



(19) **UA** (11) **75 873** (13) **C2**
(51)МПК

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
УКРАИНЫ

ГОСУДАРСТВЕННЫЙ ДЕПАРТАМЕНТ
ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ УКРАИНЫ

(21), (22) Заявка: 2002043627, 22.03.2002

(24) Дата начала действия патента: 15.06.2006

(30) Приоритет: 28.06.2001 SG PCT/SG01/00134

(46) Дата публикации: 15.06.2006 G06K 9/00
20060101CFI20060518RHUA G06K
9/62 20060101CLI20060518VHUA
G06K 9/78
20060101CLI20060518VHUA

(86) Заявка PCT:
PCT/SG02/00047, 20020322

(72) Изобретатель:

Пу Тенг Пин, МУ,
Лим Лей Чуан, МУ

(73) Патентовладелец:

ТРЕК 2000 ИНТЕРНЕШНЛ ЛТД., SG

(54) ПОРТАТИВНОЕ УСТРОЙСТВО, СПОСОБНОЕ РАСПОЗНАВАТЬ ПОЛЬЗОВАТЕЛЯ ПО
БИОМЕТРИЧЕСКИМ ХАРАКТЕРИСТИКАМ

(57) Реферат:

Устройство и способ контроля доступа к охраняемому ресурсу с применением биометрического принципа реализуются с использованием портативного устройства. В частности, в одном из примеров осуществления портативное устройство включает микропроцессор, соединенную с ним энергонезависимую память и модуль распознавания, работающий по биометрическому принципу и управляемый микропроцессором. Данная биометрическая технология использует технологию распознавания отпечатков пальцев. Модуль распознавания регистрирует отпечатки пальцев при первом использовании портативного устройства и сохраняет кодированную версию отпечатков пальцев в энергонезависимой памяти. Далее модуль распознавания может считывать отпечатки пальцев человека и точно определять,

совпадают ли данные отпечатки пальцев с зарегистрированными отпечатками пальцев, сохраненными в энергонезависимой памяти. Если соответствие подтверждено, доступ к охраняемому ресурсу разрешается; в противном случае доступ остается запрещенным. Таким образом, осуществление данного изобретения предлагает удобный, защищенный и надежный способ и систему для распознавания пользователя и контроля доступа, что не было обеспечено предыдущим уровнем техники с использованием паролей для распознавания.

Официальный бюлетьень "Промышленная собственность". Книга 1 "Изобретения, полезные модели, топографии интегральных микросхем", 2006, N 6, 15.06.2006. Государственный департамент интеллектуальной собственности Министерства образования и науки Украины.



(19) **UA** (11) **75 873** (13) **C2**
(51) Int. Cl.

MINISTRY OF EDUCATION AND SCIENCE OF
UKRAINE

STATE DEPARTMENT OF INTELLECTUAL
PROPERTY

(12) DESCRIPTION OF PATENT OF UKRAINE FOR INVENTION

(21), (22) Application: 2002043627, 22.03.2002

(24) Effective date for property rights: 15.06.2006

(30) Priority: 28.06.2001 SG PCT/SG01/00134

(46) Publication date: 15.06.2006 G06K 9/00
20060101CFI20060518RHUA G06K
9/62 20060101CLI20060518VHUA
G06K 9/78
20060101CLI20060518VHUA

(86) PCT application:
PCT/SG02/00047, 20020322

(72) Inventor:

Poo Teng Pin, MY,
Lim Lay Chuan, MY

(73) Proprietor:

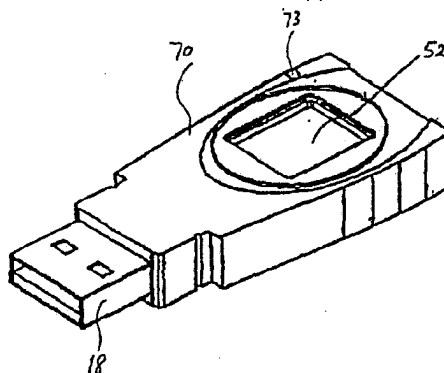
TREK 2000 INTERNATIONAL LTD., SG

(54) PORTABLE DEVICE ABLE TO IDENTIFY USER BY BIOMETRIC CHARACTERISTICS

(57) Abstract:

Apparatus and method for implementing biometrics-based authentication. In a preferred embodiment, the present invention is embodied in a portable device. Specifically, in one embodiment, the portable device includes a microprocessor, a non-volatile memory coupled thereto, and a biometrics-based authentication module controlled by the microprocessor. Preferably, the biometrics technology used is fingerprint authentication technology. The authentication module is capable of registering a fingerprint upon first use of the portable device, storing an encoded version of the fingerprint in the non-volatile memory. Subsequently, the authentication module can read a person's fingerprint and reliably determine whether the fingerprint matches the registered fingerprint stored in the non-volatile memory. If a match is found, access to information in the non-volatile memory is granted to that person; otherwise, access is denied. Embodiment of the present invention thus provides a highly

convenient, secured and reliable method and system for user authentication and access control which was not achievable in prior art password-based authentication approaches.



Official bulletin "Industrial property". Book 1 "Inventions, utility models, topographies of integrated circuits", 2006, N 6, 15.06.2006. State Department of Intellectual Property of the Ministry of Education and Science of Ukraine.



(19) **UA** (11) **75 873** (13) **C2**
(51)МПК

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

(12) ОПИС ВІНАХОДУ ДО ПАТЕНТУ УКРАЇНИ

(21), (22) Дані стосовно заявки:
2002043627, 22.03.2002

(24) Дата набуття чинності: 15.06.2006

(30) Дані стосовно пріоритету відповідно до Паризької
конвенції : 28.06.2001 SG PCT/SG01/00134

(46) Публікація відомостей про видачу патенту
(деклараційного патенту): 15.06.2006G06K 9/00
20060101CFI20060518RHUA G06K
9/62 20060101CLI20060518VHUA
G06K 9/78
20060101CLI20060518VHUA

(86) Номер та дата подання міжнародної заявки
відповідно до договору PCT:
PCT/SG02/00047, 20020322

(72) Винахідник(и):
Пу Тенг Пін , МҮ,
Лім Лей Чуан , МҮ

(73) Власник(и):
ТРЕК 2000 ІНТЕРНЕШНЛ ЛТД., SG

(54) ПОРТАТИВНИЙ ПРИСТРІЙ, ЗДАТНИЙ РОЗПІЗНАВАТИ КОРИСТУВАЧА ЗА БІОМЕТРИЧНИМИ
ХАРАКТЕРИСТИКАМИ

(57) Реферат:

Пристрій і спосіб контролю доступу до ресурсу, що охороняється, з застосуванням біометричного принципу реалізуються з використанням портативного пристрою. Зокрема, у одному з втілень портативний пристрій включає мікропроцесор, енергонезалежну пам'ять, що сполучена з ним, і модуль розпізнавання, що працює за біометричним принципом, що керується мікропроцесором. Дана біометрична технологія використовує технологію розпізнавання відбитків пальців. Модуль розпізнавання реєструє відбитки пальців при першому використанні портативного пристрою і зберігає кодовану версію відбитків

пальців у енергонезалежній пам'яті. Надалі модуль розпізнавання може зчитувати відбитки пальців особи і напевне визначати, чи дані відбитки пальців співпадають із зареєстрованими відбитками пальців, збережених у енергонезалежній пам'яті. Якщо відповідність підтверджена, доступ до ресурсу, що охороняється, дозволяється; у іншому випадку доступ залишається забороненим. Таким чином, втілення даного винаходу пропонує зручний, захищений і надійний спосіб та систему для розпізнавання користувача і контролю доступу, що не було забезпечено попереднім рівнем техніки з використанням паролів для розпізнавання.

Опис винаходу

Даний винахід стосується портативного пристрою, і зокрема, портативного пристрою зберігання даних і контролю доступу, здатного розрізняти користувача за біометричними характеристиками.

Портативні пристрої зберігання даних стали класом необхідної периферії, що широко використовується у бізнесі, освіті і для домашніх користувачів. Такі пристрої звичайно не прилаштовуються для постійного користування до спеціальної хост-платформи, наприклад, такої як персональний комп'ютер (ПК). Скоріше навпаки, вони можуть бути відповідним чином зняті та прилаштовані до будь-якого комп'ютера, що має відповідний контактний порт (наприклад, послідовний магістральний порт, такий як порт УПМ (порт УПМ - універсальний послідовний магістральний порт), IEEE 1394 ("Firewire") порт). Таким чином, такі портативні пристрої зберігання даних надають можливість користувачу здійснювати передачу даних між різними комп'ютерами, якщо вони не з'єднані у якийсь інший спосіб. У широко відомому портативному пристрої пам'яті використовується енергонезалежна твердотільна пам'ять (наприклад, флеш-пам'ять) як пам'ять носія і таким чином, для отримання даних вона не потребує рухомих деталей або механічного приводу. Відсутність механізму приводу надає таким портативним твердотільним пристроям пам'яті більшої компактності у порівнянні з такими пристроями поверхневої пам'яті як магнітні диски і CD-ROM'и.

Так як портативні пристрої пам'яті використовуються все більш широко у різноманітному середовищі установ і персональних користувачів, запобігання отримання інформації, що збережена на портативному або встановленому носії пам'яті несанкціонованими користувачами є однією з найбільш важливих проблем у інформаційній технології сьогодення. Наприклад, для забезпечення конфіденційності бізнес інформації, персональної інформації, такої як медична, фінансова або інша інформація, що має секретний характер, важливо мати надійні засоби захисту, прості у використанні, зручні та такі, які б забезпечували відповідний рівень захисту для відповідного типу інформації, що підлягає захисту.

До цього часу, користувачам портативних пристроїв пам'яті в більшості випадків пропонувалось використовувати систему паролів для захисту від несанкціонованого доступу. В той час як користування паролем як механізмом розпізнавання користувача забезпечує певний рівень захисту проти несанкціонованого доступу, цей спосіб часто розглядається користувачами як громіздкий і незручний завдяки необхідності пам'ятати пароль і використовувати його кожного разу, коли користувач потребує доступу. У більшості випадках, користувачеві необхідно також періодично змінювати свій пароль для забезпечення додаткового рівня захисту. Це додатково додає незручностей. Більш того, оскільки звичайний користувач часто потребує доступу до декількох комп'ютерних систем і/або мереж, що потребують контрольованого доступу, користувачу необхідно пам'ятати різні численні паролі через те, що вони не є обов'язково ідентичними для різних систем. Таким чином, є досить перспективним забезпечити надійний механізм розпізнавання для запобігання несанкціонованого доступу до інформації, що збережена на портативному або встановленому носії пам'яті, який не був би громіздким або незручним для користувача.

До того ж, паролі різних користувачів не є унікальними і є також об'єктом уваги більшості кваліфікованих хакерів. Якщо пароль був зламаний, хоч би і випадково, чесним користувачем або зловмисним хакером, та розшифрований для несанкціонованої сторони, конфіденційні дані, що вважалися захищеними, вже більше не є такими. Насправді, несанкціонований доступ до такої інформації може відбуватися непомітно протягом значного періоду часу. Такі систематичні втручання звичайно залишаються непоміченими до того часу, поки користувач, що став жертвою, нарешті виявляє, що до даних був доступ і/або вони були зруйновані, або до того часу, коли системний адміністратор виявляє залишки підозрілої активності. Саме тому виявляється перспективним запропонувати механізм захисту доступу для захисту від несанкціонованого доступу до даних, накопичених у пам'яті портативного носія і різноманітних комп'ютерних системах, який важко зламати хакеру, і який найкращим чином забезпечує унікальним "ключем доступу" кожного окремого користувача.

Відповідно до цього, у даному винаході пропонується спосіб і система, що репрезентує високонадійний, зручний у користуванні механізм розпізнавання для запобігання несанкціонованого доступу до інформації, що збережена у пам'яті портативного або встановленого носія. Більш того, втілення даного винаходу також пропонують механізм захисту доступу для захисту проти несанкціонованого доступу до накопичених даних і комп'ютерних ресурсів, так само як і для захисту від несанкціонованого доступу до приміщень. Аспекти даного винаходу, що використовують унікальний біометричний відбиток як основу для ідентифікації розпізнавання і як "ключ доступу" для кожного окремого користувача, описані детально нижче.

