric information acquisition sensor, dynamic biometric information from a body of a user;

wirelessly transmitting the acquired dynamic biometric information to a second information processing device;

performing communication relating to an authentication result based on static biometric information with the second information processing device;

executing an unlock operation to unlock the first information processing device in response to the communication relating to the authentication result;

acquiring the dynamic biometric information from the dynamic biometric information acquisition sensor after the unlocking; and

maintaining the unlocked state during a condition that the dynamic biometric information can be acquired,

wherein the dynamic biometric information is transmitted to the second information processing device via wireless communications such that the dynamic biometric information is used to determine a state of the user and generate information for display on the second information processing device, and

wherein the dynamic biometric information is continuously acquired after the first information processing device is unlocked and the dynamic biometric information is transmitted to the second information processing device continuously or based on starting of an application on the second information processing device.

17. The method according to claim 16,

wherein the wireless communication is one of Bluetooth wireless communication or Wi-Fi wireless communication.

18. The method according to claim 16,

wherein the dynamic biometric information is one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.

19. A method, comprising:

acquiring dynamic biometric information from a body of a user by a dynamic biometric information acquisition sensor of a first device;

transmitting the acquired dynamic biometric information through a first communication interface of the first device to a second device;

acquiring static biometric information by a static biometric information acquisition sensor of the second device;

performing user authentication to obtain an authentication result based on the acquired static biometric information;

performing communication with a second communication interface relating to the authentication result with the first communication interface and receiving the dynamic biometric information transmitted from the first communication interface;

performing communication relating to the authentication result between the first communication interface and the second communication interface and executing an unlock operation to unlock the first device in response to the communication relating to the authentication result,

acquiring the dynamic biometric information from the dynamic biometric information acquisition sensor of the first device after unlocking, and

maintaining the unlocked state during a condition that the dynamic biometric information can be acquired;

receiving the dynamic biometric information by the second device via communication between the first communication interface and the second communication interface; and

displaying on a display screen information based on a state of the user that is determined using the received dynamic biometric information.

20. The method according to claim 19,

wherein the first communication interface and the second communication interface are Bluetooth interfaces and the communication performed between the first communication interface and the second communication interface is Bluetooth wireless communication.

21. The method according to claim 19,

wherein the first communication interface and the second communication interface are Wi-Fi interfaces and the communication performed between the first communication interface and the second communication interface includes establishing a Wi-Fi Direct connection.

22. The method according to claim 19,

wherein the acquiring of dynamic biometric information

acquires one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.

23. The method according to claim 19,

wherein the acquiring of dynamic biometric information by the acquisition sensor of the first device acquires the dynamic biometric information with a wearable device at least by being physically in contact with the body.

24. The method according to claim 19,

wherein the dynamic biometric information is acquired by a smartwatch as the first device and the dynamic biometric information acquired by a smartphone or tablet as the second device.

25. The method according to claim 19,

wherein the dynamic biometric information is continuously acquired by the first device after being unlocked and the second device receives the dynamic biometric information transmitted from the first device continuously or based on starting of an application on the second device.

26. The method according to claim 19,

wherein the second device gets position information denoting a position of the second device and automatically transmits the position information to a predetermined address based on reception of a user input that is determined to be a predetermined type of user input during a time period, wherein the predetermined address is not inputted by the user during the time period.

27. The method according to claim 26,

wherein the position information is automatically transmitted in response to the user input and without requiring additional user input that explicitly requires approval of the automatic transmission of the position information during the time period.

28. The method according to claim 19,

wherein upon determining that the user is in a state matching predetermined criteria, the second device limits an operation of the second device by displaying on the display screen a message seeking confirmation from the user that the user intended to execute the operation.

29. The method according to claim 28,

wherein the operation is executed on the second device after

the user provides confirmation in response to the displaying of the message on the display screen.

ABSTRACT

The purpose of the present invention is to provide a portable terminal and an application software start-up system whereby the application software that is started up is limited depending on the state of a user, thereby providing an improved ease of use. For this purpose, an application software start-up method for an information processing device comprises: performing identity authentication based on static biological information; determining the state of the user by comparing dynamic biological information acquired from the body of the user with previously measured dynamic biological information; and limiting the application software that is started up in accordance with the determined state of the user and on the basis of a permission level that is set in advance for each application software item.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

申請データシート(37 CFR 1.76)を使った実用及び意匠登録出願宣言書(37 CFR 1.63)
DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET
(37 CFR 1.76)

発明の名称 Title of Invention	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD
下記発明者である私は、つぎのことがらを宣言します。 As the below named inventor, I hereby declare that: 本宣言は This declaration ☐ 添付されている、あるいは is directed to: The attached application, or ☒ 年 月 日に出席された米国出願番号またはPCT国際出願番号 宛てられています。 United States application or PCT International application number PCT/JP2014/065644 filed on June 12, 2014 上記の出願は私自身、あるいは私が権限を授与したものによって行われたものです。 The above-identified application was made or authorized to be made by me. 私は本出願書中にあらわれるもとの発明者、あるいはもとの共同発明者です。 I believe that I am the original inventor or an original joint inventor of a claimed invention in the application. 本宣言書において故意に虚偽の申し立てを行った場合は 18 U.S.C. 1001 により、罰金あるいは最高五(5)年の禁固刑、あるいはその両方による罰則の対象となることを認めます。 I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both. 警告: WARNING: 請願者/出願者は ID 盗難を助けるような個人情報を、特許出願書類中に含まないよう、注意が必要です。社会保障番号、銀行口座番号、あるいはクレジットカード番号のような個人情報の提出は(支払いを目的とした、小切手あるいはクレジットカード使用認証書類である PTO-2038 への記入を例外として) USPTO(米国特許商標庁)は、請願あるいは出願申請のうえでいっさい要求していません。このような個人情報が USPTO に提出する書類に含まれることがないよう、請願者/出願者は、USPTO に書類を提出する前によく注意し、もしあった場合は訂正し、抹消せねばなりません。請願者/出願者は、特許出願の記録内容は、出願の公開、あるいは特許交付後は、(37 CFR 1.213(a) の規制に合致した非公開申請が申請書のなかでなされている場合を除き)、一般人が入手可能なものとなることを知っておく必要があります。さらに、出願が放棄された記録であっても、その出願が公開された、あるいは特許が交付された出願書中に参考として言及されている場合は、一般人の入手が可能となる場合があります。小切手およびクレジットカード承認用紙であり、支払い目的のために提出された PTO-2038 様式は出願ファイルには保持されず、したがって一般人が入手することはできません。 Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available. 発明者の正式氏名 LEGAL NAME OF INVENTOR 発明者: Masayuki HIRABAYASHI 日付(任意): 11 / 7 / 2016 Inventor: Date (Optional): 署名: Masayuki Hirabayashi Signature: 備考: 出願データシート(PTO/SB/14 あるいはその同等用紙)は、発明の自主独立体全体の命名を含め、本用紙に添付すること。なお残余の発明者ごとに PTO/SB/AIA01 用紙を使用する。 Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional PTO/SB/AIA01 form for each additional inventor.	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

プライバシー保護法声明書

1974 年プライバシー保護法 (P.L. 93-579) は、特許出願あるいは特許に関する添付種類の提出に関連して、特定情報があなたに与えられるよう規定しています。したがって、同法規の規定にしたがい、下記のことを銘記してください。(1) 本情報の収集を律する法規は 35 U.S.C. 2(b)(2)です。(2) 求められた情報の提供は、本人の任意です。さらには、(3) 米国特許商標庁がこの情報を使用する主目的は、特許出願または特許の提出を処理し、あるいは審査するためです。求められた情報を提供しなかった場合、米国特許商標庁は提出されたものを処理、審査できなくなる場合がありますので、その結果として、処理の打ち切り、あるいは出願の破棄、あるいは特許失効に終わることがあります。

本用紙に記載された情報は、下記の通常使用目的に従います。

1. 本用紙に記載されている情報は、情報公開法 (5 U.S.C. 552) およびプライバシー保護法 (5 U.S.C. 552a) が許容する範囲において極秘扱いとなります。本記録システムの記録は、本記録の開示が情報公開法で要求されているか否かを判断するために、司法省に開示される場合があります。
2. 本記録システムの記録は通常使用目的として、示談交渉手順における反対側弁護士への開示を含め、証拠の提示として法廷、予審判事、あるいは行政裁判所に開示される場合があります。
3. 本記録システム中の記録は通常使用目的として、記録に関する個人が該当する記録に関して、米国会議員に支援を要請する場合、個人の関与を要請する米国会議員に開示される場合があります。
4. 本記録システム中の記録は通常使用目的として、契約を執行するためにその情報を必要とする、本庁の契約業者に開示される場合があります。情報の受取者は 5 U.S.C. 552a(m) に基づき、1974 プライバシー法の規定要件を順守しなければなりません。
5. 特許協力条約のもとで出願された国際出願に関する本記録システム内の記録は、通常使用目的として、特許協力条約に基づき、世界的な所有権機関に開示される場合があります。
6. 本記録システムの記録は通常使用目的として、国家安全保障 (35 U.S.C. 181) による再審理、および原子力法 (42 U.S.C. 218(e)) にもとづく再審理の目的において、他の連邦政府機関に開示される場合があります。
7. 本記録システムの記録は通常使用目的として、44 U.S.C. 2904 及び 2908 に基づく記録管理慣行及びプログラムの改善を推奨するために、米一般調達局長官(GSA)により、当機関の責任の一部として行われる記録の検査機関中に、GSA、またはその被指名人に開示される場合があります。上記の開示は、本目的のための記録検査を規定する GSA 規定、及び関連 (GSA あるいは商務省) の指令に準拠して行われます。かかる開示は、個人を特定する目的のもとに使用されてはなりません。
8. 本記録システムの記録は通常使用目的として、35 U.S.C. 122(b) に基づく出願公開後あるいは 35 U.S.C. 151 に基づく特許発行後に、一般に開示される場合があります。さらに記録は通常使用目的として、37 CFR 1.14 の制限のなかで、出願がなされても放棄され、またはその処理が終決しており、なおかつそれが公開出願で参照されている、特許出願が一般審査のために公開されている、または特許が発行されている場合は、一般に公開されることがあります。
9. 本記録システムの記録は、通常使用目的として、米国特許商標庁が、法律や法規の違反した、あるいは潜在的に違反があると判断した場合は、連邦、州、または地方自治体の警察等に関示される場合があります。

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

申請データシート(37 CFR 1.76)を使った実用及び意匠登録出願宣言書(37 CFR 1.63)
DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET
(37 CFR 1.76)

発明の名称 Title of Invention	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD
下記発明者である私は、つぎのことがらを宣言します。 As the below named inventor, I hereby declare that: 本宣言は This declaration is directed to: ☐ 添付されている、あるいは The attached application, or ☒ 年 月 日に提出された米国出願番号またはPCT国際出願番号 に宛てられています。 United States application or PCT international application number PCT/JP2014/065644 filed on June 12, 2014 上記の出願は私自身、あるいは私が権限を授与したのものによって行われたものです。 The above-identified application was made or authorized to be made by me. 私は本出願書中にあらわれるもとの発明者、あるいはもとの共同発明者です。 I believe that I am the original inventor or an original joint inventor of a claimed invention in the application. 本宣言書において故意に虚偽の申し立てを行った場合は 18 U.S.C. 1001 により、罰金あるいは最高五(5)年の禁固刑、あるいはその両方による罰則の対象となることを認めます。 I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both. 警告: WARNING: 請願者/出願者は ID 盗難を助けるような個人情報を、特許出願書類中に含まないよう、注意が必要です。社会保障番号、銀行口座番号、あるいはクレジットカード番号のような個人情報の提出は(支払いを目的とした、小切手あるいはクレジットカード使用認証書類である PTO-2038 への記入を例外として)USPTO(米国特許商標庁)は、請願あるいは出願申請のうえでいっさい要求していません。このような個人情報が USPTO に提出する書類に含まれることがないよう、請願者/出願者は、USPTO に書類を提出する前によく注意し、もしあった場合は訂正し、抹消せねばなりません。請願者/出願者は、特許出願の記録内容は、出願の公開、あるいは特許交付後は、(37 CFR 1.213(a) の規制に合致した非公開申請が申請書のなかでなされている場合を除き)、一般人が入手可能なものとなることを知っておく必要があります。さらに、出願が放棄された記録であっても、その出願が公開された、あるいは特許が交付された出願書中に参考として言及されている場合は、一般人の入手が可能となる場合があります。小切手およびクレジットカード承認用紙であり、支払い目的のために提出された PTO-2038 様式は出願ファイルには保持されず、したがって一般人が入手することはできません。 Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available. 発明者の正式氏名 LEGAL NAME OF INVENTOR 発明者: Yasunobu HASHIMOTO Inventor: _____ 署名: <i>Yasunobu Hashimoto</i> Signature: _____ 日付(任意): 11/7/2016 Date (Optional): _____ 備考: 出願データシート(PTO/SB/14 あるいはその同等用紙)は、発明の自主独立体全体の命名を含め、本用紙に添付すること。なお残余の発明者ごとに PTO/SB/AIA01 用紙を使用する。 Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional PTO/SB/AIA01 form for each additional inventor.	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

