(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 282 104**

(51) Int. Cl.:
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **00925345 .1**
(86) Fecha de presentación : **27.04.2000**
(87) Número de publicación de la solicitud: **1185914**
(87) Fecha de publicación de la solicitud: **13.03.2002**

(54) Título: **Procedimiento para asegurar un software de utilización a partir de una unidad de tratamiento y de memorización de un secreto y sistema para su aplicación.**

(30) Prioridad: **28.04.1999 FR 99 05570**

(45) Fecha de publicación de la mención BOPI:
16.10.2007

(45) Fecha de la publicación del folleto de la patente:
16.10.2007

(73) Titular/es: **VALIDY**
Zone Industrielle - 18, rue Claude Bernard
26100 Romans sur Isère, FR

(72) Inventor/es: **Cuenod, Jean-Christophe y**
Sgro, Gilles

(74) Agente: **Ungría López, Javier**

DESCRIPCIÓN

Procedimiento para asegurar un software de utilización a partir de una unidad de tratamiento y de memorización de un secreto y sistema para su aplicación.

Campo técnico

La presente invención pertenece al campo técnico de los sistemas de tratamiento de datos en sentido general y se refiere, más precisamente, a los medios para asegurar la utilización de un programa o de un software que funciona en dichos sistemas de tratamiento de datos.

El objeto de la invención se refiere, más particularmente, a los medios para asegurar un software de utilización a partir de una unidad de tratamiento y de memorización de un código secreto, designado comúnmente por tarjeta de chip.

Técnica anterior

En el campo técnico anterior, el principal inconveniente se refiere al empleo no autorizado de software por usuarios que no han adquirido derechos de licencia. Esta utilización ilícita de software provoca un perjuicio manifiesto para los editores y los distribuidores de software. Para evitar tales copias ilícitas, se ha propuesto en el estado de la técnica diversas soluciones para proteger software. Así, por ejemplo, se conoce una solución de seguridad que consiste en utilizar un sistema material de protección, tal como un elemento físico llamado clave de protección o "dongle" en terminología anglo-sajona. Tal clave de protección debería garantizar al editor de un software la ejecución del software únicamente en presencia de la clave.

Ahora bien, debe constatarse que tal solución es ineficaz, puesto que presenta el inconveniente de ser fácilmente eludible. Una persona mal intencionada o pirata puede suprimir, con la ayuda de herramientas especializadas, tales como desensambladores, las instrucciones de control. Entonces es posible realizar copias ilícitas que corresponden a versiones modificadas del software que no tienen ya ninguna protección. Además, esta solución no se puede generalizar a todos los software, en la medida en que es difícil conectar más de dos claves de protección en una misma máquina.

La solicitud de patente EP 0 191 162 describe un procedimiento para asegurar el cifrado de un software para evitar una utilización no autorizada. Tal procedimiento consiste en cifrar el programa con la ayuda de una clave única, registrarlo en un soporte de distribución, utilizar para la ejecución del programa un ordenador que comprende una memoria protegida y medios criptográficos protegidos que incluyen una clave secreta única para este ordenador. El procedimiento cosiste en suministrar al usuario del programa una palabra de paso secreta única que depende de la clave del programa y de la clave del ordenado, con el fin de que el ordenador pueda descifrar y ejecutar el programa en su memoria protegida. De acuerdo con una segunda forma de realización, una tarjeta de chip que posee una clave única puede ser asociada al ordenador, de tal manera que en este caso, la palabra de paso secreta única suministrada al usuario depende de la clave del programa y de la clave de la tarjeta de chip.

El inconveniente principal de este procedimiento es que se necesita para la utilización del programa un ordenador que tiene una memoria protegida. Ahora bien, los ordenadores convencionales no poseen tal característica, lo que limita considerablemente el desarrollo de este procedimiento.

Otro inconveniente en su aplicación práctica que necesita, por parte del usuario, la gestión de solicitar a un centro de distribución de palabra de paso, la palabra de paso que corresponde al programa y que depende del ordenador o de la tarjeta de chip del usuario.

Otro inconveniente de este procedimiento es que se necesita tantos códigos secretos como tarjetas de chip existen, y obligar al centro de distribución de las palabras de paso a generar todos estos códigos secretos.

El documento WO-A-97/03398 describe un método según el preámbulo de la reivindicación 1.

Descripción de la invención

El objeto de la invención pretende remediar los inconvenientes de la técnica anterior proponiendo un procedimiento para asegurar la utilización de un software a partir de una unidad de tratamiento y de memorización de un código secreto, concebido para ser ejecutado en un ordenador convencional, y que no necesita ninguna gestión por parte del usuario ante un centro de distribución de palabras de paso.

Para conseguir tal objetivo, el procedimiento según la invención pretende asegurar un software de utilización a partir de una unidad de tratamiento y de memorización de reconstitución que comprende al menos un código secreto de reconstitución, funcionando dicho software en un sistema de tratamiento de datos de utilización.

El procedimiento de la invención se define en la reivindicación 1.

El procedimiento según la invención permite de esta manera asegurar un software de utilización para la ejecución de una unidad de tratamiento y de memorización de un código secreto de reconstitución, que presenta la particularidad de conservar la información confidencial incluso después de varias utilizaciones del código secreto. De esta manera, parece que toda versión derivada del software que trate de funcionar en dicha unidad "*ad hoc*", es incapaz de servirse de los datos producidos por un software de generación, en la medida en que el código secreto de reconstitución contenido en la unidad de tratamiento y de memorización de reconstitución está fuera de toda previsión. La utilización de un código secreto de generación permite modificar de manera no previsible el formato de almacenamiento de datos, de tal manera que la utilización de los datos modificados no permite obtener el funcionamiento correcto del software si el usuario no posee el código secreto de reconstitución. El objeto de la invención encuentra una aplicación particularmente ventajosa, principalmente en el caso de software asociado a la distribución frecuente de bibliotecas en sentido general, cuyo contenido constituye datos que presentan un interés en ser protegidos, como por ejemplo las enciclopedias o los juegos.

Un dispositivo según la invención se define igualmente en la reivindicación independiente 12. Otros modos de realización según la invención son específicos en las reivindicaciones dependientes alternativas.

Otras diversas características se deducen a partir de la descripción realizada a continuación con referencia a los dibujos anexos que muestran, a título de ejemplos no limitativos, formas de realización y de ejecución del objeto de la invención.

Breve descripción de los dibujos

La figura 1 es un esquema que ilustra un ejemplo de realización material que permite la ejecución del objeto de la invención durante una primera fase, a saber, de generación de datos modificados.

La figura 2 es un esquema que ilustra un ejemplo de realización material que permite la ejecución del objeto de la invención durante una tercera fase, a saber, de ejecución del software con sus datos modificados.

Las figuras 3 a 6 son esquemas de principio de utilización de los datos modificados saciados a un software, según diversas variantes de realización.

