



**ФЕДЕРАЛЬНАЯ СЛУЖБА  
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,  
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ**

**(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ**

(21), (22) Заявка: 2008124967/12, 20.11.2006

(24) Дата начала отсчета срока действия патента:  
20.11.2006

(30) Конвенционный приоритет:  
23.11.2005 FR 0511835

(45) Опубликовано: 20.03.2010 Бюл. № 8

(56) Список документов, цитированных в отчете о  
поиске: WO 02/33682 A, 25.04.2002. US 4118057 A,  
03.10.1978. GB 2324065 A, 14.10.1998. RU  
2000118007 A, 27.06.2002.

(85) Дата перевода заявки РСТ на национальную  
фазу: 23.06.2008

(86) Заявка РСТ:  
FR 2006/002564 (20.11.2006)

(87) Публикация РСТ:  
WO 2007/060323 (31.05.2007)

Адрес для переписки:  
129090, Москва, ул.Б.Спасская, 25, стр.3,  
ООО "Юридическая фирма Городисский и  
Партнеры", пат.пов. А.В.Миц, рег.№ 364

(72) Автор(ы):

**БУРРЬЕР Франсис (FR),  
КЕЗЕР Клеман (FR),  
БУРРЬЕР Франк (FR)**

(73) Патентообладатель(и):

**НОВАТЕК СА (FR)**

**(54) ЗАЩИЩАЮЩАЯ ОТ ВСКРЫТИЯ И ПОВТОРНО ИСПОЛЬЗУЕМАЯ ПЛОМБА  
ВЫСОКОЙ ЗАЩИЩЕННОСТИ**

(57) Реферат:

Изобретение относится к системам для проверки несанкционированного проникновения и касается пломбы высокой защищенности, которая может быть повторно использована неограниченное число раз, т.к. аутентифицирующая часть изменяется хаотическим образом каждый раз, когда пломба открывается и когда возвращается в эксплуатацию. Такая пломба состоит, по меньшей мере, из двух аутентификаторов и, по меньшей мере, один из которых подвижен по отношению к другому в открытом положении. Эти два аутентификатора становятся

неподвижными и устойчивыми в закрытом положении. В каждом новом неподвижном положении два аутентификатора соединяются с созданием новым аутентифицирующим признаком, который сохраняется в базе данных для сравнения в процессе проверки. Данный признак будет удален и заменен на другой, когда упомянутая пломба несанкционированным путем или умышленно открывается и, таким образом, будет обеспечивать доказательство того, что была открыта. Предложенная пломба обеспечивает высокую защищенность объектов и может многократно использоваться. 5 з.п. ф-лы, 3 ил.



FEDERAL SERVICE  
FOR INTELLECTUAL PROPERTY,  
PATENTS AND TRADEMARKS

(51) Int. Cl.

*G09F 3/03* (2006.01)*E05B 39/02* (2006.01)*G06K 19/06* (2006.01)**(12) ABSTRACT OF INVENTION**(21), (22) Application: **2008124967/12, 20.11.2006**(24) Effective date for property rights:  
**20.11.2006**(30) Priority:  
**23.11.2005 FR 0511835**(45) Date of publication: **20.03.2010 Bull. 8**(85) Commencement of national phase: **23.06.2008**(86) PCT application:  
**FR 2006/002564 (20.11.2006)**(87) PCT publication:  
**WO 2007/060323 (31.05.2007)**

Mail address:

**129090, Moskva, ul.B.Spaskaja, 25, str.3, OOO  
"Juridicheskaja firma Gorodisskij i Partnery",  
pat.pov. A.V.Mits, reg.№ 364**

(72) Inventor(s):

**BURR'ER Fransis (FR),  
KEZER Kleman (FR),  
BURR'ER Frank (FR)**

(73) Proprietor(s):

**NOVATEK SA (FR)****(54) HIGH SECURITY REUSABLE SEAL FOR PROTECTION FROM OPENING**

(57) Abstract:

FIELD: physics, signalling.

SUBSTANCE: invention relates to systems for checking for unauthorised penetration and a high security seal which can be used an unlimited number of times since the authenticating part changes randomly each time the seal is opened and when reused. Such a seal consists of at least two authenticators and at least one of them can be moved relative the other in open position. These two authenticators are immovable and stable in closed

position. In each new fixed position, the two authenticators are joined to create a new authentication feature which is stored in a database for comparison during verification. This feature will be removed and replaced by another when the said seal is illegally or deliberately opened such that there will be evidence that the seal has been opened.

EFFECT: seal provides high security of objects and can be repeatedly used.

6 cl, 5 dwg

## ОБЛАСТЬ ТЕХНИКИ ИЗОБРЕТЕНИЯ

Изобретение предлагает очень высоко защищенную пломбу многоразового использования без какого-либо ухудшения механизма и делает возможным проверять несанкционированное проникновение. Такой тип пломбы может быть использован  
 5 либо для контроля и проверки несанкционированного проникновения в соединение, систему или неудачной попытки сохранения целостности объекта или его содержимого неправомерным лицом, или наоборот, быть открытой доверенным лицом для того, чтобы проконтролировать и проверить его доступ.

### УРОВЕНЬ ТЕХНИКИ

Существует большое число систем для проверки несанкционированного проникновения или попытки несанкционированного проникновения в систему или  
 10 расположение, защищенное от неавторизованных лиц, и для идентификации и удостоверения объектов, являющихся оригиналами. Наиболее общими современными способами являются:

- электронные сирены, эти системы поднимают тревогу, когда происходит несанкционированное проникновение, тогда сигнал тревоги продолжает работать пока не будет, например, использован секретный код или пока не будет авторизован  
 20 биометрический отпечаток,

- системы видеонаблюдения делают возможным регистрировать или управлять в реальном времени доступом или точками пересечения,

- карты (с чипом, магнитные...), секретные коды или биометрики делают возможным управлять доступом к расположению или защищаемой системе.

