

(19) Japanese Patent Office
(JP)

(12) Japanese Unexamined
Patent Application
Publication (A)

(11) Japanese Unexamined Patent
Application Publication Number

2001-109855
(P2001-109855A)

(43) Publication date April 20, 2001 (4.20.2001)

(51) Int.Cl. ⁷	Identification codes	FI	Theme codes (reference)
GO6K 17/00		G06K 17/00	V 5B043
GO6T 7/00		G06F 15/62	460 5B058
			465K

Number of unclaimed claims for review 2 OL (4 pages in total)

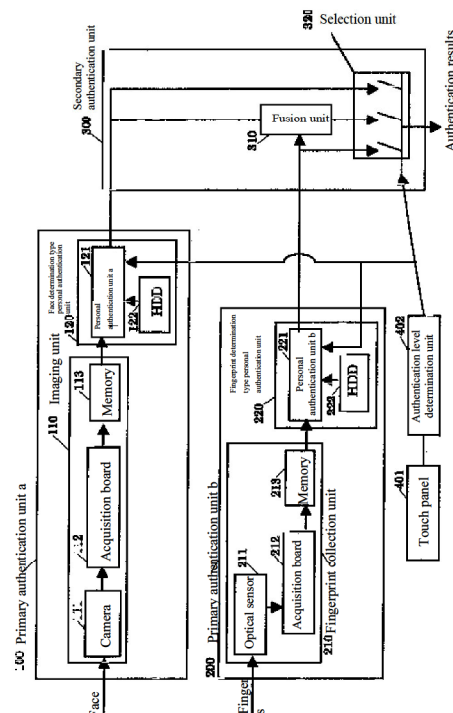
(21) Application number	Japanese Patent Application H11-290684	(71) Applicant	000005821 Matsushita Electric Industry Co., Ltd 1006 Kadoma, Kadoma-shi, Osaka Prefecture
(22) Application date	October 13, 1999 (10.13.1999)	(72) Inventor	Kazushi Mizusawa c/o Matsushita Research Institute Co., Ltd., 3-10-1 Higashi-Mita, Tama-ku, Kawasaki City, Kanagawa Prefecture
		(72) Inventor	Kenji Nagao c/o Matsushita Research Institute Co., Ltd., 3-10-1 Higashi-Mita, Tama-ku, Kawasaki City, Kanagawa Prefecture
		(74) Agent	100097445 Patent attorney Fumio Iwahashi (and 2 others)
		F terms (reference)	5B043 AA09 BA02 BA04 DA05 GA01 GA13 5B058 KA38

(54) [Title of the Invention] Personal authentication device

(57) [Abstract]

[Problem] The purpose of the present invention is to realize a personal authentication device that provides an excellent user interface that always minimizes the burden on the person being authenticated while maintaining the required authentication accuracy.

[Means for Solving] The system includes a plurality of primary authentication means that use different personal authentication methods, and a secondary authentication means that ultimately authenticates the individual using the output result of the primary authentication unit. In addition, to minimize the burden on the person being authenticated, the system is designed to include a method of authenticating an individual by face as one of the primary authentication methods. This makes it possible to maintain the required authentication accuracy at all times and to minimize user failures depending on the safety level, thereby improving the user interface during operation.



[Scope of Patent Claims]

[Claim 1] A personal authentication device having a plurality of primary authentication units each having a different personal authentication method and a secondary authentication unit which finally authenticates the individual using the output result of the primary authentication units, wherein one of the primary authentication units is a primary authentication unit which authenticates the individual using an acquired facial image, and the secondary authentication unit is comprised of a primary authentication unit selection unit which selects the primary authentication means to be used for authentication, and a final determination unit which selects or combines the results of any of the primary authentication units to output the authentication result for the individual.

[Claim 2] A personal authentication device according to Claim 1, characterized in that the primary authentication unit comprises a primary authentication unit that authenticates an individual using a facial image and a primary authentication unit that authenticates an individual using a fingerprint.

[Detailed Description of the Invention]

[0001]

[Technical field to which the invention pertains] The present invention relates to the field of personal authentication, such as matching an ID card with its bearer and verifying the identity of the bearer through a registered database.