Mejor manera de realizar la invención

Conforme al objeto de la invención, el procedimiento según la invención comprende una primera etapa o fase llamada de generación de datos modificados, durante la cual se generan datos modificados a partir de datos originales que deben ser protegidos y asociados a un software de utilización. El procedimiento según la invención comprende una segunda etapa o fase de puesta a disposición de un usuario del software o de los datos modificados asociadas, y una tercera etapa o fase de ejecución, en el curso de la cual se utiliza el software de utilización con datos modificados asociados.

La figura 1 ilustra un dispositivo de generación 1_g que permite llevar a cabo la fase de generación de datos modificados del procedimiento conforme a la invención. Este dispositivo de generación 1_g está adaptado para aplicar un software de generación 2_g de datos modificados, cuya función aparecerá más claramente en la siguiente descripción. En el ejemplo de realización ilustrado, el dispositivo de generación 1_g comprende un sistema de tratamiento de datos, llamado de generación 3_g de todos los tipos conocidos en sí, llamado sistema de generación 3_g en la siguiente descripción. En el ejemplo considerado, el sistema de generación 3_g constituye un ordenador, pero debe considerarse que tal sistema de generación 3_g puede formar parte integrante de diversos dispositivos, en sentido general. En el ejemplo considerado, el sistema de generación 3_g comprende al menos un procesador 4_g, al menos una memoria de trabajo 5_g, al menos un soporte de memorización de datos 6_g y al menos un circuito de interfaz de entradas y salidas 7_g. Clásicamente, los diversos componentes del sistema de generación 3_g están conectados entre sí por medio de un bus de comunicaciones 8_g.

Según una primera variante de realización, el circuito de interfaz 7_g está conectado a un lector 10_g de una unidad 11_g de tratamiento y de memorización, llamada de generación, que comprende al menos un código secreto de generación S_g. Según este ejemplo, esta unidad de generación 11_g está destinada para ser escrita o leída por el lector 10_g, pero debe considerarse que tal unidad de generación 11_g se puede presentar en forma de una clave material de todos los tipos, conectada sobre un circuito de entrada / salida, directamente sobre el bus de comunicación 8_g o por cualquier otro medio de comunicación, tal como una conexión de radio, por ejemplo. De una manera general, la unidad de generación 11_g comprende al menos un código secreto de generación S_g o un dispositivo de memorización de una información codificada, medios algoritmos de tratamiento de datos y un sistema de intercambio de datos entre la unidad de generación 11_g y el sistema de generación 3_g. Clásicamente, la unidad de generación 1_g se realiza por una tarjeta de chip.

De acuerdo con una segunda variante de realización, el código secreto de generación S_g es un parámetro del software de generación 2_g.

Tal dispositivo de generación 1_g permite ejecutar una sub-fase de creación de datos. Durante esta sub-fase, se establecen con relación al software de utilización 2_u unos datos llamados originales D asociados. Estos datos originales

D, que están destinados a ser asociados al software de utilización 2_u durante la ejecución de este último, constituyen datos que deben ser protegidos, teniendo en cuenta su interés económico. Estos datos originales D pueden constituir, por ejemplo, una biblioteca asociada a un software de enciclopedia o escenas de juegos asociadas a un software de juego.

A partir de al menos una parte de estos datos originales D, el procedimiento asegura en una sub-fase de modificación, la determinación de datos modificados D' aplicando un código secreto de generación S_g. Los datos originales D y los datos modificados D' se obtienen a partir de un software de generación 2_g en sentido general. De acuerdo con la primera variante de realización, el código secreto de generación S_g puede estar incluido en una unidad de tratamiento y de memorización, llamada de generación 11_g. La utilización de esta unidad de generación 11_g permite, cuando el código secreto de generación S_g no es conocido, hacer difícil, si no imposible, la deducción de los datos modificados D' a partir de los datos originales D, incluso para la persona que ha generado los datos modificados asociados al software. De acuerdo con la segunda variante de realización, el código secreto de generación S_g puede ser asociado directamente al software de generación 2_g de tal manera que su carácter secreto existe con la exclusión del o de los desarrolladores del software.

Esta fase de generación de datos modificados es seguida por una fase de puesta a disposición para la que los datos modificados D son suministrados a los usuarios en asociación con el software de utilización 2_u. De esta manera, al término de una fase de generación de datos, se pone a la disposición de al menos un usuario el software de utilización 2_u y los datos modificados D' obtenidos a partir de un código secreto de generación S_g y de al menos una parte de los datos originales D asociados al software de utilización 2_u.

Tal software de utilización con sus datos modificados D' puede ser utilizado entonces por al menos un usuario durante una fase de utilización, llamada fase de utilización. Esta fase de utilización se descompone en una sub-fase llamada funcional, en el curso de la cual el usuario utiliza las funcionalidades del software y en una sub-fase de reconstitución de los datos originales D. En el curso de la sub-fase de reconstitución, cada usuario provisto con un código secreto de reconstitución asociado al software de utilización 2_u, está en condiciones de modificar de manera inversa o decodificar los datos modificador D', con el fin de recuperar y de utilizar los datos originales D. Debe comprenderse que los datos modificador D' son traducidos de nuevo por el software de utilización 2_u para permitir recuperar o reconstituir los datos originales D, en presencia del código secreto de reconstitución S_u.

La figura 2 ilustra un dispositivo de utilización 1_u que permite aplicar la tercera fase del procedimiento conforme a la invención. En el ejemplo de realización ilustrado, el dispositivo de utilización 1_u comprende un sistema de tratamiento de datos, llamado de utilización 3u de todos los tipos conocidos en sí, designado por sistema de utilización 3_u en la descripción siguiente. En el ejemplo considerado, el sistema de utilización 3_u constituye un ordenador, pero hay que indicar que tal sistema de utilización 3_u puede formar parte integrante de diversas máquinas, dispositivos o vehículos en sentido general. En el ejemplo considerado, el sistema de utilización 3_u comprende al menos un procesador 4_u, al menos una memorias de trabajo 5_u, al menos un soporte de memoria de datos 6_u y al menos un circuito de interfaz de entradas y salidas 7_u. Clásicamente, los diversos componentes del sistema de utilización u están conectados entre sí por medio de un bus de comunicación 8_u. El circuito de interfaz 7_g está conectado a un lector 10_g de una unidad 11_g de tratamiento y de memorización, llamada de reconstitución 11_u, que comprende al menos un código secreto de reconstitución S_u. En el ejemplo ilustrado, esta unidad 11_u, llamada de reconstitución en la descripción siguiente, está destinada para ser escrita o leída por el lector 10_u, pero debe considerarse que tal unidad de reconstitución 11_u se puede presentar en forma de una clave material de todos los tipos, conectada sobre un circuito de entrada / salida, directamente sobre el bus de comunicación 8_u o por cualquier otro medio de comunicación, tal como una conexión de radio, por ejemplo. De una manera general, la unidad de reconstitución 11_u comprende al menos un código secreto de reconstitución S_u o un dispositivo de memorización de una información codificada, medios algorítmicos de tratamiento de datos y un sistema de intercambio de datos entre la unidad de reconstitución 11_u y el sistema de utilización 3_u. Clásicamente, la unidad de reconstitución 1_u se realiza por una tarjeta de chip.