Все эти способы приспособлены к доступу и управлению входом лиц в частные или  
 25 публичные места. Для защиты доступа к системе или даже для предотвращения общего доступа в расположение или систему, за исключением авторизованного персонала, в основном используются защитные пломбы, делающие возможным избежать и запретить несанкционированное проникновение в защищаемую систему  
 30 или расположение. Пломбы также используются, чтобы обеспечить целостность или подлинность объекта. Эти пломбы могут быть различных форм согласно применению. Проверка физической целостности пломбы делает возможным, в теории, гарантирование, что не было нарушения системы или объекта. Наименование  
 35 "система" взято в широком смысле, это может быть, например, сборка связанных элементов, узел или неспецифические условия, такие как бутылка, требующая сохранения целостности содержимого, это также может быть информационная система.

Настоящее изобретение в частности направлено на применение обработки важных  
 40 данных, как это будет в дальнейшем описано.

Самая старая пломба - восковая, как правило, означавшая авторизованную пломбу. Также существуют металлические пломбы или пластиковые, интегрирующие  
 45 кольцевой идентификатор, находящийся над непрерывной затяжкой. Такие пломбы не являются повторно используемыми потому, что неизбежно их разрушение, когда происходит нарушение входа в расположения или защищаемую систему. Также существуют "четкообразные" металлические пломбы в форме гофрированных нитей, чьи два конца загружены в звенья мягкого металла, обычно свинца, использующие  
 50 специальное зажатие, которое маркирует пломбу рельефом вышеупомянутого свинцового звена; это также называется наполнителем (заливкой). Этот последний тип пломбы часто используется на водных, газовых, счетчиках электроэнергии для того, чтобы препятствовать доступу к электрическим или механическим измерительным

устройствам. Таким образом, в большом семействе пломб, можно классифицировать идентифицирующие пластины или защиту всех типов, которые часто являются выгравированными металлическими пластинами, штампованным пластиком или распечаткой. Эти пластины или защита в общем идентифицируют объект, комплексную систему, машину или персону посредством идентификационной карты, такая защита является произведенной помеченной пломбой прав, что делает возможным произвести аутентификацию. Применения, развивающие идентификационные пластины или защиты, многочисленны и разнообразны, среди наиболее частых можно встретить автомобили, которые имеют идентификационные пластины производителя и инспекционные номерные пластины; идентификационные пластины и санкционирующие пластины станков; пластины на материалах, электрических и электронных машинах и т.д. В общем, эти идентификационные пластины проиндексированы в архивах у производителя или в административных базах данных.

Все эти типы идентификационных пломб или защит представляют два главных неудобства: первое - это то, что они очень легко воспроизводимы с идентичными средними параметрами, включающими аутентифицирующий элемент или пломбу, кроме того, возможно получить их в большом количестве на рынке; второе - это замена объекта или защищаемой системы. Для части из них соединение между пломбой или защитой, с частями для которых необходимо запретить отделение или вскрытие, неэффективно и может быть легко разрушено, сохраняя нетронутыми пломбу или защиту; например соединение, которое может быть растворено химическим или подходящим растворителем, который сделает возможным высвободить пломбу, получить доступ к закрытой зоне и переставить пломбу на тоже самое место и, таким образом, достигнуть или модифицировать данные без обнаружения. Также становится возможным заменить оригинальную пломбу копией и, таким образом, сделать копию заменителем оригинальной.

Еще одна важная проблема - это соотношение цены/защищенности. В общем, чем больше защищенность, тем выше затраты, которые определяют главную проблему для множества применений, которые используют пломбы, и где необходимо было бы одновременно иметь небольшую цену с высоким уровнем защиты, что противоречит существующим решениям.

Тем же образом, чтобы препятствовать физическому доступу к электронным системам, содержащим конфиденциальную информацию, стало общеизвестно использовать очень специфические голограммы и даже для некоторых систем высокого уровня защиты. Тем не менее, определитель высокого уровня защиты был приспособлен, конечно, для систем, известных ранее, в настоящее время, действующие сейчас методы позволяют очень легко воспроизвести идентичные определители с уровнем качества, сравнимым с оригиналом.

Кроме того, голограммы не являются индивидуальными, т.е. они все идентичны в одной серии, и неправомочному лицу становится просто получить эти голограммы, открыть защищаемый контейнер, разрушив голограмму, и заменить ее полностью идентичной. Если голограмму невозможно получить, контрафактор может всегда отделить ее от контейнера, не разрушая ее, и таким же образом поместить ее обратно. Таким образом, одним способом или другим становится крайне легко для оговоренной личности вторгнуться в систему и физически достигнуть конфиденциальной информации, например в «черный ящик», содержащий запоминающее устройство, или заменить объект другим. Главным образом и в любом

методе использования защитная пломба должна, с одной стороны, предотвращать физическую опасность доступа к контейнеру и содержимому, и с другой стороны, обнаруживать такие вторжения, когда несмотря ни на что это произошло. Защитная пломба не имеет возможности сделать попытку вторжения в систему, доступ к расположению или неспецифический контейнер невозможными; с другой стороны, если она хорошо сконструирована и интегрирована с защищаемым продуктом или расположением, она разубедит активного взломщика и оставит следы попытки взлома. Она действует всеми способами защиты, которые, как правило, способны отобразить попытку взлома, на физическую целостность системы или объекта, на котором она смонтирована. В соответствии с изобретением пломба, известная как защитная пломба, может иметь несколько форм. Пломба фактически является обычным соединением, представляющим объединение себя самой и одного или более элементов, отмеченных авторизованной пломбой (пломбой Штата, например).