Зокрема, найбільш поширене втілення даного винаходу являє собою портативний пристрій, що включає мікропроцесор, сполучену з ним енергонезалежну пам'ять і модуль розпізнавання на біометричному принципі, контрольований мікропроцесором. Переважно, біометрична технологія використовує для розпізнавання відбитки пальців, і як енергонезалежна пам'ять використовується флеш-пам'ять. У даному втіленні модуль розпізнавання відбитків пальців автоматично реєструє відбитки пальців користувача на портативному пристрої при його першому використанні. У найбільш поширеному втіленні компактна зашифрована версія відбитків пальців зберігається у портативному пристрої флеш-пам'яті, коли реєстраційний процес завершується. При наступному користуванні модуль розпізнавання зчитує відбитки пальців користувача, порівнює їх із зареєстрованими відбитками пальців у флеш-пам'яті та достовірно встановлює їх відповідність одне одному. Якщо відповідність встановлена, ідентифікація особистості користувача вважається успішною, і ідентифікованому користувачеві надається доступ до засекреченого ресурсу, доступ до якого був заборонений даною системою контролю доступу. З іншого боку, якщо відповідність між відбитками пальців користувача і зареєстрованими відбитками

пальців не виявлена, доступ до засекреченого ресурсу залишається забороненим. Тому дане втілення даного винаходу являє собою більш зручну, захищену і надійну систему для розпізнавання користувача і дозволу доступу, у порівнянні з попередніми системами розпізнавання з паролями. У даному винаході високо оцінюється і використовується саме те, що відбитки пальців мають унікальні характерні ознаки для кожного окремого індивідуума, юридично і всесвітньо визнані для проведення ідентифікації вже протягом століття, що користувач не може їх забути, так як це може трапитися з паролями, і також те, що їх практично неможливо підробити, дублювати або зламати за допомогою хакером. Таким чином, відбитки пальців та інша технологія на біометричному принципі є найбільш придатною для використання і вирішення питань розпізнавання і/або контрольованого доступу, як втілено у даному винаході.

Переваги даного винаходу будуть наведені далі, частково у наступному описі та будуть зрозумілими для фахівців у цій галузі з того ж наведеного опису.

Супровідні креслення, які включено до опису як його частина, ілюструють декілька втілень винаходу і разом з даним описом слугують для пояснення принципів винаходу.

Фіг.1А є блок-схемою, що ілюструє функціональні модулі одного з втілень портативного пристрою даного винаходу, а також ілюстративну операційну конфігурацію.

Фіг.1Б є блок-схемою, що ілюструє функціональні модулі інших втілень портативного пристрою даного винаходу.

Фіг.2 є фронтальною проекцією портативного пристрою з інтегрованим модулем відбитків пальців згідно з одним з втілень даного винаходу.

Фіг.3 є задньою проекцією портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.2.

Фіг.4 є видом знизу портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.2.

Фіг.5 є видом зверху портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.2.

Фіг.6 є лівою частиною вертикальної проекції портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.2.

Фіг.7 є правою частиною вертикальної проекції портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.2.

Фіг.8 є фронтальною вертикальною проекцією портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.2.

Фіг.9 є задньою вертикальною проекцією портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.2.

Фіг.10 є схемою послідовності операцій, що ілюструє стадії користувача у процесі реєстрації/розпізнавання з використанням портативного пристрою згідно з одним з втілень даного винаходу.

Фіг.11А і 11Б є задніми проекціями другого портативного пристрою згідно з втіленням даного винаходу;

Фіг.12 є видом зверху другого портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.11А і 11Б;

Фіг.13 є видом знизу другого портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.11А і 11Б;

Фіг.14 є лівою частиною проекції другого портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.11А і 11Б;

Фіг.15 є правою частиною проекції другого портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.11А і 11Б;

Фіг.16 є фронтальною вертикальною проекцією другого портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.11А і 11Б;

Фіг.17 є задньою вертикальною проекцією другого портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.11А і 11Б.

Даний винахід надалі буде описаний більш повно з посиланнями на супровідні креслення, на яких представлені найбільш поширені втілення даного винаходу. Даний винахід може, однак, бути втілений у інших різноманітних формах і не повинен тлумачитись тільки як такий, що обмежений втіленнями наведеними далі у описі; скоріше опис таких втілень подається тут таким чином, щоб детально і повно донести ідею даного винаходу до професіоналів у даній галузі. Фактично задачею даного винаходу є охопити можливі альтернативи, модифікації і еквіваленти наведених втілень, що будуть входити у обсяг і відповідати ідеї даного винаходу як визначено у наведених далі пунктах формули. Більш того, у наведеному нижче детальному описі даного винаходу численні специфічні подробиці наведені далі для забезпечення глибокого розуміння даного винаходу. Однак для професіоналів повинно бути зрозумілим, що даний винахід може бути реалізований і без таких специфічних подробиць. У інших випадках добре відомі способи, процедури, компоненти і схеми не були описані детально, щоб зайвим чином не обтяжувати розуміння аспектів даного винаходу.

Фіг.1А є блок-схемою, що ілюструє функціональні модулі одного з втілень портативного пристрою даного винаходу та ілюстративну операційну конфігурацію. На Фіг.1А зображено портативний пристрій 70, сполучений з хост-платформою 90. У цьому втіленні хост-платформа 90 сполучена з схемою джерела живлення 80, розміщеного у портативному пристрої 70. Схема джерела живлення 80 подає живлення від хост-платформи 90 і слугує як джерело живлення для різноманітних компонентів портативного пристрою 70.

Звертаючись знову до Фіг.1А, портативний пристрій 70 додатково включає інтегральну схему 10,

флеш-пам'ять 20, енергонезалежну пам'ять 30 і модуль відбитків пальців 50. Інтегральна схема 10 може застосовуватися відповідним чином як інтегральна схема спеціального призначення (ASIC). На даний час у найбільш поширеному втіленні флеш-пам'ять 20 може мати ємність від 8МВ до 512МБ, тобто такий обсяг пам'яті, який може використовуватися, щоб зберігати один або більше зразків, отриманих згідно з даним винаходом, як описано нижче. Більш того, у найбільш поширеному втіленні, зразок(зразки) зберігаються у резервній зоні флеш-пам'яті 20, що призначена саме для цього і ні в який спосіб не є доступною для користувача. До того ж, як описано детально нижче, у найбільш поширеному на даний час втіленні зразок зашифровується до того, як він запам'ятовується у флеш-пам'яті 20, забезпечуючи в такий спосіб додатковий захист проти хакерів. У одному з втілень енергонезалежна пам'ять 30 встановлюється зовнішнім чином по відношенню до інтегральної схеми 10 і містить в собі або динамічну оперативну пам'ять (DRAM) або статичну оперативну пам'ять (SRAM). Поряд з іншими функціями, енергонезалежна пам'ять 30 може слугувати як попередня пам'ять і область переміщення блоків даних для зображень відбитків пальців, отриманих згідно з даним винаходом.

Інтегральна схема 10 включає мікропроцесор 11, що у одному з втілень є процесором скороченого набору команд (RISC). У найбільш поширеному на даний час втіленні до інтегральної схеми 10 входить процесор розпізнавання 12. Процесор розпізнавання 12 у свою чергу включає генератор зразка 12а і верифікаційний модуль 12б. Генератор зразка 12а використовується для вироблення розкодованої версії зображення відбитків пальців. У обсязі даного винаходу, для такого розкодованого зображення відбитків пальців вжитий термін "зразок". Треба звернути увагу, що відповідно до сучасної біометричної технології відбитки пальців можуть бути однозначно ідентифіковані, використовуючи від 8 і 13 відмінних пунктів вихідних зображень відбитків пальців. Інформація з відбитків пальців може бути відповідним чином збережена в ущільненому вигляді як дані, властиві вказаним з 8-13 відповідних відмінних пунктів. У найбільш поширеному втіленні даного винаходу відбитки пальців зберігаються у компактній формі як зразок для порівняння. У цьому втіленні, зразок займає об'єм 512 байт. Інші втілення можуть використовувати зразки різних об'ємів. Такі компоненти, як процесор розпізнавання 12, верифікаційний модуль 12б використовуються для порівняння нових отриманих зразків з зразками, що знаходяться в пам'яті для підтвердження автентичності з відбитками пальців офіційно визнаного користувача. Таким чином, процесор розпізнавання 12 працює у поєднанні з модулем відбитків пальців 50, що описаний більш детально нижче, для здійснення розпізнавання користувача згідно з даним винаходом.

Треба звернути увагу, що процесор розпізнавання 12 є добре пристосованим до численних застосувань у обсязі даного винаходу. У одному з втілень процесор розпізнавання 12 застосовується як програмне забезпечення, розміщене у енергонезалежній пам'яті портативного пристрою 70. У інших втіленнях процесор розпізнавання 12 застосовується як частина мікропроцесора 11. Крім цього, у інших втіленнях процесор розпізнавання 12 застосовується як процесор окремо від мікропроцесора 11. У подальших втіленнях процесор розпізнавання 12 включає такі самі компоненти і виконує такі самі функції, що вже наведені тут, але він розміщений у хост-платформі 90 на відміну від розміщення у портативному пристрої 70. Іншими словами, у обсязі даного винаходу процесор розпізнавання 12 не потребує розміщення у портативному пристрої 70. Замість цього, розміщення процесору розпізнавання 12 залежить від вибору конструктора, тобто існує можливість гнучких рішень у різноманітних застосуваннях, для яких може використовуватися даний винахід.

Звертаючись знову на Фіг.1А, у найбільш поширеному втіленні інтегральна схема 10 також включає шину інтерфейсу 13, що забезпечує зв'язок інтегральної схеми 10 з іншими компонентами, такими як енергонезалежна пам'ять 30. Інтегральна схема 10 також включає флеш-контролер 14 для контролю доступу до флеш-пам'яті 20. У одному з втілень, після успішного утворення зразка при реєстрації користувача, флеш-контролер 14 взаємодіє з генератором зразка 12а для збереження нових утворених зразків у флеш-пам'яті 20 для використання при наступній ідентифікації користувача. Більш того, у найбільш поширеному на даний час втіленні, портативний пристрій 70 є сумісний з стандартною універсальною послідовною магістраллю (УПМ) і включає конектор УПМ (не зображений). У даному втіленні інтегральна схема 10 також включає УПМ пристрій контролера 15, що слугує для контролю зв'язку портативного пристрою 70 і хост-платформи 90, так як УПМ - сумісний персональний комп'ютер (ПК), що має хост-контролер УПМ 93.

Звертаючись знову до Фіг.1А, інтегральна схема 10 також включає енергонезалежну пам'ять 16 і не енергонезалежну пам'ять 17. У найбільш поширеному втіленні, енергонезалежна пам'ять 16 є оперативною пам'яттю (RAM), що працює як оперативна пам'ять мікропроцесора 11 при його функціонуванні. У даному втіленні енергонезалежна пам'ять 17 - це постійний запам'ятовувачий пристрій (ПЗП), що може використовуватися для зберігання програмного забезпечення з метою реалізації різноманітних функцій портативного пристрою 70. До того ж, інтегральна схема 10 включає процесор для виявлення і виправлення помилок (ВВП) 19 для забезпечення різноманітних задач з виявлення помилок під час роботи портативного пристрою 70. Треба звернути увагу на те, що процесор ВВП 19, як і процесор розпізнавання 12, є найбільш придатним для численних застосувань у обсязі даного винаходу. Наприклад, процесор ВВП 19 може бути реалізований за допомогою програмного забезпечення (наприклад, програмного забезпечення, збереженого у не енергонезалежній пам'яті) як частина мікропроцесора 11, або як самостійний процесор окремо від мікропроцесора 11.

Звертаючись знову до Фіг.1А, модуль відбитків пальців 50 включає сенсор 52, що використовується для зчитування зображень відбитків пальців власне з самого пальця, розміщеного на ньому. Модуль відбитків пальців 50 також включає конвертер 54, що конвертує отримане зображення відбитків пальців у електричні сигнали зображень. У найбільш поширеному на даний час втіленні відбитки пальців зображень конвертуються конвертером 54 у пакет даних об'ємом 64KB і надсилаються до енергонезалежної пам'яті 30 портативного пристрою 70 для тимчасового зберігання. У інших втіленнях конвертер 54 може продукувати зображення даних різних об'ємів. Модуль відбитків пальців 50 може додатково включати блок управління 56, як у найбільш

поширеному на даний час втіленні, що керується мікропроцесором 11 портативного пристрою 70 і використовується для перевірки якості зображення відбитків пальців, отриманих сенсором 52, тобто для визначення того, чи якість отриманих зображень є прийнятною чи ні. Як описано більш детально нижче, якщо визначається, що якість отриманих зображень недостатня, користувач буде змушений встановити свій палець на сенсор 52, щоб таким чином можна було знову отримати нове зображення.

На Фіг.1Б зображена блок-схема, що ілюструє функціональні модулі інших втілень портативного пристрою даного винаходу. У даному втіленні портативний пристрій 170 є сумісним зі стандартною універсальною послідовною магістраллю УПМ і включає рознімне з'єднання УПМ 118, що, як зображено на Фіг.1Б, сполучено з хост-контролером УПМ 193 хост-платформи. За необхідності портативний пристрій 170 включає додатковий порт УПМ (універсальний послідовний магістральний порт) 162, що є сполученим з рознімним з'єднанням УПМ 118. Порт УПМ (універсальний послідовний магістральний порт) 162 забезпечує зручне сполучення інших сумісних пристроїв УПМ з власне УПМ через портативний пристрій 170. У даному втіленні портативний пристрій 170 також включає контролер УПМ 115 для управління зв'язком між портативним пристроєм 170 і хост-платформою через хост-контролер УПМ 193. У одному з втілень програмний драйвер 177 і програмний інтерфейс додатку (Application Programming Interface-API) 197, що в свою чергу включає програмне забезпечення контролю 199, розміщується у хост-платформі і здійснює зв'язок з хост-контролером УПМ 193 для сприяння роботі портативного пристрою 170.