La figura 3 ilustra una primera variante de realización del procedimiento conforme a la invención, que permite traducir de forma inversa los datos modificados D', con el fin de recuperar o de reconstituir los datos originales D empleando el dispositivo de utilización 1_u. El procedimiento consiste en elegir al menos un parámetro de entrada Pe para la unidad de reconstitución 11_u. Este parámetro de entrada P_e está constituido por al menos una parte de los datos modificados D'. El parámetro de entrada Pe es transferido desde el sistema de utilización 3_u a la unidad de reconstitución 11_u. Esta unidad de reconstitución 11_u asegura la determinación de al menos un parámetro de salida P_s a partir de al menos un código secreto de reconstitución Su y del parámetro de entrada P_e.

Hay que indicar que el código secreto de reconstitución Su puede estar constituido o bien por al menos una función secreta que, a partir del parámetro de entrada P_e, genera el parámetro de salida P_s, o sea por al menos una información secreta y al menos una función de conversión conocida o no, que permite suministrar a partir del parámetro de entrada P_e y de la información secreta, el parámetro de salida P_s. La aplicación de la unidad de reconstitución 11_u permite, cuando el secreto de reconstitución no se conoce, hacer difícil, incluso imposible, la deducción del parámetro de salida P_s, a partir del parámetro de entrada Pe.

La unidad de reconstitución 11_u asegura a continuación la transferencia del parámetro de salida P_s al sistema de utilización 3_u. Tal sistema de utilización 4u asegura la aplicación de al menos una función de reconstitución F_u que, utilizando al menos en parte el parámetro de salida P_s, permite obtener los datos originales D.

En un ejemplo preferido de la variante de realización ilustrada en la figura 3, el parámetro de entrada P_s es igual a los datos modificados D', mientras que el parámetro de salida P_s es igual a los datos originales D reconstituidos. Durante la fase de generación de los datos modificados, el código secreto de generación S_g asegura una función de transformación inversa del código secreto de reconstitución S_u, es decir, que su parámetro de entrada es igual a los datos originales D, mientras que el parámetro de salida de la unidad de generación es igual a los datos modificados D'.

Aparece así que el titular de una unidad de reconstitución 11_u asignada a un software de utilización 2u determinado puede recuperar y utilizar los datos originales D asociados a dicho software. En efecto, la aplicación del software de utilización 2_u permite, en presencia de la unidad de reconstitución 11_u "*ad hoc*" traductor los datos modificados D' asociados a dicho software 2_u, con el fin de obtener los datos originales D. Por el contrario, un usuario que no posee la unidad de reconstitución 11_u correspondiente al software de utilización 2_u puede utilizar este último, a excepción de los datos originales D y en el mejor de los casos con los datos modificados.

Además, la eficacia del procedimiento según la invención es real, incluso si la función de reconstitución F_u es conocida y si los parámetros de entrada P_e y de salida P_s pueden ser observados y modificados por una persona mal intencionada, considerando, bien entendido, que se conserva el código secreto de reconstitución S_u. En efecto, tal persona es incapaz de recuperar la modificación de los datos D' en datos D, sin la ayuda de la unidad de reconstitución 11_u.

Una persona mal intencionada puede intentar modificar el software de utilización 2_u, de manera que no tenga necesidad ya de la unidad de reconstitución 11u correspondiente. Para hacer esto, conviene disponer, en primer lugar, de la unidad de reconstitución 11_u "*ad hoc*". A continuación, es necesario que esta persona enumere el conjunto de los datos modificados D' ya sea para establecer una tabla de correspondencia entre todos los parámetros de entrada Pe y los parámetros de salida P_s, con vistas a generar un pseudo-simulador e la unidad de reconstitución 11_u, ya sea para reconstituir el conjunto de los datos originales D y establecer una nueva distribución de un software de utilización $2'_u$ que incluye estos datos originales reconstituidos en lugar de los datos modificados y que permite eludir la fase de reconstitución o de traducción en sentido inverso de los datos modificados. No obstante, tal cometido es difícil en razón del gran número de datos originales.

En el ejemplo de realización ilustrado en la figura 3, los datos modificados D' son transferidos totalmente a la unidad de reconstitución 11_u. Para mejorar la velocidad de tal dispositivo, las figuras 4 a 6 describen diversas variantes preferidas de realización del procedimiento de seguridad de acuerdo con la invención.

La figura 4 ilustra una segunda variante de realización para la fase de ejecución del software de utilización 2_u con los datos modificados. Según este ejemplo, los datos modificados D' son descompuestos en al menos una primera parte D'_1 y una segunda parte D'_2. Al menos la primera parte D'_1 de los datos modificados es elegida como parámetro de entrada P_e. Este parámetro de entrada P_e es transferido a la unidad de reconstitución 11u que, con la ayuda del código secreto de reconstitución S_u determina un parámetro de salida P_s. La unidad de reconstitución 11_u transfiere el parámetro de salida P_s al sistema de utilización 3_u. El sistema de utilización 3_u aplica una función de reconstitución F_u que comprende una función de traducción inversa Ti que, utilizando al menos en parte el parámetro de salida P_s y la segunda parte D'_2 de los datos modificados D', permite recuperar o reconstituir los datos originales D.

Según un ejemplo preferido de realización de la variante ilustrada en la figura 4, se elige como primera parte y segunda parte de los datos modificados D', respectivamente, un número pseudo-aleatorio que ha sido elegido durante la fase de generación, y datos originales que han sido modificados durante la fase de generación y llamados datos originales modificados D'_2. Este número pseudo-aleatorio es utilizado como parámetro de entrada P_e y transformado por el código secreto de reconstitución S_u para obtener el parámetro de salida P_s. La función de traducción inversa T_i permite, a partir del parámetro de salida P_s y de los datos originales modificados D'_2, obtener los datos originales D. En la fase de generación de datos modificados, que corresponde a este ejemplo preferido de realización, se elige un número pseudo-aleatorio como parámetro de entrada del código secreto de generación S_g que proporciona un parámetro de salida de generación. Tal parámetro de salida es utilizado para modificar, por una función de traducción T, los datos originales D, con vistas a obtener los datos originales modificados. Estos datos originales modificados forman en asociación con el número pseudo-aleatorio, los datos modificados D'. Bien entendido, la función de traducción inversa Ti está constituida por la función inversa de la función de traducción o por una combinación de funciones elementales equivalentes.

Según la variante ilustrada en la figura 4, la modificación de los datos originales D es totalmente independiente de estos datos D.