[0002]

[Prior art] Conventional personal authentication devices often authenticate individuals using only one of their unique characteristics, such as their face, fingerprint, voiceprint, or iris. For example, Japanese Unexamined Patent Application No. 9-319877 lists face and voiceprint features as features to be used for personal authentication.

[0003] In general, iris and fingerprint authentication have excellent authentication accuracy but place a heavy burden on the person being authenticated, while face authentication places less of a burden on the person being authenticated but has inferior authentication accuracy. Furthermore, even if two features are used to further improve authentication accuracy, those features are fixed and it is not possible to authenticate an individual by selecting only one of the features. For example, "Integrating Faces and Fingerprints for Personal Identification" IEEE on pattern analysis and machine intelligence vol.20 No.12 (1998) presents a method that combines a personal authentication method using faces and a personal authentication method using fingerprints.

[0004]

[Problems to be Solved by the Invention] Personal authentication technology is often used in the security field, where there are demands for accuracy of authentication and system security against unauthorized attacks. At the same time, it is also necessary to minimize the burden on those being certified. There is generally a positive correlation between authentication accuracy and the burden on the person being authenticated, and the higher the authentication accuracy, the greater the burden on the person being authenticated tends to be.

[0005] In the conventional technology, since the authentication method is fixed to one, it is not possible to always maintain an optimal balance between authentication accuracy and burden on the person to be authenticated. In other words, in order to adopt a method capable of realizing the highest authentication accuracy required for the system, an excessive burden is imposed on the person to be authenticated even in cases where authentication accuracy is

not required to be that high.

[0006] The present invention aims to realize a personal authentication device that provides an excellent user interface that always minimizes the burden on the person being authenticated while maintaining the required authentication accuracy.

[0007]

[Means for Solving the Problems] To solve this problem, the present invention has multiple primary authentication means that use different personal authentication methods, and a secondary authentication means that finally authenticates an individual using the output result of the primary authentication unit. Furthermore, in order to minimize the burden on the person to be authenticated, the system is characterized in that one of the primary authentication means always includes a means of authenticating an individual by face.

[0008] The secondary authentication means is characterized by having a means for controlling the authentication accuracy according to the required authentication accuracy. This control means is realized by a means for selecting a primary authentication means and a means for selecting or combining the results of the selected primary authentication means.

[0009] This configuration maintains the required authentication accuracy at all times, while making it possible to select the optimal authentication method depending on the security level, improving the user interface during operation.

[0010]

[Embodiments of the Invention] The invention described in Claim 1 of the present invention is an apparatus for authenticating an individual, which is provided with a plurality of primary authentication units having different methods of personal authentication and a secondary authentication unit that finally authenticates an individual using the output result of the primary authentication units, one of which is a primary authentication unit that authenticates an individual using an acquired facial image, and which is equipped with a secondary authentication unit composed of a primary authentication unit selection unit that selects the primary authentication means to be used for authentication, and a final determination unit that selects or combines the results of any of the primary authentication units to output the authentication result of the individual, and by always including a means for authenticating individuals by face as one of the primary authentication means, it has the effect of providing an excellent user interface that always minimizes the burden on the person to be authenticated while maintaining the required authentication accuracy.

[0011] The invention described in Claim 2 is characterized in that, in the personal authentication device described in Claim 1, the primary authentication unit comprises a primary authentication unit that authenticates an individual using a face image and a primary authentication unit that authenticates an individual using a fingerprint, and by combining the two, it is possible to perform authentication with higher accuracy.

[0012] Hereinafter, an embodiment of the present invention will be described with reference to FIG. 1.

[0013] (Embodiment 1) FIG. 1 shows a configuration diagram of a personal authentication device in embodiment 1 of the present invention, and will be described below.

[0014] In FIG. 1, the user selects a desired action using

touch panel 401. The authentication level determination unit 402 outputs an authentication level that has been set in advance according to the desired action input of the user from the touch panel 401 to the secondary authentication unit 300, the primary authentication unit A100, and the primary authentication unit b200. The primary authentication unit a 100 is composed of an imaging unit 110 that captures a facial image of the person to be authenticated, and a face determination type personal authentication unit 120 that authenticates the individual using the facial image data captured by the imaging unit 110, and performs a pre-set operation such as stop or normal authentication depending on the authentication level input from the authentication level determination unit 402.