Портативний пристрій 170 додатково включає інтегральну схему 110, флеш-пам'ять 120 і енергонезалежну пам'ять 130. Інтегральна схема 110 може відповідним чином застосовуватися як спеціалізована інтегральна схема (CIC)-ASIC (application specific integrated circuits). У найбільш поширеному втіленні зона резервування 122 флеш-пам'яті 120 використовується для збереження одного або більше зразків, утворених згідно з даним винаходом. Далі у даному втіленні зона резервування флеш-пам'яті 122 включає прапорець стану 121, що вказує на те, чи був портативний пристрій 170 попередньо зареєстрований згідно з даним винаходом. Таким чином прапор стану 121 надає можливість портативному пристрою 170 автоматично активізувати реєстраційний процес на початку використання, як описано детально нижче. У одному з втілень, енергонезалежна пам'ять 130 включає або динамічну оперативну пам'ять (ДОП), або статичну оперативну пам'ять (СОП), що функціонують як область попередньої пам'яті для зображень відбитків пальців, отриманих згідно з даним винаходом.

Звертаючись знову до Фіг.1Б, інтегральна схема 110 включає мікропроцесор 111, що переважним чином є процесором скороченого набору команд (ПСНК). Інтегральна схема 110 додатково включає флеш-контролер 114 для контролю доступу до флеш-пам'яті 120 і контролер пам'яті 133 для контролю доступу до енергонезалежної пам'яті 130. Інтегральна схема 110 також включає енергонезалежну пам'ять 116 і не енергонезалежну пам'ять 117. Переважним чином, енергонезалежна пам'ять 116 включає ОЗП, що використовується як оперативна пам'ять для мікропроцесора 111 при його функціонуванні, в той час як не енергонезалежна пам'ять 117 включає ПЗП для зберігання програмно-апаратного засобу, що здійснює різноманітні функції портативного пристрою 170. Зокрема, у одному з втілень, ПЗП 117 зберігає такі програми програмно-апаратного засобу: програмно-апаратний засіб 117 для зчитування відбитків пальців сенсором 152, програмно-апаратний засіб 117б для обробки зображення відбитків пальців, програмно-апаратний засіб 117в для утворення зразків, програмно-апаратний засіб 117г для розшифровки зображення відбитків пальців і/або зразків, і програмно-апаратний засіб 117д для встановлення автентичності відбитків пальців. Однак, треба віддати належне, що у альтернативному втіленні даного винаходу такий програмно-апаратний засіб може бути збережений у не енергонезалежній пам'яті хост-платформи, а не у портативному пристрої 170.

Додатково інтегральна схема 110 включає пристрій для виявлення і виправлення помилок (ПВВП), процесор 119 для забезпечення різноманітних задач з виявлення помилок під час роботи портативного пристрою 170. Треба звернути увагу, що у обсязі даного винаходу, процесор ВВП 119 може застосовуватися як програмне забезпечення (наприклад, програмно-апаратні засоби), або як технічні засоби (наприклад, процесор/модуль процесора).

Звертаючись знову до Фіг.1В, модуль відбитків пальців 150 включає сенсор 152, конвертер 154 і додатковий контролер 156. У даному втіленні, сенсор 152 використовується для зчитування зображення відбитків пальців з пальця розміщеного на ньому, конвертер 154 конвертує отримані зображення відбитків пальців у електричні сигнали, що представляють зображення, додатковий контролер 156 використовується для контролю якості зображень відбитків пальців, отриманих сенсором 152 для визначення, чиє дане зображення прийнятним. Треба звернути увагу, що такі можливості обробки зображень можуть бути забезпечені використанням програмного забезпечення (наприклад, програмно-апаратних засобів) або технічних засобів (наприклад, процесор/модуль процесора) у обсязі даного винаходу.

У найбільш поширеному на даний час втіленні, як проілюстровано на Фіг.1Б, мікропроцесор 111 контролює різноманітні компоненти портативного пристрою 170, включаючи флеш-контролер 114, контролер УПМ пристрою 115, ОЗП 116, ПЗП 117 (і забезпечення роботи збереженого тут програмно-апаратного засобу), процесор ВВП 119, контролер пам'яті 133, контролер 156, модуль відбитків пальців 150. У даному втіленні, портативний пристрій 170 також включає перемикач для захисту від запису 140, який в стані активації запускає мікропроцесор 111, що забороняє доступ для запису до флеш пам'яті 120.

Далі на Фіг.2 зображена фронтальна проекція зовнішнього виду портативного пристрою з інтегрованим модулем відбитків пальців згідно з одним з втілень даного винаходу. На Фіг.2, портативний пристрій 70 зображений разом з конектором УПМ (універсальна послідовна магістраль) 18, що виступає з його фронтальної сторони. Модуль відбитків пальців 50 зображений як структурно інтегрований з портативним пристроєм 70 у цілісній конструкції, з сенсором 52, розміщеним на горішній поверхні портативного пристрою 70. Світловипромінювальний діод (СВД) 73 також зображений розміщеним біля краю горішньої поверхні

портативного пристрою 70. У одному з втілень СВД 73 світиться, коли доступ до даних портативного пристрою дозволений і, таким чином, діод слугує як індикатор дії. У іншому втіленні СВД 73 світиться для індикації процесу розпізнавання.

Далі, на Фіг.3, відповідно до Фіг.2, зображена задня проекція портативного пристрою з інтегрованим модулем відбитків пальців. Знову портативний пристрій 70 зображений разом з конектором УПМ 18, що виступає з його фронтальної сторони, і модуль відбитків пальців 50 зображений як структурно інтегрований з портативним пристроєм 70 у цілісній конструкції, з сенсором 52, розміщеним на його горішній поверхні. СВД 73 знову зображений розміщеним біля краю горішньої поверхні портативного пристрою 70. Додатковий перемикач захисту від запису 40 також зображений розміщеним з задньої сторони портативного пристрою 70.

На Фіг.4 демонструється вид знизу портативного пристрою з інтегрованим модулем відбитків пальців, зображеного на Фіг.2. На Фіг.4 зображено досить значне напівкругле заглиблення 77, що є ще одною додатковою особливістю, завдяки якій користувач може надійно утримувати портативний пристрій 70 під час з'єднання або роз'єднання портативного пристрою 70 з хост-платформою 90 (Фіг.1А), що знаходиться знизу портативного пристрою 70. Там також зображений конектор УПМ 18.

Далі на Фіг.5 представлений вид зверху портативного пристрою з інтегрованим модулем відбитків пальців, зображеного на Фіг.2. Портативний пристрій 70 зображений разом з конектором УПМ 18, що виступає з його фронтальної сторони, і модуль відбитків пальців 50 зображений структурно інтегрованим з портативним пристроєм 70 у цілісній конструкції, з сенсором 52, розміщеним на його горішній поверхні. СВД 73 знову зображений розміщеним біля краю горішньої поверхні портативного пристрою 70.

На Фіг.6 зображена ліва частина вертикальної проекції портативного пристрою з інтегрованим модулем відбитків пальців, зображеного на Фіг.2. Конектор УПМ 18 зображений виступаючим з фронтальної сторони портативного пристрою 70, і периферійний сенсор 52 зображений злегка виступаючим з горішньої сторони портативного пристрою 70.

Далі, Фіг.7 є правою частиною вертикальної проекції портативного пристрою з інтегрованим модулем відбитків пальців, як було представлено на Фіг.2. Знову ж таки, конектор УПМ 18 зображений виступаючим з фронтальної сторони портативного пристрою 70, і периферійний сенсор 52, зображений злегка виступаючим з горішньої сторони портативного пристрою 70.

Далі на Фіг.8 зображена фронтальна вертикальна проекція портативного пристрою з інтегрованим модулем відбитків пальців, зображеного на Фіг.2. Контактні поверхні конектора УПМ 18 зображені в центрі, а периферійний сенсор 52 зображений злегка виступаючим з горішньої сторони портативного пристрою 70.

На Фіг.9 зображена задня вертикальна проекція портативного пристрою з інтегрованим модулем відбитків пальців, зображеного на Фіг.2. Периферійний сенсор 52 зображений злегка виступаючим з горішньої сторони портативного пристрою 70, і можна також бачити додаткове заглиблення 77 знизу портативного пристрою 70. Додатковий перемикач для захисту від запису 40 також зображений розміщеним з задньої сторони портативного пристрою 70.

Далі на Фіг.11А зображена перша задня проекція другого портативного пристрою 370 з інтегрованим модулем відбитків пальців згідно з одним з втілень даного винаходу. Електронна конструкція пристрою 370 ідентична пристрою 70 (і через це більшість цифрових посилань, що наведені на Фіг.11А аналогічні тим, що використовуються на Фіг.2, але вони є більшими на число 300), але крім більших зовнішніх розмірів, він має ще дві додаткові властивості. По-перше, тут є рухома кришка 300, що закриває сенсор 352. На Фіг.11А рухома кришка 300 зображена у закритому стані, а на Фіг.11Б зображена друга задня проекція портативного пристрою 370, зображеного на Фіг.11А, але тут рухома кришка 300 зображена у відкритому стані. По-друге, сенсор 352 під час зняття відбитків пальців обертається таким чином, щоб зняти круговий відбиток пальця. Другий варіант другого портативного пристрою 370 описаний більш детально далі.

На Фіг.11А і 11Б портативний пристрій 370 зображений разом з конектором УПМ 318, що виступає з його фронтальної сторони. Модуль відбитків пальців 350 зображений структурно інтегрованим з портативним пристроєм 370 у цілісній конструкції, з сенсором 352 (зображеним на Фіг.11Б), розміщеним на горішній поверхні портативного пристрою 370.

Світловопромінювальний діод (СВД) 373 також зображений розміщеним на задній стороні портативного пристрою 370. У одному з втілень СВД 373 засвічується тоді, коли є доступ до даних портативного пристрою, тобто таким чином слугує як індикатор дії. У іншому втіленні СВД 373 світиться для індикації того, що відбувається процес розпізнавання.

Рухома кришка 300 являє собою пластину, встановлену таким чином, що вона може пересуватися у площині горішньої поверхні портативного пристрою 372 вздовж L-подібних напрямних 400, що виступають з горішньої поверхні портативного пристрою 370. Рухома кришка 300 забезпечена контактними засобами для пальця (наприклад, жолобками) 450 таким чином, що користувач може пересувати кришку від першої позиції (Фіг.11А), у якій рухома кришка 300 закриває і захищає сенсор 352, і до другої позиції (Фіг.11Б), у якій кришка не закриває сенсор.

Додатковий перемикач захисту від запису 340 також зображений розміщеним із задньої сторони портативного пристрою 370.

Далі на Фіг.12 зображено вид зверху портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.11А і 11Б. Портативний пристрій 370 зображений разом з конектором УПМ 318, що виступає з його фронтальної сторони, а модуль відбитків пальців 350 зображений структурно інтегрованим з портативним пристроєм 370 у цілісній конструкції, з сенсором 52, розміщеним на горішній поверхні пристрою. На Фіг.11Б рухома кришка 300 зображена у відкритому стані.

На Фіг.13 зображено вид знизу портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.11А і 11Б. Знизу портативного пристрою 370 на Фіг.13 зображено досить значне напівкругле заглиблення 377, що є додатковою особливістю, яка дозволяє користувачу надійно утримувати портативний пристрій 370 при з'єднанні або роз'єднанні портативного пристрою 370 з хост-платформою 90 (Фіг.1А). Там також зображений конектор УПМ 318.

На Фіг.14 зображена ліва частина вертикальної проекції портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.11А і 11Б. Конектор УПМ 318 зображений виступаючим з фронтальної сторони портативного пристрою 370, а рухома кришка 300 і напрямні 400 зображені злегка виступаючими з горішньої сторони портативного пристрою 370.

Далі на Фіг.15 зображена права частина вертикальної проекції портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.11А і 11Б. Знову ж таки, конектор УПМ 318 зображений виступаючим з фронтальної сторони портативного пристрою 370, а рухома кришка 300 і напрямні 400 зображені злегка виступаючими з горішньої сторони портативного пристрою 370.

Далі на Фіг.16 зображена фронтальна вертикальна проекція портативного пристрою 370 з інтегрованим модулем відбитків пальців, представленого на Фіг.11А і 11Б. Контактні поверхні конектора УПМ 318 зображені в центрі, а рухома кришка 300 і напрямні 400 зображені злегка виступаючими з горішньої сторони портативного пристрою 370.

На Фіг.17 зображена задня вертикальна проекція портативного пристрою з інтегрованим модулем відбитків пальців, представленого на Фіг.11А і 11Б. Рухома кришка 300 і напрямні 400 зображені злегка виступаючими з горішньої сторони портативного пристрою 370. Додатковий перемикач захисту від запису 340 також зображений розташованим з задньої сторони портативного пристрою 370.

Як було згадано вище, суттєва різниця між першим варіантом портативного пристрою 70 і другим варіантом портативного пристрою 370 полягає в тому, що сенсор 352 у другому варіанті портативного пристрою 370 виконаний як циліндр, осі якого проходять паралельно горішній і задній поверхням пристрою 370. Іншими словами, ці осі проходять вздовж через пристрій 370 як проміжний шар між нижньою і горішньою поверхнею, зліва направо.

