(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 374 975**

(51) Int. CI.:
G06K 9/52 (2006.01)
G07D 7/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06830821 .2**
(96) Fecha de presentación: **22.12.2006**
(97) Número de publicación de la solicitud: **1971960**
(97) Fecha de publicación de la solicitud: **24.09.2008**

(54) Título: **MÉTODO DE EXTRACCIÓN DE CARACTERIZACIONES ALEATORIAS A PARTIR DE UN ELEMENTO MATERIAL Y MÉTODO PARA GENERAR UNA BASE DE DESCOMPOSICIÓN PARA IMPLEMENTAR EL MÉTODO DE EXTRACCIÓN.**

(30) Prioridad:
23.12.2005 FR 0513231
15.02.2006 FR 0601342
21.02.2006 US 774618 P

(45) Fecha de publicación de la mención BOPI:
23.02.2012

(45) Fecha de la publicación del folleto de la patente:
23.02.2012

(73) Titular/es:
SIGNOPTIC TECHNOLOGIES
SAVOIE TECHNOLAC 12, ALLEE LAC DE GARDE
73370 LE BOURGET DU LAC, FR

(72) Inventor/es:
BOUTANT, Yann;
FOURNEL, Thierry y
BECKER, Jean-Marie

(74) Agente: **Ungría López, Javier**

DESCRIPCIÓN

Método de extracción de caracterizaciones aleatorias a partir de un elemento material y método para generar una base de descomposición para implementar el método de extracción

La presente invención se refiere al área técnica de la extracción de caracterización a partir de un elemento material concreto, con vistas a identificar este elemento material completo, o con vistas a usar la caracterización extraída en un proceso dependiente del elemento material objeto, o independientemente de este elemento material objeto.

El problema con la caracterización de un elemento material objeto radica en la necesidad de garantizar la unicidad de esta caracterización, para asegurar o casi asegurar que dos elementos materiales diferentes tendrán dos caracterizaciones diferentes, independientemente del tamaño de la muestra de los dos elementos materiales objeto.

La invención propone conseguir este objetivo de unicidad de la caracterización extrayendo esta caracterización de las características estructurales del elemento material objeto. Por características estructurales del elemento material objeto se entiende, en particular, las características geométricas o morfológicas, internas y/o externas, opcionalmente asociadas con las características de composición química o físico-química, color, estructura u otras, relacionadas con su localización en el espacio sobre el elemento material objeto. Las características estructurales usadas por la invención son aquellas que pueden generarse por estimulación de un elemento material, y adquirirse por uno o más detectores adecuados.

BOUTANT Y et al. “Randomness analysis of images of aggregates”, 2005 INTERNATIONAL SYMPOSIUM ON SIGNALS, CIRCUITS AND SYSTEMS, páginas 75-78, IASI, ROMANIA, 14-15 de JULIO de 2005, describe la descomposición de imágenes de ensayo predefinidas usando un análisis independiente de los componentes, y menciona la medición de la independencia real de los componentes como una suma de sus negentropías para evaluar su aleatoriedad.

Por lo tanto, la invención se refiere a un método para extraer una caracterización aleatoria de un elemento material objeto de acuerdo con la reivindicación 7, y un método complementario para generar una base de descomposición de acuerdo con la reivindicación 1.

De acuerdo con la invención, el resultado del método se califica como una caracterización aleatoria puesto que, en primer lugar, tiene todas las características de una caracterización y, en particular, la de unicidad para cada elemento material objeto y, más particularmente, para cada región del elemento material objeto y, en segundo lugar, los componentes constitutivos del vector de caracterización aleatoria son casi independientes y casi equiprobables, incluso independientes y equiprobables.

Por lo tanto, el método de la invención se aparta por sí mismo de otros métodos de generación de caracterización en el sentido de que la caracterización tiene una naturaleza aleatoria pura o casi pura, y se extrae de un elemento material objeto mediante una señal, preferentemente una señal multidimensional bidimensional denominada “señal de imagen” después de la descomposición en una “base”, siendo generada la propia base, posiblemente, a partir del mismo elemento material o de un elemento material diferente.

A diferencia de los métodos de la técnica anterior, el método objeto de la invención transcurre reduciendo la señal de imagen sin que se requiera ninguna operación algorítmica principal después de la extracción.

La generación de la caracterización aleatoria puede hacerse por descomposición, usando una base de descomposición como se ha explicado previamente, o usando cualquier otro método adecuado para el procesamiento de señales, tal como autocorrelación, por ejemplo. A diferencia de la técnica anterior, la caracterización aleatoria de la invención, en particular respecto a la parte estable, no depende de procesamiento o algoritmo usado, sino de la propia estructura del elemento material objeto.

Las realizaciones preferidas se definen en las reivindicaciones dependientes.

Los ejemplos de uso de una caracterización aleatoria o un vector de caracterización aleatoria producido usando el método de extracción de la invención pueden encontrarse en las solicitudes FR 2866139, WO 200578651, WO 2005122100, US 2005262350, FR 2870376.

La presente invención se refiere también a un aparato o dispositivo que comprende medios de adquisición, medios de procesamiento y medios de memoria, estando los medios de procesamiento y memoria al menos adaptados para implementar el método de extracción de caracterización aleatoria y/o el método para generar una base de descomposición de acuerdo con la invención. De acuerdo con la invención, el dispositivo puede comprender adicionalmente medios de comunicación.

La presente invención se refiere también a un programa informático que está adaptado para implementar el método de extracción de caracterización aleatoria y/o el método para generar una base de descomposición de acuerdo con

la invención.

Otras varias características de la invención resultarán evidentes a partir de la descripción dada a continuación, que hace referencia a los dibujos adjuntos que ilustran ejemplos no limitantes para implementar los métodos que son el objeto de esta invención.

La Figura 1 es una vista esquemática de una instalación o dispositivo para implementar los métodos para generar una base de descomposición y para extraer una caracterización aleatoria de un elemento material.
La Figura 2 es una vista esquemática de la superficie de adquisición de un detector matricial y de una abertura de adquisición usada para los métodos de la invención.
La Figura 3 es un diagrama resumen de la realización de un método de generación de una base de descomposición de acuerdo con la invención.
Las Figuras 4 y 5 muestran ejemplos de la trayectoria de exploración que puede usarse para los métodos de generación y extracción de la invención.
Las Figuras 6 a 8 muestran ejemplos de partes de las bases de descomposición generadas usando el método de la invención.
La Figura 9 ilustra la forma de la abertura de adquisición usada para generar la base, tal como se ilustra en la Figura 8.
La Figura 10 ilustra otra forma de la abertura de adquisición que puede usarse en una variante de los métodos para generar una base de descomposición y extraer una caracterización aleatoria de acuerdo con la invención.
La Figura 11 es un diagrama resumen de la realización de un método para extraer una caracterización aleatoria de acuerdo con la invención.
La Figura 12 ilustra una etapa de clasificación y cuantificación usada en el método de extracción de caracterización aleatoria descrito con referencia a la Figura 11.
La Figura 13 da una imagen digital (13A) en transmisión de parte de una hoja de papel, y una vista (13B) que da el resultado del procesamiento estadístico aplicado a la caracterización aleatoria extraída de la hoja de papel usando el método de la invención.
Las Figuras 14 a 17 ilustran ejemplos del uso de parte de los componentes aleatorios estables, que son partes constitutivas de una caracterización aleatoria extraída usando el método de la invención.
Las Figuras 18 a 21 ilustran ejemplos del uso de parte de los componentes aleatorios estables e inestables, que son partes constitutivas de una caracterización aleatoria extraída usando el método de la invención.

Como se ha mencionado anteriormente, la invención se refiere a un método para extraer una caracterización digital aleatoria, casi pura, parcial o completamente estable, a partir de un elemento material objeto **1** que tiene una microestructura estable con el tiempo, parcialmente caótica, revelada por acción física, química, biológica u otra acción estimulante. La invención se refiere también al uso de esta caracterización para producir secuencias aleatorias por ejemplo, o claves privadas, pares de claves privada/pública, identificadores autoprotegidos del elemento objeto **1**.

De acuerdo con la invención, el material constitutivo del elemento material objeto **1**, por ejemplo, puede ser de origen biológico muerto, orgánico o de origen mineral, o el resultado de la mezcla, composición o depósito de materiales de origen biológico muerto, orgánico o mineral. El material constitutivo del elemento material objeto **1** se elige por la naturaleza caótica estable en el tiempo de su microestructura, que pretende revelarse por estimulación física, química o de otro tipo.

Algunos materiales, tales como papel, contienen intrínsecamente una estructura que es al menos parcialmente caótica, que surge de la variabilidad de sus componentes, la variabilidad en su disposición y/o la complejidad del proceso de fabricación. De acuerdo con la realización ilustrada de la invención, el material objeto **1** es una hoja de papel.

La invención pone de manifiesto la extracción o adquisición de al menos parte de las características estructurales del elemento material objeto **1**, que da información sobre la complejidad o estructura caótica de su estructura. Para este fin una o más estimulaciones, preferentemente no destructivas, elegidas de acuerdo con el tipo de elemento material objeto **1**, se aplican a al menos parte del material objeto **1**. La estimulación puede derivar de la acción mecánica, una fuente de rayos de luz u otra fuente física. La respuesta a esta estimulación por el elemento material objeto **1** se registra después mediante un detector apropiado, elegido de acuerdo con el tipo de estimulación hecha y el tipo de elemento material objeto **1**.

Para un material translúcido tal como papel, la estimulación física puede aplicarse mediante una fuente de luz que emite un rayo de luz, coherente o no, polarizada o no, que ilumina un trozo de papel en transmisión o reflexión, correspondiendo la imagen a la respuesta del material a la estimulación de la luz posiblemente adquirida usando una cámara digital.

Por tanto, de acuerdo con el ejemplo ilustrado, el elemento material objeto **1**, que consiste en papel, se ilumina mediante una lámpara **2** que emite luz blanca incoherente. La imagen resultante de la transmisión de luz blanca por la parte **3** del elemento material objeto **1** se adquiere usando un detector matricial **4** integrado en una cámara **5**

unida a una unidad de procesamiento $\mathbf{5_1}$.

La forma de esa parte **3** del elemento material objeto **1**, cuya imagen es adquirida por el detector **4**, está definida por la forma de una abertura de adquisición, cuyos límites o bordes están fijados por la forma del detector, o por la forma de un diafragma, ajustable o no, o por el procesamiento aplicado a la señal derivada del detector **4**, de manera que solo se mantiene una parte de los datos. Por ejemplo, si la superficie del detector **4** es de forma rectangular tal como se ilustra en la figura 2, los límites de la abertura de adquisición, en ausencia de procesamiento y diafragma, corresponden a los límites físicos de la superficie del detector. Sin embargo, de acuerdo con la invención, puede elegirse definir una abertura de adquisición cuyos límites o forma no correspondan a los del detector **4**. Por ejemplo, puede elegirse una abertura de adquisición **6** que solo corresponda a parte del detector y que sea de forma irregular, tal como se ilustra mediante las líneas de puntos en la figura 2. Esta abertura de adquisición **6** puede ser el resultado entonces de la colocación de un diafragma físico, insertado entre el elemento material objeto **1** y el detector **4**, o del procesamiento aplicado a la señal desde el detector **4**.