Во всех этих применениях проблема определена в возможности воспроизводить идентичные пломбы для обманного доступа к физическому содержимому расположений или систем.

Патент FR2848698 этого же заявителя и изобретателя относится к процессу идентификации и аутентификации без специального считывателя объекта или существа. В этом документе рекомендовано связывать идентификатор, сложный или невозможный к воспроизведению, объектом или существом, подлежащими идентификации или аутентификации. Как раскрыто выше, этот патент не относится к системе мониторинга вмешательства в защищенное расположение или сохранности объекта, что является точно объектом данного заявленного изобретения. Процесс, описанный в патенте FR2848698, не делает возможным в любом случае гарантировать системе или защищаемому расположению полную защиту. На самом деле, прикрепление идентификатора к объекту не предотвращает получения доступа к объекту, его изменения, его анализа и от замены того же идентификатора без удаления, даже если он невоспроизводим. В самых наихудших случаях возможно даже взять аутентификатор без разрушения объекта и прикрепить его к другому объекту.

Международная публикация WO 01/11591 описывает устройство, которое делает возможным идентифицировать объекты. Такой идентификатор имеет матрицу линз, которые создают визуальный образ в трех измерениях. То, что раскрывается в этом документе, полностью отличается от данного изобретения главным образом в следующем:

- Следуя примеру патента FR2848698, этот идентификатор не позволяет гарантировать отображения взлома или вторжения в защищаемый объект или расположение.

- Идентификатор, описанный в данном документе, является воспроизводимым сколько угодно, так как он базируется на процессе производства, комплексном, но полностью контролируемым. Следовательно, уникальность такого идентификатора не гарантируется.

- Идентификатор не ассоциируется с базой данных.

Документ EP 1087334 описывает систему пломб, использующих ретранслятор, который делает возможным содержать удаленную электронную и вопросную идентификацию. Такой тип ретранслятора не уникален, так как лицо или организации, имеющие средства производства, могут произвести несколько имеющих такой же номер пломб. Следовательно, вполне возможно открыть описанное устройство для доступа к его содержимому и полностью воспроизвести две капсулы, идентичные

первым ответам с ретранслятором, дающим тот же ответ как первый. Фактически, недостаток такого типа устройства - это цепочка поставок капсул и ретрансляторов, если недобросовестное лицо или организация может изменить маршрут движения  
 5 деталей, будет возможным воспроизводить пломбы, идентичные первой. Кроме того, такой тип пломбы не может повторно использоваться после вскрытия. В настоящем изобретении, как будет показано далее, процесс вторжения основывается на уникальном аутентификаторе, не являющемся воспроизводимым и записываемым в  
 10 базу данных, следовательно, даже если лицо управляет аутентификаторами, последние не будут поддерживать какую-либо утилиту, потому что они не будут записаны в устаревшей базе.

Патент WO02/3368A описывает повторно использующиеся пломбы, где переход закрытого положения в открытое положение содержит активацию генератора случайных электронных кодов. Посредством считывания такого кода отображается,  
 15 что пломба была открыта, если код изменился, и наоборот, не открывалась, если код не изменился. Если цели этого патента идентичны целям заявленного изобретения, средства, реализующие указанные цели, отличаются и в результате степень безопасности является намного выше в заявленном изобретении. На самом деле, подтверждение о непроникновении обеспечивается в этом патенте считыванием  
 20 электронного положения, но такое положение может быть идентично воспроизведено, зная алгоритмы генерации кода. Так же, без знаний алгоритмов генерации кода, эта повторно используемая пломба может быть заменена другой, которая во всех отношениях идентична, где запись может воспроизводить код, идентичный оригиналу,  
 25 но программирование будет осуществлено внутренней электронной системой, которая подделывает коды по требованию. Таким образом, полностью невозможно заменить такой тип пломбы другой, имея идентичные аутентифицирующие характеристики.

Патент US-A-4118057 описывает повторно используемую пломбу, где часть  
 30 аутентифицирующих характеристик представлена случайно подогнанными шарами различного цвета, появляющимися в окне. Чрезвычайно большое число комбинаций делает возможным утверждать, что невозможно воспроизвести две идентичные логические комбинации, что необходимо для защиты от взлома или от распломбирования. Система является полностью механической, не имеет электроники,  
 35 замена пломбы другой во всех отношениях идентичной и представляющей те же расположения шаров теоретически возможна, потому что даже шары отлично воспроизводятся и в размере, и в цвете. Таким образом, достаточно обеспечить дисплей и расположить идентичные шары. Подобным способом, если станет сложным  
 40 модифицировать устройство в ходе использования, всегда легко обеспечить другое подобное устройство, приготовленное заранее, с идентичным расположением аутентифицирующих частей, т.е. идентичным положением разноцветных шаров.

Патент US2003/04647 описывает аутентификаторы с пузырьками, всегда  
 45 уникальными и невозможными к воспроизводству со связанными с ними средствами для их интерпретации. Такой пузырьковый аутентификатор, хотя невозможен к воспроизводству, не может действовать один в границах изобретения для повторно используемой пломбы, потому что он не может подтвердить, что пломба не была  
 50 открыта и закрыта снова. С другой стороны, как это будет видно в описании изобретения далее, такой тип аутентификатора чрезвычайно хорошо подходит настоящему изобретению как индивидуальный аутентификатор, связанный с другим аутентификатором подобного типа, но неизбежно отличный в этих характеристиках. Такое объединение взаимодействует хаотичным образом для получения бесконечного

количества новых устойчивых невоспроизводимых положений.