プライバシー保護法声明書

1974 年プライバシー保護法 (P.L. 93-579) は、特許出願あるいは特許に関する添付種類の提出に関連して、特定情報があなたに与えられるよう規定しています。したがって、同法規の規定にしたがい、下記のことがらを銘記してください。(1) 本情報の収集を律する法規は 35 U.S.C. 2(b)(2)です。(2) 求められた情報の提供は、本人の任意です。さらには、(3) 米国特許商標庁がこの情報を使用する主目的は、特許出願または特許の提出を処理し、あるいは審査するためです。求められた情報を提供しなかった場合、米国特許商標庁は提出されたものを処理、審査できなくなる場合がありますので、その結果として、処理の打ち切り、あるいは出願の破棄、あるいは特許失効に終わることがあります。

本用紙に記載された情報は、下記の通常使用目的に従います。

1. 本用紙に記載されている情報は、情報公開法 (5 U.S.C. 552) およびプライバシー保護法 (5 U.S.C. 552a) が許容する範囲において極秘扱いとなります。本記録システムの記録は、本記録の開示が情報公開法で要求されているかどうかを判断するために、司法省に開示される場合があります。
2. 本記録システムの記録は通常使用目的として、示談交渉手順における反対側弁護士への開示を含め、証拠の提示として法廷、予審判事、あるいは行政裁判所に開示される場合があります。
3. 本記録システム中の記録は通常使用目的として、記録に関する個人が該当する記録に関して、米国会議員に支援を要請する場合、個人の関与を要請する米国会議員に開示される場合があります。
4. 本記録システム中の記録は通常使用目的として、契約を執行するためにその情報を必要とする、本庁の契約業者に開示される場合があります。情報の受取者は 5 U.S.C. 552a(m) に基づき、1974 プライバシー法の規定要件を順守しなければなりません。
5. 特許協力条約のもとで出願された国際出願に関する本記録システム内の記録は、通常使用目的として、特許協力条約に基づき、世界知的所有権機関に開示される場合があります。
6. 本記録システムの記録は通常使用目的として、国家安全保障 (35 U.S.C. 181) による再審理、および原子力法 (42 U.S.C. 218(c)) にもとづく再審理の目的において、他の連邦政府機関に開示される場合があります。
7. 本記録システムの記録は通常使用目的として、44 U.S.C. 2904 及び 2906 に基づく記録管理慣行及びプログラムの改善を推奨するために、米一般調達局長官(GSA)により、当機関の責任の一部として行われる記録の検査機関中に、GSA、またはその被指名人に開示される場合があります。上記の開示は、本目的のための記録検査を規定する GSA 規定、及び関連 (GSA あるいは商務省) の指令に準拠して行われます。かかる開示は、個人を特定する目的のもとに使用されてはなりません。
8. 本記録システムの記録は通常使用目的として、35 U.S.C. 122(b) に基づく出願公開後あるいは 35 U.S.C. 151 に基づく特許発行後に、一般に開示される場合があります。さらに記録は通常使用目的として、37 CFR 1.14 の制限のなかで、出願がなされても放棄され、またはその処理が終決しており、なおかつそれが公開出願で参照されている、特許出願が一般審査のために公開されている、または特許が発行されている場合は、一般に公開されることがあります。
9. 本記録システムの記録は、通常使用目的として、米国特許商標庁が、法律や法規の違反した、あるいは潜在的に違反があると判断した場合は、連邦、州、または地方自治体の警察等に関与される場合があります。

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

申請データシート(37 CFR 1.76)を使った実用及び意匠登録出願宣言書(37 CFR 1.63)
DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET
(37 CFR 1.76)

発明の名称 Title of Invention	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD
--------------------------------	--

下記発明者である私は、つぎのことがらを宣言します。
As the below named inventor, I hereby declare that:

本宣言は ☐ 添付されている、あるいは
This declaration is directed to: The attached application, or
☒ 年 月 日に出願された米国出願番号またはPCT国際出願番号 宛てられています。
United States application or PCT international application number PCT/JP2014/065644 filed on June 12, 2014

上記の出願は私自身、あるいは私が権限を授与したものによって行われたものです。
The above-identified application was made or authorized to be made by me.

私は本出願書中にあらわれるもとの発明者、あるいはもとの共同発明者です。
I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

本宣言書において故意に虚偽の申し立てを行った場合は 18 U.S.C. 1001 により、罰金あるいは最高五(5)年の禁固刑、あるいはその両方による罰則の対象となることを認めます。
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

警告:
WARNING:

請願者/出願者は ID 盗難を助けるような個人情報を、特許出願書類中に含まないよう、注意が必要です。社会保障番号、銀行口座番号、あるいはクレジットカード番号のような個人情報の提出は(支払いを目的とした、小切手あるいはクレジットカード使用認証書類である PTO-2038 への記入を例外として)USPTO(米国特許商標庁)は、請願あるいは出願申請のうえでいっさい要求していません。このような個人情報が USPTO に提出する書類に含まれることがないよう、請願者/出願者は、USPTO に書類を提出する前によく注意し、もしあった場合は訂正し、抹消せねばなりません。請願者/出願者は、特許出願の記録内容は、出願の公開、あるいは特許交付後は、(37 CFR 1.213(a)の規制に合致した非公開申請が申請書のなかでなされている場合を除き)、一般人が入手可能なものとなることを知っておく必要があります。さらに、出願が放棄された記録であっても、その出願が公開された、あるいは特許が交付された出願書中に参考として言及されている場合は、一般人の入手が可能となる場合があります。小切手およびクレジットカード承認用紙であり、支払い目的のために提出された PTO-2038 様式は出願ファイルには保持されず、したがって一般人が入手することはできません。

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

発明者の正式氏名
LEGAL NAME OF INVENTOR

発明者: Kazuhiko YOSHIZAWA
Inventor:

日付(任意): 11/7/2016
Date (Optional):

署名: Kazuhiko Yoshizawa
Signature:

備考: 出願データシート(PTO/SB/14 あるいはその同等用紙)は、発明の自主独立体全体の命名を含め、本用紙に添付すること。なお残余の発明者ごとに PTO/SB/AIA01 用紙を使用する。

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional PTO/SB/AIA01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

プライバシー保護法声明書

1974 年プライバシー保護法 (P.L. 93-579) は、特許出願あるいは特許に関する添付種類の提出に関連して、特定情報があなたに与えられるよう規定しています。したがって、同法規の規定にしたがい、下記のことをごらねを銘記してください。(1) 本情報の収集を律する法規は 35 U.S.C. 2(b)(2) です。(2) 求められた情報の提供は、本人の任意です。さらには、(3) 米国特許商標庁がこの情報を使用する主目的は、特許出願または特許の提出を処理し、あるいは審査するためです。求められた情報を提供しなかった場合、米国特許商標庁は提出されたものを処理、審査できなくなる場合がありますので、その結果として、処理の打ち切り、あるいは出願の破棄、あるいは特許失効に終わることがあります。

本用紙に記載された情報は、下記の通常使用目的に従います。

1. 本用紙に記載されている情報は、情報公開法 (5 U.S.C. 552) およびプライバシー保護法 (5 U.S.C. 552a) が許容する範囲において極秘扱いとなります。本記録システムの記録は、本記録の開示が情報公開法で要求されているかどうかを判断するために、司法省に開示される場合があります。
2. 本記録システムの記録は通常使用目的として、示談交渉手順における反対側弁護士への開示を含め、証拠の提示として法廷、予審判事、あるいは行政裁判所に開示される場合があります。
3. 本記録システム中の記録は通常使用目的として、記録に関する個人が該当する記録に関して、米国会議員に支援を要請する場合、個人の関与を要請する米国会議員に開示される場合があります。
4. 本記録システム中の記録は通常使用目的として、契約を執行するためにその情報を必要とする、本庁の契約業者に開示される場合があります。情報の受取者は 5 U.S.C. 552a(m) に基づき、1974 プライバシー法の規定要件を順守しなければなりません。
5. 特許協力条約のもとで出願された国際出願に関する本記録システム内の記録は、通常使用目的として、特許協力条約に基づき、世界知的所有権機関に開示される場合があります。
6. 本記録システムの記録は通常使用目的として、国家安全保障 (35 U.S.C. 181) による再審理、および原子力法 (42 U.S.C. 218(c)) にもとづく再審理の目的において、他の連邦政府機関に開示される場合があります。
7. 本記録システムの記録は通常使用目的として、44 U.S.C. 2904 及び 2906 に基づく記録管理慣行及びプログラムの改善を推奨するために、米一般調達局長官(GSA)により、当機関の責任の一部として行われる記録の検査機関中に、GSA、またはその被指名人に開示される場合があります。上記の開示は、本目的のための記録検査を規定する GSA 規定、及び関連 (GSA あるいは商務省) の指令に準拠して行われます。かかる開示は、個人を特定する目的のもとに使用されてはなりません。
8. 本記録システムの記録は通常使用目的として、35 U.S.C. 122(b) に基づく出願公開後あるいは 35 U.S.C. 151 に基づく特許発行後に、一般に開示される場合があります。さらに記録は通常使用目的として、37 CFR 1.14 の制限のなかで、出願がなされても放棄され、またはその処理が終決しており、なおかつそれが公開出願で参照されている、特許出願が一般審査のために公開されている、または特許が発行されている場合は、一般に公開されることがあります。
9. 本記録システムの記録は、通常使用目的として、米国特許商標庁が、法律や法規の違反した、あるいは潜在的に違反があると判断した場合は、連邦、州、または地方自治体の警察等に関示される場合があります。