La figura 5 ilustra una tercera variante de realización para la fase de ejecución del software de utilización 2_u con los datos modificados D'. Según esta variante de realización, los datos modificados D' están formados por una primera parte D_1 y una segunda parte D'_2. Al menos una parte de esta primera parte D_1, que corresponde al parámetro de entrada P_e, es transferida a la unidad de reconstitución 11_u, que determina un parámetro de salida P_s con la ayuda del código secreto de reconstitución S_u. El parámetro de salida P_s es transferido al sistema de utilización 3_u que aplica una función de reconstitución F_u que comprende una función de traducción inversa T_i que, utilizando al menos en parte al parámetro de salida P_s y la segunda parte D'_2 de los datos, permite recuperar o reconstituir la segunda parte original D_2 de los datos. La función de reconstitución F_u suministra igualmente la primera parte D_1 de los datos originales que asociada a la segunda parte D_2, forman los datos originales D.

De acuerdo con un segundo ejemplo preferido de realización de la variante ilustrada en la figura 5, la primera parte D_1 corresponde a una parte de los datos originales, mientras que la segunda parte D'_2 corresponde a la otra parte de los datos originales que han sido modificados durante la fase de generación y que se llama segunda parte modificada D'_2 de los datos. La primera parte D_1 de los datos originales es transformada por el código secreto de reconstitución Su para obtener el parámetro de salida P_s. Por otra parte, la función de reconstitución F_u comprende una función de traducción inversa Ti que, a partir del parámetro de salida P_s y de la segunda parte modificada D'_2 de los datos, permite recuperar la segunda parte D_2 de los datos originales. Además, la función de reconstitución F_u está adaptada para suministrar también la primera parte D_1 de los datos originales que, en combinación con la segunda parte D2 de los datos originales, forman los datos originales D. En la fase de generación que corresponde a este ejemplo preferido de realización, los datos originales D son descompuestos en una primera parte D_1 y una segunda parte D_2. Al menos una parte de la primera parte D_1 es utilizada como parámetro de entrada del código secreto de generación S_g que suministra un parámetro de salida de generación. Al menos una parte del parámetro de salida de generación es utilizada por una función de traducción que forma pare de una función de generación para traducir la segunda parte D_2 de los datos originales, con vistas a obtener una segunda parte modificada D'_2 de los datos. A la primera parte D1 de los datos originales está asociada una segunda parte modificada D'_2 de los datos, con vistas a constituir los datos modificados D'.

Según esta variante de realización, la modificación de los datos originales D depende únicamente de estos datos D.

La figura 6 ilustra una cuarta variante de realización para la fase de ejecución del software de utilización 2_u con los datos modificados D'. Según este ejemplo, los daos modificados D' son descompuestos en una primera parte D1, una segunda parte D'2 y una tercera parte D_3. El parámetro de entrada P_e está constituido por al menos una parte de la primera parte D_1 y de la tercera parte D_3. El parámetro de entrada P_e es transferido a la unidad de reconstitución 11_u que determina un parámetro de salida P_s con la ayuda de un código secreto de reconstitución S_u. El parámetro de salida P_s es transferido al sistema de utilización 3_u que aplica una función de reconstitución Fu que comprende una función de traducción inversa T_i que, utilizando al menos en parte el parámetro de salida P_s y la segunda parte D'_2 de los datos, permite recuperar o reconstituir la segunda parte original D_2 de los datos. La función de reconstitución Fu suministra igualmente la primera parte D_1 de los datos originales que, asociada a la segunda parte original D_2 de los datos, forma los datos originales D.

Según un ejemplo preferido de realización de la variante ilustrada en la figura 6, la tercera parte D_3 corresponde a un número seudo-aleatorio que ha sido elegido durante la fase de generación, mientras que la primera parte D_1 corresponde a una parte de los datos originales D, cuando la segunda parte D'_2 corresponde a la otra parte de los datos originales que ha sido modificada durante la fase de generación y que se llama segunda parte modificada D'_2 de los datos. Al menos una parte de la primera parte D_1 de los datos originales y al menos una parte del número pseudo-aleatorio forman el parámetro de entrada P_e que es transformado por el código secreto de reconstitución S_u para obtener el parámetro de salida P_s. Por otro lado, la función de reconstitución F_u comprende una función de traducción inversa T_i que, a partir del parámetro de salida P_s y de la segunda parte modificada D'_2 de los datos, permite recuperar o reconstruir la segunda parte D_2 de los datos originales. Además, la función de reconstitución F_u está adaptada para suministrar también la primera parte D_1 de los datos que, en combinación con la segunda parte D_2 de los datos originales, forma los datos originales D. En la fase de generación que corresponde a este ejemplo preferido de realización, los datos originales D son descompuestos en una primera parte D_1 y una segunda parte D_2, mientras que un número pseudo-aleatorio es elegido como tercera parte D_3. Al menos una parte de la primera parte D1 de los datos y al menos una parte del número pseudo-aleatorio son utilizados como parámetros de entrada del número secreto de generación S_g que suministra un parámetro de salida de generación. Al menos una parte del parámetro de salida de generación es utilizada para una función de generación para traducir la segunda parte D2 de los datos originales, con vistas a obtener una segunda parte modificada D'2 de los datos. El número pseudo-aleatorio D3 y la primera parte d1 de los datos originales son asociados a esta segunda parte modificada D'_2, con el fin de constituir los datos modificados D'.

Según esta variante de realización, la modificación de los datos originales D depende simultáneamente de estos datos D y de un número pseudo-aleatorio.

Según una variante preferida de realizada anexa a los ejemplos descritos con referencia a las figuras 5 y 6, la primera parte D_1 de los datos destinados a ser transferidos a la unidad de reconstitución 11_u, es tratada para facilitar las operaciones de tratamiento ejecutadas por la unidad de reconstitución 11_u. Esta parte D_1 de los datos es suministrada así en entrada al menos a una función de traducción de utilización intermedia H_u, tal como una función no inversible, por ejemplo del tipo "one way hash", con el fin de obtener al menos un parámetro de entrada intermedio P_{ei}. Este parámetro de entrada intermedio P_{ei} determinado por el sistema de utilización 3_u, es combinado eventualmente con la tercera parte D_3 para formar el parámetro de entrada P_e. Este parámetro de entrada Pe es transferido a la unidad de reconstitución 11_u, de manera que esta última puede asegurar la determinación del parámetro de salida P_s a partir del código secreto de reconstitución S_u y del parámetro de entrada intermedio P_{ei} y eventualmente de la tercera parte D_3.

Bien entendido, durante la fase de generación de los datos modificados D', el sistema de generación aplica al menos una función de traducción intermedia de generación, con el fin de obtener al menos un parámetro de entrada intermedio de generación.