Сенсор 352 спроектований таким чином, щоб обертатися навколо своєї вісі (або цілком, або частково в межах певного кута). Коли рухома кришка 300 відкрита, частина циліндричної поверхні сенсору 352 розташована у найвищому положенні і є доступною через отвір кожуха портативного пристрою 370, але доступ до цієї частини змінюється при обертанні сенсору 352. Коли користувач вперше використовує пристрій, він спочатку відсуває рухома кришку 300 (і таким чином відкриває частину циліндричної поверхні сенсору 352), далі просуває який-небудь палець (або великий палець) по циліндричній поверхні сенсору 352, змушуючи цю поверхню обертатися і послідовно підставляти нові частини циліндричної поверхні у відкриту зону. У такий спосіб користувач має змогу контактувати з сенсором 352 в цілому більшою площею поверхні свого пальця, ніж площа циліндричної поверхні, що є відкритою у будь-який час.

Перевагою такого рішення є те, що навіть якщо частина горішньої поверхні портативного пристрою 370, яку займає сенсор 352, залишається приблизно такою ж, як у пристрої 70 Фіг.2, сенсор 352 дозволяє (за одну операцію зчитування) обробляти більшу поверхню пальця, ніж сенсор 52. Автори винаходу вважають, що це є корисною особливістю, через те, що тим самим пристроєм можуть користуватися багаторазово особи, розміри пальців яких відрізняються досить суттєво, наприклад, представники різних рас.

Далі на Фіг.10 зображена схема послідовності операцій 200, що ілюструє стадії дій користувача у процесі реєстрації/розпізнавання при використанні або першого варіанту пристрою 70, або другого варіанту пристрою 370 з інтегрованим модулем відбитків пальців згідно з одним з втілень даного винаходу. У наступному описі різноманітні модулі і компоненти, на які є посилання, були описані вище з посиланням на Фіг.1А і з використанням таких самих цифрових позначень. На стадії 210, при сполученні з хост-платформою, портативні пристрої 70, 370 піддаються процедурі ініціалізації. У найбільш поширеному на даний час втіленні, процедура ініціалізації передбачає встановлення зв'язку з хост-платформою і засвідчення того, що для хост-платформи є відомим те, що портативні пристрої 70, 370 були сполучені з системою.

На стадії 220 портативні пристрої 70, 370 визначають, чи є необхідною реєстрація користувача. Наприклад, якщо портативні пристрої 70, 370 використовуються вперше і у флеш-пам'яті 20 ще не були збережені ніякі зразки, портативні пристрої 70, 370 будуть стимулювати користувача завершити реєстраційний процес (стадії 225, 235, 245 і 255, як описано нижче) через інтерфейс користувача (наприклад, спливаюче вікно повідомлень) хост-платформи. Таким чином, якщо портативні пристрої 70, 370 використовуються вперше (наприклад, зразу після придбання), у найбільш поширеному втіленні автоматично ініціюється реєстраційний процес для створення першого ("головного") зразка. Цей процес переважно завершується встановленням прапорця стану (наприклад, прапорець 121 флеш-пам'яті 120 на Фіг.1Б). Наступні реєстрації, як описано нижче, можуть бути активовані окремими користувачами через програмне забезпечення хост-платформи.

У одному з втілень портативні пристрої 70, 370 підтримують більш ніж одного користувача. У іншому втіленні той самий користувач може реєструвати багаторазово відбитки пальців як окремі зразки. У подальших втіленнях той самий відбиток пальця користувача може бути зареєстрований багаторазово як різні зразки. Таким чином, портативні пристрої 70, 370 можуть полегшувати реєстрацію додаткових користувачів і/або додаткових зразків або періодично (наприклад, під час запуску) запитуючи, чи є необхідність додати нового користувача/зразок, або внаслідок запиту користувача на стадії 220. Якщо додатковий користувач/зразок має бути зареєстрований, реєстраційний процес буде спричинений. Якщо визначається, що нова реєстрація не є необхідною, процес 200 продовжується з процесу розпізнавання (стадії 230, 240 і 260, як описано нижче).

Треба звернути увагу на те, що згідно з даним винаходом може виникати необхідність встановлення програмного забезпечення (наприклад, програмного забезпечення драйвера) у хост-платформі до першого користування портативними пристроями 70, 370 для забезпечення можливості використання інтерфейсу користувача хост-платформи для зв'язку з користувачем. При цьому треба також зауважити, що якщо операційна система хост-платформи має власну вбудовану підтримку таких функцій, то не є необхідним встановлення додаткового програмного забезпечення.

Звертаючись знову до Фіг.10, надалі описано реєстраційний процес. Реєстраційний процес ініціюється на стадії 225. У одному з втілень це передбачає інформування користувача про початок процесу реєстрації і його мотивацію встановлення свого пальця на сенсорі 52.

На стадії 235 сенсор 52 призначений для зчитування зображень відбитків пальця користувача, що розміщений на сенсорі. У найбільш поширеному на даний час втіленні стадія 235 також включає виконання перевірки достатньої якості отриманих зображень для їх подальшої обробки (наприклад, створення зразків). Це переважним чином виконується блоком контролю 56 з мікропроцесором 11. У одному з втілень стадії 235 будуть повторюватись, якщо якість отриманих зображень відбитків пальців недостатня. За таких обставин користувач буде змушений встановити свій палець на сенсорі 52 знову таким чином, щоб можна було отримати нове зображення. Переважним чином, кількість спроб може визначатися залежно від конкретного користувача.

Після отримання прийнятного зображення відбитків пальців на стадії 235, процес 200 продовжується до стадії 245, де утворюється зразок на основі отриманих зображень відбитків пальців. Як описано вище, у найбільш поширеному втіленні отримані зображення конвертуються у пакет даних 64KB, що надалі використовується як вхідний сигнал для генератора зразка 12а для утворення зразка 512-байт.

На стадії 248 зразок, утворений на стадії 245, зашифровується. У одному з втілень шифрування здійснюється програмно-апаратним засобом (наприклад, шифрувальним програмно-апаратним засобом 117г, Фіг.1Б), забезпечуючи в такий спосіб додатковий рівень захисту від хакерів.

На стадії 255 зашифрований зразок зберігається у флеш-пам'яті 20. У одному з втілень при успішному утворенні і шифруванні зразка генератор зразка 12а змушує флеш-контролер 14 зберігати нові утворені і зашифровані зразки у флеш-пам'яті 20 для використання у наступній ідентифікації користувача. Більш того, як описано вище, у найбільш поширеному втіленні зразок зберігається у резервній зоні флеш-пам'яті 20, що призначена саме для зберігання зразка і ні в який інший спосіб не є доступною для користувача.

На стадії 280 видається сигнал або повідомлення про успішне завершення реєстраційного процесу. У тому втіленні, де портативні пристрої 70, 370 використовуються як пам'ять пристроїв забезпечення секретності, ступінь 280 може також викликати відмикання портативного пристрою, а саме, надання новим зареєстрованим користувачам доступу (наприклад, для зчитування і запису даних) до портативних пристроїв 70, 370 і внесення портативних пристроїв 70, 370 до існуючого імені дисководу хост-платформи 90.

Далі на Фіг.10, описаний процес розпізнавання з використанням портативних пристроїв 70, 370. На стадії 230 сенсори 52, 352 призначені для зчитування зображень відбитків пальця користувача, розміщеного на сенсорі. У найбільш поширеному на даний час втіленні на стадії 230 також здійснюється контроль якості отриманих зображень блоком контролю 56, таким чином, що зчитування зображень буде повторюватись, якщо якість отриманих зображень відбитків пальців недостатня для утворення належних зразків. Якщо повторне зчитування стає необхідним, користувач буде до цього залучений. Переважним чином, кількість спроб може відповідати конфігурації користувача. У найбільш поширеному на даний час втіленні стадія 230 також включає утворення зразка на основі отриманих зображень відбитків пальців і зберігання остаточних зразків у енергонезалежній пам'яті 16.

На стадії 240 збережений зразок зчитується з флеш пам'яті 20 для використання як основи для ідентифікації користувача, зображення відбитків пальців якого було отримано на стадії 230. У найбільш поширеному на даний час втіленні мікропроцесор 11 керує флеш-контролером 14, щоб видобувати зареєстровані зразки з флеш-пам'яті 20.

На стадії 250 зареєстровані зразки, що зчитуються з флеш пам'яті 20, і у найбільш поширеному втіленні зберігаються у зашифрованому вигляді, розшифровуються. У одному з втілень розшифровані зразки завантажуються у енергонезалежну пам'ять 16.

На стадії 260 визначається, чи можуть бути відбитки пальців конкретного користувача ідентифіковані з вже зареєстрованими відбитками пальців зразка/зразків, що записані. У найбільш поширеному на даний час втіленні верифікаційний модуль 12б порівнює зразок з зареєстрованими зразками. Якщо відповідність встановлена, користувач вважається ідентифікованим; у іншому випадку розпізнавання не вважається успішним. У одному з втілень, користувачу дозволяється повторити процес розпізнавання, якщо попередня спроба виявилася невдалою (наприклад, повторюються стадії 230, 240 і 250). Переважним чином, кількість повторних спроб може відповідати конфігурації користувача і може бути визначена з часу, коли офіційно визнаний користувач був ідентифікований і йому був наданий доступ.

У одному з втілень, коли спроба ідентифікації користувача як офіційно визнаного виявляється невдалою, доступ до флеш-пам'яті 20 блокується (наприклад, у втіленні, де програмне забезпечення драйвера розташоване у хост-платформі 90, це програмне забезпечення драйвера може заборонити такий доступ). У іншому втіленні мікропроцесор 11 у портативному пристрої 70 замикається або у якийсь інший спосіб блокує флеш-контролер 14 при такому невдалому розпізнаванні. Такі дії слугують як додатковий захист проти потенціальних хакерів та інших форм несанкціонованого доступу до даних, збережених у флеш-пам'яті 20 і запускаються при повторенні невдалих спроб розпізнавання.

У одному з втілень передбачається додатковий ступінь 270. У даному втіленні, якщо верифікаційний модуль

126 дає збій і відмовляється ідентифікувати офіційно визнаного користувача, чиї відбитки пальців були попередньо зареєстровані, користувач має можливість обійти процедуру розпізнавання відбитків пальців, використовуючи пароль для отримання доступу. Це втілення надає можливість користувачу уникнути безнадійної ситуації, коли доступ до вмісту флеш-пам'яті 20 неможливий до моменту відновлення роботи верифікаційного модуля 126. Якщо обхідний пароль застосовується правильно, розпізнавання користувача вважається успішним; у іншому випадку, розпізнавання користувача залишається таким, що не відбулося. Треба також звернути увагу, що пароль може застосовуватися і в тому разі, коли виникає необхідність додаткового захисту, навіть і в тому випадку, коли розпізнавання відбитків пальців відбувається звичайним чином відповідно до даного винаходу.

На стадії 280 генерується сигнал або повідомлення, що вказує на успішне розпізнавання. У втіленні, де портативні пристрої 70, 370 використовуються як пристрої пам'яті захисту, стадії 280 можуть також викликати відмикання портативних пристроїв, а саме, надання новим зареєстрованим користувачам доступу (наприклад, для існування або запису даних) до портативних пристроїв 70, 370 і включення портативних пристроїв 70, 370 до існуючого імені дисководу хост-платформи 90.

Треба звернути увагу на те, що у втіленні, де процесор розпізнавання 12 розміщений у хост-платформі 90, існує необхідність у відповідних модифікаціях процесу розпізнавання, описаного вище. Зокрема, якщо на стадії 230 було отримане задовільне зображення відбитків пальців, дані зображення спочатку зашифровуються і далі передаються до хост-платформи 90, де будуть виконуватися ті стадії, що мали б виконуватися процесором розпізнавання 12. Таким чином, в залежності від конкретного впровадження або застосування, інформація, що передається від портативних пристроїв 70, 370 до хост-платформи 90, може бути або у вигляді простого повідомлення про успішне завершення ідентифікації, або у вигляді даних зображень відбитків пальців користувача, що чекають на ідентифікацію.

У найбільш поширеному на даний час втіленні робота на різних стадіях процесу 200 контролюється мікропроцесором 11, що функціонує як програмно-апаратний засіб програми, що переважним чином зберігається у енергонезалежній пам'яті 17 портативного пристрою 70, 370.

Суттєвим є те, що у даному винаході передбачається не тільки використання портативних пристроїв 70, 370 як пристроїв захисту зберігання даних, але також як пристроїв контролю доступу. Зокрема, згідно з даним винаходом, портативні пристрої 70, 370 можуть функціонувати як "ключ доступу" до хост-платформи 90, з якою сполучені портативні пристрої 70, 370. Зокрема, у одному з втілень для доступу до будь-якого ресурсу хост-платформи 90 (наприклад, до даних, файлів, прикладних програм, периферії) і/або до будь-якого іншого допоміжного ресурсу (наприклад, доступу до мережі, принтерів, пристроїв пам'яті, електронної пошти), користувачу спочатку необхідно успішно ідентифікувати себе як офіційно визнаного користувача, використовуючи портативні пристрої 70, 370 з інтегральним модулем відбитків пальців 50. Згідно з цим втіленням, таке розпізнавання відбитків пальців використовується переважно замість (або додатково до) звичайної ідентифікації за допомогою пароля. Таким чином, згідно з даним винаходом користувач з успіхом уникає незручностей і менш надійного захисту, що притаманно попередньому рівню техніки на принципі розпізнавання за допомогою паролів.