FIG. 1

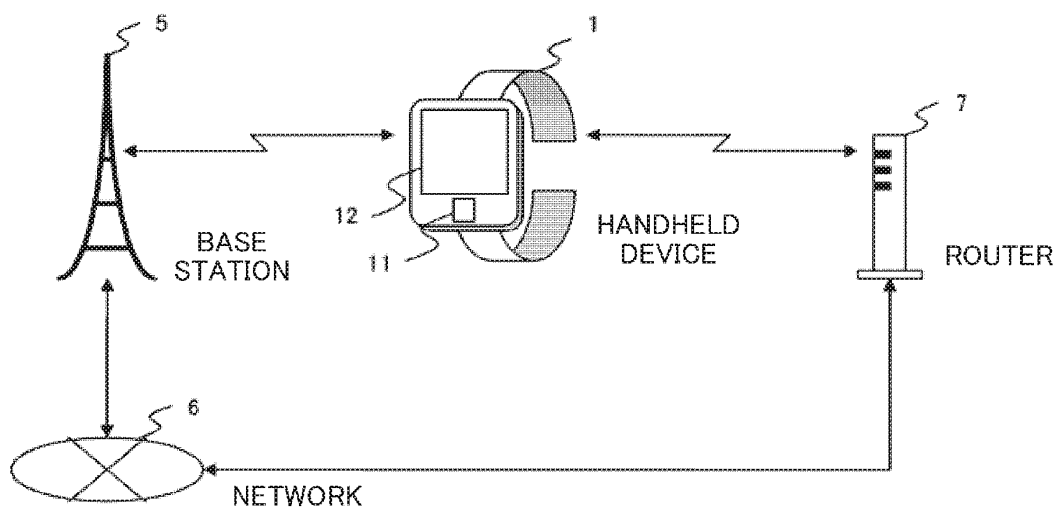
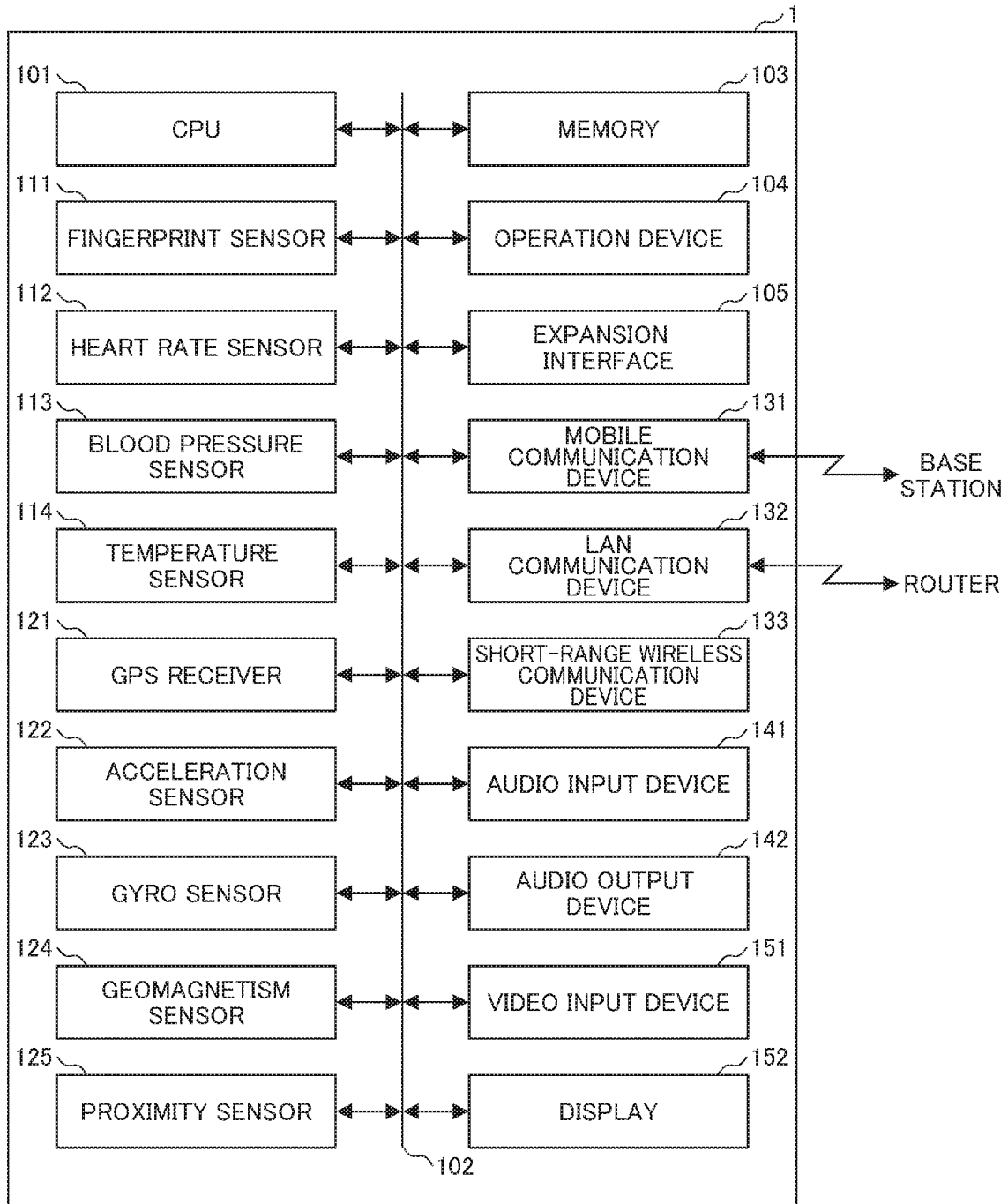