## ПОДРОБНОЕ ОПИСАНИЕ ИЗОБРЕТЕНИЯ

Изобретение направлено на совокупное решение, для устранения трех трудностей, которые возникают при использовании известных пломб:

1) сделать пломбы незаменяемыми между собой;

2) сделать физически взаимозависимыми систему пломбы, расположение или объект, подлежащий защите так, что если существует вторжение или просто попытка вторжения или замены, сама пломба визуально помечается;

3) сделать пломбу повторно используемой после каждого применения для того, чтобы уменьшить затраты, в тоже время сохраняя очень высокий уровень защиты;

4) иметь возможность контролировать на основе пятна, было или не было вскрытие или попытка вскрытия.

Согласно с первой характеристикой чрезвычайно передовой и имеющей изобретательский уровень. Пломба с высоким уровнем защиты согласно изобретению является неограниченное количество раз повторно используемой, в тоже время делая возможным определение и подтверждение вскрытия и закрытия, которое соответствует новому повторному использованию. Такая важная характеристика является основой изобретения, заключааясь в том, что она обладает новой аутентифицирующей характеристикой каждый раз, когда оно вскрывается и вследствие закрывается снова, для ввода в эксплуатацию. Оно отличается тем, что оно интегрирует устройство, позволяющее бесконтрольное изменение его аутентифицирующих характеристик в каждом изменении состояния, т.е. во время перехода из закрытого в открытое положение (фиг.1А), отменяя предыдущие аутентифицирующие характеристики, и из открытого в закрытое положение (фиг. 1В), регенерируя новые аутентифицирующие характеристики благодаря хаотическому самосозданию новых аутентифицирующих характеристик, вызванных вышеупомянутым изменением положения. Каждая аутентифицирующая характеристика сохраняется в защищенной памяти или в базе данных, чтобы подтвердить было ли вскрытие или попытка вскрытия пломбы.

Еще одна характеристика изобретения заключается в том, что используются, по меньшей мере, два аутентификатора 1, 2, которые всегда показывают уникальные невоспроизводимые неповторимые характеристики для того, чтобы избежать повторений. По меньшей мере, один из известных аутентификаторов действует отдельно изменчивым образом, когда пломба находится в разблокированном положении (фиг.1А) или открытом, и соединяется в устойчивое и считываемое состояние, когда пломба находится в закрытом и заблокированном положении (фиг.1В). Другая характеристика изобретения - это соединение и устойчивое действие невоспроизводимых и неповторимых аутентификаторов 1, 2, что позволяет создать новые общие аутентификаторы 15, 16, 17, будущие полностью случайными, в зависимости от относительного положения, полученного от неповторимых аутентификаторов 1, 2.

Еще одна характеристика изобретения - отдельное и неустойчивое взаимодействие аутентификаторов 1, 2, произведенное, по меньшей мере, относительным движением одного аутентификатора по отношению к другому(им).

Еще одна характеристика нового изобретения - общие аутентификаторы 15, 16, 17, созданные новым положением неповторимых аутентификаторов 1, 2, что делает возможным создавать новый код или сигнатуру с каждого изображения, сохраняющегося в локальной и/или удаленной базе данных. Еще одна

характеристика - это уникальная и невоспроизводимая аутентифицирующая характеристика неповторимых аутентификаторов 1, 2, являющаяся результатом хаотического процесса.

5 Согласно еще одной характеристике изобретения аутентифицирующие характеристики - это видимые пузырьки, автоматически созданные в материале. В качестве примера, этот хаотический процесс может быть образованием пузырьков в процессе затвердевания вышеупомянутого материала, из которого состоит аутентификатор. Таким образом, в противоположность устройств, которые являются  
10 результатом процесса производства полностью контролируемого человеком, и, таким образом, воспроизводимых другим человеком, имеющим подобные инструменты, каждый аутентификатор, использованный в данном изобретении, является уникальным и невозможным к воспроизведению, потому что он является результатом неконтролируемого процесса. Эта характеристика делает возможным окончательно  
15 исключить возможность получения аутентификаторов или пломб, идентичных оригиналам. С защищенностью, свойственной каждому аутентификатору, вторая защита добавляется путем суммирования, точнее комбинацией совместных действий аутентификаторов.

20 Согласно еще одной характеристике физически неповторимые уникальные аутентификаторы невоспроизводимы с точки зрения идентичности, т.е. невозможно или чрезвычайно сложно копировать аутентификаторы, аутентификатор может использовать неоднородность, произвольным образом размещенную в прозрачной массе. Эти визуально различимые разнородности фиксируются, например, в виде  
25 фотографии, и одна или более представлений, характеризующих этот профиль идентификатора, сохраняют в памяти базы данных каждое в виде двухмерных изображений, или в цифровом виде, вычисленном, исходя из выделяющихся элементов, позиционирования, размера и т.д. разнородностей, утопленных в массе, двух форм представлений, изображений или цифровых представлений, которые могут  
30 сосуществовать. Таким же образом, возможно включать магнитные частицы в этот вид идентификации, делая возможным кодирование другим способом.

