US 20030046552A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2003/0046552 A1

Hamid (43) Pub. Date: Mar. 6, 2003

(54) METHOD AND SYSTEM FOR PROVIDING ACCESS TO SECURE ENTITY OR SERVICE BY A SUBSET OF N PERSONS OF M DESIGNATED PERSONS

(76) Inventor: **Larry Hamid**, Ottawa (CA)

Correspondence Address:
FREEDMAN & ASSOCIATES
117 CENTREPOINTE DRIVE
SUITE 350
NEPEAN, ONTARIO K2G 5X3 (CA)

(21) Appl. No.: **09/940,795**

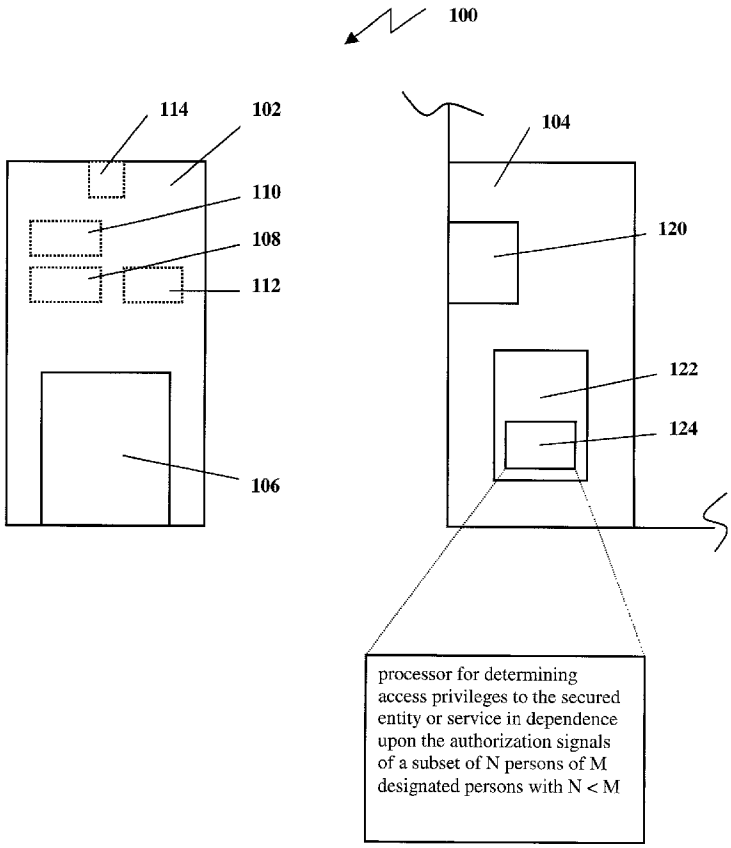
(22) Filed: **Aug. 29, 2001**

Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**
(52) **U.S. Cl.** **713/186**

(57) **ABSTRACT**

A security system for securing an entity or a service from indiscriminate access and a method for operating the same is disclosed. Each designated person of M designated persons is provided with a portable biometric device. Biometric data in dependence upon a biometric characteristic of each of the M designated persons is stored in memory of the respective portable biometric device. Biometric information representative of a biometric characteristic of each of a subset of 1<N<M persons is captured in response to each of the N persons presenting said information to the respective portable biometric device. The biometric information is encoded and biometric data in dependence thereupon is provided to the processor of each respective portable biometric device. Using the processor of each respective portable biometric device the captured biometric data is then compared with the stored biometric data to produce a comparison result. If the comparison result is indicative of a match an authorization signal is transmitted from each of the respective portable biometric devices to a receiving port of the security system. Upon receipt of the authorization signal a processor of the locking mechanism determines access privileges to the secure entity or service in dependence upon the authorization signals it received from the respective portable biometric devices of the subset of N persons. If an authorization signal of the subset of N persons is missing, the security system denies access to the secure entity or service.