Evidentemente, la forma de la abertura de adquisición **6** ilustrada en la figura 2 no es limitativa, y puede adaptarse a cualquier otra forma. Por tanto, la abertura de adquisición **6** no es necesariamente unitaria, o de una pieza, sino que puede corresponder a regiones separadas distantes entre sí. Análogamente, la forma de la abertura de adquisición no es necesariamente plana o bidimensional pero también, en relación con el detector y/o estimulación, puede corresponder a un volumen o a un objeto matemático con más de tres dimensiones. La forma de la abertura de adquisición en su significado más amplio, en concreto el aspecto de sus límites o bordes, su posición, su orientación, forma un elemento de datos de entrada o un parámetro para implementación de la invención, tanto respecto al método de generación de una base de descomposición como al método para extraer una caracterización aleatoria.

Según el principio de una realización preferida, el método de extracción de caracterización aleatoria de la invención sirve para descomponer la señal de imagen de la región predefinida **3** del elemento material objeto **1** en una suma de contribuciones de modo elementales, consistiendo cada contribución en un modo al que se asigna un escalar o componente ponderado. En la señal de imagen algunos de estos modos pueden trasladar la presencia de ciertos fenómenos físicos de evolución descritos por las ecuaciones de derivadas parciales, tal como difusión o propagación. Dichos modos, en particular, pueden formar los propios modos particulares de un operador espacial (por ejemplo, laplaciana) y dependen de los límites de las regiones de investigación predefinidas, en concreto la forma de la abertura de adquisición en su significado más amplio.

Todos los modos que pueden usarse para la descripción de la señal de imagen, es decir, su descomposición, denominada base de descomposición, pueden o no estar supercompletados. La base de descomposición puede estar fija o adaptada a la señal de imagen. Las bases adaptadas pueden derivar de un análisis de los búsquedas de proyección, en particular un análisis de componentes que puede estar basado o no en la descomposición de un tipo de descomposición de valor singular, tal como un Análisis del Componente Principal (PCA) o relacionado con PCA, tal como un Análisis del Componente Independiente (ICA) o cualquier otro análisis parecido a PCA o ICA (por ejemplo, PCA con exploración ACP).

El método de extracción de caracterización aleatoria de la invención, por lo tanto, usa una base **B**, opcionalmente supercompletada, que puede estar generada o no, en todo o en parte, a partir de un primer elemento material, sea o no de la misma familia de elementos que el elemento material objeto o del propio elemento material objeto.

En lo que respecta al uso de una base de descomposición particularmente adaptada al método de extracción de caracterización aleatoria de la invención, que es capaz de conseguir una mejor extracción de la caracterización aleatoria deseada, la invención también se refiere a un método para generar una base de descomposición **B** que puede usarse para extraer una caracterización aleatoria a partir de un elemento material objeto.

La Figura **3** muestra las etapas para generar la base de descomposición **B** a partir de un elemento material **E**.

Durante una primera etapa **G1**, N regiones diferentes del elemento material **E** son el objeto de una adquisición (movimiento estático o relativo) y, después, se digitalizan usando un dispositivo **D**, tal como se ilustra en la figura **1**. Durante esta primera etapa **G1** se generan, por tanto, N vectores de adquisición de las características estructurales de N regiones **3** del elemento material objeto **1**, en la que N es **2** o mayor y, preferentemente, mucho mayor de 2.

Si se usa un detector matricial **4**, que comprende un número M de celdas, en cada adquisición la cámara suministra un vector de adquisición que comprende M componentes; cuando la abertura de adquisición **6** tiene una superficie menor que el detector **4**, como se ilustra en la figura 2, la fase de generación **G1** comprende una etapa de reducir el vector de adquisición derivado de la cámara **5**, de manera que solo comprende los m componentes relacionados con la abertura de adquisición **6**, en la que M y m. También, la disposición de los componentes en cada vector de adquisición depende de la dirección de exploración o de la trayectoria de exploración, por ejemplo la exploración horizontal que empieza con la celda izquierda superior, como se ilustra en la figura 4, o la exploración vertical, que empieza con la celda izquierda inferior, como se ilustra en la figura **5**, o cualquier otra forma de la trayectoria de exploración, tal como la curva Peano. De acuerdo con la invención, la configuración de la trayectoria de exploración puede formar un parámetro para la implementación del método para generar la base de descomposición. En tanto

que la caracterización electrónica que se extrae es al menos parcialmente estable o reproducible, se usa preferentemente la misma trayectoria de exploración para el método de generación de la base de descomposición, y en cada implementación del método de extracción.

Las características o configuraciones de la abertura de adquisición, y las características de la trayectoria de exploración definen lo que pueden denominarse parámetros de formación de la estructura de adquisición para la implementación del método de generación de la base de descomposición.

Se pretende adquirir la organización de la microestructura estimulada, los N vectores de adquisición formados de esta manera son, preferentemente, al menos de tipo bidimensional, y se considera que representan una familia de elementos materiales.

Durante la siguiente etapa **G2** se realiza un análisis de todos los vectores de adquisición N usando un método para obtener modos elementales característicos que describen los datos. Cada vector de adquisición puede estar representado entonces por estos modos, haciendo cada modo una contribución más o menos importante. Los modos son vectores que posibilitan la descomposición de cada vector de adquisición en forma de una suma de contribución, consistiendo cada contribución en un vector de descomposición al que se asigna un escalar o componente ponderado. Todos los componentes forman un vector de imagen, que describe el vector de adquisición en consideración. Por lo tanto, los vectores de adquisición forman las columnas de una matriz de datos que puede expresarse como el producto de la matriz de los vectores de la columna de descomposición, denominados también vectores de base o vectores de descomposición, por la matriz de los vectores de la columna de imagen.

Generalmente, los métodos de análisis que constituyen las bases adaptadas a los datos son métodos candidatos capaces de ser usados por la invención. El Análisis de Componente Principal (PCA) y sus variantes forman parte del mismo. El PCA reducido centrado, por descomposición de la matriz de los vectores de adquisición reducidos centrados en valores singulares, suministra la matriz ortogonal de los vectores de base o los vectores de descomposición. Los vectores de imagen se deducen a partir de los mismos por proyección simple de los vectores de adquisición sobre esta base. Los componentes del vector de imagen tienen después la propiedad de estar centrados y descorrelacionados.

Puede usarse el Análisis del Componente Independiente (ICA), que proporciona el mismo tipo de análisis que PCA, (en que los componentes del vector de imagen obtenidos tienen la propiedad de estar centrados, descorrelacionados e incluso ser casi independientes. Los vectores de descomposición y los vectores de imagen se obtienen simultáneamente, por ejemplo maximizando la no-gaussianidad de los componentes del vector de imagen. Diferentes algoritmos satisfacen estos criterios dependiendo de la implantación (FastICA, JADE, InfoMax,...).

Todos los vectores de descomposición forman después una base de descomposición **B** que puede usarse para el método de la invención de extracción de una caracterización aleatoria a partir de un elemento material objeto. Para este fin, la base de descomposición **B** puede almacenarse o guardarse, de manera que puede usarse según se necesite, cuando se implementa el método de extracción de caracterización aleatoria de la invención, entendiendo que este método puede proporcionar también la generación de una base de descomposición **B** como se ha explicado previamente en cada extracción de una caracterización aleatoria.

Cuando se genera la base de descomposición, puede considerarse también que transcurre con un análisis de al menos parte de los vectores de imagen para identificar que este o aquel componente es altamente determinante y/o común para la mayoría e incluso todos los vectores de imagen, correspondiendo a los vectores de descomposición en la base de descomposición, denominados vectores de descomposición comunes o de cierta contribución, siendo considerados los otros componentes del vector de imagen componentes aleatorios. Al final de este análisis se guarda una lectura enmascarada que, en cada vector de imagen, da la posición de cualquier componente determinista y/o la posición de cualquier componente aleatorio, o se guarda una base de descomposición cuyos vectores de descomposición deterministas se han suprimido.

La Figura 6 ilustra un ejemplo de generación de base de descomposición preparado usando imágenes de un trozo de papel iluminado por transmisión, en luz incoherente, con una abertura de adquisición de forma cuadrada, y una trayectoria de exploración de tipo de exploración horizontal, tal como se ilustra en la figura 4. La generación de la base también se ha realización usando el Análisis del Componente Principal (PCA). La parte 6A en la figura 6 es un gráfico que muestra el espectro PCA (todos valores propios), mientras que la parte 6B muestra 25 elementos de base que pertenecen al segundo tercio del espectro.

Análogamente, la figura 7 ilustra un ejemplo de la generación de la base de descomposición, preparado usando imágenes de un trozo de papel iluminado por transmisión, en luz incoherente, con una abertura de adquisición de forma cuadrada y una trayectoria de exploración de tipo de exploración vertical, tal como se ilustra en la figura 5. La generación de la base se ha realizado también por el Análisis del Componente Principal (PCA). La parte 7A en la figura 7 es un gráfico que muestra el espectro PCA, mientras que la parte 7B muestra 25 elementos de base que pertenecen al segundo tercio del espectro.

La figura 8 ilustra otro ejemplo de la generación de una base preparada usando imágenes de un trozo de papel iluminado por transmisión, en luz incoherente, con una abertura de adquisición de forma no cuadrada, ilustrada en la figura 9, y una trayectoria de exploración de tipo de exploración horizontal, tal como la ilustrada en la figura 4. La generación de la base se ha realizado también usando el Análisis del Componente Principal (PCA). La parte 8A en la figura 8 es un gráfico que muestra el espectro PCA, mientras que la parte 8B muestra 25 elementos de base que pertenecen al segundo tercio del espectro.

De acuerdo con una variante de implementación del método de generación de la base de descomposición, la abertura de adquisición **6a** usada consiste en un número i de aberturas elementales $\mathbf{6_1}$ idénticas y no unidas juntas, como se muestra en la figura 10. De acuerdo con el ejemplo ilustrado, la abertura 6a comprende 12 aberturas elementales $\mathbf{6_1}$ de forma rectangular (i = 12). La generación de la base de descomposición usa después una fase para generar una base de descomposición elemental, cuyos vectores de descomposición elemental se generan usando el método descrito anteriormente aplicado a las aberturas elementales $\mathbf{6_1}$ tomadas individualmente, una adquisición de la abertura **6a** que se trata después como i adquisiciones de una abertura de adquisición, que es idéntica a una abertura elemental $\mathbf{6_1}$. Durante la fase de generación de la base de descomposición elemental, las aberturas elementales $\mathbf{6_1}$ y sus adquisiciones se consideran, por lo tanto, independientes entre sí, de manera que la base de descomposición elemental generada permite la descomposición de cada adquisición elemental correspondiente a una abertura de adquisición elemental $\mathbf{6_1}$ en un vector de imagen elemental con componentes aleatorios, cuyos componentes corresponden a las contribuciones respectivas de los vectores de descomposición elementales. Para obtener una base de descomposición que puede usarse para la abertura de adquisición $\mathbf{6_1}$ tomada en su conjunto, la generación de la base de descomposición usa después una etapa para crear la base de descomposición a partir de la base de descomposición elemental, formando cada vector de descomposición por concatenación de i veces un mismo vector de descomposición elemental. Por lo tanto, la base de descomposición comprende el mismo número de vectores que la base de descomposición elemental, y si cada vector de descomposición elemental comprende j componentes, entonces cada vector de descomposición comprenderá i x j componentes.