Еще одна характеристика и наилучший вариант - это объемный прозрачный неповторимый аутентификатор, изготовленный из стекла, керамики, пластика или  
35 полимеров, содержащих видимые пузырьки, число которых, форма и положение вытекает из неуправляемого хаотического процесса самогенерации. Такой тип аутентификатора особо интересен, потому что он всегда уникален и не поддается копированию человеком. Патент EP01 904039.3 того же заявителя и изобретателя раскрывает этот тип пузырькового аутентификатора с подходящей системой  
40 считывания. В случае этого изобретения это является вопросом использования этого пузырькового аутентификатора в конкретном процессе, где конечная цель - это предотвращение или запрещение доступа к системам или расположениям, или проверка целостности или идентификация информации, связанной с оригиналом. Как и  
45 ранее, представление в форме изображения и/или цифровом виде хранится в базе данных, для того чтобы было возможным проверить достоверность аутентифицирующих характеристик.

В соответствии с еще одной характеристикой память и/или база данных, в которой  
50 сохраняется представление аутентифицирующей характеристики, расположена физически в системе и/или защищенном расположении, и/или на самой защите, но содержимое которой может быть считано извне наделенным правами лицом. Такое представление аутентификатора образует ключ доступа к физической системе

и/или логической информации. В практическом применении и для множественного использования считыватель аутентифицированных характеристик запоминает результаты считывания, осуществляемые в момент последнего шага, и автоматически сравнивает новую информацию. В случае несоответствия аудио или световой сигнал информирует инспектора о том, что была попытка вскрытия. Не отступая от объема данного изобретения, идентификатор, такой как штрих-код или радиометка (RFID), может быть ассоциирован с каждой пломбой, таким образом представляя доступ в базу данных для того, чтобы более легко осуществлять сравнения.

В соответствии еще с одной характеристикой изображение и/или цифровое представление аутентификатора может быть принято стандартной телекоммуникационной сетью, такой как Интернет.

Согласно еще одной характеристике содержимое, сохраненное в цифровом виде и/или в виде изображения, может быть принято авторизованным инспектором или агентом несколькими способами. Один способ состоит из визуального сравнения представления изображения, сохраненного в локальной или удаленной базе данных, с физическим аутентификатором посредством анализа сходства положения пузырьков или разнородностей. Существует несколько способов представить изображение: либо напрямую на экран, объединенный с системой или защищаемым расположением, или на отдельный экран, или приставку (мобильный телефон с доступом в Интернет), или печатью на бумагу с объединенного принтера, или используя отдельный принтер системы или защищаемого расположения. Если база данных не локальная, а удаленная, используется код вызова, являющийся идентификатором аутентификатора в удаленной базе данных, код вызова может быть цифровым, буквенно-цифровым, штрих-кодом, магнитной полосой, микрочипом и т.д. Очевидно, что база данных, локальная или удаленная, делается безопасными и защищенными от любой попытки модификации или замены другой информацией.

Еще одна характеристика изобретения - это процесс отслеживания вторжения в систему или защищаемого расположения или вторжения в объект, осуществляемый автоматическим сравнением аутентификатора, используя приспособленный считыватель с цифровым представлением, хранящимся в локальной или удаленной базе данных.

В случае пломбы повторного использования, в соответствии с настоящим изобретением, аутентифицирующее представление, хранящееся в базе данных, будет меняться с каждым новым использованием пломбы, это то соответствие, которое хранится в базе данных и которое действительно отображается на пломбе, которое делает возможным подтвердить, что пломба не была вскрыта.

На фиг.1 изображено устройство согласно предпочтительному операционному режиму изобретения, оно составляет только один неограничивающий пример. Фиг.1А показывает открытое и свободное устройство. Фиг.1В показывает закрытое и заблокированное устройство. Фиг.1С - вид сверху устройства, представляющий аутентифицирующую часть. Крышка (4) содержит один прозрачный аутентификатор (2) с пузырьками (8), произведенными беспорядочно. Этот аутентификатор (2) закреплен на крышке (4) и содержит дисплейное окно (7). Корпус (3) содержит один прозрачный аутентификатор (1), но дно является отражающим, например посеребренным. Так же как для аутентификатора (2) пузырьки были созданы беспорядочно. В корпусе (3) расположена внешняя поверхность (10), в которой шары (11) могут свободно циркулировать. Аутентификатор (1) расположен на шарах (11) и может двигаться свободно на шарах

в пределах ограничений его размещения. Соединитель (5) обеспечивает связь, которая делает возможным связать защитную пломбу как одно целое с защищаемым объектом или контейнером. Соединитель (5) может быть удален из пломбы через вспомогательное промежуточное устройство (12), расположенное в его секции (13).  
 5 Для удаления соединителя (5), для того чтобы открыть контейнер или добраться до защищаемой системы, необходимо выровнять проход (14) крышки (4) с соответствующей частью корпуса (3).