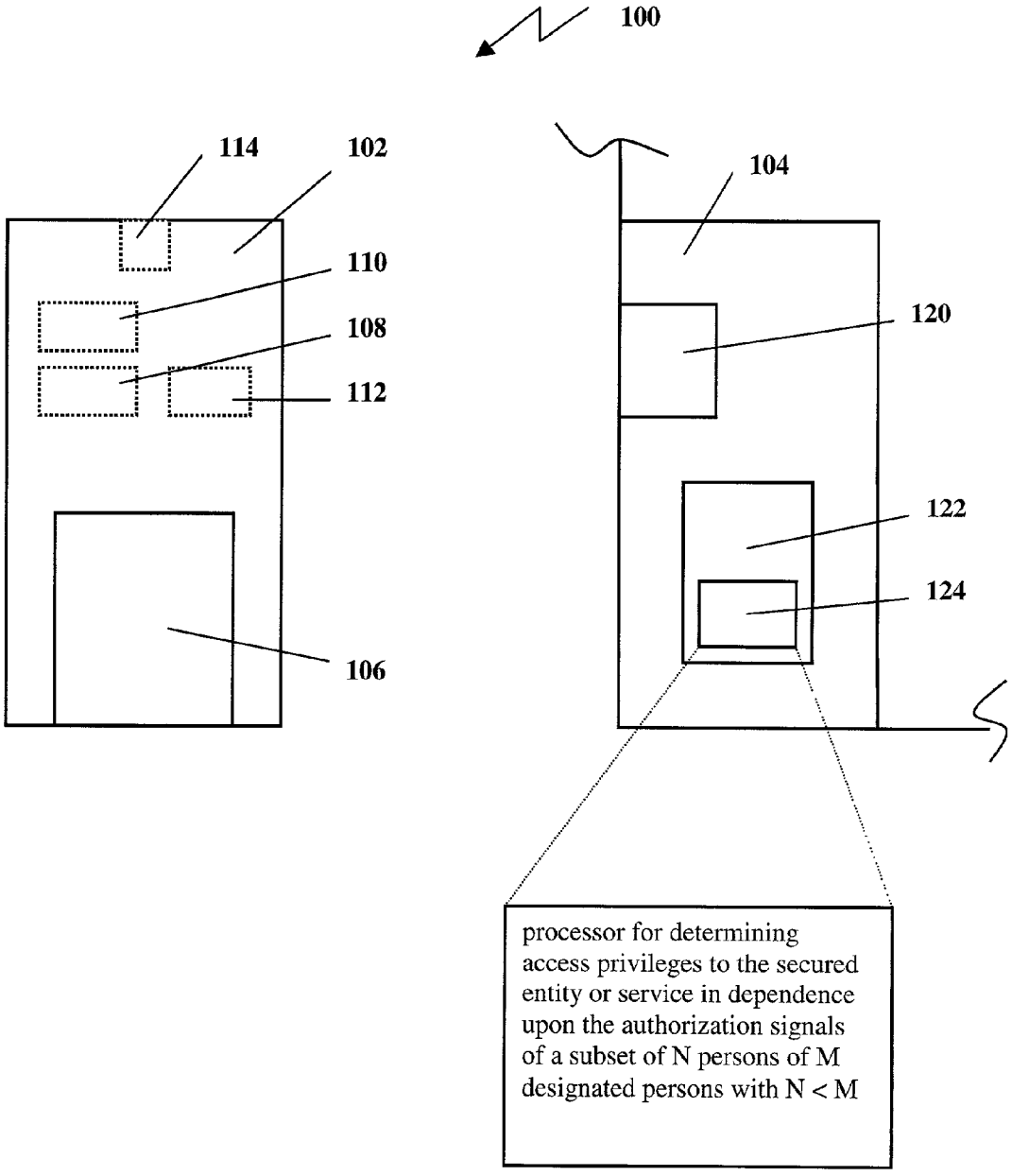


Fig. 1

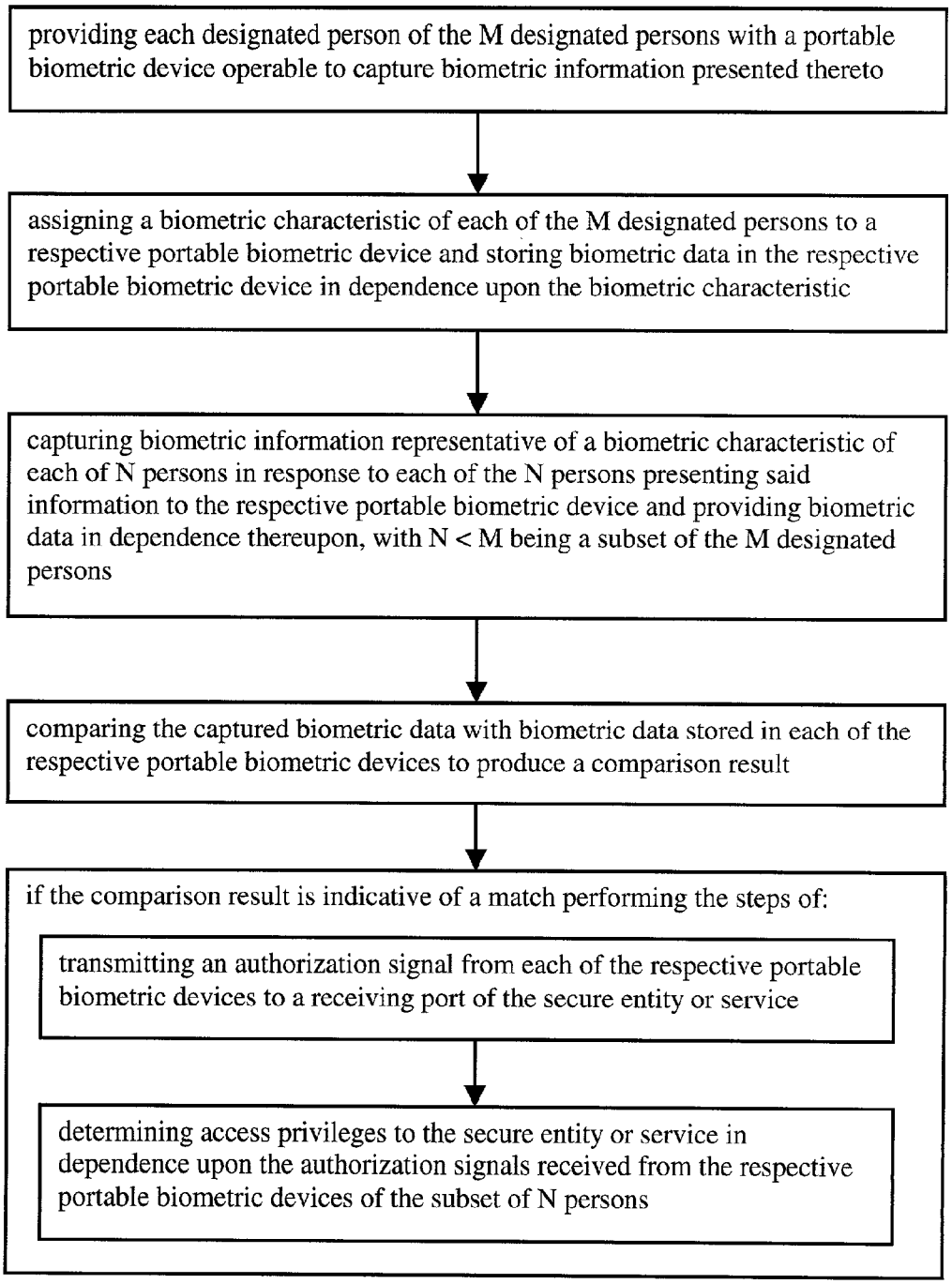


Fig. 2

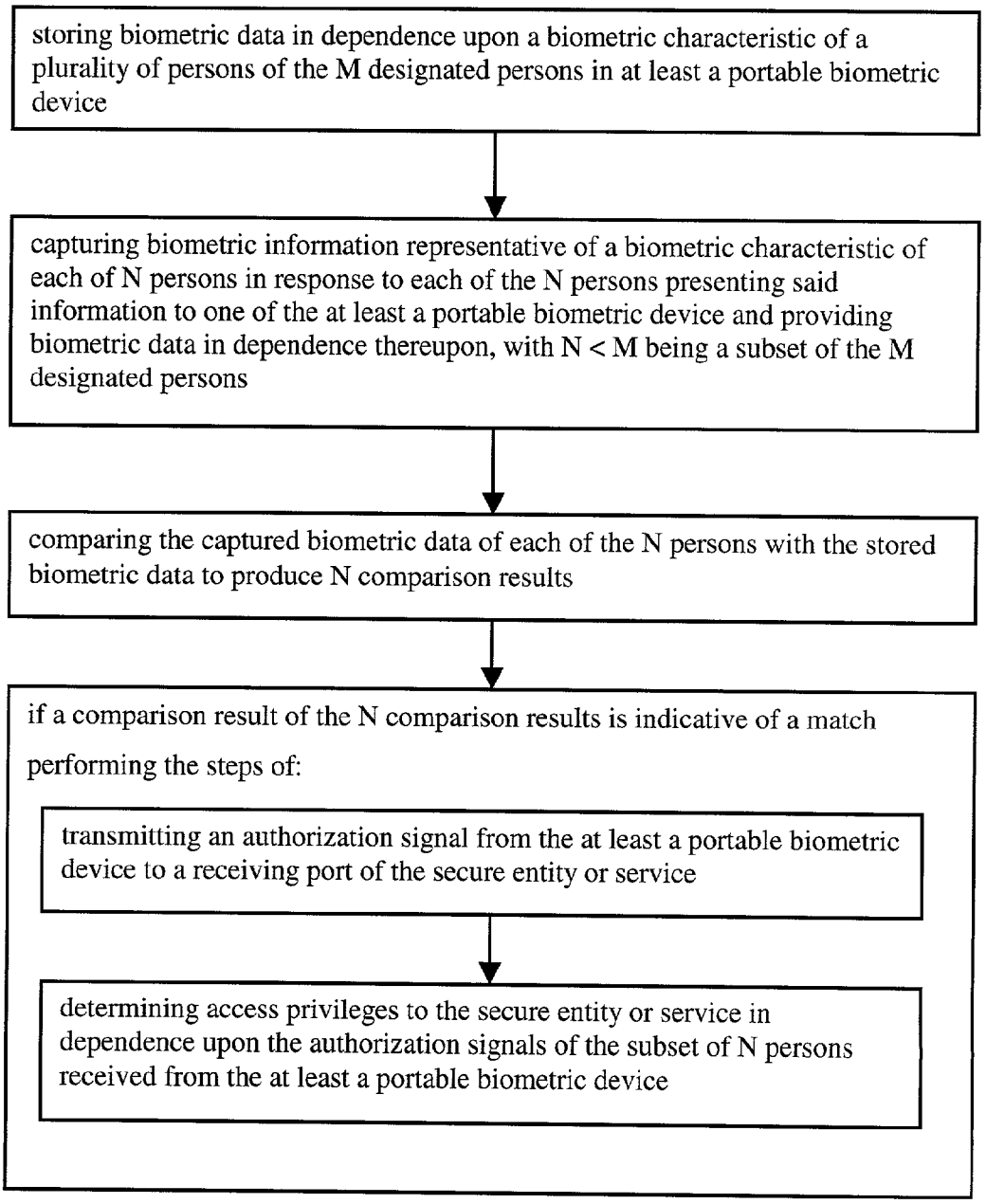


Fig. 3

METHOD AND SYSTEM FOR PROVIDING ACCESS TO SECURE ENTITY OR SERVICE BY A SUBSET OF N PERSONS OF M DESIGNATED PERSONS

FIELD OF THE INVENTION

[0001] This invention relates generally to automated security for permitting access to a service or a predefined area by designated persons and more particularly relates to a biometric security system for providing limited access to a secure entity or service by a subset of N persons of M designated persons.

BACKGROUND OF THE INVENTION

[0002] Access to most any secure entity or service is commonly limited by use of a security system. The use of security systems is generally well known. Their use is increasing with greater availability of digital electronic components at a relatively low cost. Such systems are known for securing buildings, banks, automobiles, computers and many other devices.