FIG. 2



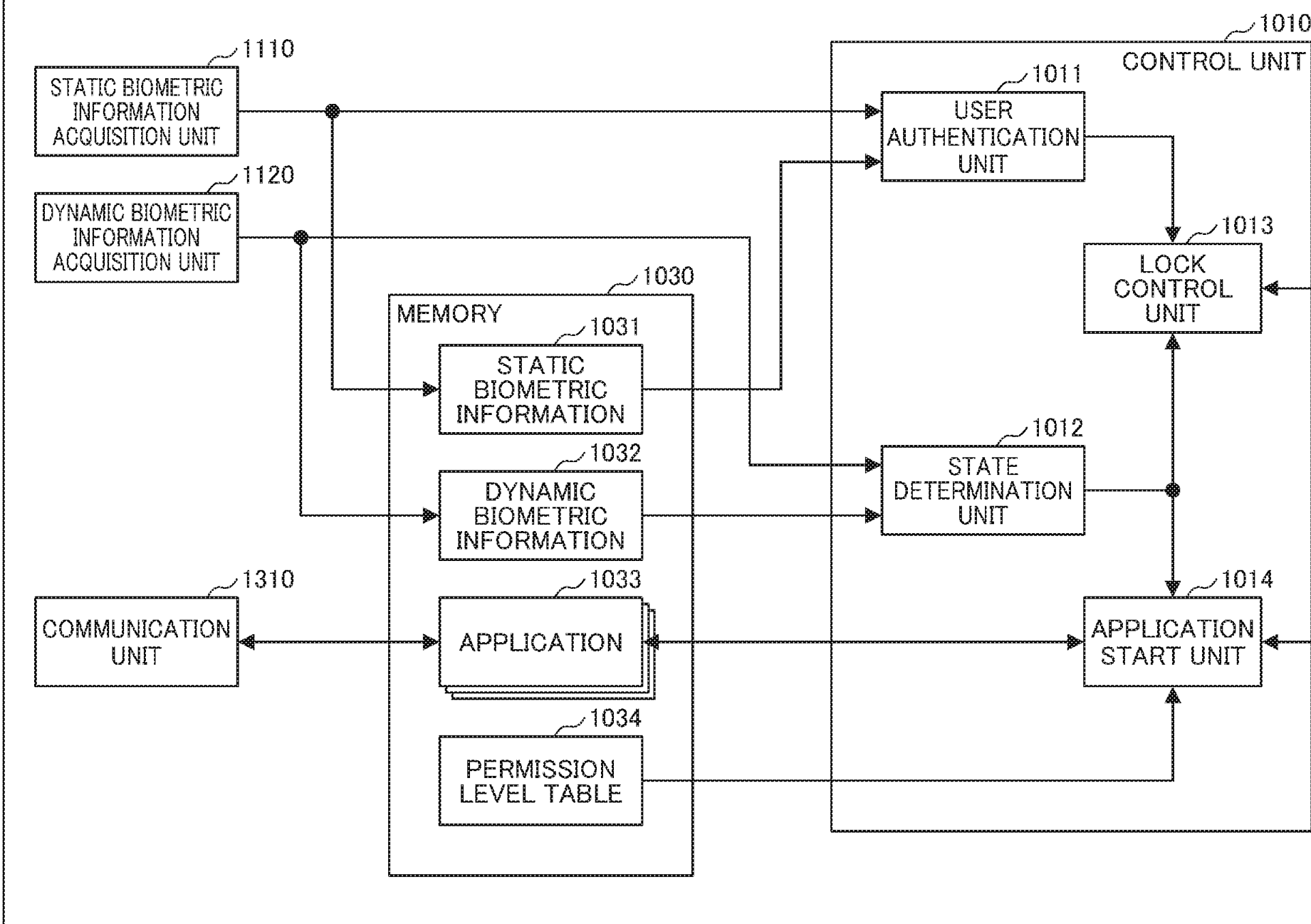


FIG. 4

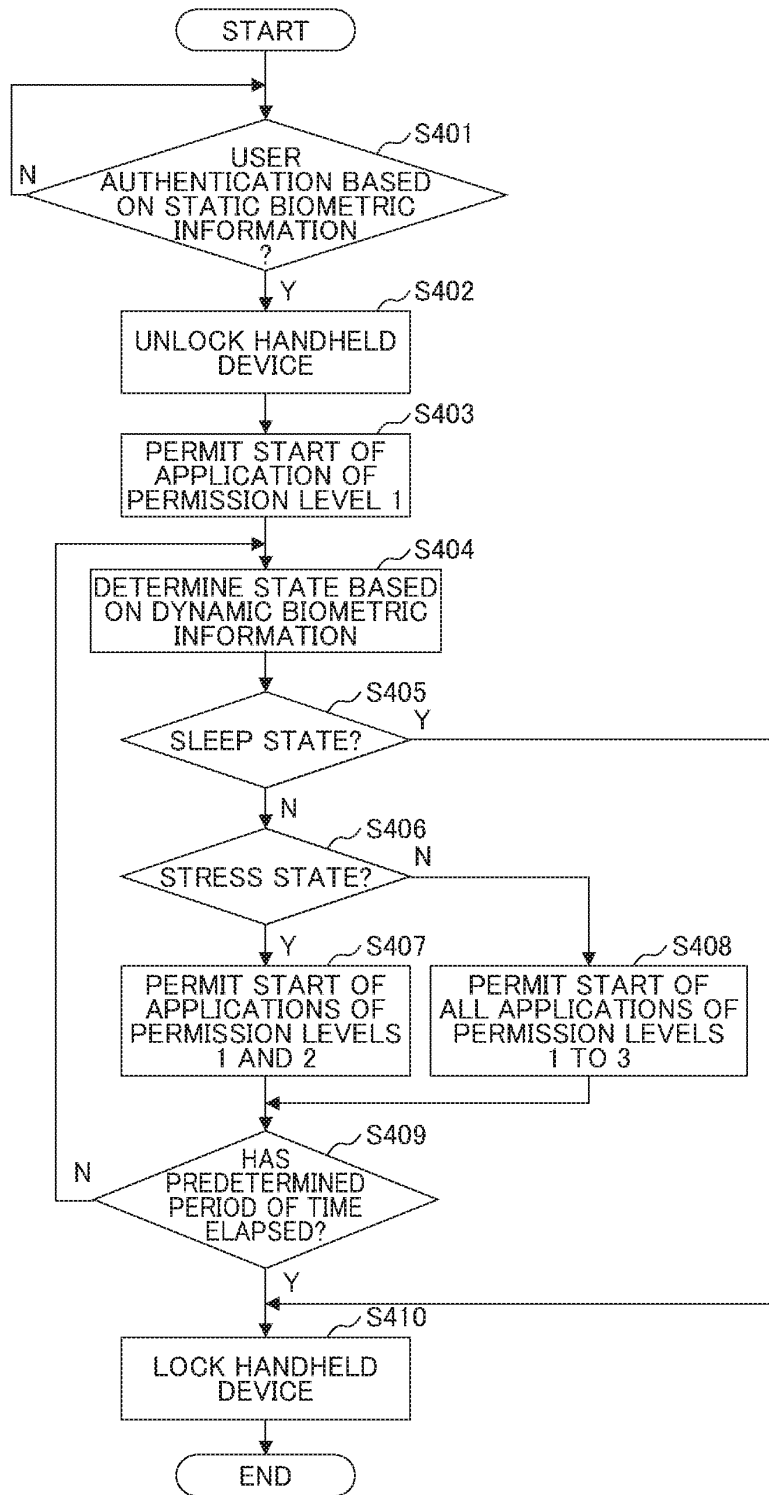


FIG. 5A

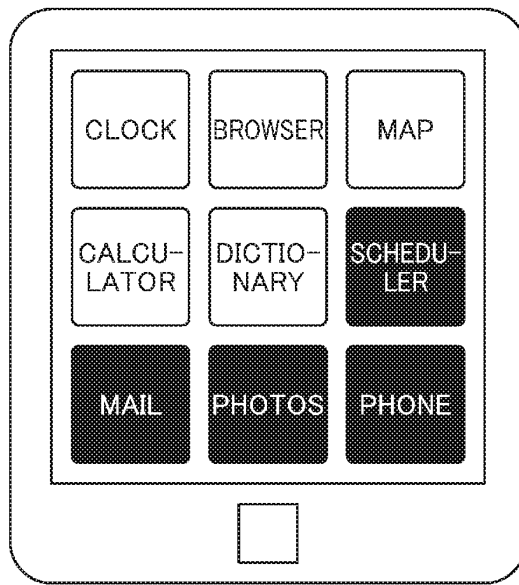


FIG. 5B

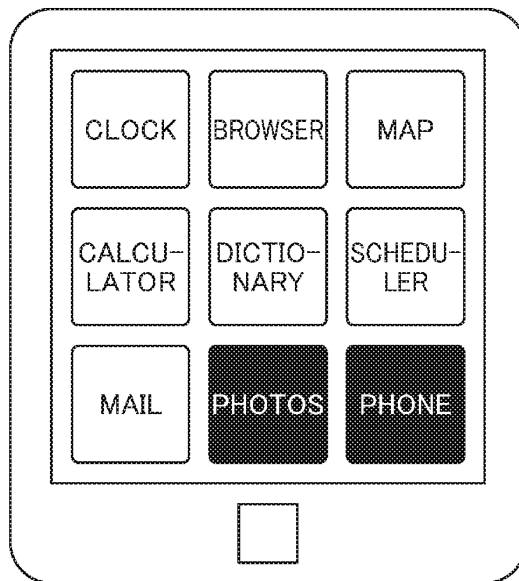