На фиг.1А крышка (4) полностью вывернута из корпуса (3), так что, с одной стороны, возможно извлечь соединитель (5) из корпуса (4), с которым он связан с целью выравнивания отверстия (14) с секцией (13), и, с другой стороны, разъединить аутентификаторы (1) и (2). В процессе этой операции аутентификатор (1), полностью независимый от шаров (11), будет двигаться и занимать изменчивое случайное положение, которое будет изменяться постоянно с малейшим действием, влияющим на систему. Аутентификаторы (1) и (2) недоступны снаружи. На фиг.1В крышка находится в закрытом и заблокированном положении. В таком положении соединитель (5) полностью прикреплен к корпусу (3), закрытому крышкой (4). Такая позиция также делает возможным блокирование аутентификаторов (1) и (2) под давлением и таким образом стабилизировать аутентификатор (1), который был подвижным во время открытого положения. Таким образом, это заблокированное положение обязательно соответствует новому относительному и устойчивому положению аутентификаторов (1) и (2), которое отличается от предшествующего устойчивого положения, при этом для достижения нового устойчивого относительного аутентифицирующего положения необходимо освободить крышку (4). С каждым устойчивым положением, записанным в базу данных посредством регистрации положения, ассоциированного с пузырьками двух прозрачных аутентификаторов, становится легко сравнить все новые относительные положения пузырьков и, таким образом, доказать открывание по этому изменению.  
 10  
 15  
 20  
 25  
 30

Фиг.2 представляет фотографию, представленную в соответствии с настоящим изобретением и показывающую начальное положение каждого аутентификатора (1) и (2), затем последовательно соединенных в аутентификаторах (15), (16) и (17) после трех высвобождений и запираций, таким образом показывая различные сочетания, представляющие разные сигнатуры.  
 35

Фиг.3 соответствует содержанию фиг.2, за исключением того факта, что отличается подсветка, созданная другим способом, в отношении связанных пузырьков.

Эта высокая защита, повторно используемая пломба в соответствии с изобретением, найдет свое применение не только в применениях, требующих защиту очень высокого уровня, например транспортировка опасных веществ, но также для более типичных применений, где требуемый уровень безопасности несомненно ниже, но где начальные инвестиции должны быть погашены очень большим количеством использований пломбы, которая является менее затратной, чем одноразовые пломбы.  
 40  
 45 В этом последнем случае и в качестве примера может быть счетчик электричества, воды, газа и т.д.

Также этот тип пломбы может быть использован для управления доступом агентам в зонах контроля, получая назад, например, используя считыватель, новую результирующую сигнатуру открывания пломбы в базе данных.  
 50

### Формула изобретения

1. Пломба с высоким уровнем защиты, повторно используемая неограниченное

число раз, делающая возможным определить и подтвердить ее вскрытие и ее повторное использование посредством интегрирования устройства, позволяющего бесконтрольное изменение его аутентифицирующих характеристик при каждом изменении состояния, т.е. во время перехода закрытого положения в открытое положение (фиг.1А), аннулируя предшествующие аутентифицирующие характеристики, и во время перехода из открытого положения в закрытое (фиг.1В), возвращая новые аутентифицирующие характеристики, благодаря хаотической самогенерации новых аутентифицирующих характеристик 15, 16, 17, вызванных вышеупомянутым изменением состояния; каждая аутентифицирующая характеристика 15, 16, 17 сохраняется в защищенной долговременной памяти для того, чтобы подтвердить вскрытие или попытку вскрытия вышеупомянутой пломбы, отличающаяся тем, что аутентифицирующие характеристики 15, 16, 17 являются результатом действия двух аутентификаторов 1, 2 уникального и невоспроизводимого с вышеупомянутыми аутентификаторами действующими по отдельности изменчивым образом для, по меньшей мере, одного из них, когда пломба находится в незаблокированном или открытом положении (фиг.1А), и действующих, соединяясь в устойчивое состояние, когда пломба находится в закрытом и заблокированном положении (фиг.1В), делая возможным создание нового кода или сигнатуры в базе данных.

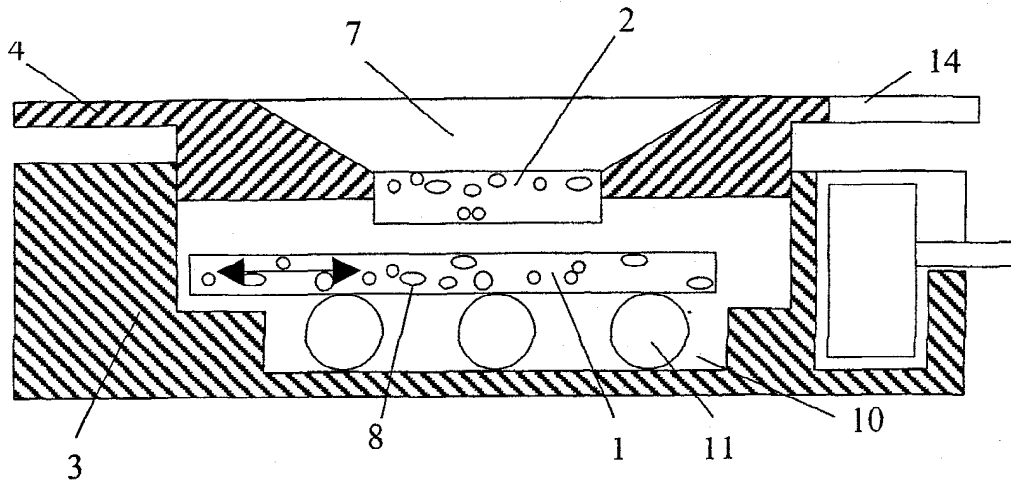
2. Пломба с высоким уровнем защиты, в соответствии с п.1, отличающаяся тем, что соединение и устойчивое действие невоспроизводимых неповторимых аутентификаторов 1, 2 делает возможным создать новый аутентификатор 15, 16, 17 абсолютно случайный, зависящий от относительной позиции известных неповторимых аутентификаторов 1 и 2.

3. Пломба с высоким уровнем защиты по п.1 или 2, отличающаяся тем, что раздельное и изменчивое действие аутентификаторов 1 и 2 формируется посредством, по меньшей мере, относительного движения одного аутентификатора относительного другого.