[0003] For example, U.S. Pat. No. 4,951,249 discloses a computer security system, which protects computer software from unauthorized access by requiring the user to supply a name and a password during the operating system loading procedure ("boot-up") of a personal computer (PC). This PC security system, utilizing password protection, is typical of many systems that are currently available. Password protection requires a user's name and a password associated with that user's name. Only once an associated password is detected for a valid user's name does the PC complete the boot-up routine. Though passwords may be useful in some instances, they are inadequate in many respects. For example, an unauthorized skilled user with a correct password in hand, can gain entry to such a processor based system. Yet another undesirable feature of the foregoing system is that passwords on occasion are forgotten; and furthermore, and more importantly, passwords have been known to be decrypted.

[0004] As of late one of the most ubiquitous electronic components is the digital processor. Multi-purpose and dedicated processors of various types control devices ranging from bank machines, to cash registers and automobiles. With ever-increasing use of these processor-based devices, there is greater concern that unauthorized use will become more prevalent. Thus, the verification and/or authentication of authorized users of processor based systems is a burgeoning industry.

[0005] Alarms and security systems to warn of unauthorized use of automobiles and other processor controlled systems are available, however, these security systems have been known to be circumvented. Unfortunately, many commercially available solutions aimed at preventing theft or unauthorized use of automobiles have also been circumvented. As of late, initiatives have been underway in the security industry, to provide biometric identification systems to validate users of electronic and other systems that are to have restricted access. A biometric identification system accepts unique biometric information from a user and identifies the user by matching the information against information belonging to registered users of the system. One such biometric identification system is a fingerprint recognition system.

[0006] In a fingerprint input transducer or sensor, the finger under investigation is usually pressed against a flat surface, such as a side of a glass plate; the ridge and valley pattern of the finger tip is sensed by a sensing means such as an interrogating light beam.

[0007] Various optical devices are known which employ prisms upon which a finger whose print is to be identified is placed. The prism has a first surface upon which a finger is placed, a second surface disposed at an acute angle to the first surface through which the fingerprint is viewed and a third illumination surface through which light is directed into the prism. In some cases, the illumination surface is at an acute angle to the first surface, as seen for example, in U.S. Pat. Nos. 5,187,482 and 5,187,748. In other cases, the illumination surface is parallel to the first surface, as seen for example, in U.S. Pat. Nos. 5,109,427 and 5,233,404. Fingerprint identification devices of this nature are generally used to control the building-access or information-access of individuals to buildings, rooms, and devices such as computer terminals.

[0008] U.S. Pat. No. 4,353,056 in the name of Tsikos issued Oct. 5, 1982, discloses an alternative kind of fingerprint sensor that uses a capacitive sensing approach. The described sensor has a two dimensional, row and column, array of capacitors, each comprising a pair of spaced electrodes, carried in a sensing member and covered by an insulating film. The sensors rely upon deformation to the sensing member caused by a finger being placed thereon so as to vary locally the spacing between capacitor electrodes, according to the ridge/trough pattern of the fingerprint, and hence, the capacitance of the capacitors. In one arrangement, the capacitors of each column are connected in series with the columns of capacitors connected in parallel and a voltage is applied across the columns. In another arrangement, a voltage is applied to each individual capacitor in the array. Sensing in the respective two arrangements is accomplished by detecting the change of voltage distribution in the series connected capacitors or by measuring the voltage values of the individual capacitances resulting from local deformation. To achieve this, an individual connection is required from the detection circuit to each capacitor.

[0009] Before the advent of computers and imaging devices, research was conducted into fingerprint characterisation and identification. Today, much of the research focus in biometrics has been directed toward improving the input transducer and the quality of the biometric input data. Fingerprint characterization is well known and can involve many aspects of fingerprint analysis. The analysis of fingerprints is discussed in the following references which are hereby incorporated by reference:

[0010] Xiao Qinghan and Bian Zhaoqi,: An approach to Fingerprint Identification By Using the Attributes of Feature Lines of Fingerprint," IEEE Pattern Recognition, pp 663, 1986;

[0011] C. B. Shelman, "Fingerprint Classification—Theory and Application," Proc. 76 Carnahan Conference on Electronic Crime Countermeasures, 1976;

[0012] Feri Pernus, Stanko Kovacic, and Ludvik Gyergyek, "Minutaie Based Fingerprint Registration," IEEE Pattern Recognition, pp 1380, 1980;

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.