Окрім контрольованого доступу до різноманітних комп'ютерних ресурсів, даний винахід може також бути успішно застосований у інших численних випадках, коли необхідна перевірка благонадійності, як, наприклад, для доступу до приватних будівель, офісів, готельних кімнат, банківських приміщень для сейфів і депозитних скриньок, і такого іншого. Даний винахід може також бути з успіхом застосований для обмеження дозволу роботи відповідно підготовленого персоналу з механізмами, такими як заводське обладнання і транспортні засоби, у одному з втілень пристрої контролю доступу 70, 370 можуть використовуватися як ключ до приватної будівлі або ключ до кімнати у готелі замість звичайних ключів. У першому прикладі власник при встановленні замка на біометричному принципі у своєму будинку спочатку реєструє свої відбитки пальців. У останньому прикладі гість готелю також спочатку реєструє свої відбитки пальців при реєстрації у готелі. Після цього доступ до будинку або готельної кімнати дозволено тільки відповідному власнику ключа (тобто власнику будинку або гостю готелю). Такі та інші різноманітні застосування технологічних пристроїв доступу на біометричному принципі, що описані тут, вважаються такими, що попадають у обсяг і відповідають ідеї даного винаходу.

Хоч втілення даного винаходу для контролю доступу, що описані при цьому, використовують технологію розпізнавання відбитків пальців, треба звернути увагу, що даний винахід не обмежується наведеним у даному описі, а скоріше навпаки, охоплює використання інших технологій розпізнавання на біометричному принципі. Одною з них є технологія сканування райдужної оболонки ока. В той час як інші аналогічні технології на біометричному принципі спеціально не описані, їх застосування для контролю доступу з використанням портативного пристрою знаходяться в межах і відповідають ідеї даного винаходу.

Більш того, в той час як найбільш поширені втілення даного винаходу, що описані тут, використовують флеш пам'ять як пам'ять носія, треба звернути увагу на те, що інші види енергонезалежної пам'яті, такі як ферроелектрична оперативна пам'ять (FRAM) або магнітна оперативна пам'ять (MRAM), можуть також використовуватися у межах даного винаходу. До того ж, в той час як такі найбільш поширені втілення описані при цьому як сумісні з стандартом УПМ, не передбачається, що портативний пристрій даного винаходу може застосовуватися тільки для даного опису. Скоріше навпаки, даний винахід передбачає охопити портативні пристрої, що підтримують інші протоколи і/або стандарти шин, такі як IEEE 1394 ("Firewire") стандарт.

В той час як найбільш поширені втілення даного винаходу, способи, системи для застосування контрольованого доступу з використанням технології на біометричному принципі, описані тут, зрозуміло, що спеціалісти у цій галузі, як зараз так і в майбутньому, можуть виконувати різноманітні вдосконалення і

розширення, що підпадають під обсяг формули, що наведена далі. Наведена формула повинна забезпечити відповідний захист даного винаходу, вперше наведеного у даному описі.

5

Формула винаходу

1. Портативний пристрій, що включає мікропроцесор і модуль розпізнавання, що працює за біометричним принципом, що сполучений з і контролюється мікропроцесором, з доступом до ресурсу, що охороняється, причому ресурс, що охороняється, має порт зв'язку, комунікаційно сполучений з портативним пристроєм, що надається користувачу, модуль розпізнавання на біометричному принципі виконано з можливістю ідентифікації особистості користувача і дозволу або заборони доступу до ресурсу, що охороняється.

2. Портативний пристрій за п. 1, в якому модуль розпізнавання на біометричному принципі є модулем розпізнавання відбитків пальців.

3. Портативний пристрій за п. 2, в якому модуль розпізнавання відбитків пальців включає сенсорний елемент відбитків пальців.

4. Портативний пристрій за п. 3, в якому сенсорний елемент виконано з можливістю обертатися при операції зчитування, підставляючи послідовно ділянки пальця користувача до рухомого контакту з сенсором, і таким чином зчитуючи послідовно ділянки відбитків пальців користувача.

5. Портативний пристрій за п. 3 або п. 4, в якому модуль розпізнавання відбитків пальців включає кришку, встановлену таким чином, що вона пересувається від першої позиції, закриваючи сенсорний елемент, до другої позиції, відкриваючи сенсорний елемент.

6. Портативний пристрій за п. 1 або п. 2, який комунікаційно сполучений з портом ресурсу, що охороняється, через універсальну послідовну магістраль (УПМ).

7. Портативний пристрій за будь-яким з попередніх пунктів, в якому модуль розпізнавання на біометричному принципі включає біометричний сенсор, розташований на поверхні портативного пристрою.

8. Портативний пристрій за будь-яким з пп. 1-7, який додатково включає енергонезалежну пам'ять, яка містить в собі та зберігає біометричну інформацію, що необхідна для ідентифікації.

9. Портативний пристрій за будь-яким з пп. 1-8, в якому мікропроцесор сконфігурований таким чином, щоб забезпечити обхідний механізм для розпізнавання у випадку пошкодження модуля розпізнавання на біометричному принципі.

10. Портативний пристрій за будь-яким з пп. 1-9, в якому ресурс, який охороняється, включає хост-комп'ютер.

11. Портативний пристрій за будь-яким з пп. 1-10, в якому ресурс, який охороняється, включає комунікаційну мережу.

12. Портативний пристрій за будь-яким з пп. 1-11, в якому ресурс, який охороняється, є ділянкою, до якої передбачається обмеження доступу.

13. Портативний пристрій за будь-яким з пп. 1-12, в якому ресурс, який охороняється, є діючими механізмами, безпечна робота з якими вимагає підготовки.

14. Система контролю доступу за біометричним принципом для контролю доступу до ресурсу, що охороняється, яка включає портативний пристрій, що включає енергонезалежну пам'ять, і модуль розпізнавання, що працює за біометричним принципом, сполучений з ним, у якому модуль розпізнавання, що працює за біометричним принципом сконфігурований так, щоб зчитувати перший біометричний відбиток, зберігати перший біометричний відбиток у енергонезалежній пам'яті, зчитувати другий біометричний відбиток і визначати, чи може другий біометричний відбиток бути ідентифікованим з першим біометричним відбитком, надавати доступ до ресурсу, що охороняється, при успішному розпізнаванні, і не надавати доступу у протилежному випадку.

15. Система контролю доступу за біометричним принципом за п. 14, в якій модуль розпізнавання на біометричному принципі є модулем розпізнавання відбитків пальців.

16. Система контролю доступу за біометричним принципом за п. 14 або п. 15, в якій портативний пристрій комунікаційно сполучений з портом ресурсу, що охороняється, через універсальну послідовну магістраль (УПМ).

17. Система контролю доступу за біометричним принципом за будь-яким з пп. 14-16, в якій модуль розпізнавання на біометричному принципі включає біометричний сенсор, який структурно інтегрований з портативним пристроєм у цілісній конструкції, причому біометричний сенсор розміщений на одній поверхні портативного пристрою.

18. Система контролю доступу за біометричним принципом за п. 17, в якій сенсор є сенсором відбитків пальців, який включає елемент, що виконано з можливістю обертатися при операції зчитування, послідовно приводячи ділянки пальця користувача у рухомий контакт з сенсором і, таким чином, зчитуючи послідовно ділянки відбитків пальців користувача.

19. Система контролю доступу за біометричним принципом за п. 17 або п. 18, в якій модуль розпізнавання на біометричному принципі включає кришку, встановлену таким чином, що вона пересувається від першої позиції, закриваючи елемент, до другої позиції, відкриваючи сенсор.

20. Система контролю доступу за біометричним принципом за будь-яким з пп. 14-19, в якій енергонезалежна пам'ять портативного пристрою включає флеш-пам'ять.

21. Система контролю доступу за біометричним принципом за будь-яким з пп. 14-19, в якій передбачено обхідний механізм для розпізнавання у випадку пошкодження модуля розпізнавання на біометричному принципі.

22. Спосіб керування доступом за біометричним принципом для контролю доступу до ресурсу, що охороняється, який застосовується з використанням портативного пристрою, що включає стадії отримання

першого біометричного відбитку користувача біометричним сенсором, встановленим на портативному пристрої, вибирання зареєстрованого біометричного відбитку з пам'яті портативного пристрою, причому даний зареєстрований біометричний відбиток був збережений у процесі реєстрації, порівняння першого біометричного відбитка з вже зареєстрованим біометричним відбитком і надання користувачу доступу до ресурсу, що охороняється, за умови, що встановлено відповідність на згаданій стадії порівняння.

23. Спосіб контрольованого доступу за біометричним принципом за п. 22, в якому зареєстрований біометричний відбиток є відбитком пальців.

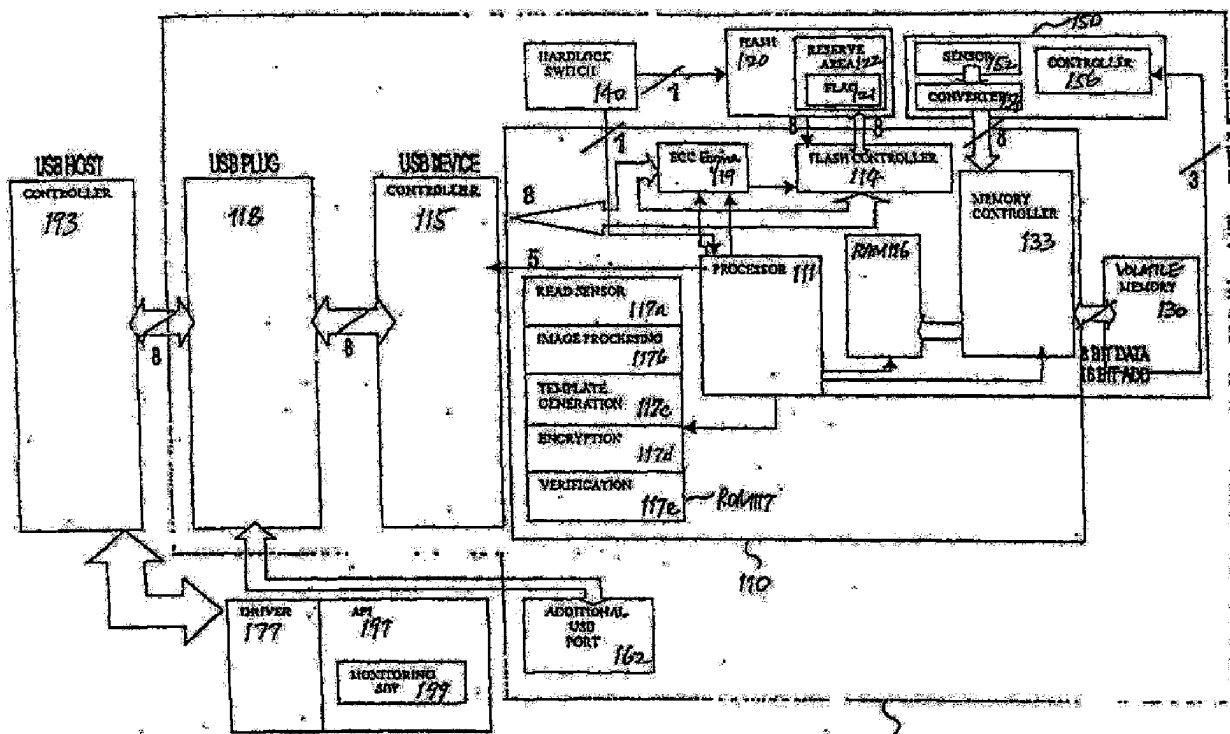
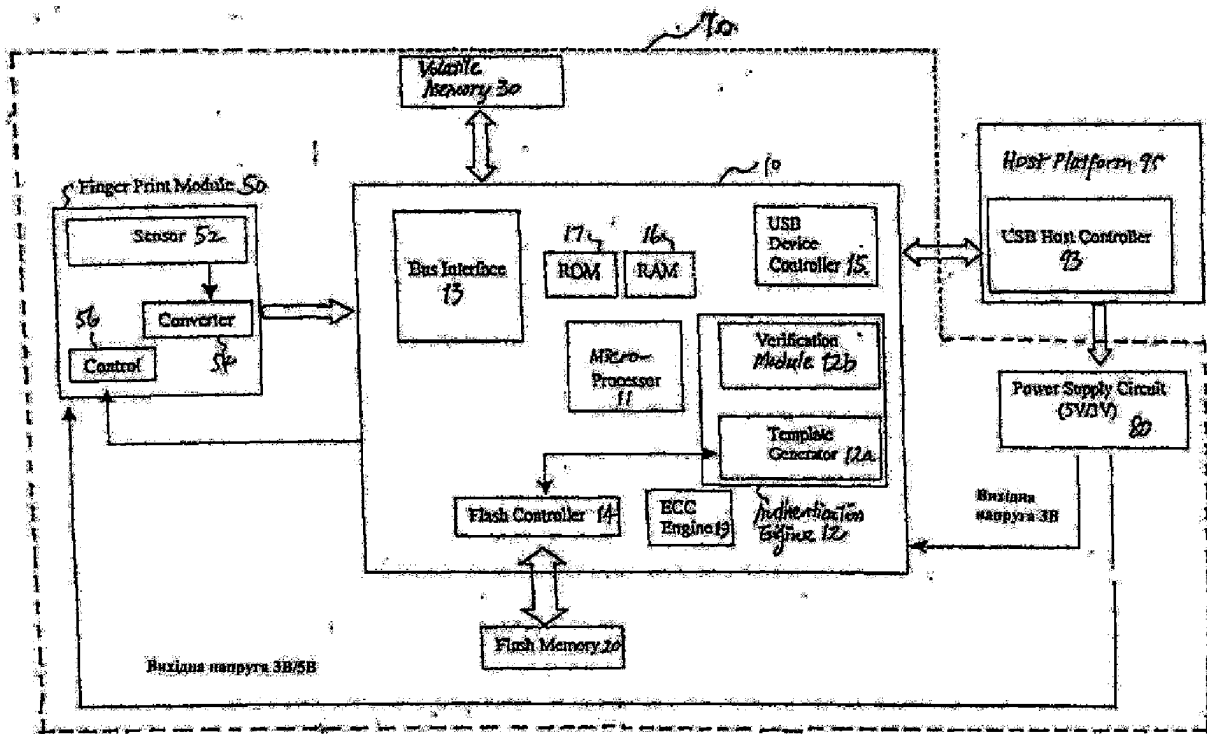
24. Спосіб контрольованого доступу за біометричним принципом за п. 22 або п. 23, в якому зареєстрований біометричний відбиток зберігається у зашифрованій формі.