Una base de descomposición generada de acuerdo con una cualquiera de las variantes anteriores del método de generación de la invención puede usarse entonces con un método de extracción de caracterización aleatoria de acuerdo con la invención.

En una realización preferida, el método para extraer una caracterización aleatoria a partir de un elemento material objeto **1**, como se observa en la figura 11, comprende las siguientes fases.

En primer lugar, si la base de descomposición **B** no se genera cuando se extrae la caracterización aleatoria, se elige una base de descomposición pre-registrada **B** que se usará para la extracción. Opcionalmente, la base de descomposición **B** está asociada con las características de una abertura de adquisición **6** y de una trayectoria de exploración que puede usarse para extraer la caracterización aleatoria.

Después, se realiza una fase de generación **I** para generar al menos uno y, preferentemente, n vectores de adquisición de las características estructurales de la región **3** del elemento material objeto **1**, en el que n es 2 o mayor y, preferentemente, mucho mayor de 2. La generación de los vectores de adquisición puede hacerse usando una abertura de adquisición **6** o **6a**, tal como se ha definido previamente. Cuando se desea extraer una caracterización aleatoria o reproducible a partir de un elemento material objeto 1, se usa la misma abertura de adquisición, o los mismos parámetros de la abertura de adquisición, para cada implementación del método de la invención, siendo preferentemente estos parámetros aquellos de la abertura de adquisición opcionalmente asociados con la base de descomposición **B**.

Cunado se usa un detector matricial **4** que comprende un número M de celdas, la cámara suministra un vector de adquisición que comprende M componentes; si la abertura de adquisición **6** tiene una menor superficie que el detector **4**, como se ilustra en la figura 2, la fase de generación **I** comprende una etapa para reducir el vector de adquisición derivado de la cámara **5**, de manera que solo contiene los m componentes relacionados con la abertura de adquisición **6**, en la que $M \geq m$.

También, la disposición de los componentes en cada vector de adquisición depende de la dirección de exploración o de la trayectoria de exploración, por ejemplo, la exploración horizontal que empieza con la celda izquierda superior, como se ilustra en la figura 4, o la exploración vertical que empieza con la celda izquierda inferior, como se ilustra en la figura 5, o cualquier otra forma de la trayectoria de exploración. De acuerdo con la invención, la configuración de la trayectoria de exploración puede formar un parámetro para la implementación del método de extracción. En tanto que se extrae una caracterización aleatoria, que es al menos parcialmente estable o reproducible, se usará la misma trayectoria de exploración para cada implementación del método, y si la base de descomposición está asociada con una trayectoria de exploración, es esta última trayectoria la que se usa preferentemente.

Las características o configuraciones de la abertura de adquisición, y las características de la trayectoria de exploración definen lo que puede denominarse la estructura de adquisición.

La fase **I**, por lo tanto, supone la generación de n vectores de adquisición. Estos n vectores de adquisición corresponden entonces a cualquiera de las n adquisiciones reales separadas, o a una adquisición real a partir de la cual se generan los n vectores de adquisición. Si la abertura de adquisición **6** tiene una superficie menor que el detector **4**, es posible generar un vector de adquisición correspondiente a la adquisición real, y n-1 vectores de adquisición generados por simulación de micro-desplazamientos de la abertura de adquisición **6** respecto al detector **4**, correspondiendo estos micro-desplazamientos a errores de posición del elemento material objeto 1 durante su colocación sucesiva n-1 veces en el dispositivo de digitalización **D** que, de acuerdo con el ejemplo ilustrado, comprende la fuente de luz **2** y la cámara **5**.

Este conjunto de vectores de adquisición, en promedio, puede usarse para reducir el ruido de adquisición con vectores de adquisición real resultantes del ruido de la cámara **5** y la fuente de radiación **2** y, en el caso de vectores de adquisición calculados o sintetizados, el ruido que puede estar provocado por la recolocación del elemento material objeto **1**.

Después de la fase **I** hay n vectores de adquisición de columna, cada uno de los cuales comprende m componentes que, por lo tanto, comprenden una matriz con m filas y n columnas.

Se realiza entonces una fase **II** para descomponer cada vector de adquisición, de acuerdo con una base de descomposición **B**, que contiene vectores de descomposición en componentes aleatorios para obtener n vectores de imagen, cada uno de los cuales comprende un número m' de componentes, en el que $m \geq m'$.

La base de descomposición usada puede ser, por ejemplo, una base pre-existente creada opcionalmente a partir de los elementos materiales del mismo tipo que el elemento material objeto, o una base creada a partir del elemento material objeto analizando varias regiones de este último, como se ha descrito anteriormente.

Al completarse la fase **II**, por lo tanto, hay una matriz de imágenes que comprende m' filas y n columnas. Esta matriz de imágenes se usa en la siguiente fase **III** para general al menos un vector de caracterización aleatoria, comprendiendo la fase **III** de acuerdo con el ejemplo ilustrado tres etapas **IIIa, IIIb** y **IIIc.**

La primera etapa **IIIa** de la fase **III** es una etapa para reducir la matriz de imágenes retirando los componentes de la imagen superactivos - denominados componentes inválidos - y que, por lo tanto, no se adaptan a la búsqueda de un componente puramente aleatorio para el vector de caracterización. La actividad de un componente de una fila dada puede medirse analizando una fila de la matriz de imágenes. La medición puede ser estadística después de estimar el histograma de la fila previa. Puede definirse también como la energía de una fila. La decisión de retirar un componente inválido puede tomarse con respecto a los otros componentes después de evaluar cada uno de los componentes. Se obtiene entonces una matriz de imágenes reducida, que comprende n vectores de imagen reducida que tienen cada uno m'' componentes en la que $m' \geq m''$.

La etapa **IIIb** clasifica los componentes de los vectores de imagen de la matriz de imágenes reducida, conduciendo a la calificación de su naturaleza como estable o inestable. Para este fin, y como se ilustra esquemáticamente en la figura 12, el eje de valores **x-x'** asociado con cada uno de estos componentes está dividido en diferentes clases estadísticas predefinidas **c**, que se usarán para la cuantificación en niveles (discretos) durante la etapa posterior **IIIc**. Si un componente dado correspondiente a una fila de la matriz se considera que pertenece a una de estas clases - denominadas clases de cuantificación - entonces se declara estable. La inclusión en dicha clase puede determinarse después del análisis estadístico de la fila correspondiente al componente. Este análisis puede transcurrir con estimación del histograma de la fila, seguido de una estimación de sus valores medios y la desviación típica. La inclusión en la clase que se está considerando puede considerarse cierta cuando el histograma **s** está casi completamente contenido en la clase que se está considerando (por ejemplo, el intervalo centrado medio de igual anchura a un cierto número de veces la desviación típica, está totalmente contenido en la clase). Si el histograma i está "equi-distribuido" entre dos clases, el componente se considera inestable y localizado en otra clase denominada la clase inestable. Finalmente, si el histograma ∅ está distribuido sobre varias clases o sobre dos clases de forma disimétrica, el componente generalmente no se considera apto, y está localizado como una clase denominada no apta.

Después de la etapa **IIIc** se realiza la cuantificación (o asignación de niveles discretos entre un grupo finito de números) de los componentes estables o inestables (válidos). Durante esta etapa, los componentes no aptos (es decir, que pertenecen a la clase no apta) no se procesan (considerados como términos ausentes o "huecos" en la matriz de imágenes) y no dan lugar a ningún componente en el vector de caracterización, que contendrá entonces m''' componentes, en la que $m'' \geq m'''$.

A los componentes estables se les dan el nivel de cuantificación correspondiente a su clase (estable). Por ejemplo, cuando los vectores de adquisición son reducidos centrados, una cuantificación de dos niveles, o binarización, puede realizarse asignando el nivel 1 a un componentes positivo, y el nivel 0 a un componente negativo.

Los componentes inestables tienen un valor que puede ser cualquier valor, en cuyo caso, al componente correspondiente del vector de caracterización se le dará el valor de la clase correspondiente al valor del componente

para un vector de imagen predefinido. Por ejemplo, cuando los vectores de adquisición son reducidos centrados y se realiza la cuantificación sobre dos niveles, o binarización, a un componente inestable se le asigna un nivel binario, 0 (por ejemplo) si el valor del componente en un vector de imagen predefinido (por ejemplo, el primero) es negativo, 1 si es positivo.

Una máscara de lectura, que identifica o separa los componentes estables de los componentes inestables en el vector de caracterización, puede generarse entonces durante la etapa **IIIc**.

Por lo tanto, de acuerdo con el ejemplo ilustrado, al completarse la fase **III** de generación de un vector de caracterización aleatoria, se obtiene una máscara de lectura **M** y un vector de caracterización aleatoria **V**. En el presente caso, la máscara de lectura **M** es un vector que comprende el mismo número m''' de componentes que el vector de caracterización aleatoria **V**. Un componente de la máscara de lectura tiene un valor 0, por ejemplo, cuando el componente correspondiente del vector de caracterización aleatoria V es inestable, y un valor de 1 cuando el componente correspondiente del vector de caracterización aleatoria V es estable.

Cada componente del vector de caracterización aleatoria V procede de un componente aleatorio de un vector de imagen considerado válido después de la etapa IIIa, y estable o inestable después de la etapa IIIb.

Las partes C en las figuras 6 a 8 muestran cada una un extracto de una secuencia binaria que pertenece a una caracterización aleatoria obtenida con el método de extracción de la invención usando la base de descomposición que se descompone en los componentes aleatorios, de los cuales parte de los elementos o vectores se muestra en la parte B de la figura correspondiente.

A modo de ejemplo, el método de extracción de caracterización aleatoria se aplicó a un trozo de papel iluminado por transmisión, en luz incoherente, usando una base de descomposición generada a partir de otro trozo de papel. Los ensayos estadísticos se realizaron sobre los componentes del vector de caracterización aleatoria **V**, que comprende una secuencia de 66048 bits extraída de imágenes del papel con una resolución de 3200 dpi, para determinar la calidad de la caracterización extraída usando el método de la invención. Los resultados fueron los siguientes:

Entropía = 1,000000
Proporción de compresión óptima = 0
Distribución Chi^2 = 0,79
Valor media aritmética = 0,5001
Error en el valor de Monte-Carlo para Pi = 0,05
Coeficiente de correlación en serie = - 0,000385

Puesto que el método de la invención genera una caracterización que es una imagen de la estructura del material del elemento material objeto, estos resultados asociados aquí con el conocimiento de la naturaleza caótica del papel, trasladan la pureza o naturaleza aleatoria del vector de caracterización aleatoria V generado por el método de la invención.