FIG. 5C

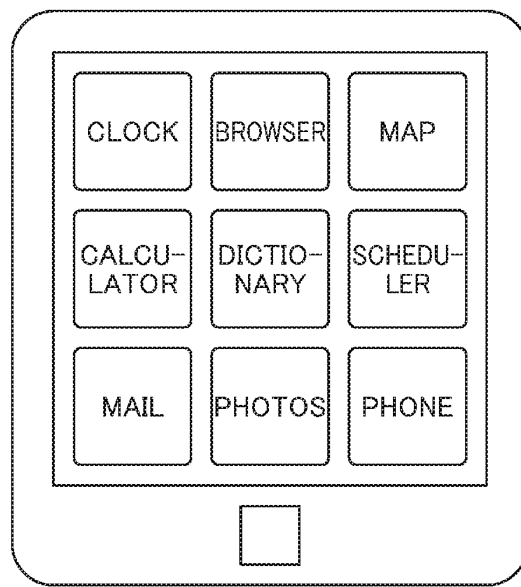
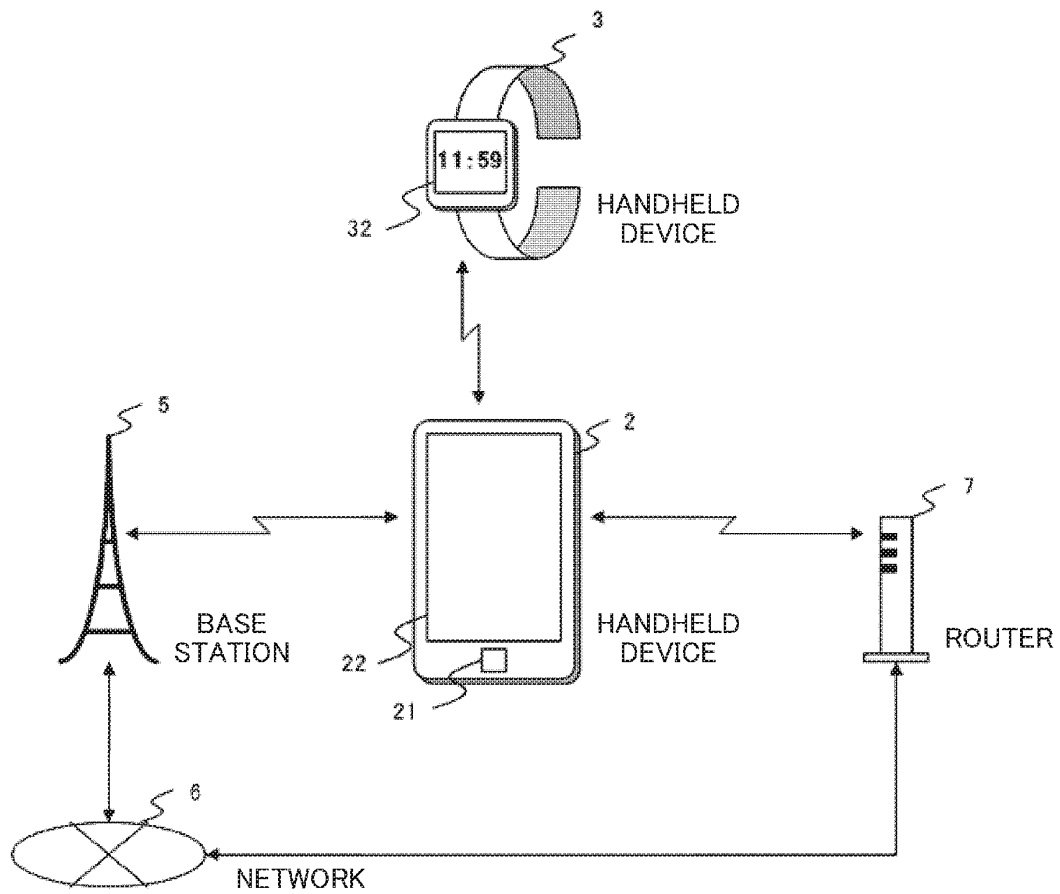
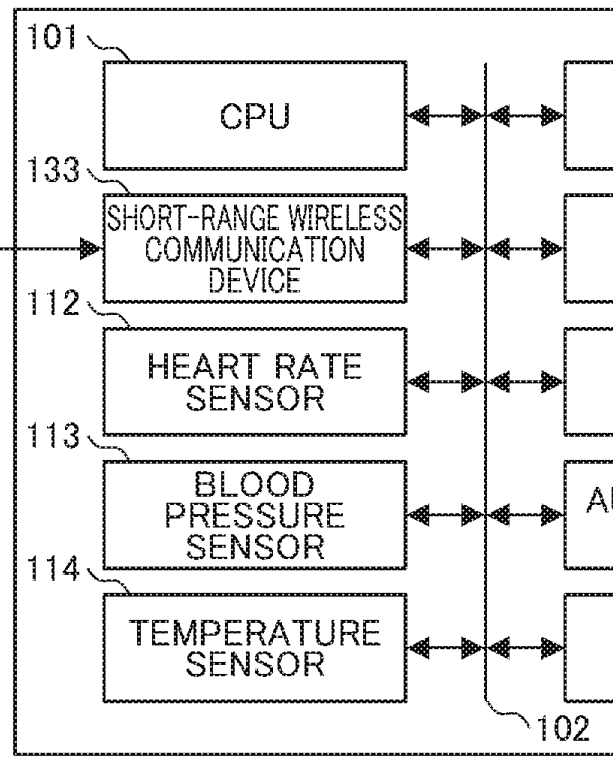
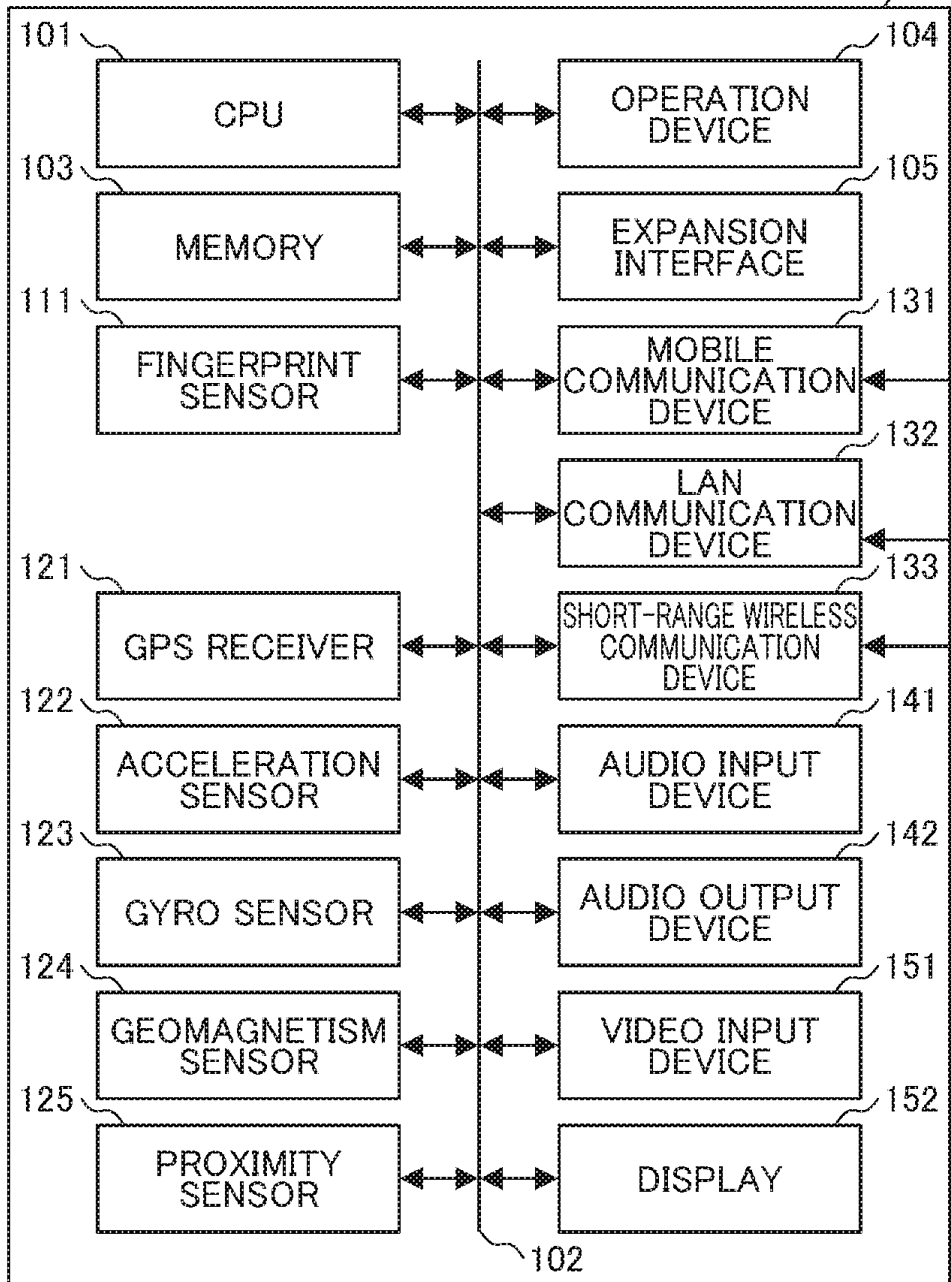
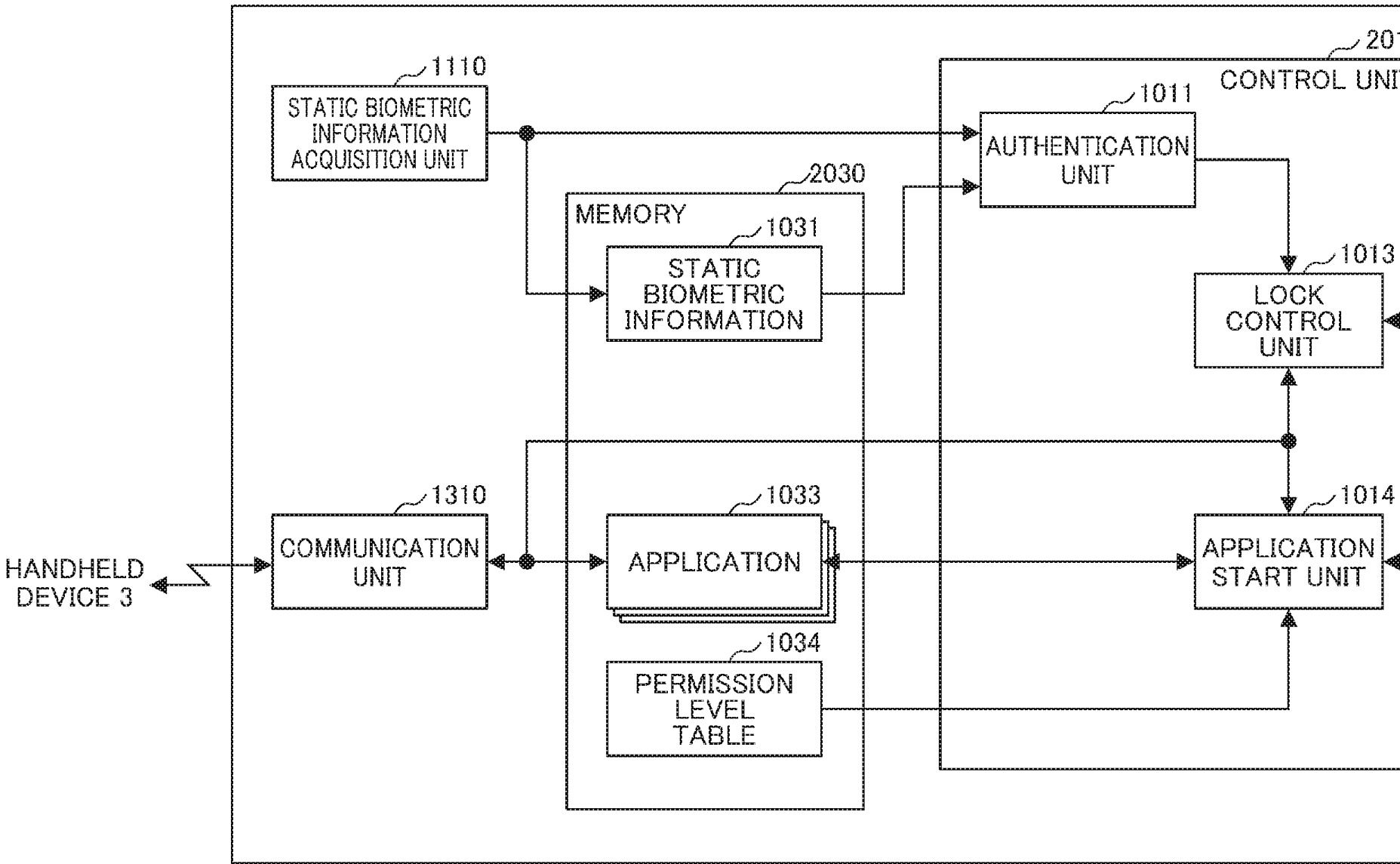