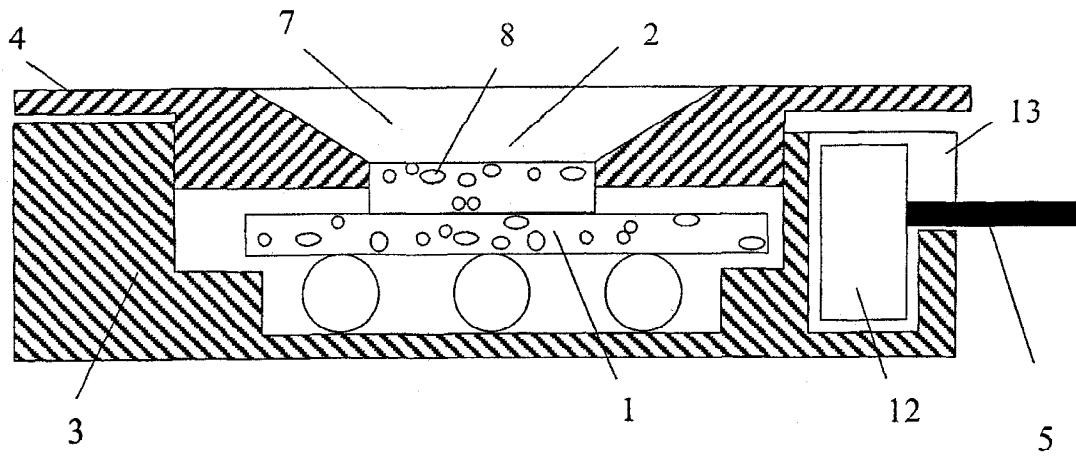
4. Пломба с высоким уровнем защиты по п.1, отличающаяся тем, что новый общий аутентификатор, созданный новой позицией неповторимых аутентификаторов 1, 2, позволяет создание новых кодов 15, 16, 17 или сигнатур, изображения которых сохраняются в локальной или удаленной базе данных.

5. Пломба с высоким уровнем защиты по п.1, отличающаяся тем, что уникальные и невоспроизводимые и неповторимые характеристики аутентификатора являются результатом хаотического процесса.

6. Пломба с высоким уровнем защиты по п.1, отличающаяся тем, что аутентифицирующие характеристики - это видимые пузырьки, автоматически созданные в материале.