Análogamente, la naturaleza fuertemente aleatoria del vector de caracterización aleatoria **V** se muestra indirectamente en la figura 13, con la búsqueda aleatoria para números primos en una caracterización aleatoria de 9.200.000 bits, extraída usando el método de la invención a partir de un trozo de papel de formato A4 y realizando una sucesión de 20 ensayos probabilísticos primarios denominados ensayos de Miller-Rabin.

La parte 13A en la figura 13 corresponde a una imagen de un área cuadrada, con lados de 2 cm, de una hoja de papel convencional iluminada por transmisión con luz incoherente. La parte 13B en la figura 13 corresponde a la representación con puntos blancos de los 100 números primos extraídos de una caracterización aleatoria entre los 125 x (86-1) números primo de 18 bits representados en forma de una imagen negra de 125 x 86 pixeles. La observación de la parte 13Bb en la figura 13 muestra la uniformidad de la distribución de los números encontrada en todos los números primos, aquí de 18 bits, una uniformidad que resulta de la naturaleza aleatoria de la caracterización extraída usando el método de la invención.

También, debe observarse que cuando se implementa el método de extracción de la invención, el valor de la parte estable de la caracterización aleatoria extraída puede estar influido por los siguientes factores:

- el elemento material objeto y, en particular, la región del elemento material objeto a partir de la cual se extrae la caracterización aleatoria,
- la forma de la abertura de adquisición y, en particular, su posición y orientación,
- la forma de la trayectoria de exploración,
- y la base de descomposición usada, en particular el elemento material (o elementos materiales) que pueden haberse usado para generar la base de descomposición, si son diferentes del elemento material objeto.

Por lo tanto, los factores pueden formar muchos parámetros para la implementación del método de extracción de caracterización aleatoria de la invención.

Por lo tanto, aunque se trata convencionalmente como ruido, la parte de la señal de imagen correspondiente al contenido caótico del elemento material objeto de acuerdo con la invención, se usa de tal manera que se extrae una caracterización aleatoria, es decir, impredecible *a priori*. Por lo tanto, los componentes del vector de caracterización aleatoria **V** son impredecibles, tanto en su conjunto pero también entre sí. También se indica que la caracterización aleatoria de la invención encuentra su origen en la estructura del material del elemento material objeto, y no en los algoritmos u operaciones de procesamiento usadas, lo que significa que la invención extrae la caracterización con un número mínimo de operaciones de procesamiento, para preservar las características estructurales intrínsecas del elemento material objeto. Además, la caracterización de la invención tiene una naturaleza digital, es decir, consiste en componentes con valores cuantificados en números finitos o "niveles". Por lo tanto, todos los componentes de la caracterización forman una secuencia aleatoria, casi pura, de niveles que pueden usarse como tales o para generar un germen aleatorio en cualquier área donde sea necesario para la caracterización, certificación, trazabilidad, criptografía, en particular para autentificación, la generación de claves privadas y/o claves públicas, el aseguramiento de datos, compartición de secretos, para esteganografía, aunque también para cálculo, o en robótica, para simular u ordenar acontecimientos aleatorios (juegos informáticos, programación, …).

Como se ha descrito anteriormente, el método objeto de la invención califica cada componente de la caracterización aleatoria como estable o inestable. Un componente de la caracterización se declara estable cuando su nivel puede reaparecer con una identidad estricta o casi estricta, y muy alta probabilidad, después de cualquier nueva estimulación del elemento material en condiciones idénticas o similares. Puede usarse entonces un detector de error/código corrector para aumentar la estabilidad de los componentes, en particular el aseguramiento de los datos o el acceso.

Una caracterización aleatoria extraída usando el método de la invención puede usarse de diferentes maneras.

Entre los componentes estables que pueden extraerse a partir de los mismos, el elemento material puede usarse como una clave física del dueño. Los componentes aleatorios estables pueden usarse también para producir una Libreta de Un Solo Uso, o para generar un identificador particular del elemento material.

La figura 14 ilustra un uso de los componentes estables **Vs** de una caracterización aleatoria generada a partir del elemento material objeto **1** usando el método de extracción **P** de la invención para asegurar la protección de las variables o parámetros **10** esenciales de un programa informático **11**. Para dicho uso, la caracterización aleatoria estable **Vs** se usa como clave de un solo uso en un proceso de codificación **12**, por ejemplo de tipo XOR, para obtener las variables esenciales aseguradas **13**. Por lo tanto, es posible proteger estas variables esenciales con el aleatorio estable derivado del elemento material **1** y someter la ejecución apropiada del programa a la presencia del elemento material auténtico en un sistema de adquisición, no mostrado, relacionado con un ordenador, tampoco mostrado, que ejecuta el programa informático **11** usando las variables esenciales. El elemento material objeto **1** es necesario entonces para descodificar las variables esenciales aseguradas **13** y volver a las variables esenciales **10** usadas por el programa informático **11**.

La figura 15 muestra un uso de los componentes estables **Vs** de una caracterización aleatoria generada a partir de un elemento material objeto **1** usando el método de extracción **P** de la invención para controlar el acceso a los locales, máquinas, actividades o incluso información. De acuerdo con este ejemplo de uso, la caracterización aleatoria estable **Vs** se usa como identificador y se compara mediante un proceso de comparación estadística **14** con el contenido de una base de datos **Bd** de identificadores auténticos para autorizar el acceso **15** si el resultado de la comparación es positivo.

La figura 16 ilustra un uso adicional de los componentes estables **Vs** de una caracterización aleatoria, generada a partir de un elemento material objeto **1** usando el método de extracción **P** de la invención para ordenar a un controlador lógico programable **16**. De acuerdo con este ejemplo de uso, el controlador lógico **16** actúa en relación a instrucciones aleatorias **17** derivadas de la caracterización aleatoria estable **Vs**. Las acciones realizadas por el controlador lógico **16** pueden ser de diversas clases, tales como aquellas correspondientes a mecanizado, trenzado, desplazamiento, apertura o cierre, dosificación de elementos o la manipulación de otros controladores lógicos o máquinas, sin que esta lista se considere exhaustiva.

Podría considerarse también asociar la caracterización aleatoria estable **Vs** con acciones predefinidas a través de una base de datos de correspondencia, relacionando valores de componentes aleatorios estables a una o más secuencias de instrucciones.

Siguiendo el mismo principio, podría considerarse controlar el funcionamiento de un programa informático usando una caracterización aleatoria estable **Vs**. En este caso, una parte de los componentes de la caracterización aleatoria estable corresponde directamente a los parámetros del programa informático, o se usa una base de correspondencia entre los componentes aleatorios estables y los parámetros predefinidos para el programa informático.

La figura 17 ilustra un uso de los componentes estables **Vs** de una caracterización aleatoria generada a partir de un elemento material objeto **1** usando el método de extracción **P** de la invención para asegurar la protección de datos

tal como los datos de trazabilidad **17**, por ejemplo, destinados a estar asociados con un producto. Para este tipo de uso, la caracterización aleatoria estable **Vs** se usa como clave de un solo uso en un proceso de codificación **18**, de tipo XOR por ejemplo, para obtener a partir de los datos de trazabilidad **17** datos de trazabilidad asegurados **19**, que pueden estar impresos en el producto. Para dicho uso, el elemento material objeto **1** en el origen de la caracterización aleatoria estable **Vs** puede unirse al producto que lleva la información asegurada, en cuyo caso el aseguramiento radicará en el dispositivo de adquisición, que sirve para asegurar la descodificación de los datos asegurados **19**. Este aseguramiento estará relacionado, en particular, con la base de descomposición usada, la forma de la abertura de adquisición o la trayectoria de exploración, que puede mantenerse secreta, y ser conocida solo por el fabricante del dispositivo de adquisición. O por el contrario, puede contemplarse que el elemento material objeto en el origen de la caracterización aleatoria estable **Vs** sea independiente del producto, y se mantenga, por ejemplo, por el usuario a cargo de verificar la autenticidad del producto que lleva los datos asegurados **19**.

Como se ha mencionado anteriormente, una caracterización aleatoria **V** generada usando el método de extracción de la invención, puede comprender componentes inestables, o puede incluso consistir únicamente en componentes inestables, en cuyo caso puede considerarse usar el método de extracción de la invención como generador de números aleatorios.

Los componentes inestables de la caracterización aleatoria pueden usarse para generar uno o más identificadores y/o una o más claves privadas, cada una protegida por componentes aleatorios estables, por ejemplo a través de una o más libretas de un solo uso.

En lo que respecta a la caracterización aleatoria de la invención, puede comprender tanto componentes estables como componentes inestables, pudiéndose aprovechar esta característica para diversas aplicaciones, de las cuales a continuación se dan algunos ejemplos no exhaustivos.

La figura 18 ilustra un ejemplo de uso de una caracterización aleatoria **V**, que comprende componentes estables **Vs** y componentes inestables **Vi**, generados por el método de extracción y, de acuerdo con la invención, a partir de un elemento material objeto **1** para proporcionar un identificador asegurado **20**. Con este tipo de uso, la parte inestable **Vi** de una caracterización aleatoria **V** se usa como identificador, mientras que la parte estable **Vs** se usa como clave de un solo uso en un proceso de codificación **21**, por ejemplo de tipo XOR, para obtener el identificador asegurado **20**. El mantenimiento del elemento material objeto **1** y de un dispositivo para implementar el método de extracción de la invención, hace posible re-acceder a la parte estable **Vs** de la caracterización aleatoria **V** y, por tanto, descodificar el identificador asegurado **20** para acceder al identificador inicial, en este caso una parte inestable **Vi** de una caracterización aleatoria **V**, generada en el momento de la asignación del identificador.

La figura 19 ilustra otro ejemplo de uso de una caracterización aleatoria **V**, que comprende componentes estables **Vs** y componentes inestables **Vi** generados por el método de extracción P de la invención, a partir de un elemento material objeto **1** para proporcionar claves públicas y privadas, incluso pares de claves en un protocolo criptográfico asimétrico. Para este tipo de uso, el método de extracción **P** se implementa una primera vez para generar una caracterización aleatoria **V** de la cual, la parte **Vi1** de los componentes inestables se usa como clave privada **25**, mientras que otra parte **Vi2** de los componentes inestables se usa como clave pública **26**. Parte de los componentes estables **Vs** se usan después como clave de un solo uso en un proceso de codificación **27**, por ejemplo de tipo XOR, para obtener a partir de la clave privada **25** una clave privada asegurada **28**. El mantenimiento del elemento material objeto **1** y el dispositivo que implementa el método de extracción de la invención hace posible entonces reacceder a la parte estable **Vs** de la caracterización aleatoria **V** y, por tanto, descodificar la clave privada asegurada **28** para acceder a la clave privada **25** generada durante el primer uso del método de la invención **P** para extraer una caracterización aleatoria.