FIG. 6







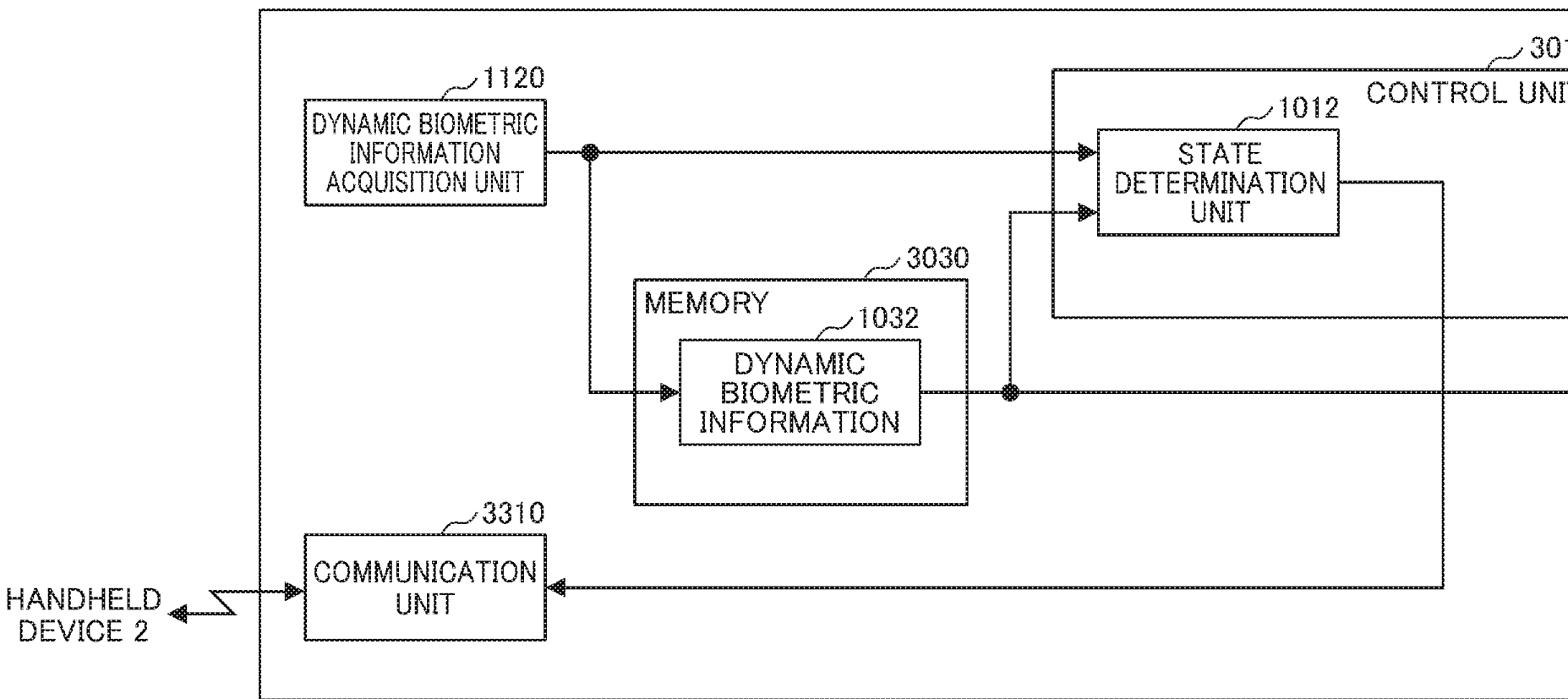


FIG. 10

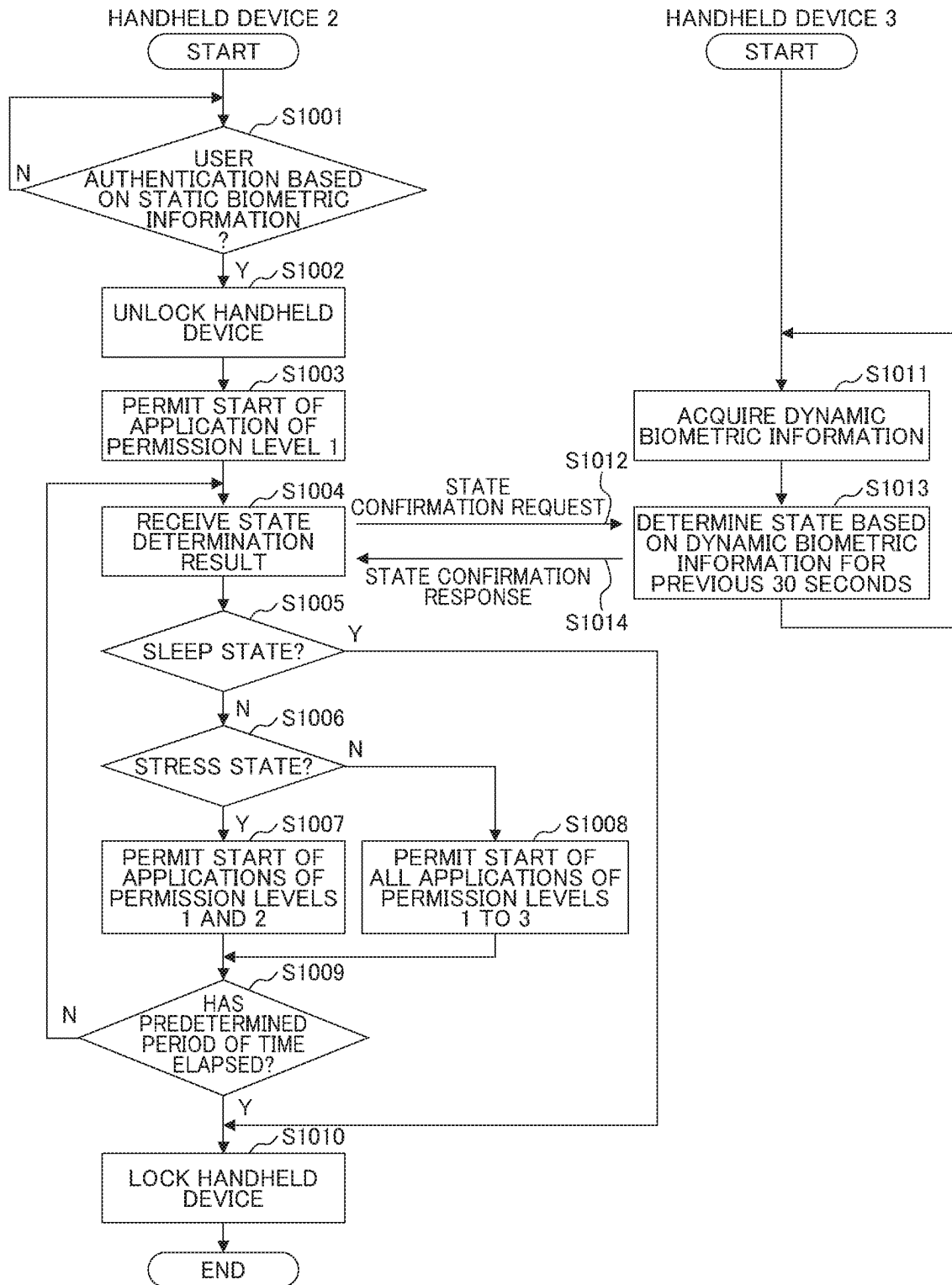


FIG. 11A

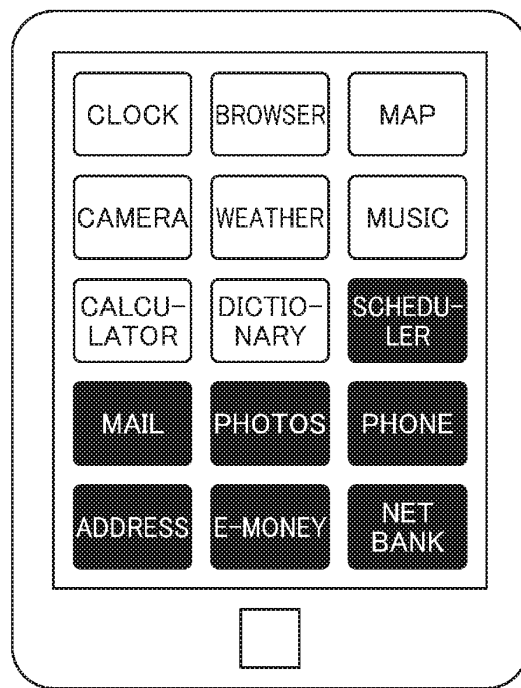


FIG. 11B

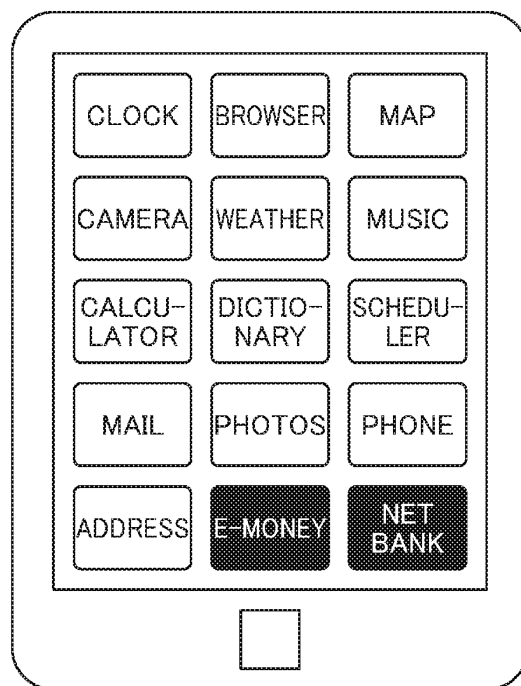


FIG. 11C

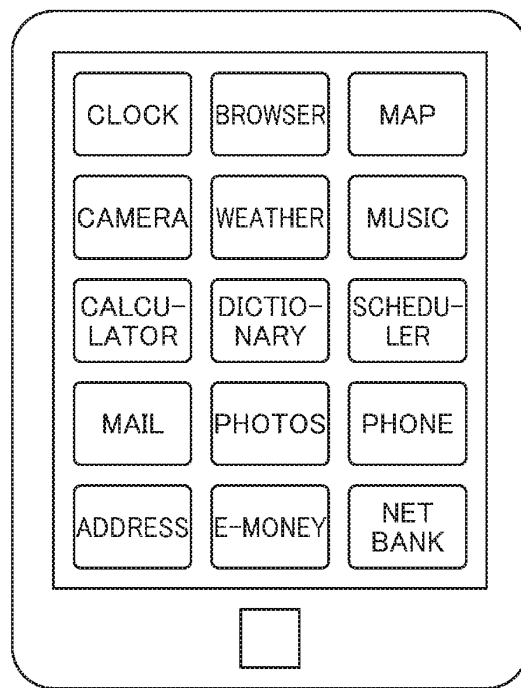


FIG. 12

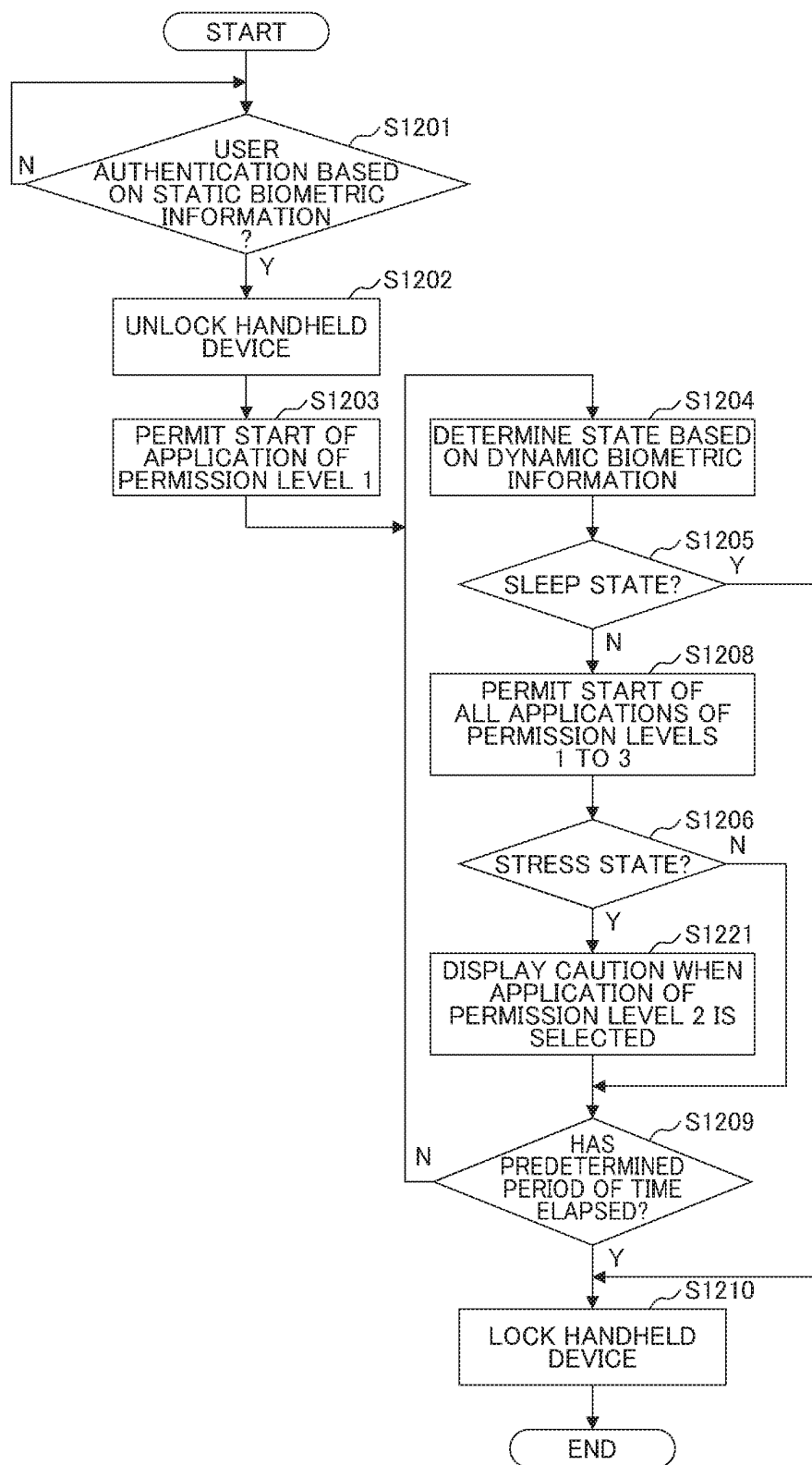


FIG. 13

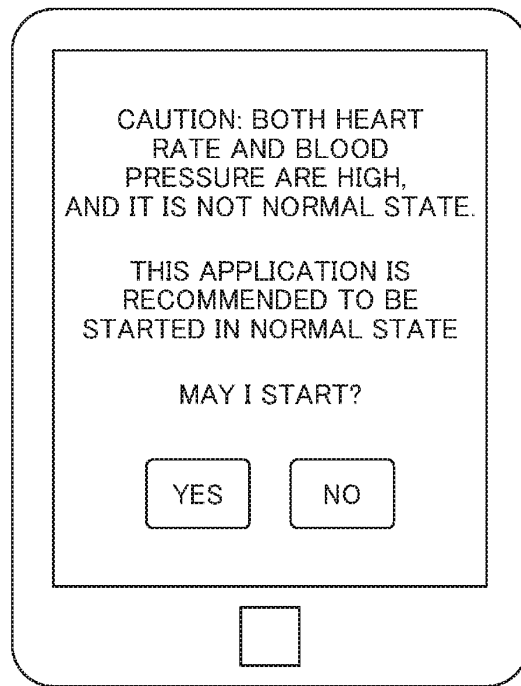


FIG. 14

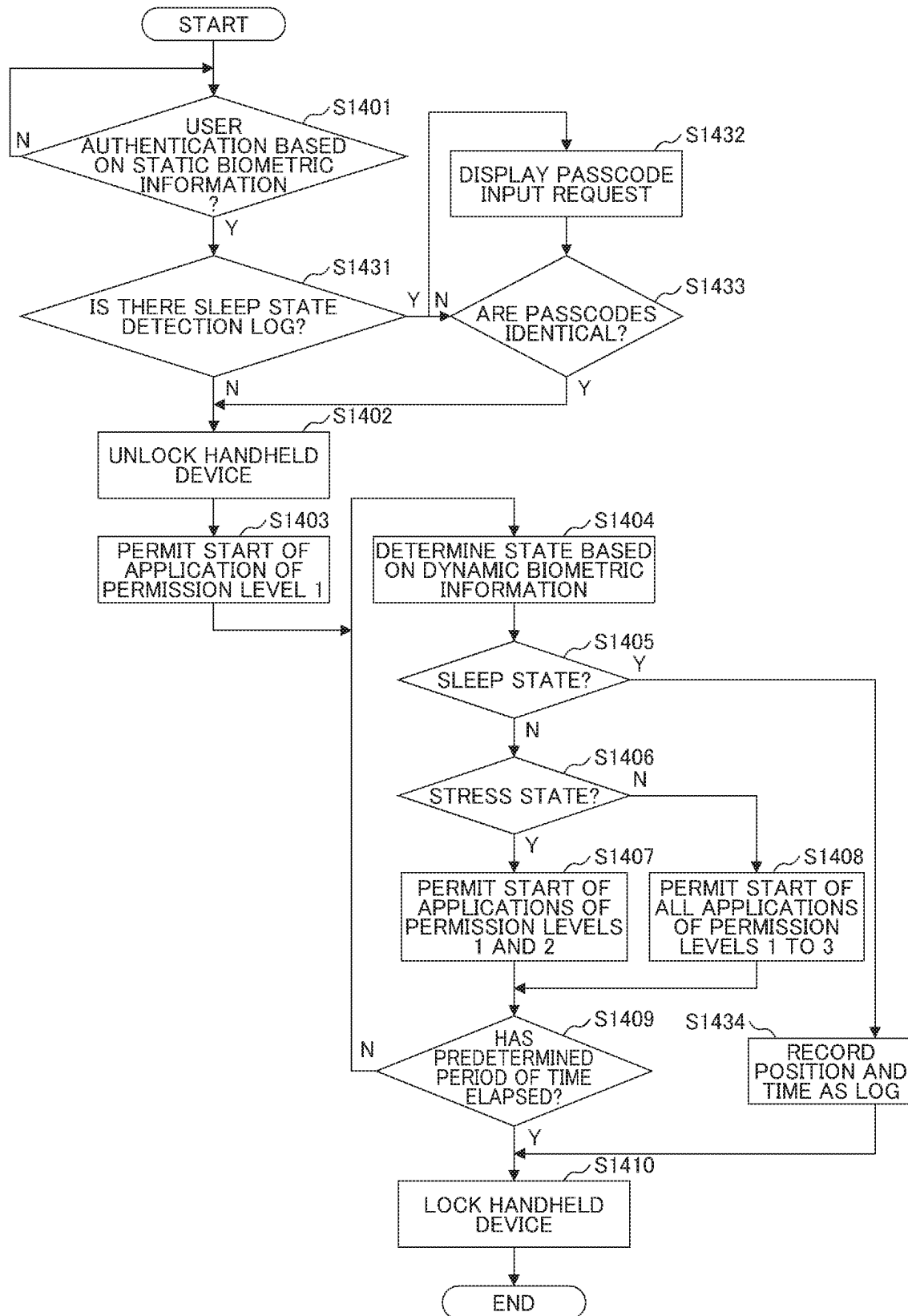


FIG. 15

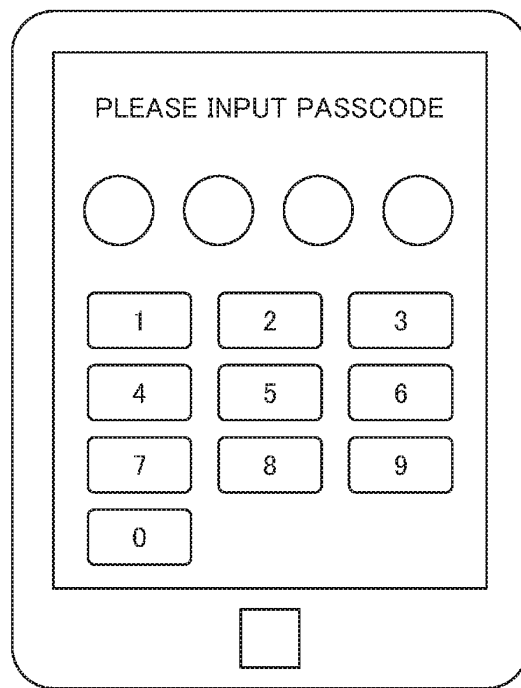


FIG. 16

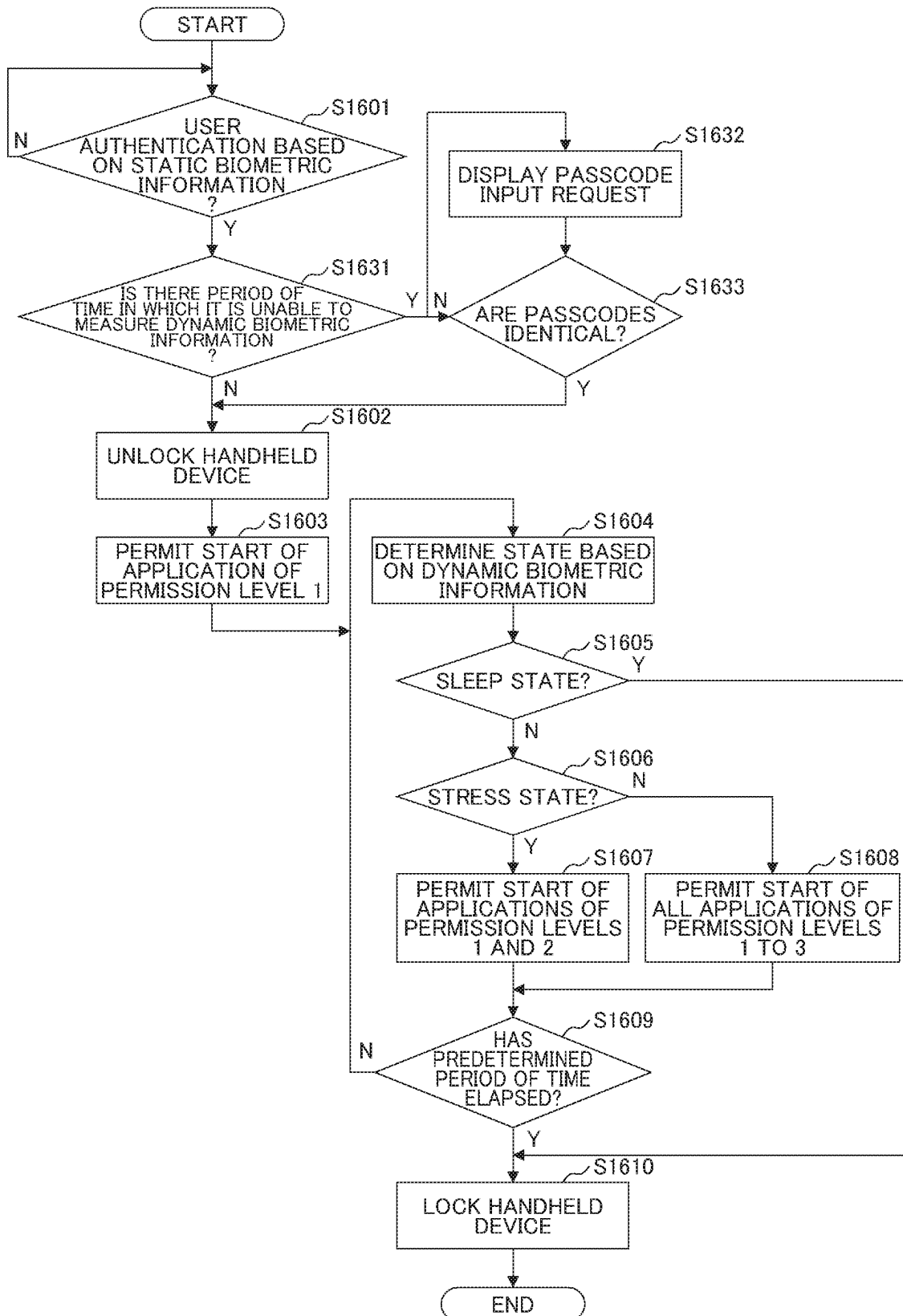
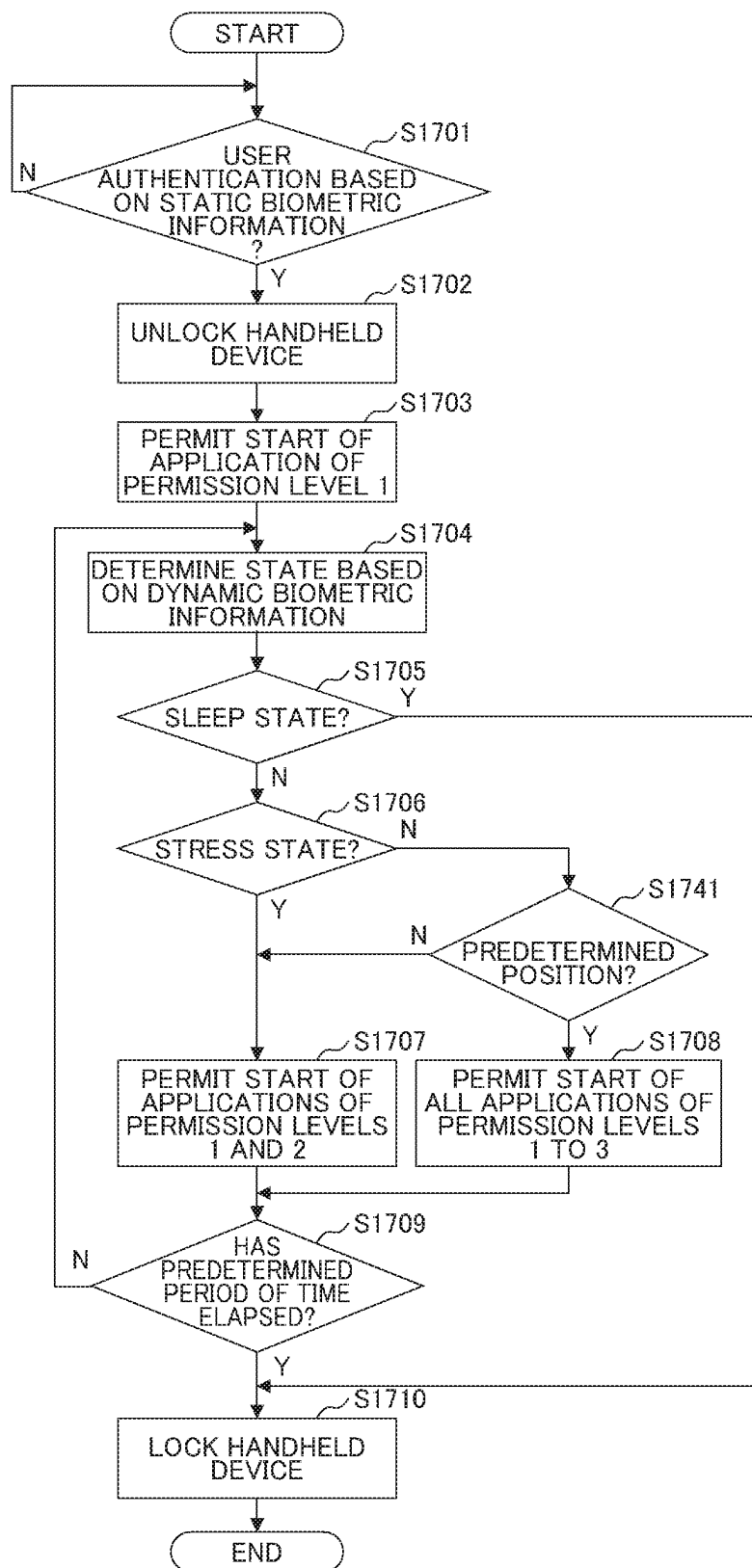


FIG. 17



Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD		
First Named Inventor/Applicant Name:		Masayuki HIRABAYASHI		
Filer:		John Roberts Mattingly/Krista Hargrove		
Attorney Docket Number:		SEI-10740-02		
Filed as Large Entity				
Filing Fees for Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
UTILITY APPLICATION FILING	1011	1	300	300
UTILITY SEARCH FEE	1111	1	660	660
UTILITY EXAMINATION FEE	1311	1	760	760
REQUEST FOR PRIORITIZED EXAMINATION	1817	1	4000	4000
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	1202	9	100	900
INDEPENDENT CLAIMS IN EXCESS OF 3	1201	1	460	460

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous-Filing:				
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
PROCESSING FEE, EXCEPT PROV. APPLS.	1830	1	140	140
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				7220

Electronic Acknowledgement Receipt	
EFS ID:	36818850
Application Number:	16535574
International Application Number:	
Confirmation Number:	5886
Title of Invention:	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD
First Named Inventor/Applicant Name:	Masayuki HIRABAYASHI
Customer Number:	24956
Filer:	John Roberts Mattingly/Krista Hargrove
Filer Authorized By:	John Roberts Mattingly
Attorney Docket Number:	SEI-10740-02
Receipt Date:	08-AUG-2019
Filing Date:	
Time Stamp:	14:35:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$7220
RAM confirmation Number	E201988E35452562
Deposit Account	501417
Authorized User	Krista Hargrove
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)					
37 CFR 1.20 (Post Issuance fees)					
37 CFR 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	TrackOne Request	10740-02-TRAC1.pdf	114270	no	2
			9d216a6d47bc188a86259dd44fb1509246ce08e		
Warnings:					
Information:					
2	Application Data Sheet	10740-02-ADS.pdf	1226519	no	9
			334f41a5bfaddc05d2f58941666905e4c4f52e60		
Warnings:					
Information:					
3	Power of Attorney	10740-02-POA.pdf	399690	no	4
			dcc1612ce1d12929d6c5449d7539d90312cd8f1c6		
Warnings:					
Information:					
4	Transmittal Letter	10740-02-IDS.pdf	16230	no	2