[0015] The imaging unit 110 is composed of a camera 111, an acquisition board 112, and a memory 113. In the imaging unit 110, the face of the individual to be authenticated is photographed by the camera 111, and the photographed image is converted into digital data by the acquisition board 112 and stored in the memory 113 as face image data.

[0016] The face determination type personal authentication unit 120 includes a personal authentication unit a 121 and an HDD 122. The personal authentication unit a 121 compares the facial image data of the person to be authenticated acquired by the imaging unit 110 with the facial image data in the authentication list previously recorded in the HDD 122, and authenticates the person to be authenticated. This authentication result is output to the secondary authentication unit 300.

[0017] The primary authentication unit b200 is composed of a fingerprint collection unit 210 that captures the fingerprint of the person to be authenticated, and a fingerprint determination type personal authentication unit 220 that authenticates the individual using the fingerprint data captured by the fingerprint collection unit 210, and performs a pre-set operation such as stop or normal authentication depending on the authentication level input from the authentication level determination unit 402.

[0018] The fingerprint collection unit 210 includes an optical sensor 211, an acquisition board 212, and a memory 213. In the fingerprint collection unit 210, the fingerprint of the individual to be authenticated is read by the optical sensor 211, and is converted into digital data by the acquisition board 212, and is stored in the memory 213 as fingerprint data.

[0019] The fingerprint determination type personal authentication unit 220 is composed of an individual authentication unit b 221 and an HDD 222. The personal authentication unit b 221 compares the fingerprint data of the person to be authenticated acquired by the fingerprint collection unit 210 with the fingerprint data in an authentication list recorded in advance in the HDD 222, and authenticates the person to be authenticated. This authentication result is output to the secondary authentication unit 300.

[0020] The secondary authentication unit 300 includes a

fusion unit 310 and a selection unit 320. The fusion unit 310 merges the authentication results of an individual input from the primary authentication unit a 100 and the primary authentication unit b200, thereby authenticating the individual with a higher accuracy than if each authentication was performed separately. The selection unit 320 performs preset operations, outputs the results of primary authentication unit a, outputs the results of primary authentication unit b, and outputs the results of the fusion unit 310, depending on the authentication level input from the authentication level determination unit 402.

[0021] It should be noted that the primary authentication unit b200 may use, for example, an authentication unit that uses a voice print or an iris to authenticate an individual.

[0022]

[Effects of the Invention] As described above, according to the present invention, by including a means for authenticating an individual by face as one of the primary authentication means, it is possible to realize a personal authentication device that provides an excellent user interface that always minimizes the burden on the person to be authenticated while maintaining the required authentication accuracy.