En los ejemplos de las figuras 5 y 6, se deduce que en la fase de ejecución, los datos originales D son obtenidos en curso de una etapa de tratamiento empleando la unidad de reconstitución 11_u. Bien entendido, puede estar previsto recomendar n veces esta etapa de tratamiento para aumentar la complejidad de decodificación de los datos. Así, las operaciones siguientes pueden ser recomendadas tantas veces como sean necesarias, a saber:

- descomponer los datos obtenidos anteriormente en al menos una primera y una segunda partes;
- determinar al menos un parámetro de salida a partir de una función de uno o de varios códigos secretos de reconstitución diferentes o idénticos al o a los utilizados anteriormente, y a partir de una parte de los datos;
- modificar al menos una de las otras partes de los datos por una función de traducción idéntica o diferente a la utilizada anteriormente;
- y reconstituir datos después de cada fase de tratamiento de los datos.

Según este ejemplo de realización, durante la sub-fase de modificación, las etapas de generación de los datos son realizadas en el orden inverso, un número de veces n idéntico al número de etapas efectuadas durante la sub-fase de reconstitución.

Según una variante preferida de realización según las figuras 5 y 6, los datos modificados D' están compuestos por al menos dos partes D'_1, D'_2, por ejemplo de tamaños sensiblemente equivalentes. En una primera etapa de tratamiento, la segunda parte D'_2 es utilizada como parámetro de entrada de la unidad de reconstitución 11u, con vistas a recuperar la primera parte D_1 de los datos originales. Después de una primera etapa de tratamiento, se obtienen datos intermedios constituidos por al menos la primera parte D_1 de los datos originales y la segunda parte modificada D'_2 de los datos. En una segunda etapa de tratamiento, el papel de las partes D_1 y D'_2 se invierte. Así, al menos la primera parte D_1 de los datos es utilizada como parámetro de entrada de la unidad de reconstitución 11_u, mientras que la segunda parte modificada D'2 de los datos originales es modificada por una función de traducción, con vistas a recuperar la segunda parte D_2 de los datos originales. Se deduce que el conjunto de los datos originales D son reconstituidos de acuerdo con una decodificación de la totalidad de los datos modificados D'. Bien entendido, durante la sub-fase de modificación, se efectúan operaciones inversas con el fin de codificar o de modificar el conjunto de los datos originales D.

Según una característica preferida de aplicación de la invención, los datos modificados D' son escritos o registrados sobre el soporte 6_u de memorización de datos, asociado al sistema de utilización 3u para permitir la utilización de los datos modificados D' durante la fase de ejecución del software de utilización 2_u. Bien entendido, el soporte 6_u de memorización de datos puede estar constituido de cualquier manera conocida, tal como por ejemplo un disco duro, una banda magnética, un CD ROM, o cualquier otro dispositivo de memorización utilizado con vistas a almacenar o transmitir estos datos.

El procedimiento según la invención descrito anteriormente puede ser ejecutado con diferentes funciones de reconstitución F_u según los objetivos deseados por el editor del software protegido. Por ejemplo, la función de reconstitución F_u puede comprende runa función de cifrado. En este caso, los datos traducidos son manifiestamente incomprensibles. Según otro ejemplo de realización, la función de reconstitución F_u puede ser una función de modificación menor pseudo-aleatorio de las cifras contenidas en los datos originales. De esta manera, el usuario de un software pirateado $2'_u$ puede utilizar los datos asociados a la versión original del software, pero conducen a un funcionamiento erróneo del software pirateado $2'_u$.

REIVINDICACIONES

1. Procedimiento para asegurar un software de utilización (2_u) a partir de una unidad de reconstitución (11_u), que comprende al menos un código secreto de reconstitución (Su), funcionando dicho software lógico en un sistema de tratamiento de datos de utilización (3u)

→ en una fase de generación de datos modificados (d'):

- en una sub-fase de creación de datos, para establecer, a partir de un software de generación, datos llamados originales (D) asociados al software de utilización (2_u),

- en una sub-fase de modificación, para asegurar la determinación de datos modificados (D') a partir de un código secreto de generación (Sg) y de al menos una parte de los datos originales (D) asociados,

→ en una fase de puesta a disposición, para distribuir a un usuario el software de utilización (2u) y los dados modificados (D') asociados,

→ y en una fase de ejecución en un sistema de utilización (3_u) del software de utilización (2_u) con los datos modificados (d') asociados, en una sub-fase de reconstitución de los datos originales:

- para un usuario que posee una unidad de reconstitución (11_u) que comprende un código secreto de reconstitución (S_u)

  ➢ para elegir por dicho sistema de tratamiento de datos de utilización (3_u) parte de los datos modificados (D'),

  ➢ para transferir el parámetro de entrada (P_e) del sistema de tratamiento de datos de utilización (38) a la unidad de reconstitución (11_u),

  ➢ para asegurar la determinación por dicha unidad de reconstitución (11_u), con la ayuda del sistema de tratamiento de datos de utilización, de al menos un parámetro de salida (P_s) a partir del código secreto de reconstitución (S_u) y del parámetro de entrada (P_e),

  ➢ para transferir el parámetro de salida (P_s) de la unidad de reconstitución (11_u) al sistema de tratamiento de datos de utilización (3_u),

  ➢ y para ejecutar en el sistema de tratamiento de datos de utilización al menos una función de reconstitución (F_u) utilizando al menos en parte el parámetro de salida (P_s), con vistas a obtener los datos originales (D),

caracterizado porque consiste en

- permitir a un usuario que no posee la unidad de reconstitución (11_u), utilizar el software de utilización (2_u), con la ayuda del sistema de tratamiento de datos de utilización, a lo mejor con los datos modificados.

2. Procedimiento según la reivindicación 1, **caracterizado** porque consiste:

- en descomponer los datos modificados (D') en al menos una primera parte (D'_1) y una segunda parte (D'_2),

- seleccionar como parámetro de entrada (P_e), la primera parte (S'_1) de los datos modificados,

- y en ejecutar una función de reconstitución (F_u) que suministra los datos originales (D) utilizando el parámetro de salida (P_s) y la segunda parte (D'_2) de los datos modificados.

3. Procedimiento según la reivindicación 1, **caracterizado** porque consiste:

- en descomponer los datos modificados (D') en al menos una primera parte (D'_1) y una segunda parte (D'_2),

- seleccionar como parámetro de entrada (P_e), la primera parte (S'_1) de los datos modificados,

- y en ejecutar una función de reconstitución (F_u) que suministra los datos originales (D) utilizando el parámetro de salida (P_s), la primera parte (D_1) y la segunda parte (D'_2) de los datos modificados.

4. Procedimiento según la reivindicación 1, **caracterizado** porque consiste:

- en descomponer los datos modificados (D') en al menos una primera parte (D'_1), una segunda parte (D'_2) y una tercera parte (D_3),

- en determinar el parámetro de entrada (P_e), a partir de al menos la primera parte (D_1) y de al menos la tercera parte (D_3),

- y en ejecutar una función de reconstitución (F_u) que suministra los datos originales (D) utilizando el parámetro de salida (P_s), la primera parte (D1) y la segunda parte (D'_2) de los datos modificados.