			e2c45ac97571745a2bd2574b13392371f3f00cbf		
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	10740-02-SB08A.pdf	614026	no	7
			20fd325b192f6c13769f014defe04edda15083b8		
Warnings:					
Information:					
6		10740-02-SPEC-Rev1.pdf	183458	yes	70
			b3aebc9e9c637b6a21b6024fa6cab9cb6503224c		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	

	Specification	1	56		
	Claims	57	69		
	Abstract	70	70		
Warnings:					
Information:					
7	Oath or Declaration filed	10740-02-DEC.pdf	448831	no	6
			b9e1230ddecc416babfd8058c469ca03f745c5f4		
Warnings:					
Information:					
8	Drawings-only black and white line drawings	10740-02-DWG.pdf	1517877	no	19
			da478727757ff65b5d890b41b22baae6c5420b71		
Warnings:					
Information:					
9	Fee Worksheet (SB06)	fee-info.pdf	43362	no	2
			7c42aa1112bbaa7c313129cac59449637be83b1f		
Warnings:					
Information:					
Total Files Size (in bytes):			4564263		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

**CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION
UNDER 37 CFR 1.102(e) (Page 1 of 1)**

First Named Inventor:	M. HIRABAYASHI	Nonprovisional Application Number (if known):	
Title of Invention:	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1) and the prioritized examination fee set forth in 37 CFR 1.17(c) have been filed with the request. The publication fee requirement is met because that fee, set forth in 37 CFR 1.18(d), is currently \$0. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.
2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims, and that any request for an extension of time will cause an outstanding Track I request to be dismissed.
3. The applicable box is checked below:
 - I. ☒ **Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)**
 - i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.
---OR---
 - (b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.
 - ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, or the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.
 - II. ☐ **Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)**
 - i. A request for continued examination has been filed with, or prior to, this form.
 - ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
 - iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
 - iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
 - v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature <u>/JOHN R. MATTINGLY/</u>	Date <u>August 8, 2019</u>
Name (Print/Typed) <u>JOHN R. MATTINGLY</u>	Practitioner Registration Number <u>30293</u>
Note: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required.*	
☒ *Total of <u>1</u> forms are submitted.	