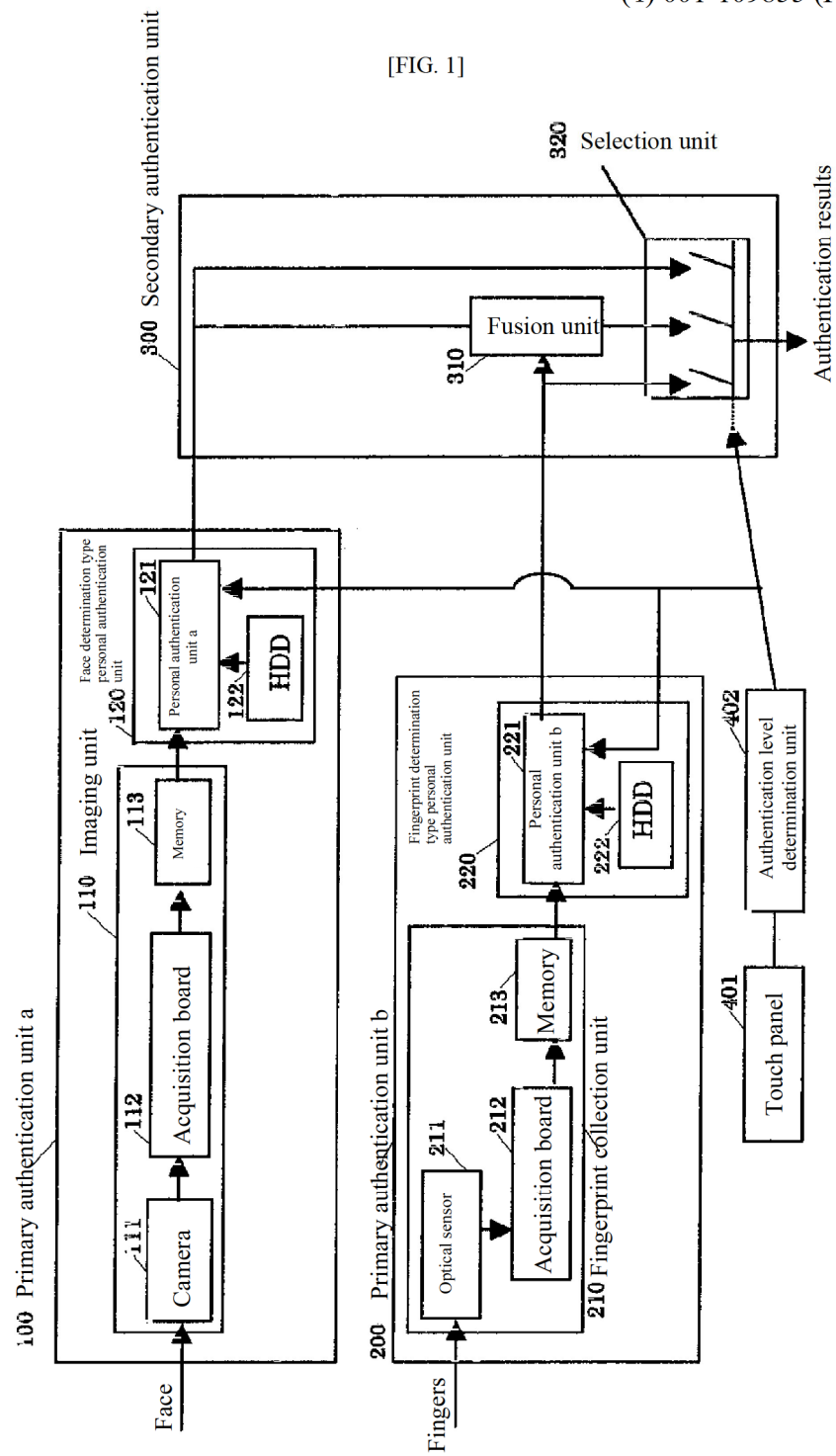
[Brief Description of the Drawings]

[FIG. 1] A configuration diagram showing a personal authentication device according to an embodiment of the invention

[Reference Signs List]

100	Primary authentication unit a
110	Imaging unit
111	Camera
112	Acquisition board
113	Memory
120	Face determination type personal authentication unit
121	Personal authentication unit a
122	HDD
200	Primary authentication unit b
210	Fingerprint collection unit
211	Optical sensor
212	Acquisition board
213	Memory
220	Fingerprint determination type personal authentication unit
221	Personal authentication unit b
222	HDD
300	Secondary authentication unit
310	Fusion unit
320	Selection unit
401	Touch panel
402	Authentication level determination unit

[FIG. 1]



TRANSLATOR'S DECLARATION

I, John Andrews, hereby declare and state as follows:

1. I reviewed the Japanese-language document titled "JP_2001109855_A."
2. I prepared the English-language translation document "JP_2001109855_A" by reviewing and translating the Japanese-language document "JP_2001109855_A."
3. The English-language translation document "JP_2001109855_A" is, to the best of my knowledge and belief, a true and accurate English-language translation of the Japanese-language document "JP_2001109855_A."
4. I am competent and trained to translate documents, including patents and patent applications, from Japanese to English. I possess advanced knowledge of the Japanese and English languages. My qualifications include:
 - I am fluent in speaking and reading both English and Japanese language, and have been so for 15 years;
 - I attended and graduated from Durham University.
 - Master's degree in Translation Studies.
 - I am a Project Manager at Stonebridge Chinese Services Ltd. (UK).
 - In my 15 years as a professional translator, I have translated many technical documents, including patents and patent applications, from Japanese to English.
5. I declare that all statements made on information and belief are believed to be true. I further understand and have been warned that willful false statements and the like are punishable by fine or imprisonment, or both and may jeopardize the validity of the application or

any patent issuing thereon. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on: January 14, 2025

A handwritten signature in black ink, appearing to read "John Andrews", is positioned above a horizontal line.

John Andrews