La figura 20 ilustra otro ejemplo de uso de una caracterización aleatoria **V**, que comprende componentes estables **Vs** y componentes inestables **Vi**, generados por el método de extracción **P** de la invención a partir de un elemento material objeto **1** para proporcionar, en primer lugar, un identificador y, en segundo lugar, una libreta de un solo uso, y también claves públicas y privadas de un protocolo criptográfico asimétrico. Para este tipo de uso, el método de extracción **P** se usa una primera vez para generar una caracterización aleatoria **V**, de la cual una parte **Vi1** de los componentes inestables se usa como identificador, una segunda parte **Vi2** de los componentes inestables se usa como clave privada **31**, mientras que una tercera parte **Vi3** de los componentes inestables se usa como clave pública **32**. La clave privada **31** se usa después en un proceso de cifrado **33** para obtener, a partir del identificador **30**, un identificador caracterizado o cifrado **34**. Una parte de los componentes estables **Vs** se usa después como una clave de un solo uso en el proceso de codificación **35**, por ejemplo de tipo XOR, para obtener a partir del identificador caracterizado **34** un identificador caracterizado asegurado **36**. El mantenimiento del elemento material objeto **1** y un dispositivo que implementa el método de extracción **P** de la invención hace posible entonces reacceder a la parte estable **Vs** de la caracterización aleatoria **V** y, de esta manera, descodificar el identificador de caracterización asegurado **36** para acceder al identificador caracterizado **34** generado durante el primer uso del método de la invención **P** para extraer una caracterización aleatoria.

La figura 21 ilustra un uso del método de extracción de la invención bajo el protocolo para codificación RSA, con clave pública y clave privada. La caracterización aleatoria extraída de un elemento material objeto se usa después

para generar los números primos fuertes **p** y **q**. El número n es el producto pq. El número **e** es un entero elegido para que sea primo con (φ(n), mientras **d** se elige de manera que ed $\equiv$ 1 (modφ(n)). La clave privada **Cs** consiste entonces en los enteros p, q y d, mientras que la clave pública consiste en los enteros n y e. Si el número con referencia **40** es un identificador a codificar, entonces el número con referencia **41** es el identificador codificado mediante el protocolo RSA usando las claves públicas **Cp** y privada **Cs** anteriores.

Evidentemente, el método para extraer una caracterización aleatoria de acuerdo con la invención puede comprender diferentes fases que usan, al menos, parte de los componentes estables e inestables en diversos procesos para generar al menos un código único y para cifrar este código.

También, los métodos de la invención pueden usarse en muchas otras aplicaciones sin alejarse del alcance de la presente invención.

REIVINDICACIONES

1. Método para generar una base de descomposición para extraer una caracterización aleatoria a partir de un elemento material objeto, que comprende las siguientes etapas:

- definir una abertura de adquisición y una trayectoria de exploración,
- generar un número N de adquisiciones, de acuerdo con la abertura de adquisición, de características estructurales de al menos una región del propio elemento material objeto, o de un elemento material diferente,
- digitalizar, a lo largo de la trayectoria de exploración, cada una de las adquisiciones en forma de un vector de adquisición,
- analizar todos los vectores de adquisición usando métodos estadísticos para obtener una base de descomposición formada por vectores de descomposición, que posibilita la representación de cada vector de adquisición en forma de un vector de imágenes formado por componentes y que corresponde a la contribución de un vector de descomposición en el vector de adquisición,
- analizar al menos parte de los vectores de imagen para identificar componentes deterministas comunes a todos los vectores de imagen, siendo los otros componentes componentes aleatorios, y que comprende una o más de las siguientes etapas:

    - grabar una máscara de lectura que, en cada vector de imagen generado con la base de descomposición, da la posición de cualquier componente determinista y/o la posición de cualquier componente aleatorio, o retirar los componentes deterministas de la base de descomposición borrando los vectores de descomposición deterministas y grabando una base de descomposición reducida.

2. Método para generar una base de descomposición de acuerdo con la reivindicación 1, **caracterizado porque** comprende adicionalmente la etapa de grabar la base de descomposición.

3. Método para generar una base de descomposición de acuerdo con cualquiera de las reivindicaciones 1 o 2 **caracterizado porque** cada vector de adquisición es de una naturaleza al menos bidimensional.

4. Método para generar una base de descomposición de acuerdo con cualquiera de las reivindicaciones 1 a 3, **caracterizado porque** usa un análisis de proyección que persigue obtener la base de descomposición, tal como un análisis de componente como un algoritmo del Análisis del Componente Principal de un algoritmo del Análisis del Componente Independiente.

5. Método para generar una base de descomposición de acuerdo con cualquiera de las reivindicaciones 1 a 4, **caracterizado porque** la identificación de los componentes deterministas de los vectores de imagen se consigue mediante un algoritmo de descomposición espectral e identificación de cierta contribución de los vectores de descomposición por filtración.

6. Método para generar una base de descomposición de acuerdo con cualquiera de las reivindicaciones 1 a 5, **caracterizado porque** cada elemento material usado para la generación de los vectores de adquisición se elige entre: materiales de origen biológico muerto, materiales de origen orgánico, materiales de origen mineral o materiales obtenidos por mezcla y/o composición y/o depósito de varios de los materiales anteriores.

7. Método para extraer una caracterización aleatoria a partir de un elemento material objeto, que comprende:

- una fase para generar n vectores de adquisición, siendo n igual a o mayor de 2, a partir de al menos una adquisición real de las características estructurales de al menos una región del elemento material objeto,
- una fase de descomposición de cada vector de adquisición de acuerdo con una base de descomposición formada por vectores de descomposición que posibilitan la representación de cada vector de adquisición en forma de un vector de imagen, que contiene componentes aleatorios, y que corresponde a la contribución de un vector de descomposición en el vector de adquisición,
- una fase para generar al menos un vector de caracterización aleatoria a partir del vector de adquisición, usándose un número de clases estadísticas para calificar la naturaleza de los componentes de los vectores de imagen después del análisis estadístico de las filas de los vectores de imagen, que define una matriz de imágenes, que comprende la estimación del histograma de cada fila, seguido de una estimación de su valor medio y la desviación típica, siendo dicha naturaleza:
- estable si el histograma es una fila que está totalmente contenida en una de las clases estadísticas c,
- inestable si el histograma de una fila está distribuido equitativamente entre dos clases estadísticas c,
- no apto si el histograma de una fila está distribuido sobre varias clases estadísticas o disimétricamente sobre dos clases,
- el vector de caracterización aleatoria comprende:

    - al menos un componente aleatorio que tiene una naturaleza estable,
    - y/o al menos un componente aleatorio que tiene una naturaleza inestable,

- obteniéndose cada componente del vector de caracterización aleatoria por extracción y/o procesamiento de al menos un componente aleatorio de al menos un vector de imagen, y
- usando el vector de caracterización aleatoria como caracterización aleatoria.

8. Método para extraer una caracterización aleatoria de acuerdo con la reivindicación 7, **caracterizado porque** el al menos un vector de caracterización aleatoria contiene el mismo número de componentes, o menos, que el número de componentes aleatorios de cada vector de imagen.

9. Método para extraer una caracterización aleatoria de acuerdo con la reivindicación 7 u 8, **caracterizado porque** durante la fase para generar un vector de caracterización aleatoria, la cuantificación se realiza de manera que cada componente aleatorio del vector de caracterización aleatoria es capaz de presentar un número finito de valores o niveles.

10. Método para extraer una caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 7 a 9, **caracterizado porque** durante la fase de generar al menos un vector de adquisición, los n vectores de adquisición se generan de una misma región del elemento material objeto, y **porque** se usan n vectores de imagen, cada uno de los cuales corresponde a un vector de adquisición.

11. Método para extraer una caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 9 o 10, **caracterizado porque** durante la fase de generar al menos un vector de caracterización aleatoria, el valor o nivel de cada componente del vector de caracterización aleatoria está definido por el resultado de los ensayos y/o procesos estadísticos aplicados a todos los valores del componente en una fila dada de los n vectores de imagen.

12. Método para extraer una caracterización aleatoria de acuerdo con la reivindicación 11, **caracterizado porque** durante la fase de generar al menos un vector de caracterización aleatoria, los componentes de los vectores de imagen experimentan un procesamiento estadístico que consiste en su reducción centrada.

13. Método para extraer una caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 7 a 12, **caracterizado porque** los n vectores de adquisición se generan prácticamente a partir de un número de adquisiciones reales menor de n.

14. Método para extraer una caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 7 a 13, **caracterizado porque** comprende una fase para generar una base de descomposición de acuerdo con el método definido por cualquiera de las reivindicaciones 1 a 6.

15. Método para extraer una caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 7 a 14, **caracterizado porque** el vector de caracterización aleatoria comprende al menos un componente aleatorio que tiene una naturaleza estable, pudiendo encontrarse el valor de este componente aleatorio estable en cada implementación del método en una misma región del elemento material objeto.

16. Método para extraer una caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 7 a 15, **caracterizado porque** el vector de caracterización aleatoria comprende al menos un componente aleatorio de naturaleza inestable, siendo probable que el valor de este componente aleatorio inestable varíe en cada implementación del método en la misma región del elemento material objeto.

17. Método para extraer una caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 7 a 16, **caracterizado porque** durante la fase de generación de al menos un vector de caracterización aleatoria, se genera lo siguiente:

- un vector de caracterización aleatoria estable, cuyos componentes aleatorios tienen una naturaleza estable, pudiendo encontrarse el valor de cada componente aleatorio estable en cada implementación del método en la misma región del elemento material objeto,
- un vector de caracterización aleatoria inestable, cuyos componentes aleatorios tienen una naturaleza inestable, siendo probable que el valor de cada componente aleatorio inestable varíe en cada implementación del método en una misma región del elemento material objeto.

18. Método para extraer una caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 16 y 17, **caracterizado porque** durante la fase de generación de al menos un vector de caracterización aleatoria se genera una máscara de lectura que da la posición en el vector de caracterización aleatoria de los componentes aleatorios estables y/o los componentes aleatorios inestables.

19. Método para extraer una caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 7 a 18, **caracterizado porque** la fase para generar al menos un vector de adquisición comprende las siguientes etapas:

- generar al menos una adquisición, de acuerdo con una abertura de adquisición, de las características estructurales de una región del elemento material objeto,

- digitalizar, a lo largo de una trayectoria de exploración, cada adquisición en un vector de adquisición.

20. Método para extraer una caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 7, 16 o 17, **caracterizado porque** comprende una fase que usa al menos parte de los componentes inestables como identificador del elemento material objeto, o de un objeto asociado con el elemento material objeto, y una fase que usa al menos parte de los componentes aleatorios estables como una libreta de un solo uso, para codificar el identificador para obtener un identificador asegurado.

21. Método para extraer una caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 7, 16 o 17, **caracterizado porque** comprende:

- una fase que usa al menos parte de los componentes aleatorios inestables como clave privada en un proceso criptográfico con clave pública/clave privada,
- una fase que usa al menos parte de los componentes aleatorios estables como una libreta de un solo uso para codificar la clave privada para obtener una clave privada asegurada.

22. Método para extraer una caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 7, 16 o 17, **caracterizado porque** comprende:

- una fase que usa parte de los componentes aleatorios inestables como clave privada en un proceso criptográfico con clave pública/clave privada,
- una fase que usa parte de los componentes aleatorios inestables como clave pública en el proceso criptográfico con clave pública/clave privada,
- una fase que usa al menos parte de los componentes aleatorios estables como una libreta de un solo uso para codificar la clave privada para obtener una clave privada asegurada.