5. Procedimiento según la reivindicación 3 ó 4, **caracterizado** porque consiste:

- en seleccionar como parámetro de entrada (Pe), un parámetro de entrada intermedio (P_{ei}) definido por el sistema de utilización (3_u) de tratamiento de datos, a partir de una función de traducción intermedia (H_u) utilizando una parte de los datos modificados,

- y en asegurar la determinación del parámetro de salida a partir del código secreto de reconstitución (S_u) y del parámetro de entrada (P_e), constituido por el parámetro de entrada intermedio (P_{ei}) y eventualmente por la tercera parte de los datos (D_3).

6. Procedimiento según la reivindicación 1, **caracterizado** porque consiste en asegurar la determinación de datos modificados (D') a partir del código secreto de generación (S_g) contenido en una unidad de tratamiento y de memorización de generación (11_g).

7. Procedimiento según la reivindicación 1, **caracterizado** porque consiste en asegurar la determinación de datos modificados (D') a partir del código secreto de generación (S_g) asociado a un software de generación (2_g).

8. Procedimiento según la reivindicación 3 ó 4, **caracterizado** porque consiste en recomendar n veces, con $n \geq 1$, las operaciones

- de descomposición de los datos obtenidos anteriormente en al menos una primera y una segunda partes;

- de determinación de al menos un parámetro de salida a partir de una función de uno o de varios códigos secretos de reconstitución diferentes o idénticos al o a los utilizados anteriormente, y a partir de una parte de los datos;

- de modificación de al menos una de las otras partes de los datos por una función de traducción idéntica o diferente a la utilizada anteriormente;

- y reconstitución de los datos después de cada fase de tratamiento de los datos.

9. Procedimiento según la reivindicación 8, **caracterizado** porque consiste, en la sub-fase de reconstitución de los datos originales (D):

- en una primera etapa de tratamiento:

  ➢ en descomponer los datos modificados (D') en al menos una primera parte (D'_1) y una segunda parte (D'_2),

  ➢ en utilizar al menos en parte, la segunda parte (D'_2) como parámetro de entrada de la unidad de reconstitución (11_u), con vistas a recuperar la primera parte (D_1) de los datos originales,

  ➢ y en constituir datos intermedios compuestos por al menos la primera parte (D1) de los datos originales y la segunda parte modificada (D'2) de los datos,

- y en una segunda etapa de tratamiento:

  ➢ en utilizar, al menos en parte, la primera parte (D_1) de los datos, como parámetro de entrada de la unidad de reconstitución (11_u), con vistas a recuperar la segunda parte (D_2) de los datos originales,

  ➢ y en reconstituir los datos originales (D) por la primera parte (D_1) y la segunda parte (D_2) de los datos.

10. Procedimiento según la reivindicación 8 ó 9, **caracterizado** porque consiste en efectuar n veces, con $n \geq 1$, en el orden inverso de las operaciones de traducción de los datos modificados (D') en datos originales (D), las operaciones de traducción de los datos originales (D) para obtener los datos modificados (D').

11. Procedimiento según la reivindicación 1, **caracterizado** porque consiste en escribir los datos modificados (D') sobre un soporte (6_u) de memorización de datos, asociado al sistema de tratamiento de datos de utilización (3_u) para permitir la utilización de los datos modificados (D') durante la fase de ejecución del software de utilización (2_u).

12. Dispositivo para asegurar un software de utilización (2_u) a partir de una unidad de reconstitución (11_u) que comprende al menos un código secreto de reconstitución (S_u), funcionando dicho software sobre un sistema de uti-

lización (3_u), que comprende una unidad de generación (11_g) que atribuye a dicho software de utilización (2_u) datos modificados (D') obtenidos durante una fase de generación de los datos modificados (D') a partir de un código secreto de generación (S_g) y de al menos una parte de los datos originales (D), asociados a dicho software de utilización, comprendiendo dicho sistema de utilización (3_u) y aplicando durante una fase de ejecución de dicho software de utilización (2_u) con los datos modificados (D'):

- ➢ medios que permiten determinar un parámetro de entrada (P_e) constituido por al menos una parte de los datos modificados (D'),
- ➢ medios de transferencia del parámetro de entrada (Pe) del sistema de utilización (3_u) a la unidad de reconstitución (11_u),
- ➢ al menos una función de reconstitución (Fu),

- y dicha unidad de reconstitución (11u) comprende y aplica durante una fase de ejecución de dicho software de utilización (2_u) con los datos modificados (D'):

  - ➢ medios que aseguran la determinación de al menos un parámetro de salida (P_s), a partir del código secreto de reconstitución (S_u) y del parámetro de entrada (Pe),
  - ➢ medios de transferencia del parámetro de salida (P_s) de dicha unidad de reconstitución (11_u) al sistema de utilización (3_u) que utiliza al menos la función de reconstitución (F_u) y al menos en parte, el parámetro de salida (P_s), con vistas a obtener los datos originales,

caracterizado porque el sistema de utilización está dispuesto para permitir a un usuario que no tiene dicha unidad de reconstitución (11_u) utilizar el software de utilización a lo menor con los datos modificados (D').

13. Dispositivo según la reivindicación 12, **caracterizado** porque en la fase de generación de datos modificados (D'), dicha unidad de generación (11g) contiene dicho código secreto de generación que permite asegurar la determinación de los datos modificados (D').