25. Спосіб контрольованого доступу за біометричним принципом згідно з будь-яким з пп. 22-24, який додатково включає стадії заборони доступу користувача до ресурсу, що охороняється, за умови, що відповідність на згаданій стадії порівняння не встановлена.

26. Спосіб контрольованого доступу за біометричним принципом за будь-яким з пп. 22-25, який додатково включає стадії забезпечення користувача обхідною процедурою розпізнавання за умови, що відповідність на згаданій стадії порівняння не встановлена.

U A 7 5 8 7 3 C 2

U A 7 5 8 7 3 C 2



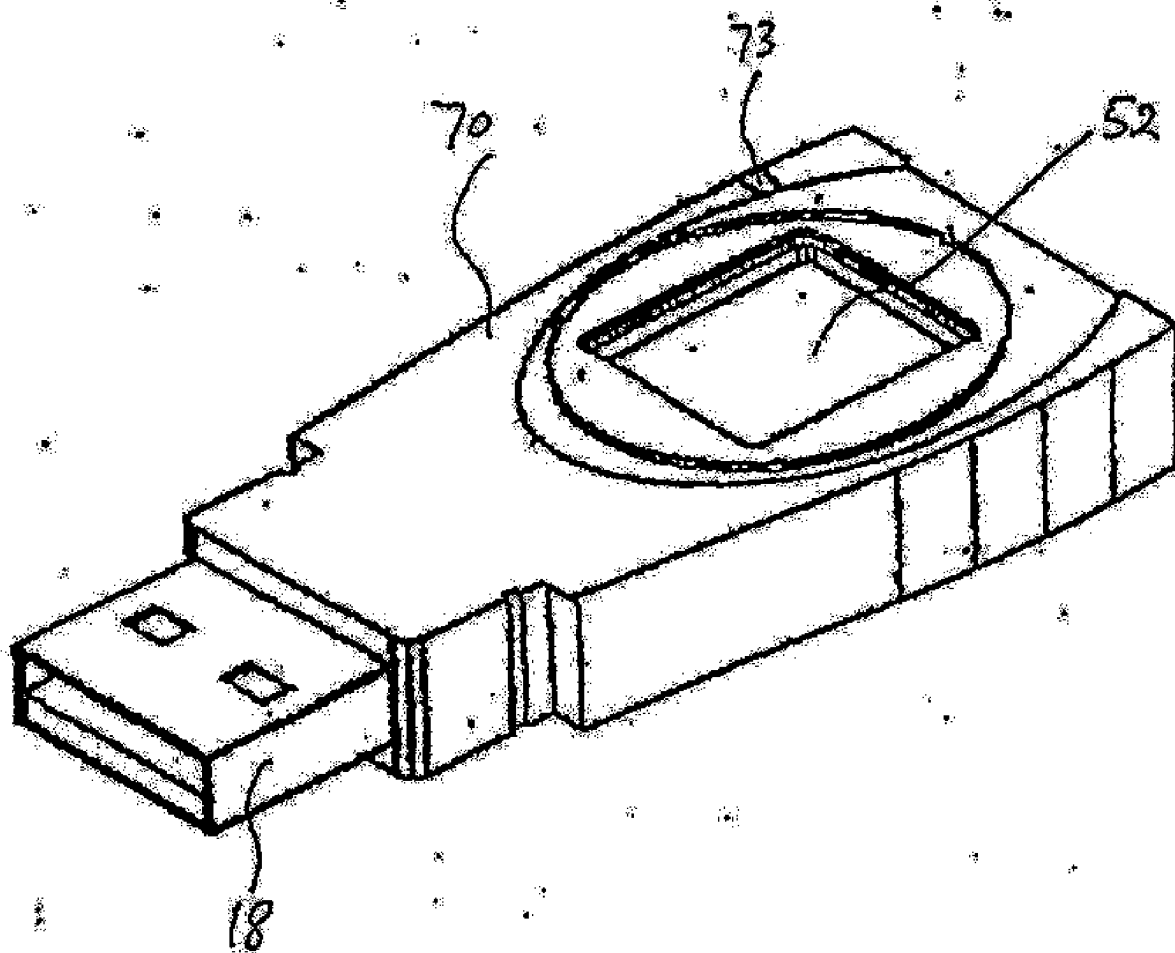


Fig. 2

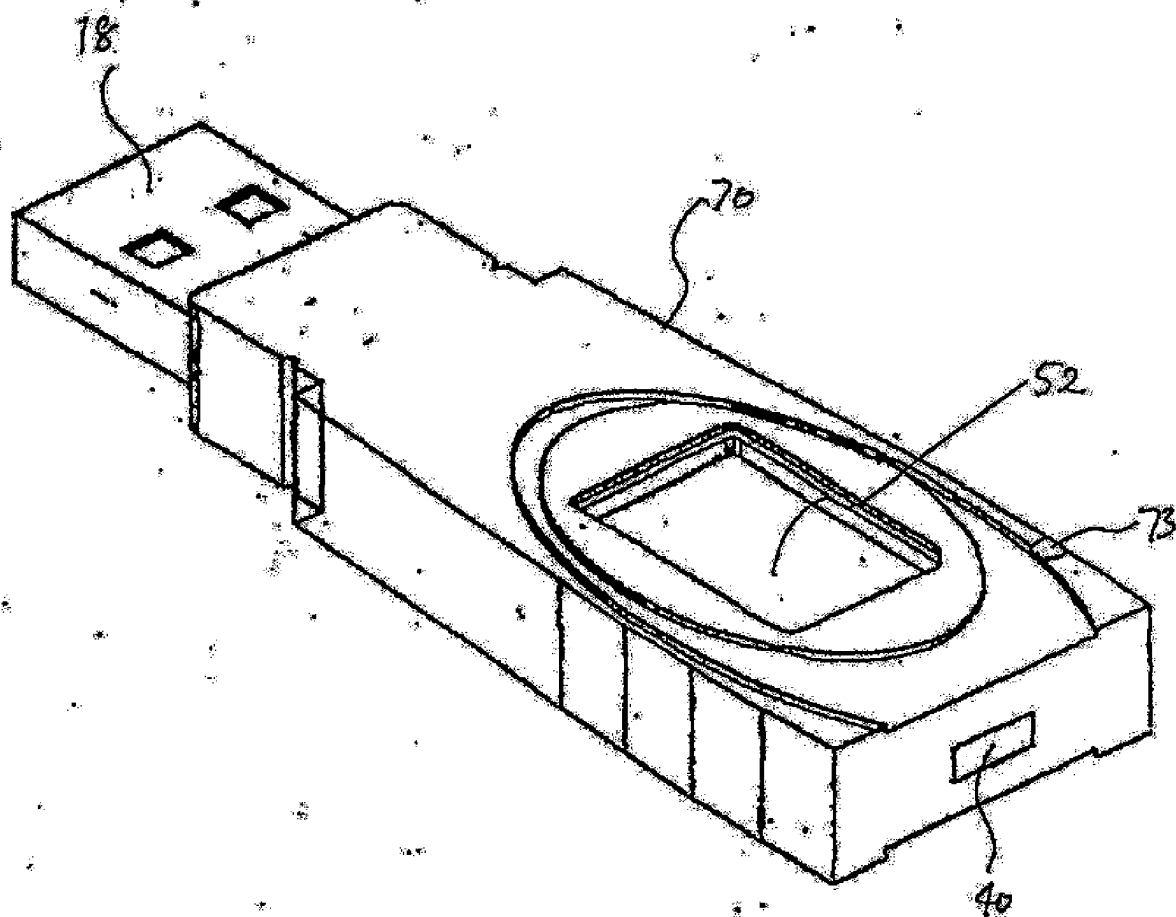


Fig. 3

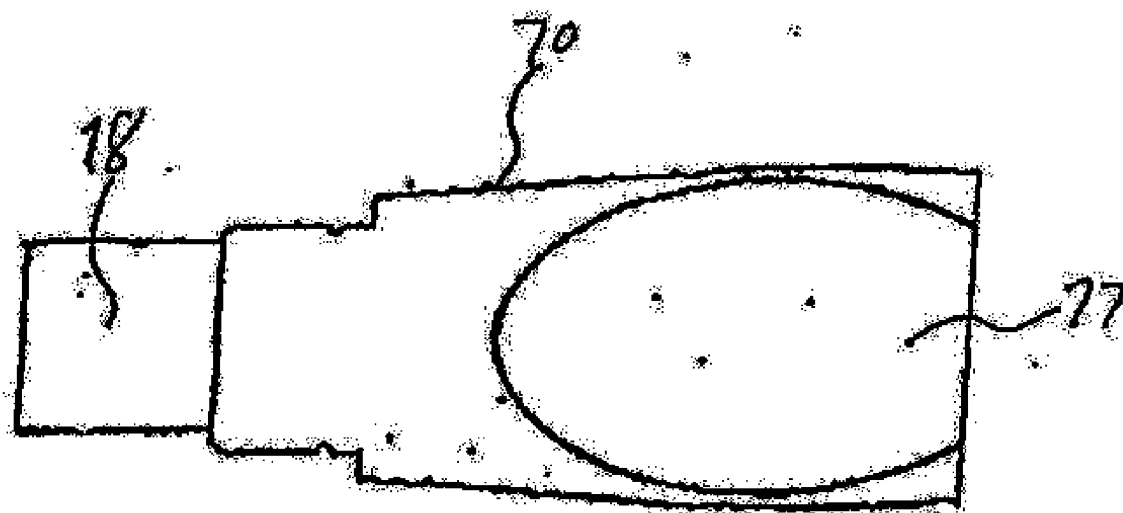
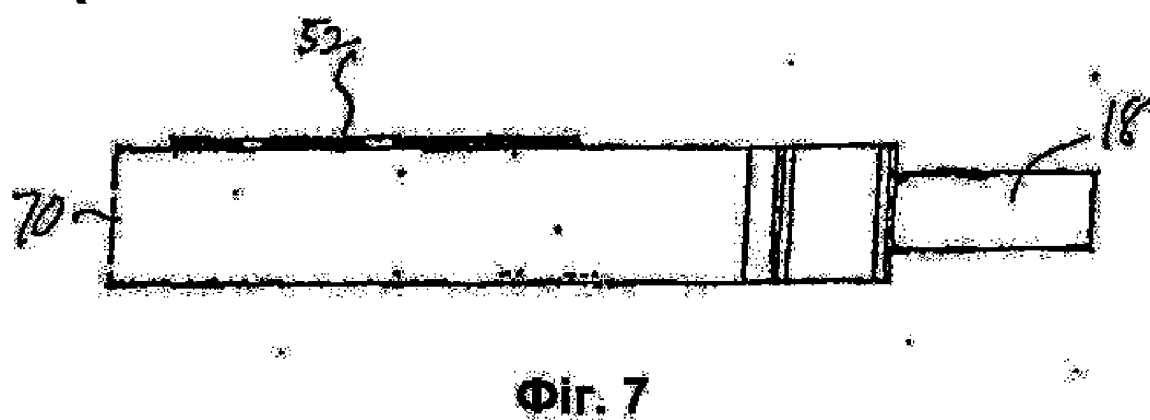
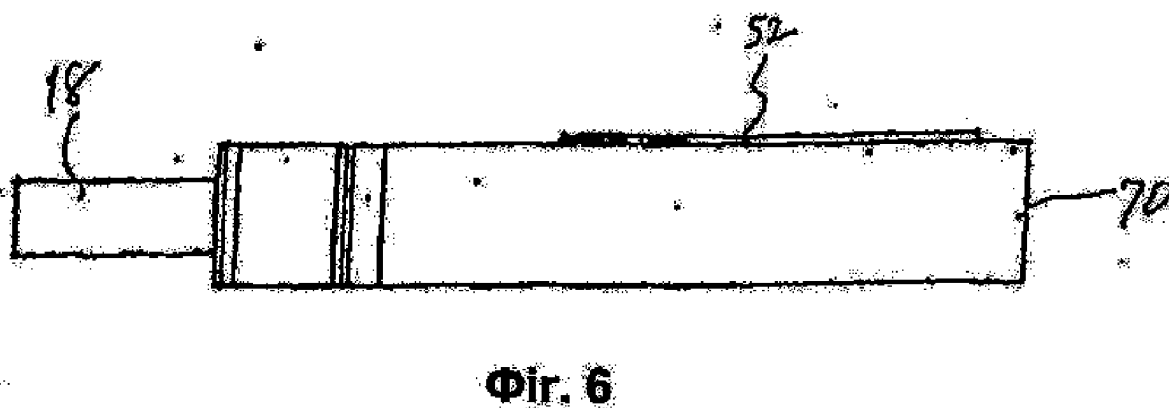
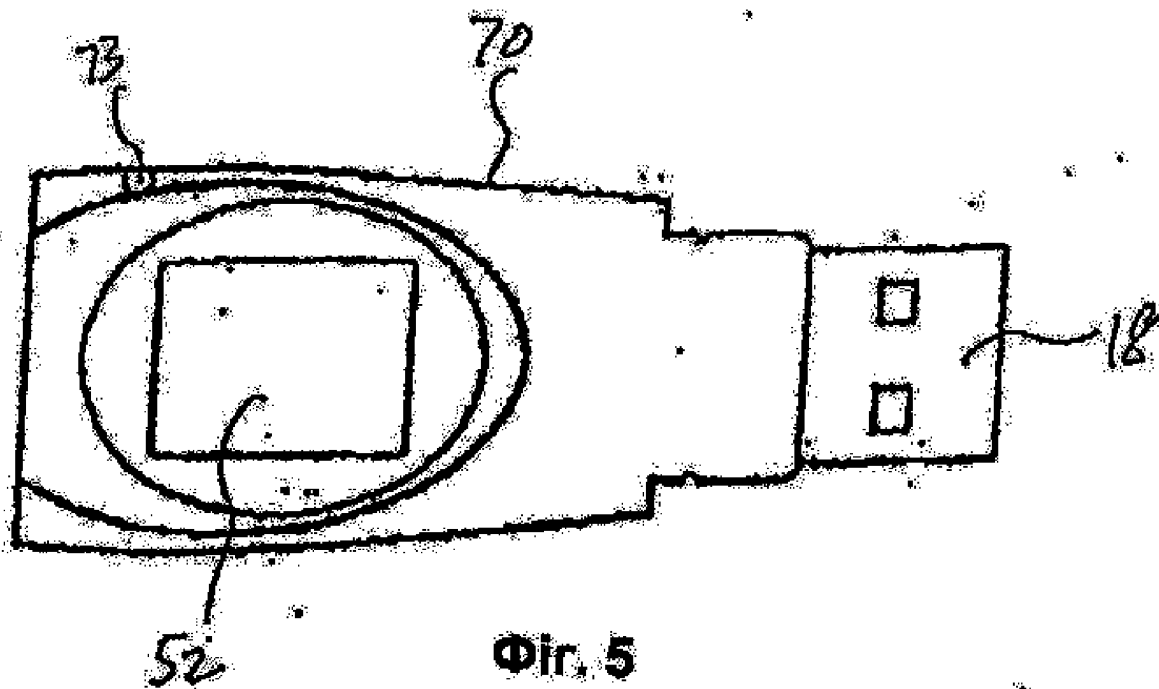


Fig. 4



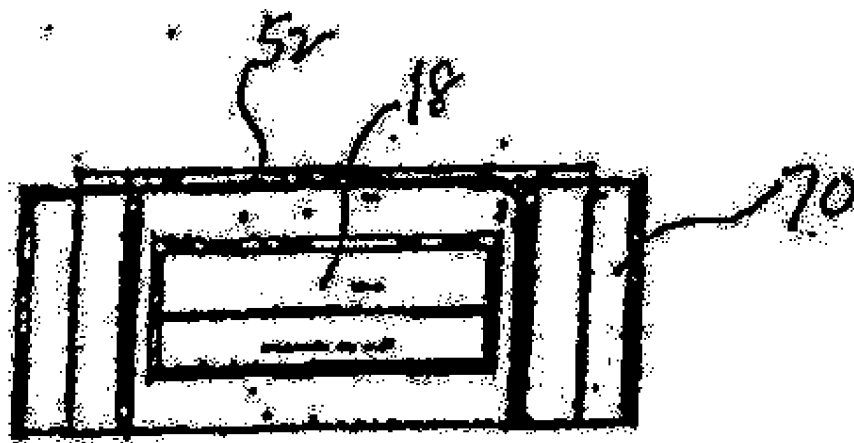


Fig. 8

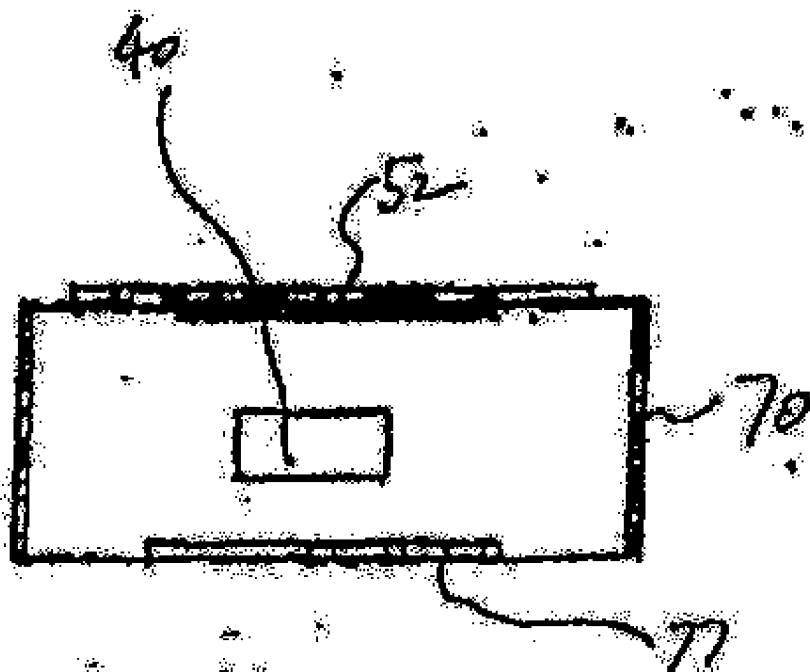


Fig. 9

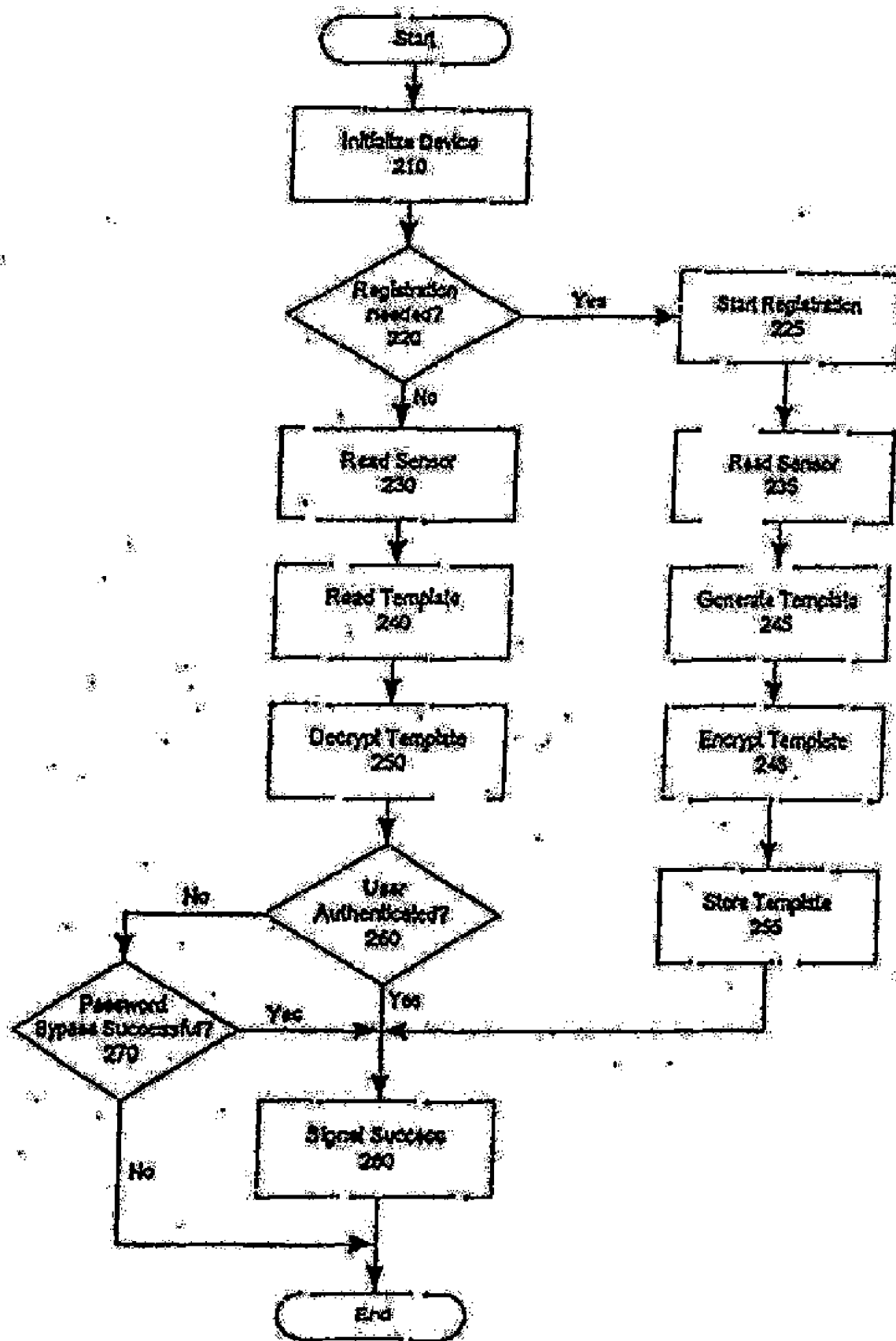
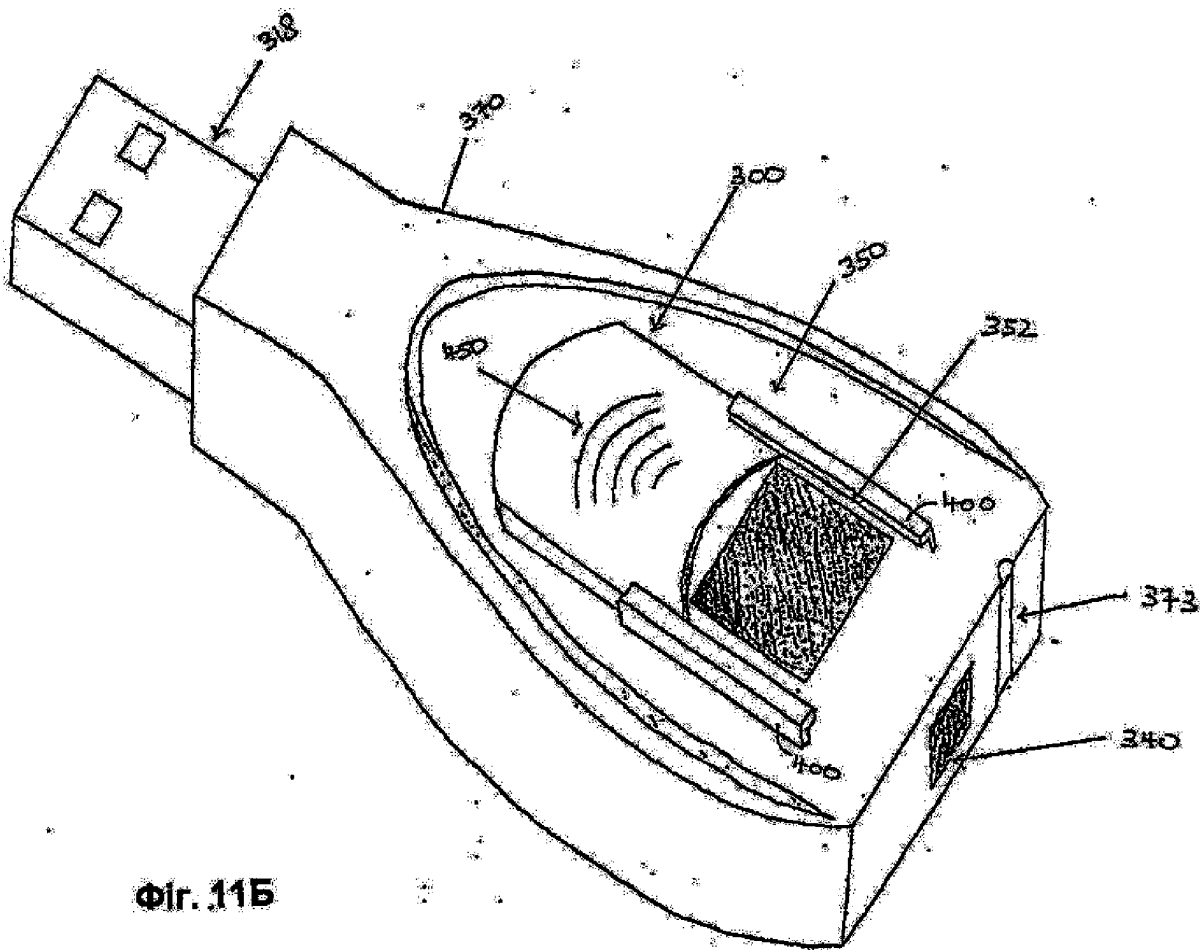
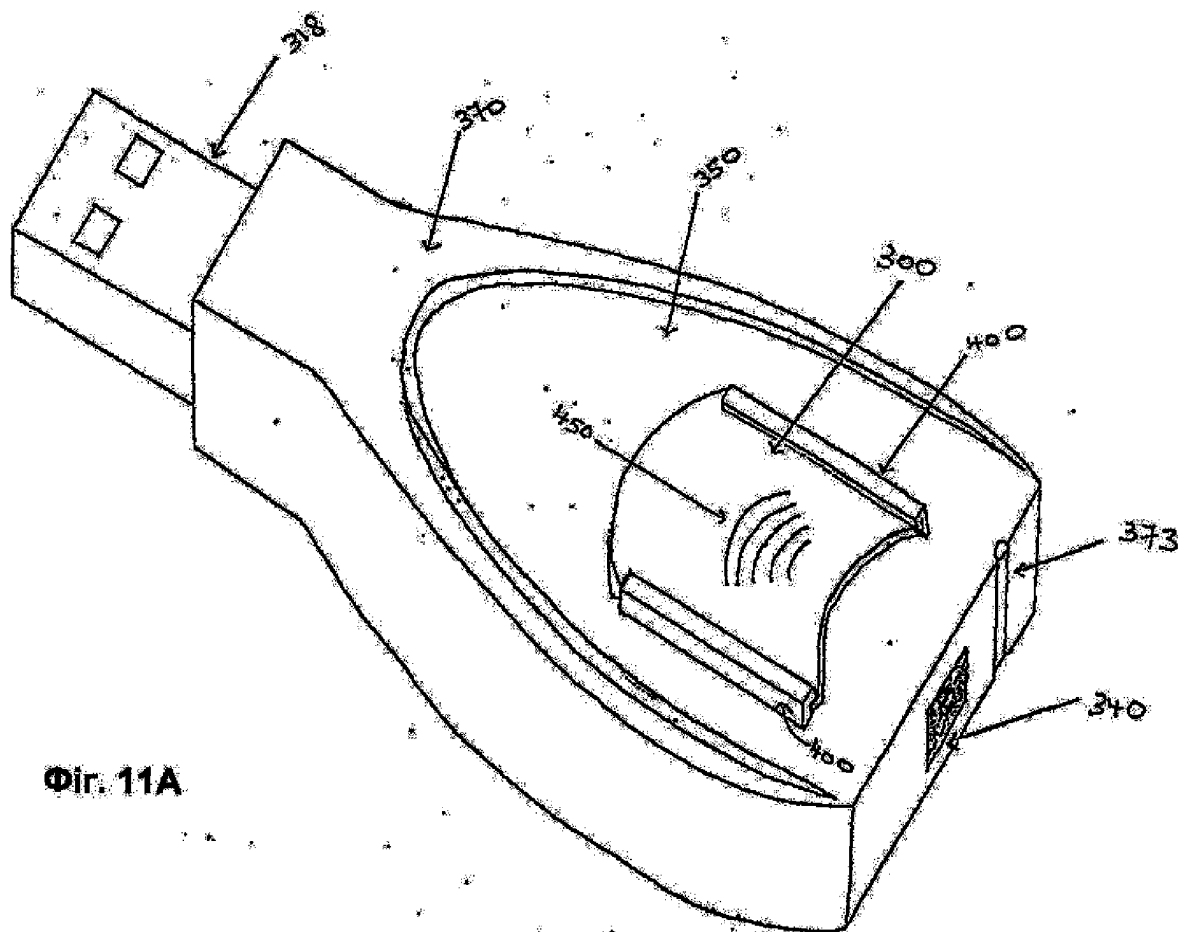