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record in this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	SEI-10740-02
		Application Number	
Title of Invention	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor	1				Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Masayuki		HIRABAYASHI		
Residence Information (Select One) US Residency • Non US Residency Active US Military Service					
City	Ibaraki-shi, Osaka		Country of Residence ⁱ	JP	
Mailing Address of Inventor:					
Address 1	c/o Maxell, Ltd.				
Address 2	1, Koizumi, Oyamazaki, Oyamazaki-cho Otokuni-gun				
City	Kyoto	State/Province			
Postal Code	618-8525	Country ⁱ	JP		
Inventor	2				Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Yasunobu		HASHIMOTO		
Residence Information (Select One) US Residency • Non US Residency Active US Military Service					
City	Ibaraki-shi, Osaka		Country of Residence ⁱ	JP	
Mailing Address of Inventor:					
Address 1	c/o Maxell, Ltd.				
Address 2	1, Koizumi, Oyamazaki, Oyamazaki-cho Otokuni-gun				
City	Kyoto	State/Province			
Postal Code	618-8525	Country ⁱ	JP		
Inventor	3				Remove
Legal Name					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	SEI-10740-02
		Application Number	
Title of Invention	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD		

Prefix	Given Name	Middle Name	Family Name	Suffix
	Kazuhiko		YOSHIZAWA	
Residence Information (Select One) US Residency ☒ Non US Residency Active US Military Service				
City	baraki-shi, Osaka		Country of Residence ⁱ	JP
Mailing Address of Inventor:				
Address 1	c/o Maxell, Ltd.			
Address 2	1, Koizumi, Oyamazaki, Oyamazaki-cho Otokuni-gun			
City	Kyoto	State/Province		
Postal Code	618-8525	Country ⁱ	JP	
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button. Add				

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).	
☐ An Address is being provided for the correspondence Information of this application.	
Customer Number	24956
Email Address	ptomail@mmiplaw.com Add Email Remove Email

Application Information:

Title of the Invention	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD		
Attorney Docket Number	SEI-10740-02	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	19	Suggested Figure for Publication (if any)	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country ⁱ

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	SEI-10740-02
		Application Number	
Title of Invention	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD		

Publication Information:

☐	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐	Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.			
Please Select One:			
☒	Customer Number	☐	Limited Recognition (37 CFR 11.9)
Customer Number	24956		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	15315735	2016-12-02
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
15315735	a 371 of international	PCT/JP2014/065644	2014-06-12
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			Add

Foreign Priority Information:

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	SEI-10740-02
		Application Number	
Title of Invention	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD		

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)	Remove

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	SEI-10740-02
		Application Number	
Title of Invention	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD		

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	SEI-10740-02
		Application Number	
Title of Invention	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD		

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.			
Applicant	1		Remove
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.			
		Clear	
☒ Assignee	Legal Representative under 35 U.S.C. 117		Joint Inventor
Person to whom the inventor is obligated to assign.		Person who shows sufficient proprietary interest	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
Name of the Deceased or Legally Incapacitated Inventor:			
If the Applicant is an Organization check here. ☒			
Organization Name	Maxell, Ltd.		
Mailing Address Information For Applicant:			
Address 1	1, Koizumi, Oyamazaki, Oyamazaki-cho Otokuni-gun		
Address 2			
City	Kyoto	State/Province	
Country	JP	Postal Code	618-8525
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button. Add			

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	SEI-10740-02
		Application Number	
Title of Invention	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD		

Assignee 1				
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.				
				Remove
If the Assignee or Non-Applicant Assignee is an Organization check here. ☐				
Prefix	Given Name	Middle Name	Family Name	Suffix
Mailing Address Information For Assignee including Non-Applicant Assignee:				
Address 1				
Address 2				
City		State/Province		
Country i		Postal Code		
Phone Number		Fax Number		
Email Address				
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.				Add

Signature:[Remove](#)

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/John R. Mattingly/		Date (YYYY-MM-DD)	2019-08-08
First Name	John	Last Name	Mattingly	Registration Number
			30,293	
Additional Signature may be generated within this form by selecting the Add button.				Add

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	SEI-10740-02
		Application Number	
Title of Invention	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD		

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

単数又は複数の特許弁護士への委任状伝送書
TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

注記：37 CFR 1.5に従い、委任状が示す出願を特定するため、本書類は「出願人による委任状(PTO/AIA/82B)」と共に提出すること。ただし、「出願人による委任状」で出願番号および出願日が特定されている場合を除く。委任状が示す出願が、PTO/AIA/82AおよびPTO/AIA/82Bのどちらにもおいても特定されていない場合、同出願においての代理権は認められない。

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA/82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

出願番号 Application Number	NEW
出願日 Filing Date	August 8, 2019
第一発明者 First Named Inventor	Masayuki HIRABAYASHI
名称 Title	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD
技術審査部門 Art Unit	To Be Assigned
審査官氏名 Examiner Name	To Be Assigned
特許弁護士整理番号 Attorney Docket Number	SEI-10740-02

出願人または特許弁護士の署名
SIGNATURE of Applicant or Patent Practitioner

署名 Signature	/John R. Mattingly/	署名日(任意) Date (Optional)	August 8, 2019
氏名 Name	John R. Mattingly	登録番号 Registration Number	30,293
役職(出願人が法人の場合) Title (if Applicant is a juristic entity)			

出願人名(出願人が法人の場合) Applicant Name (if Applicant is a juristic entity)	
---	--

注記：本書類は37 CFR 1.33に基づき署名されなければならない。署名に関する要件および証明については37 CFR 1.4(d)を参照。出願人が複数の場合は複数の用紙を使うこと。

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☒ *提出書類 計 _____ 枚。
*Total of 3 _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

出願人による委任状
POWER OF ATTORNEY BY APPLICANT

私はここに、添付の伝送書もしくは下記枠内で特定された出願に対して、現時点より前に与えられたすべての委任状を破棄します。
I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

出願番号 Application Number	出願日 Filing Date

(注記: PTO/AIA/82Aに同じ情報が明記されている場合、上の枠内は空欄でも可)
(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)



私は、下記顧客番号に関連する特許弁護士を、当方の弁護士あるいは代理人に指名し、添付の伝送書 (PTO/AIA/82A) 内もしくは上記に記載の特許出願に関連した米国特許商標庁との業務の全てを同弁護士あるいは代理人に委任します。

I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above:

24956

又は
OR



私は、添付のリスト (PTO/AIA/82C) に記載の特許弁護士を、当方の弁護士あるいは代理人に指名し、添付の伝送書 (PTO/AIA/82A) 内もしくは上記に記載の特許出願に関連した米国特許商標庁との業務の全てを同弁護士あるいは代理人に委任します。(注記: PTO/AIA/82C を記入すること。)

I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

添付の伝送書又は上記枠内にて特定された出願に対する郵便物送付先を下記のいずれかに登録または変更してください。

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:



上記顧客番号に付随する住所
The address associated with the above-mentioned Customer Number

又は
OR



顧客番号に付随する住所
The address associated with Customer Number:

又は
OR

事務所または個人名 Firm or Individual Name				
住所 Address				
市 City	州 State	郵便番号 Zip		
国 Country				
電話番号 Telephone	メールアドレス Email			

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

出願人による委任状 POWER OF ATTORNEY BY APPLICANT

私は出願人であり（出願人が法人の場合、出願人名を下記枠内に記入）：

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

Maxell, Ltd.

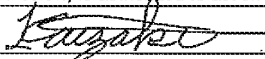
- ☐ 発明者もしくは共同発明者である（下記役職の明記は不要）
Inventor or Joint Inventor (title not required below)
- ☐ 死亡したもしくは成年被後見人である発明者の法定代理人である（下記役職の明記は不要）
Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)
- ☒ 被譲渡人もしくは発明者が譲渡する義務を負う人物である
Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)
- ☐ 上記以外で、十分な独占的所有権を示す人物である（例：37 CFR 1.46(b)(2)に基づく申請が本出願において認められた、又は本書類と共にその申請がなされている場合）（出願人が法人の場合、署名者の役職を明記すること）
Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

特許出願人の署名

SIGNATURE of Applicant for Patent

下記署名者（役職は下記に記載）は出願人の代理人と認められている（出願人が法人の場合等）

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

署名 Signature		署名日（任意） Date (Optional)	Oct. 17, 2017
氏名 Name	Kazuhiro Kaizaki		
役職 Title	Vice President		

注記：署名 - 本書類は37 CFR 1.33に基づき署名されなければならない。署名の要件および証明に関しては37 CFR 1.4を参照。出願人が複数いる場合は、複数の書類を使うこと。

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ 提出書類 計 _____ 枚。
Total of _____ forms are submitted.

Privacy Act Statement

1974年プライバシー保護法(P.L. 93-579)により、特許出願あるいは特許に関する添付書類の提出に関連し、特定情報を提供することが求められています。同法の規定要件に基づき、下記の事項に注意してください。(1) 本情報の収集は35 U.S.C 2(b)(2)により認められています。(2) 求められた情報の提供は任意です。(3) 米国特許商標庁による本情報の主な使用目的は、特許出願あるいは特許に関する提出書類の処理や審査であり、求められた情報を提出しない場合、米国特許商標庁による提出書類の処理や審査に支障をきたす場合があります。その場合、特許出願の手続中止や放棄、または特許失効につながる場合があります。

本用紙に記載された情報は以下の通常使用目的に使われます。

1. 本用紙に記載の情報は、情報公開法(5 U.S.C. 552)およびプライバシー法(5 U.S.C 552a)が許容する範囲において機密情報扱いとなります。本記録システムの記録は、同記録の開示が情報公開法で要求されるものに該当するか否かを判断する目的で、司法省に開示される場合があります。
2. 本記録システムの記録は、通常使用として、法廷、予審判事、行政裁判所に証拠として開示される場合があります。これには示談交渉における反対側弁護士への情報開示も含まれます。
3. 本記録システムの記録は、同記録に関連する個人から、同記録についての支援を依頼され、当該個人に関連した要求を行う米国会議員に対し、通常使用の範囲として開示される場合があります。
4. 本記録システムの記録は、契約を履行するために同記録を必要とする本庁の契約業者に対し、通常使用の範囲として開示される場合があります。情報を受け取る側は、5. U.S.C. 552a(m)に基づき、1974年プライバシー法修正法の規定要件を遵守しなければなりません。
5. 本記録システム内の、特許協力条約に基づき出願された国際出願に関する記録は、通常使用の範囲として、特許協力条約に従い世界的な所有権機関に開示される場合があります。
6. 本記録システムの記録は、通常使用の範囲として、国家安全保障(35 U.S.C. 181)および原子力法(42 U.S.C. 218(c))に拠る検討目的で、他の連邦政府機関に開示される場合があります。
7. 本記録システムの記録は、通常使用の範囲として、44 U.S.C 2904および2906に基づき、記録管理方法およびプログラムに対する改善を提案するという米一般調達局長官(GSA)の職務の一部として実施される記録監査において、GSAまたはその委任による代理人に対し開示される場合があります。この開示は、上記目的による記録監査を規定するGSA法規およびその他関連する(GSAまたは商務省)指令に従って行われます。この開示は、個人を特定する目的に使用されてはなりません。
8. 本記録システムの記録は、通常使用の範囲として、特許出願公開後(35. U.S.C 112(b))、または特許発行後(35 U.S.C. 151)に一般に開示される場合があります。さらに、同記録が、放棄されたもしくは処理が集結している特許出願に記載されており、かつ公開後の出願、一般審査に公開された出願、または発行済み特許の中で参照されている場合には、37. CFR 1.14の制限に従い、通常使用の範囲として、一般に開示される場合があります。
9. 本記録システムの記録は、法律に違反している、もしくは違反する可能性があるとして米国特許商標庁により判断された場合、通常使用の範囲として、連邦、州、または地方自治体の警察等に開示される場合があります。

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s) : M. HIRABAYASHI, et al. Confirmation No.: TBD
Serial No. : To be assigned
Filed : August 8, 2019
For : INFORMATION PROCESSING DEVICE, APPLICATION
SOFTWARE START-UP SYSTEM, AND APPLICATION
SOFTWARE START-UP METHOD
Group : To be assigned
Examiner : To be assigned
Docket No. : SEI-10740-02
Customer No.: 24956

INFORMATION DISCLOSURE STATEMENT (IDS)
UNDER § 1.97 AND § 1.98

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

August 8, 2019

Sir:

In the matter of the above-identified application, Applicants are submitting herewith a copy, where required, of the documents listed in the attached form PTO/SB/08a. It is requested that the information be considered by the Examiner during prosecution of the application, and that the references be made of record therein.

Applicants note that:

One or more references cited on the attached PTO/SB/08a was cited by or submitted to the U.S. Patent and Trademark Office in parent application No. 15/315,735, filed December 2, 2016, which is relied upon for an earlier filing date under 35 U.S.C. §120. No copies of the references are attached pursuant to 37 CFR §1.98(d).

The Commissioner is authorized to charge any shortage in the fees due, or credit any overpayment, to Deposit Account No. 50-1417.

If the PTO determines that part(s) of the required content is inadvertently omitted, then it is requested that the Applicant(s) be given additional time and specific identification of such omission(s) to enable full compliance.

Respectfully submitted,

MATTINGLY & MALUR, PC

/John R. Mattingly/
John R. Mattingly
Registration No. 30,293
703-684-1120