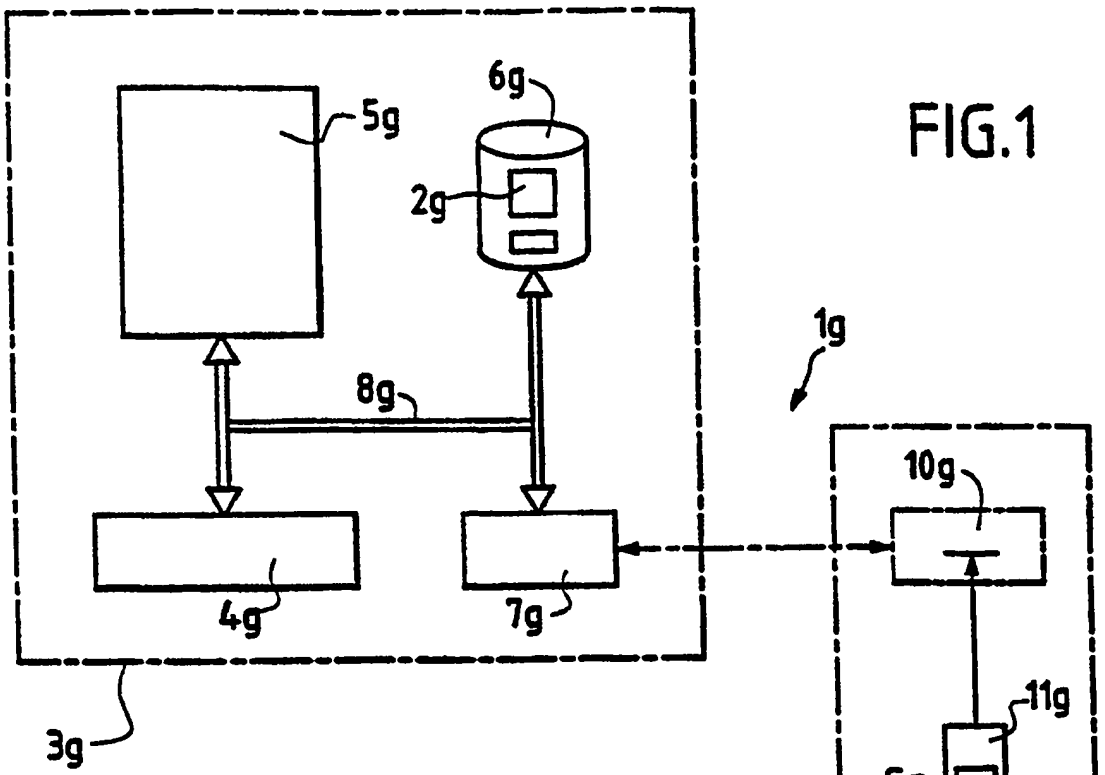

FIG.1

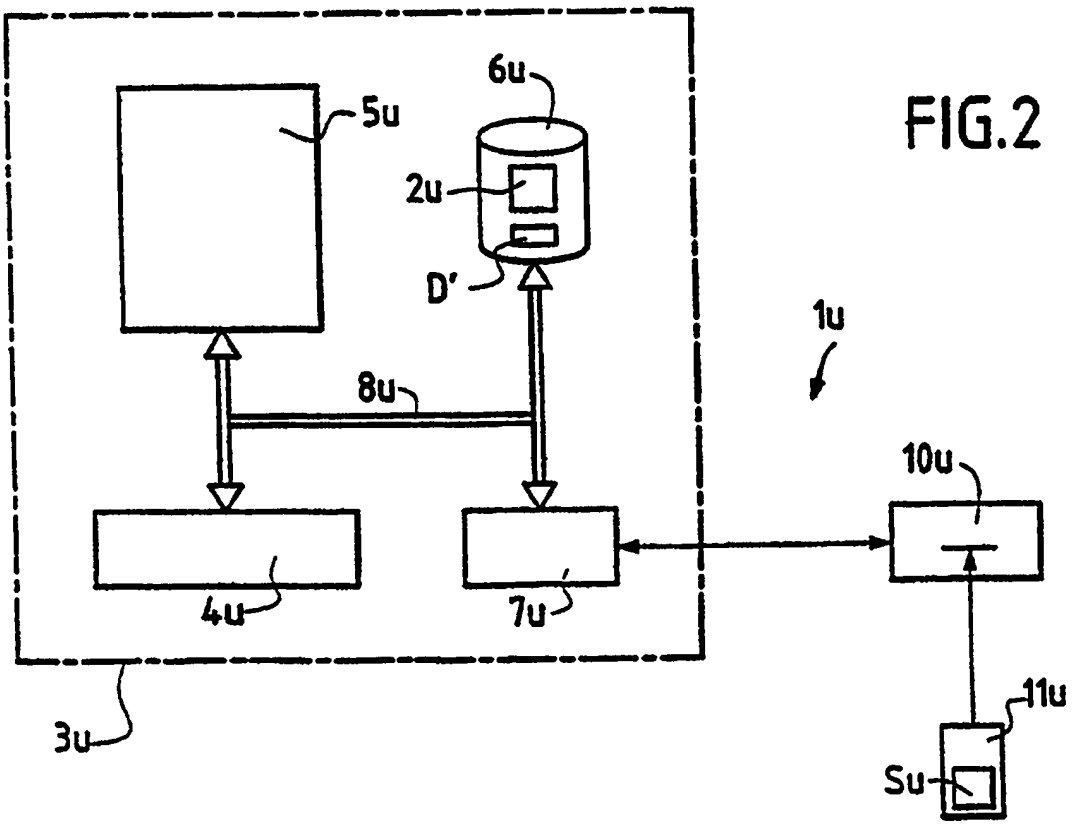

FIG.2

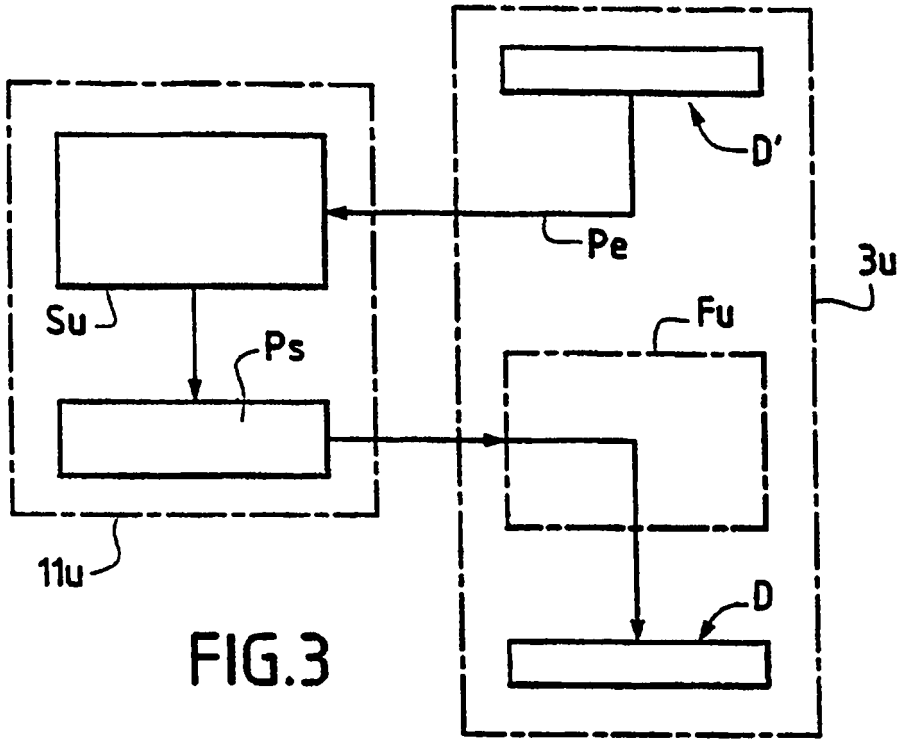

FIG.3

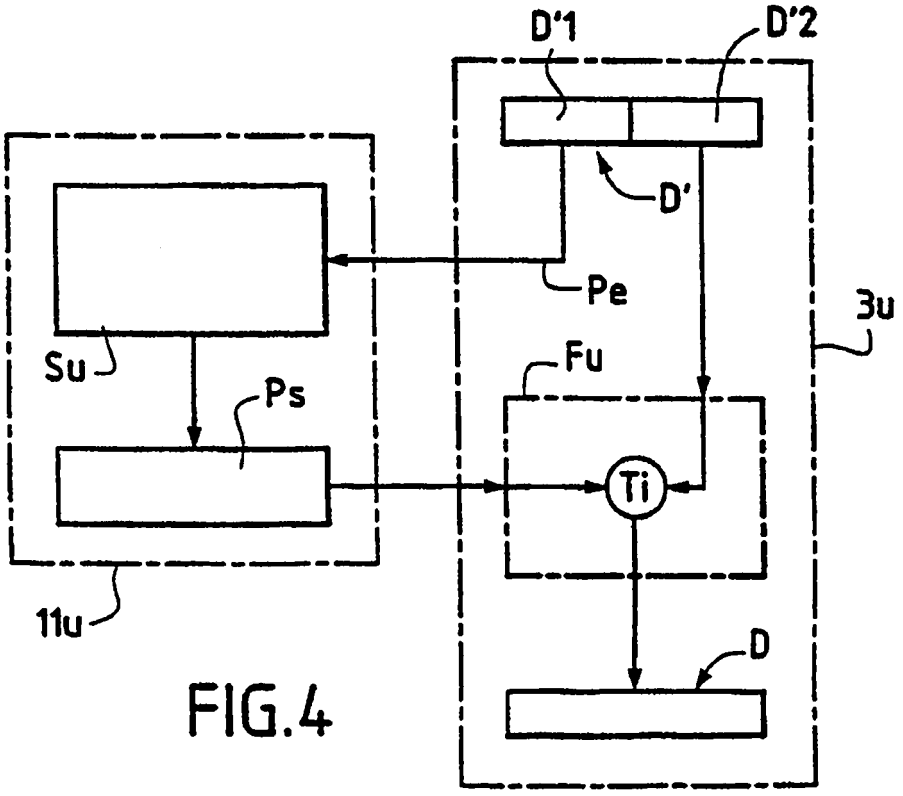

FIG.4