Fig. 10



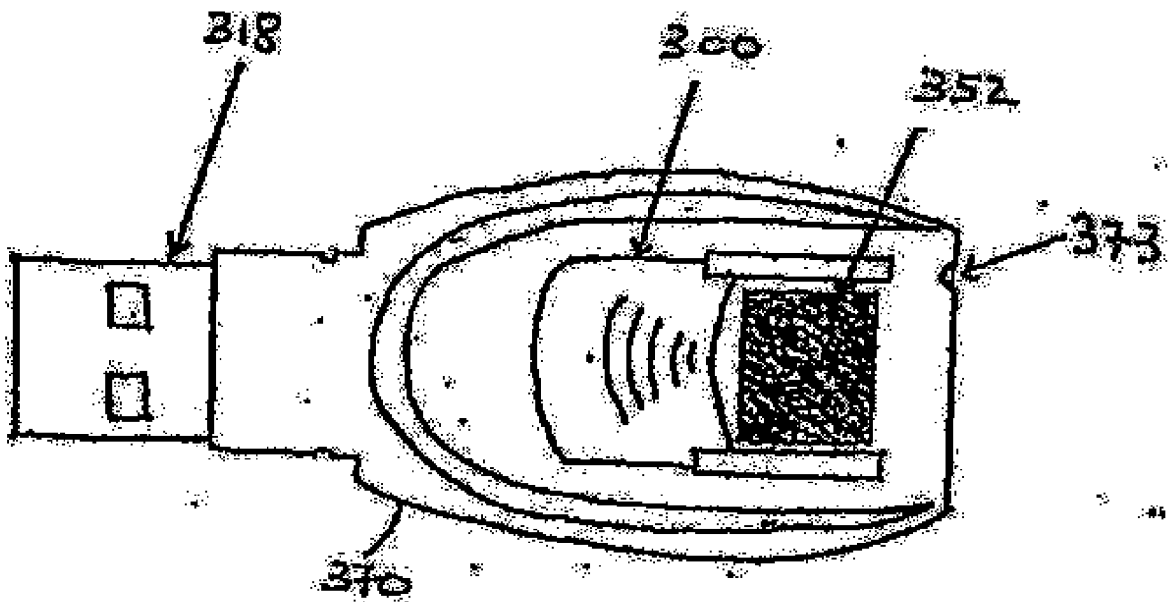


Fig. 12

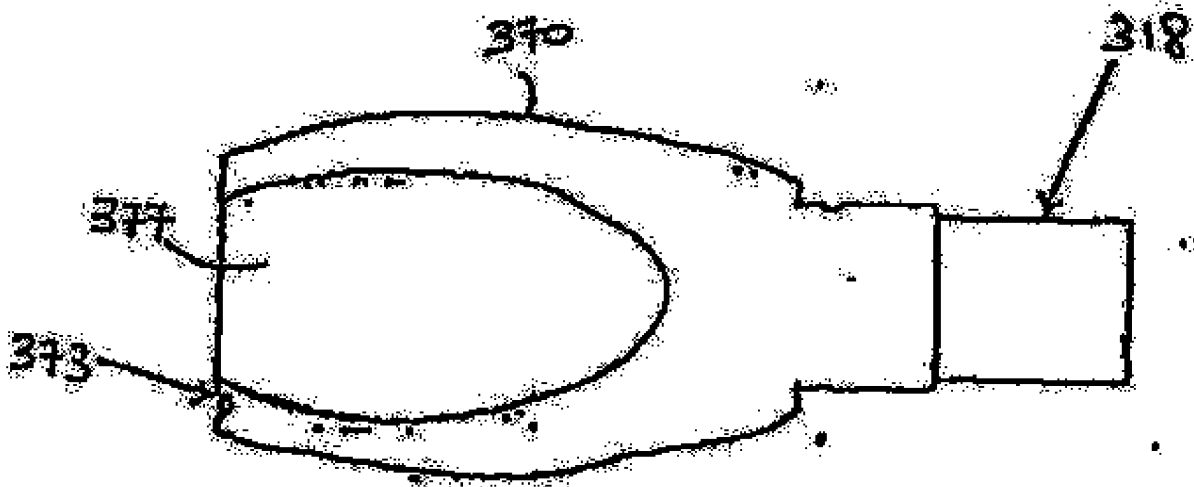


Fig. 13

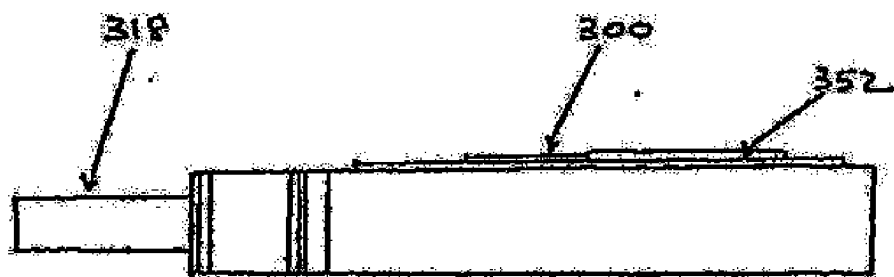


Fig. 14

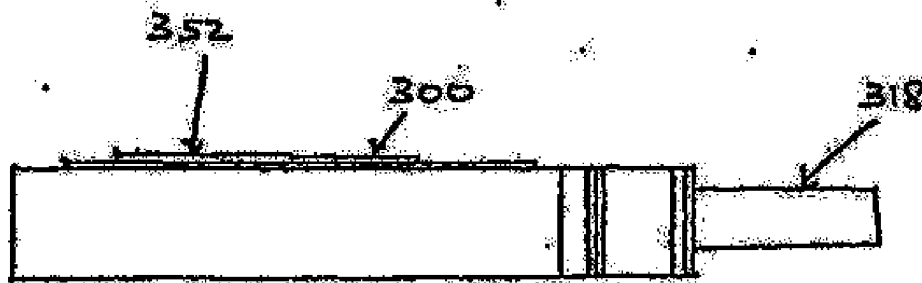


Fig. 15

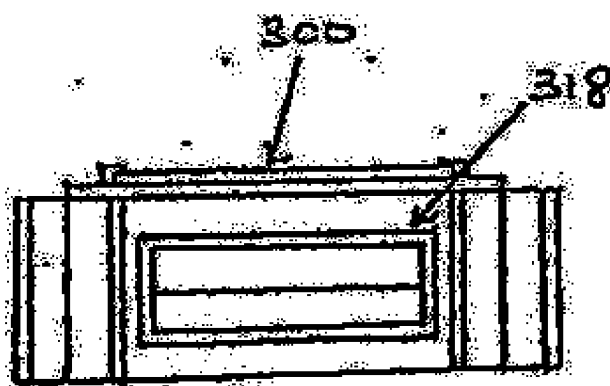


Fig. 16

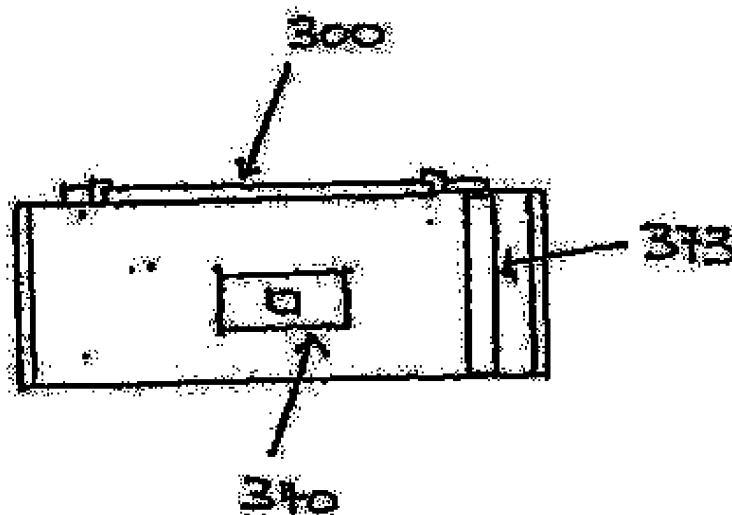


Fig. 17

Офіційний бюлетень "Промислова власність". Книга 1 "Винаходи, корисні моделі, топографії інтегральних мікросхем", 2006, N 6, 15.06.2006. Державний департамент інтелектуальної власності Міністерства освіти і науки України.