23. Método para extraer una caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 7, 16 o 17, **caracterizado porque** comprende:

- una fase que usa al menos parte de los componentes aleatorios inestables como identificador del elemento material objeto o de un objeto asociado con el elemento material objeto,
- una fase cifrada del identificador que usa un proceso criptográfico con clave pública/clave privada para obtener un identificador cifrado o caracterizado,
- una fase que usa al menos parte de los componentes aleatorios estables como una libreta de un solo uso para codificar el identificador cifrado o caracterizado, para obtener un identificador cifrado asegurado.

24. Dispositivo que comprende medios de adquisición, medios de procesamiento y medios de memoria, estando adaptados los medios de procesamiento y memoria para implementar el método de extracción de caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 7 a 23 y/o el método para generar una base de descomposición de acuerdo con cualquiera de las reivindicaciones 1 a 6.

25. Producto de programa informático que está adaptado para implementar el método de extracción de caracterización aleatoria de acuerdo con cualquiera de las reivindicaciones 7 a 23 y/o el método para generar una base de descomposición de acuerdo con cualquiera de las reivindicaciones 1 a 6 en un dispositivo de acuerdo con la reivindicación 24.

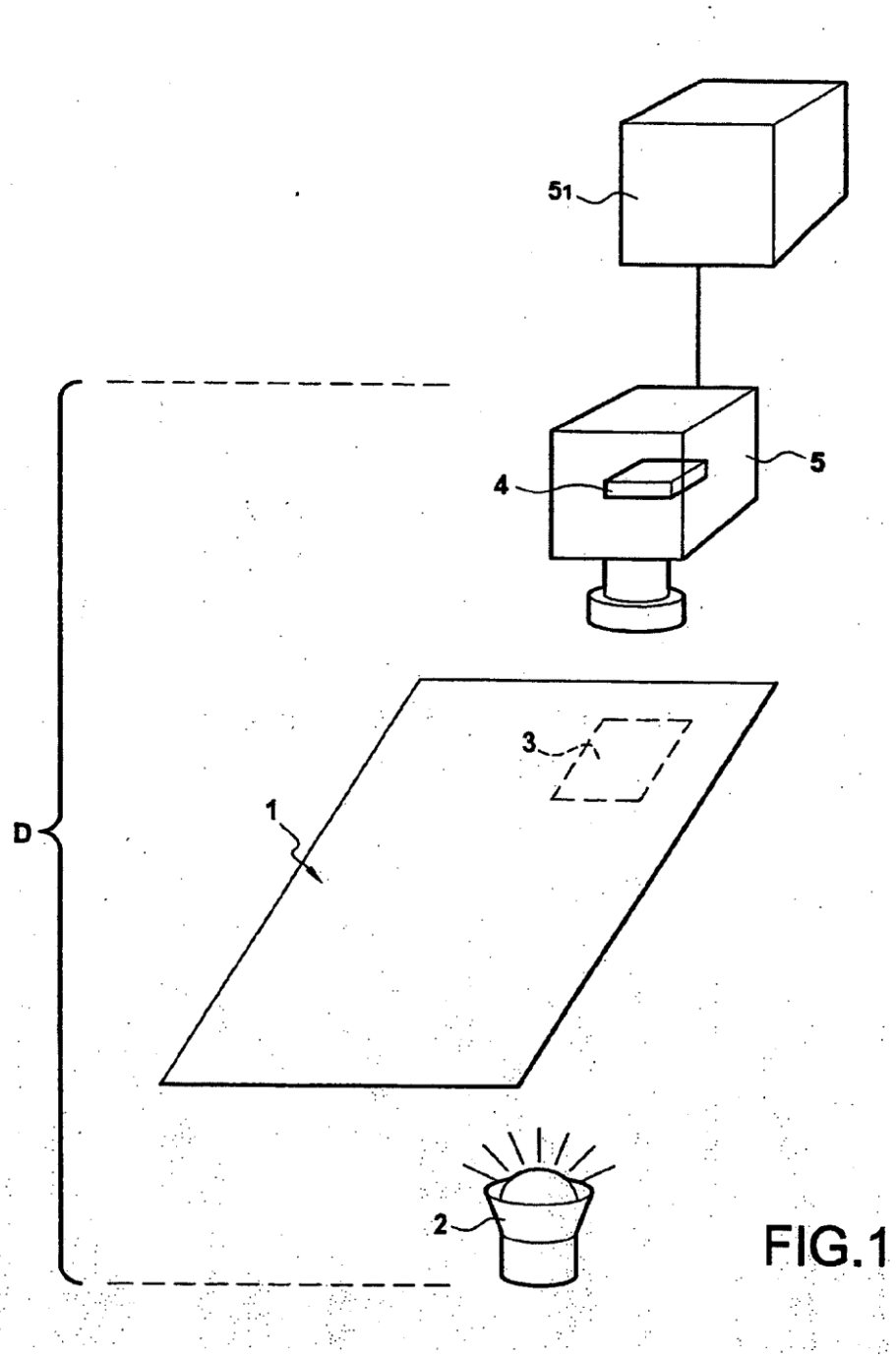
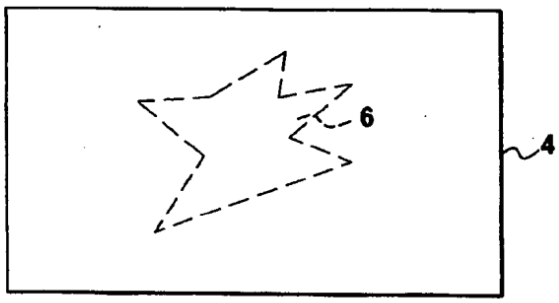