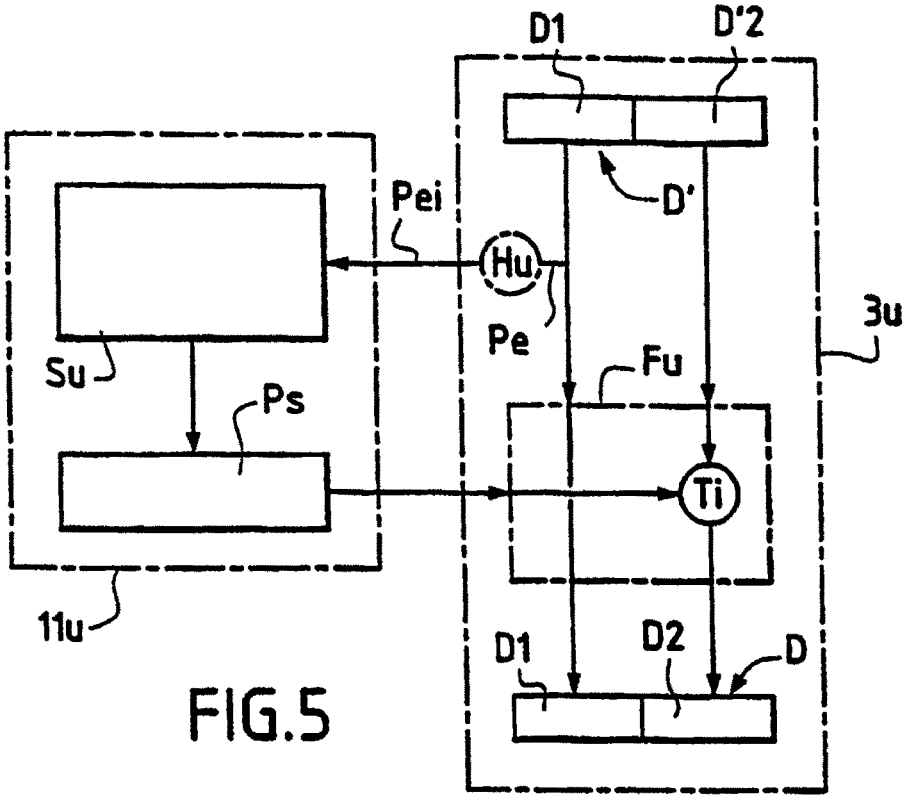
D1
D'2
D'
Pei
Hu
Pe
3u
Su
Ps
Fu
Ti
11u
D1
D2
D

FIG.5

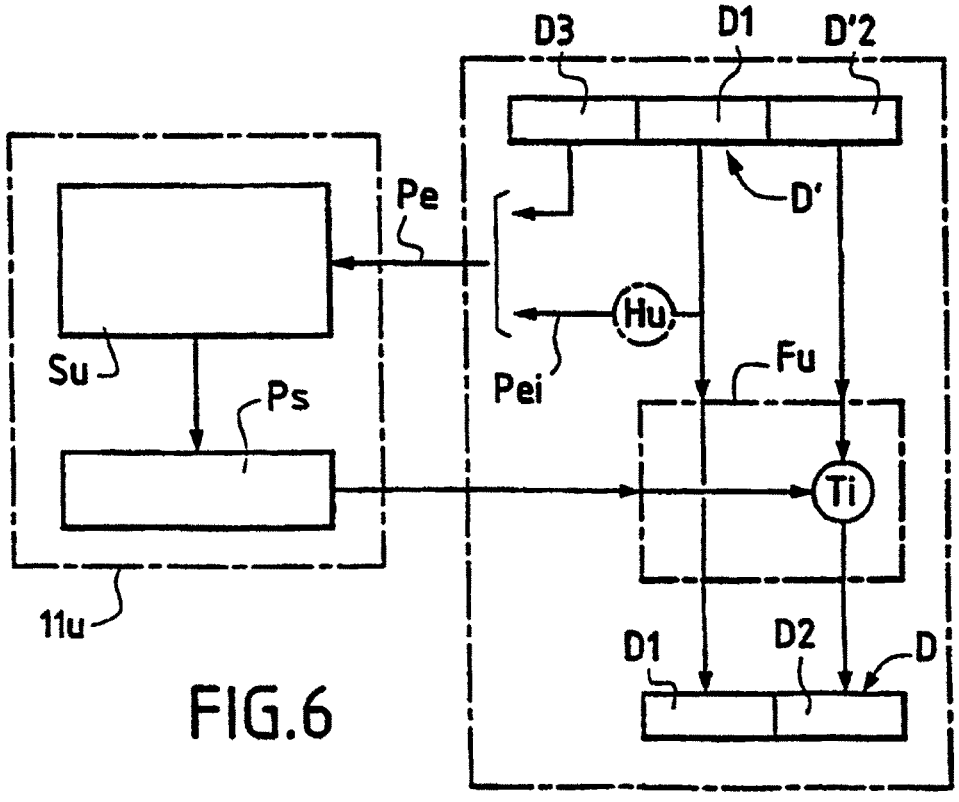
D3
D1
D'2
D'
Pe
Hu
Pei
Fu
Su
Ps
Ti
11u
D1
D2
D

FIG.6