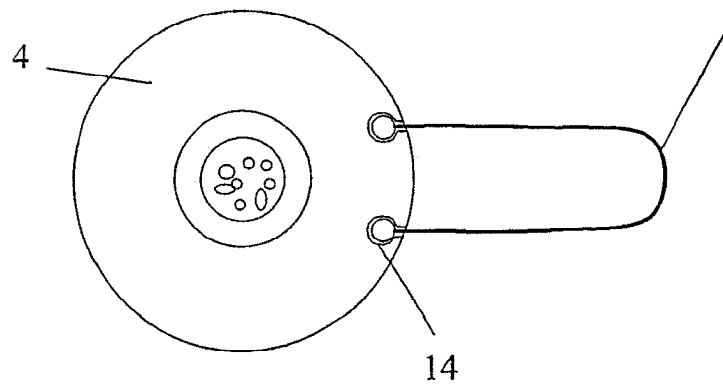


ФИГ.1А

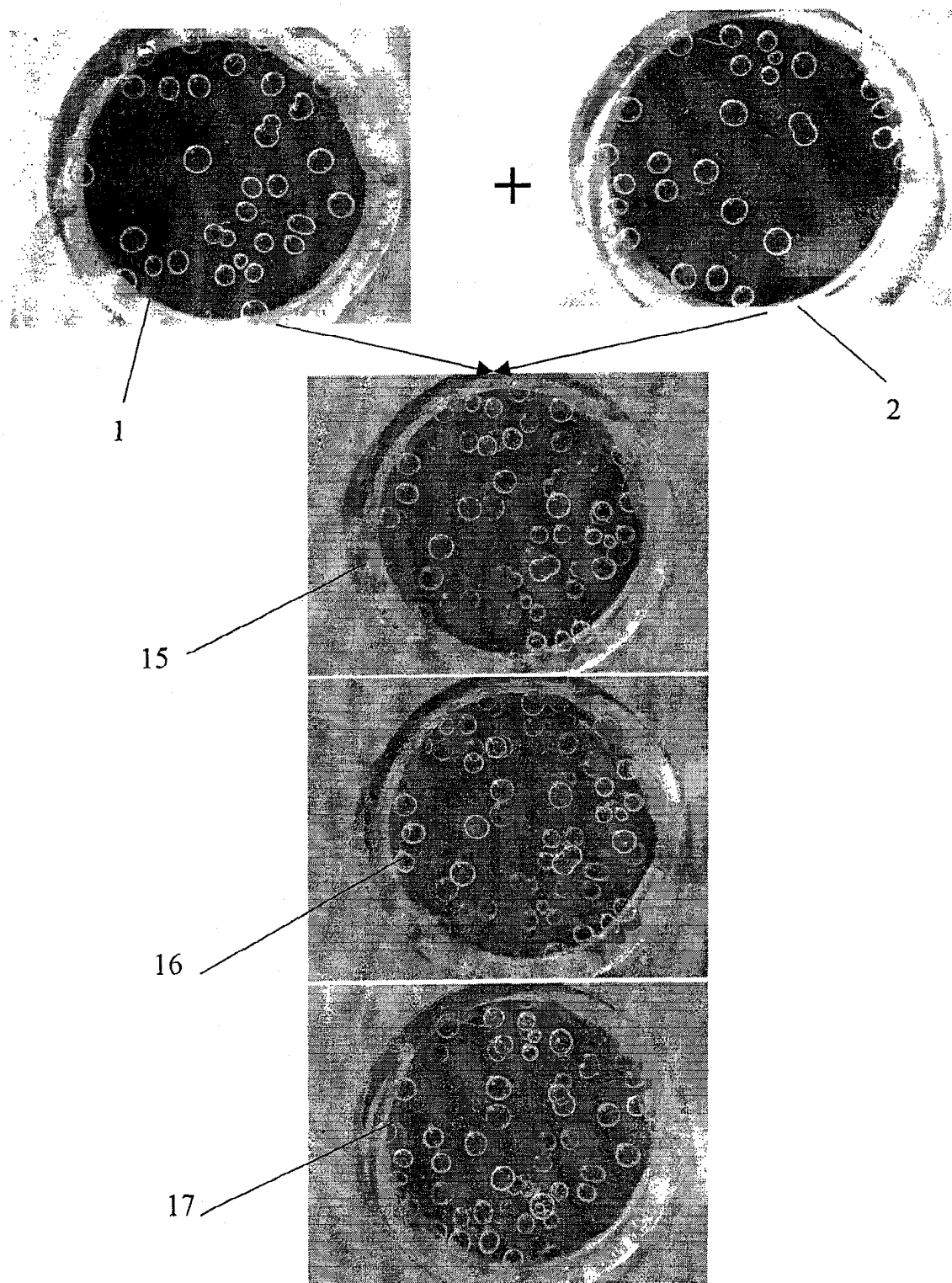


ФИГ.1В

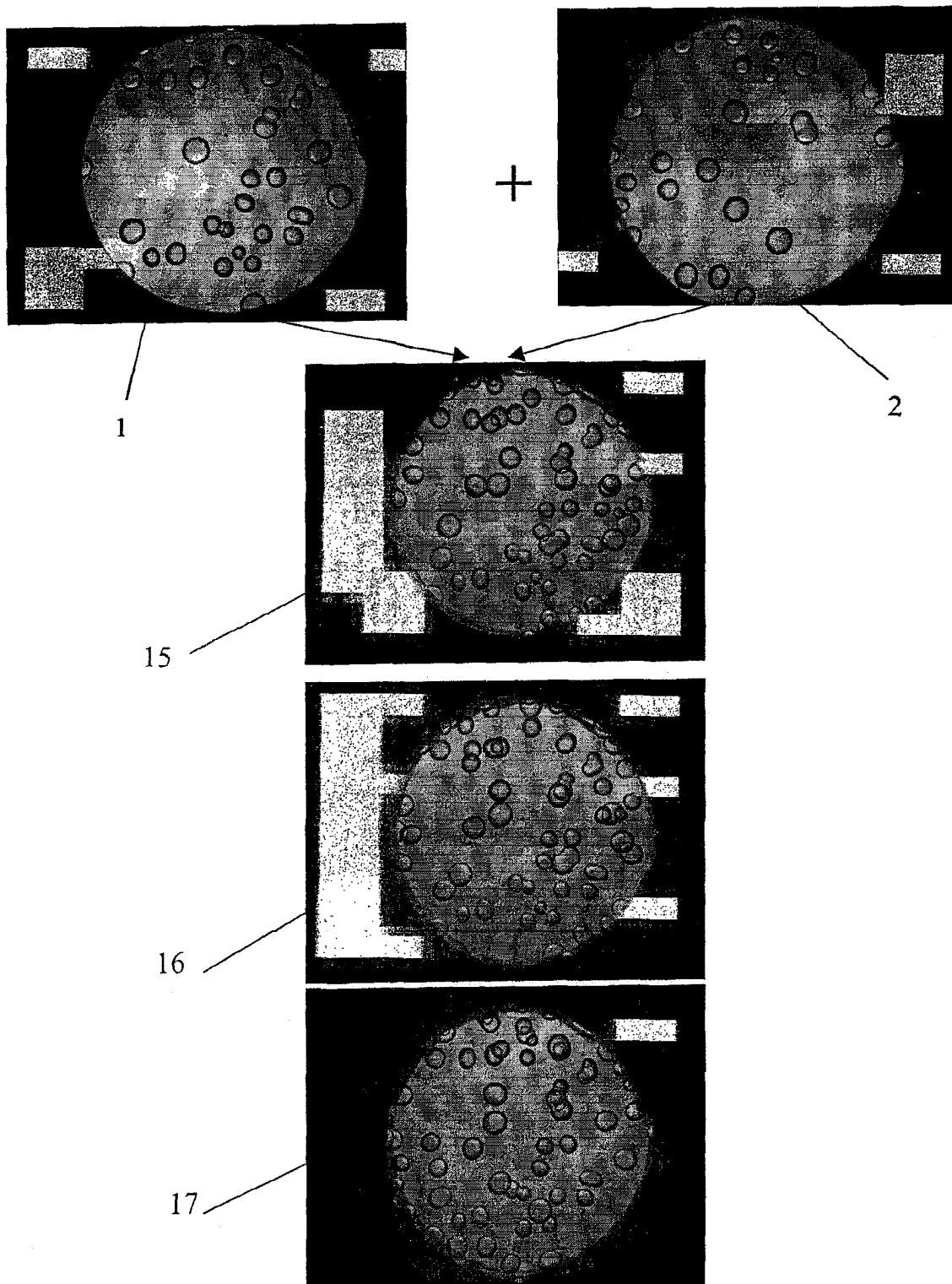
5



ФИГ.1С



ФИГ.2



ФИГ.3