FIG.1

FIG.2



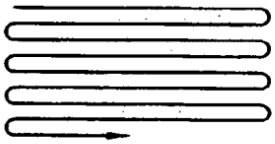


FIG.4

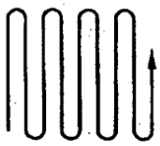


FIG.5

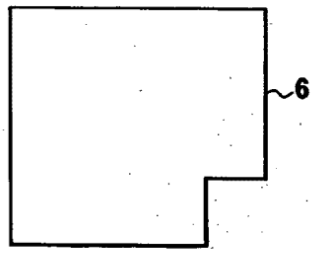


FIG.9

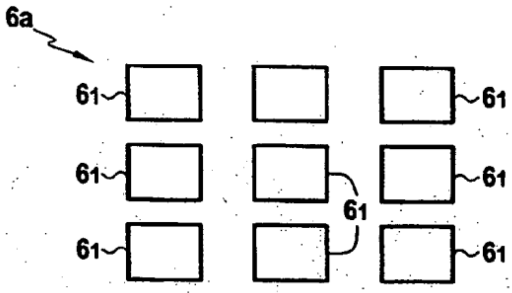


FIG.10

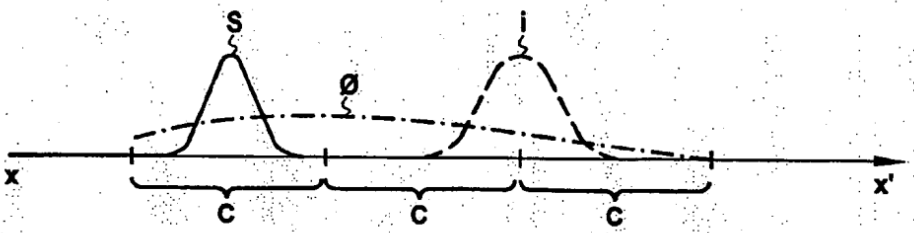


FIG.12

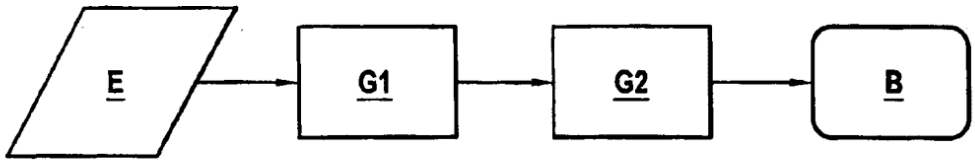


FIG.3

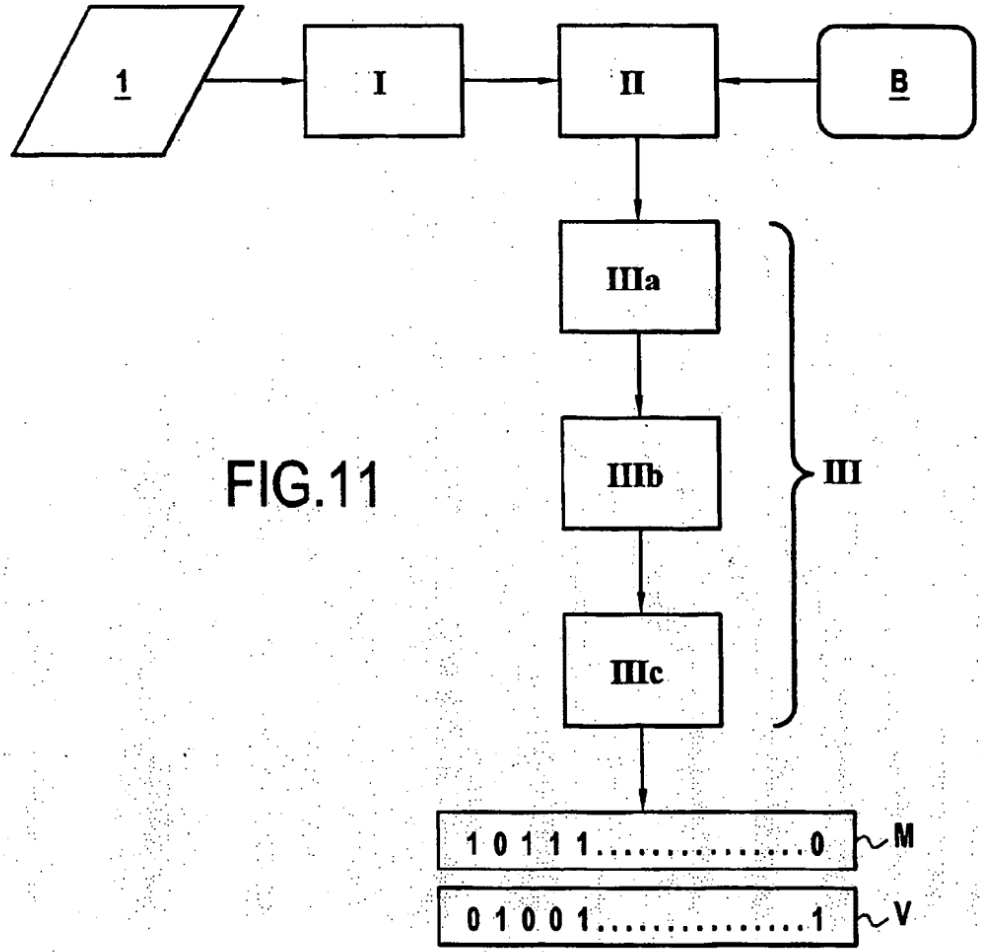


FIG.11

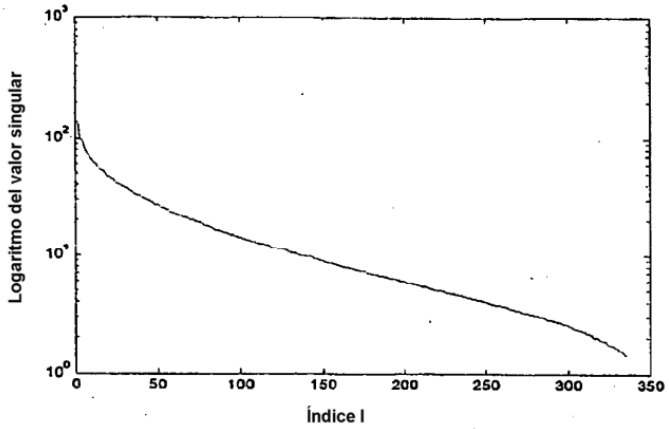


FIG.6A

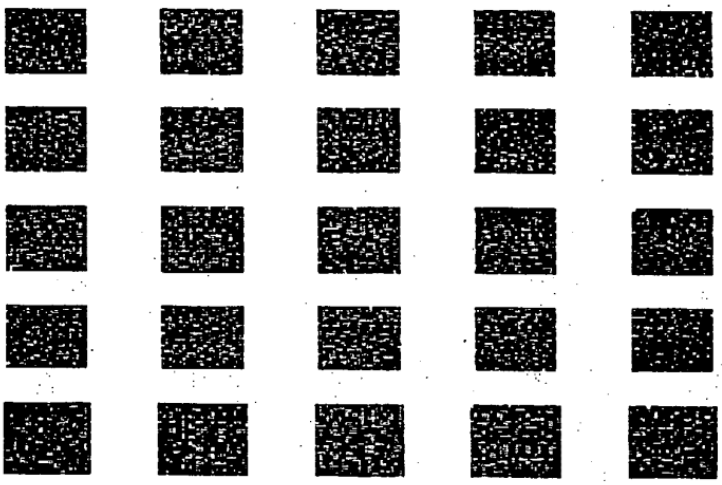


FIG.6B

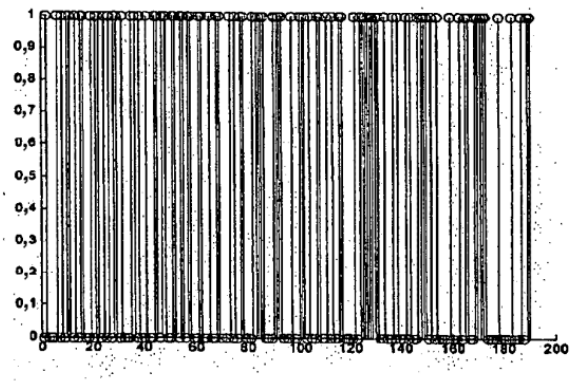


FIG.6C

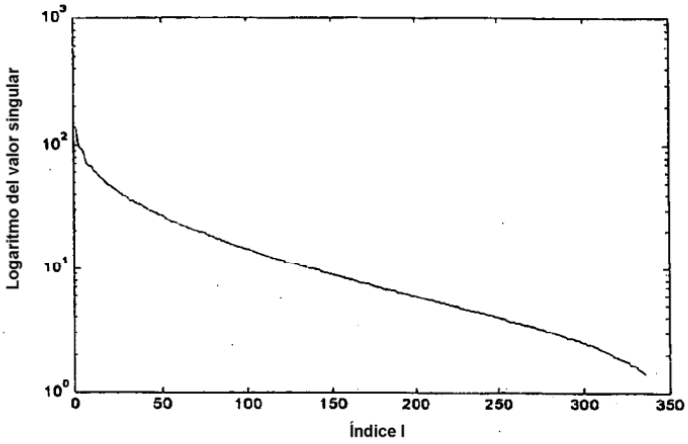


FIG.7A

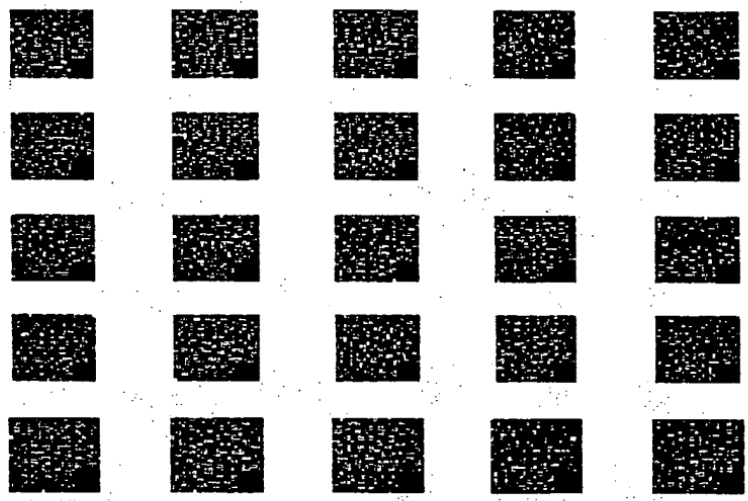


FIG.7B

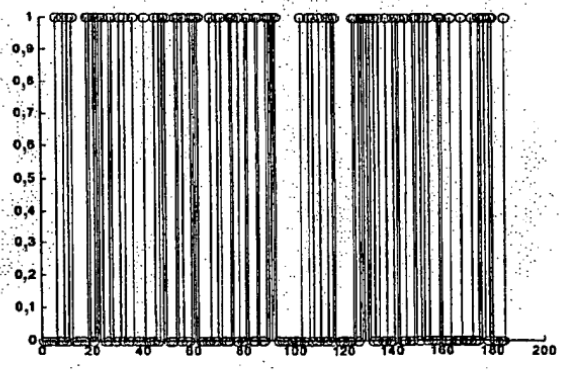


FIG.7C

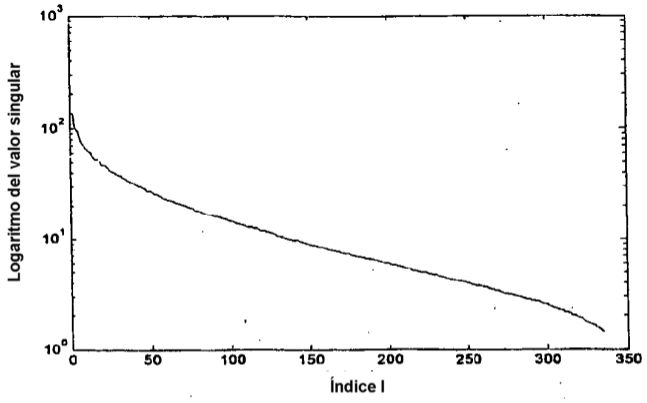


FIG.8A

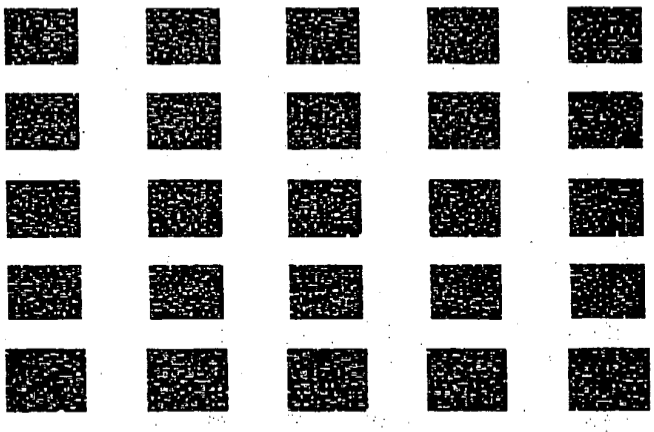


FIG.8B

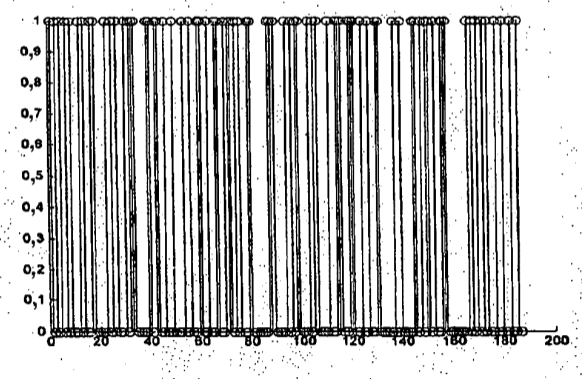


FIG.8C

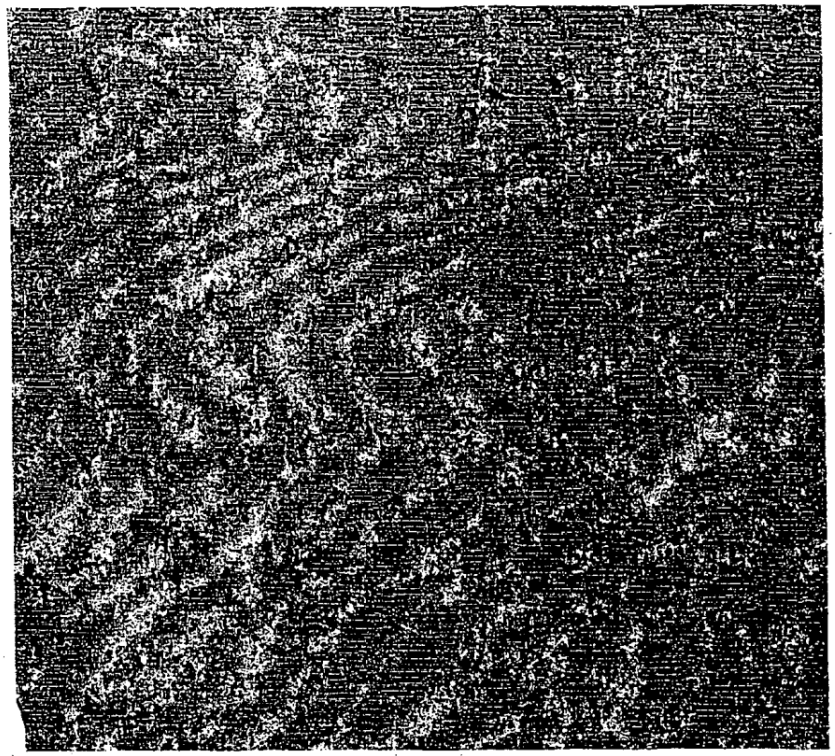


FIG.13A

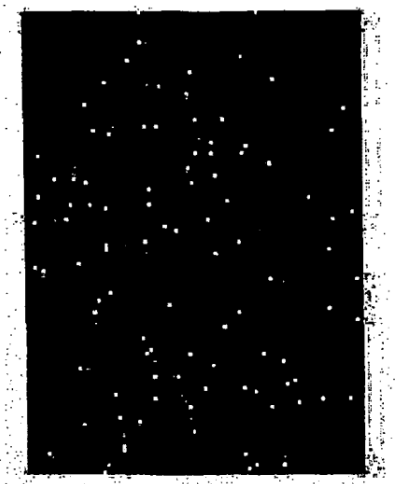


FIG.13B

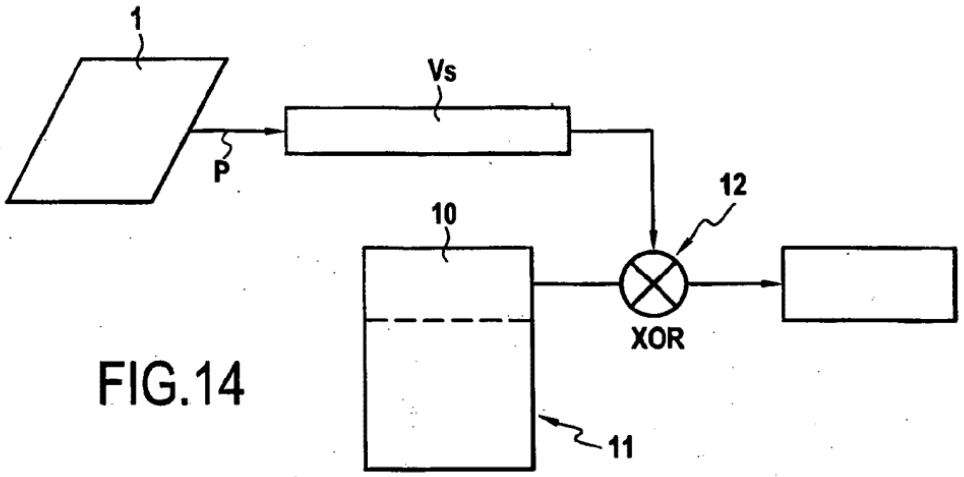


FIG.14

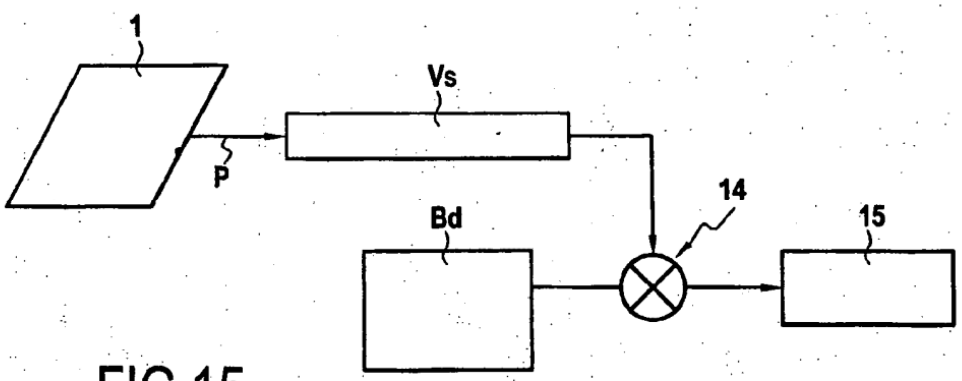


FIG.15

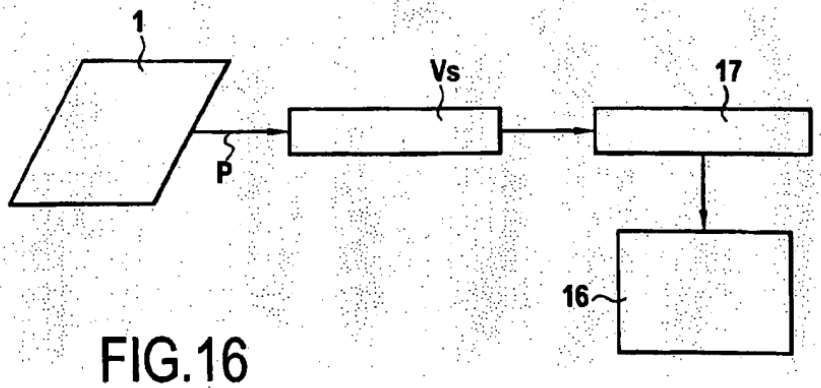


FIG.16

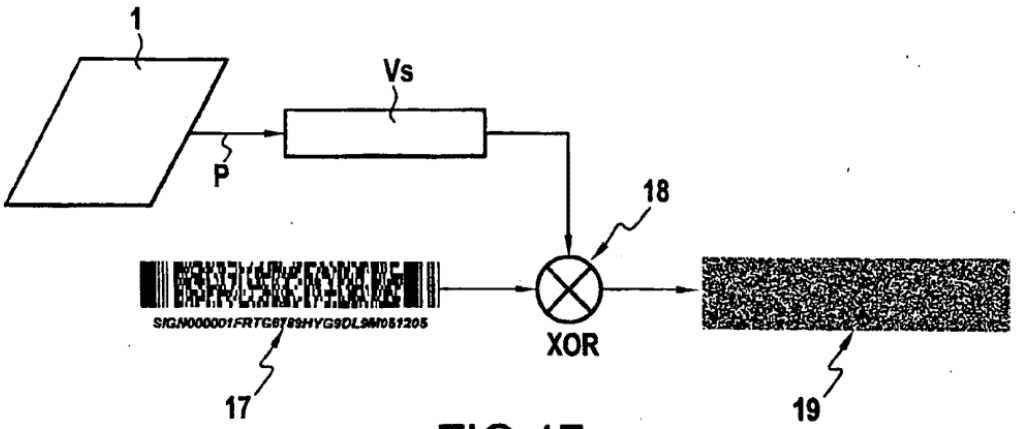


FIG.17

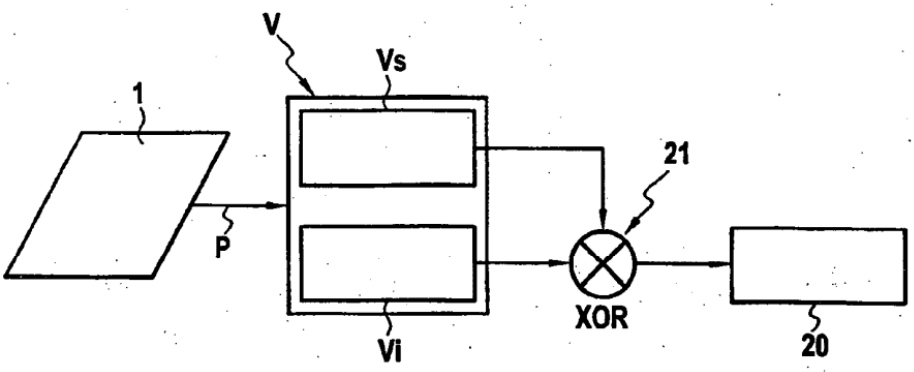


FIG.18

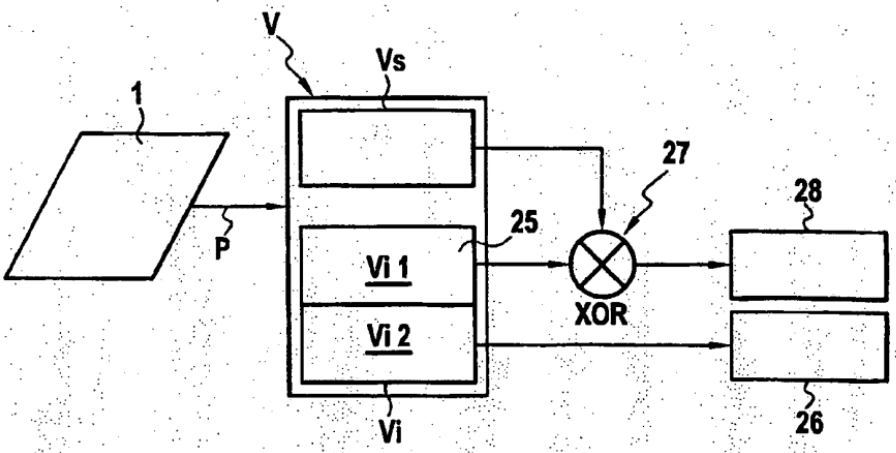


FIG.19

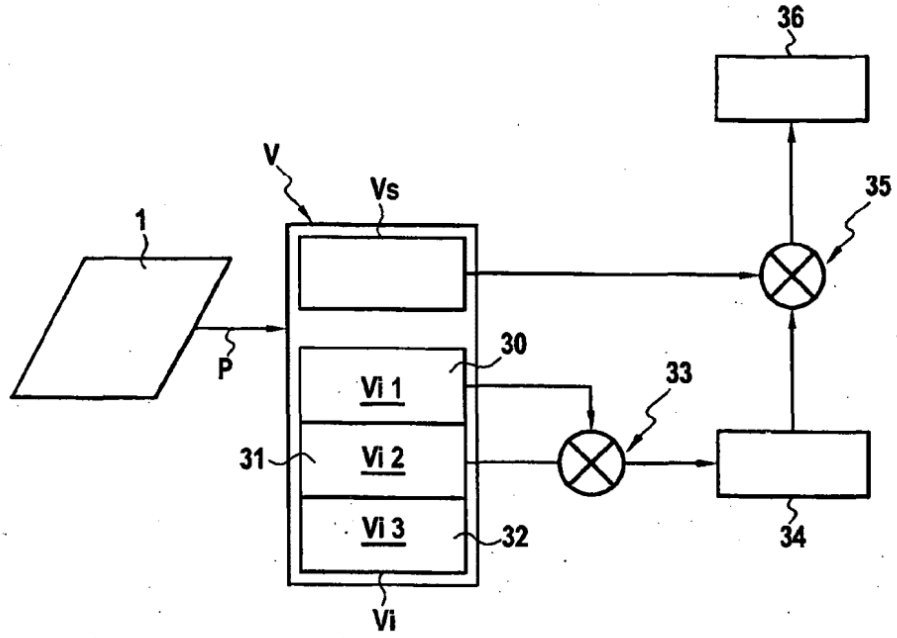
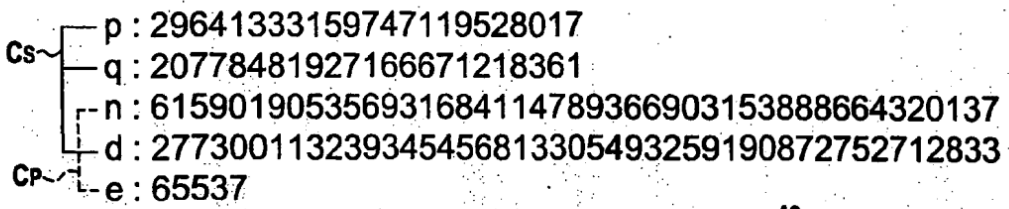

36
V
Vs
35
1
P
30
Vi 1
33
31
Vi 2
Vi 3
32
34
Vi

FIG.20


Cs
p : 29641333159747119528017
q : 20778481927166671218361
n : 615901905356931684114789366903153888664320137
d : 27730011323934545681330549325919087275271283 3
Cp
e : 65537

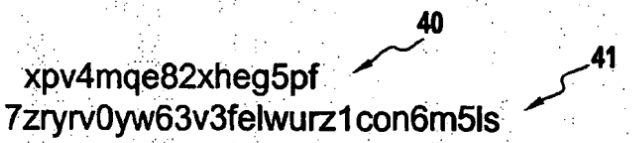

40
41
xpv4mqe82xheg5pf
7zryrv0yw63v3felwurz1con6m5ls

FIG.21